Finansē Eiropas Savienība NextGenerationEU

2027 Nacionālais attīstības plāns

Viedās administrācijas un reģionālās attīstības ministrija

Infrastruktūras un kiberdrošības jomu mērķarhitektūras apraksts

Viedās administrācijas un reģionālās attīstības ministrija

Rīga 2025

Versija	v.05.
Datums	22.01.2025

Izmaiņu vēsture

Versija	Datums	Izmaiņas	Autors
v.0.1.	16.09.2024	Dokumenta sākotnējā versija	G.Ieviņš, J.Irbe, T.Štālbergs
v.0.2.	24.10.2024	Papildināts un pilnveidots jomas arhitektūras tvērums, mērķi un citas sadaļas.	G.Ieviņš, J.Irbe, T.Štālbergs
v.0.3.	20.11.2024	Papildināts un pilnveidots Jomas arhitektūras tvērums, saistītie dokumenti, principi un citas sadaļas.	G.Ieviņš, J.Irbe, T.Štālbergs
v.0.4.	08.01.2025	Papildināts un pilnveidots Jomas esošās arhitektūras novērtējums, jomas mērķarhitektūra un citas sadaļas.	G.Ieviņš, J.Irbe, T.Štālbergs
v.0.5.	22.01.2025	Papildināts un pilnveidots jomas mērķarhitektūra, mērķarhitektūras ieviešanas ceļa karte un citas sadaļas.	G.Ieviņš, J.Irbe, T.Štālbergs

Satura rādītājs

1 Ievads

Dokuments izstrādāts projekta Nr. 2.1.1.1.i.0/1/23/I/VARAM/010 “Valsts pārvaldes informācijas un komunikācijas tehnoloģiju attīstības projektu programmu un arhitektūras pārvaldība” ietvaros. To plānots izmantot, lai īstenotu labas pārvaldības praksei atbilstošu IKT infrastruktūras un kiberdrošības jomu funkcionēšanu un attīstību.

Dokumentā apkopota informācija par:

- Jomas regulējušajiem normatīvajiem aktiem un principiem;
- Jomu ietvaros nodrošinātajiem valsts pārvaldes pakalpojumiem un funkcijām;
- Jomas ietvaros izmantotajiem IKT risinājumiem un to pārvaldības un atbalsta procesiem;
- Jomas attīstības mērķi un principi;
- Projekti ar kuru palīdzību tiks realizēti jomas mērķi.

1.1 Dokumenta nolūks un mērķauditorija

Dokuments apraksta IKT Infrastruktūras un kiberdrošības jomas mērķarhitektūru un risinājumus nosakot tās konceptuālos attīstības virzienus laika posmā no 2024. līdz 2029. gadam.

Jomas mērķarhitektūra nosaka jomas attīstības mērķus un principus, kā arī apraksta arhitektūru šādos arhitektūras skatos:

1. Juridiskais skats identificē paredzamās jomas regulējošo normatīvo aktu izmaiņas;
2. Organizācijas skats apraksta jomas mērķa funkcijas, pakalpojumus un lomas;
3. Semantiskais skats definē izmaiņas jomu resursos un procesos;
4. Tehniskais skats raksturo jomu resursus, to savstarpējo saistību, tehniskā nodrošinājuma informācijas sistēmas, to sadarbību un izvietošanas principus.

Dokumenta mērķauditorija ir:

- Valsts pārvaldes darbinieki, kas ir atbildīgi par IKT projektu plānošanu un īstenošanu;
- Projektu īstenotāji – IT projektu un risinājumu arhitektūras plānošanai;
- Viedās administrācijas un reģionālās attīstības ministrijas darbinieki, kas ir atbildīgi par iestāžu iesniegto IKT attīstības projektu izvērtēšanu, saskaņošanu (būvvalde);
- Jomas iestādes – IT projektu un risinājumu arhitektūras plānošanai.
- Valsts IKT politikas plānotāji – valsts IKT arhitektūras plānošanai un pārvaldībai.

Dokuments ietver augsta līmeņa attīstības virzienus, konkrētu rīku, sistēmu un tehnoloģiju izvēle veicama risinājumu arhitektūras izveides laikā, vērtējot to kopējo atbilstību arhitektūras principiem, to funkcionālo un tehnoloģisko atbilstību biznesa un IT prasībām (drošība, sadarbspēja u.c.), pieejamos resursus un kompetences.

1.2 Jomas arhitektūras tvērums

IKT Infrastruktūras un kiberdrošības jomas ietver nacionālā līmeņa publiskās pārvaldes IKT Infrastruktūras un kiberdrošības darbības pakalpojumu sniedzēju nodrošinātās infrastruktūras, sistēmas, pakalpojumus, funkcijas un saistītos pamatdarbības procesus.

Ietver šādas augsta līmeņa komponentes:

- Valsts datu apstrādes datu centri un mākoņdatošana;
- Programmatūras dzīves cikla nodrošināšana;
- Datorizētās darba vietas un tīkli;
- Datu dublēšana un sistēmu pieejamība ārpus Latvijas teritorijas.

1.2.1 Datu centri un mākoņdatošana

Valsts datu apstrādes mākonis – tehniskās infrastruktūras un koplietošanas pakalpojumu kopums, kas nodrošina valsts pārvaldes iestādēm valsts pārvaldes funkcijas vai deleģēta valsts pārvaldes uzdevuma veikšanai drošu valsts datu un infrastruktūras izmitināšanu, kā arī ar to saistītos pakalpojumus.

Sasniedzamie rezultāti:

- būtiski samazināta negatīvā ietekme uz valsts pārvaldes darbības nepārtrauktības nodrošināšanai;
- tiek nodrošināta nepieciešamo IKT infrastruktūru un pakalpojumu pieejamība krīzes situācijās;
- būtiski samazināta negatīvā ietekme uz lietotāju pieredzi valsts pārvaldes IKT infrastruktūras pārslodzes situācijās;
- turpināts valsts pārvaldes institūciju savrupo sistēmu konsolidācija valsts vienotajā datu apstrādes mākonī;
- uzlabota kiberdrošība veidojot konsolidētu, federatīvu, savstarpēji aizvietojošu infrastruktūru.
- atbilstība Uptime Institute TIER3 vai augstāka drošības līmenis visās kategorijās - projektēšana, būvniecība, operacionālā darbība.

Jomas arhitektūras ietvarā veicamās aktivitātes:

- atjaunināt un papildināt projektu realizētāju mākoņdatošanas infrastruktūras fiziskās, virtuālās un pārvaldības komponentes;
- turpināt resoru un iestāžu savrupo sistēmu konsolidāciju valsts vienotajā datu apstrādes mākonī;
- ieviest Valsts datu apstrādes mākoņa pakalpojumu saņēmēju pašapkalpošanās vienotās piekļuves risinājumu;
- ievērojot spēkā esošos ES un Latvijas normatīvo regulējumu attiecībā uz datu drošību, tostarp, konfidencialitāti, izveidot datu vēstniecības ārpus Latvijas teritorijas;
- izvērtēta valsts datu apstrādes mākoņa datu centru atbilstība ISO/IEC 22237:2021 – Information technology Data centre facilities and infrastructures standarta prasībām;
- federatīvā mākoņdatošanas risinājuma arhitektūras izveide, ievērojot pielietojumam specifiskos standartus un kiberdrošības prasības;
- federatīvā mākoņdatošanas risinājuma arhitektūras saskaņošana ar valsts vienotā datu apstrādes mākoņa dalībniekiem, ārpakalpojumu sniedzējiem, iesaistītajiem resoriem un sistēmu īpašniekiem;
- savrupo sistēmu migrācijas plānu uz valsts vienoto datu apstrādes mākoni izstrāde sistēmu īpašniekiem sadarbībā ar izvēlēto pakalpojuma sniedzēju;
- federatīvajam mākoņdatošanas risinājumam nepieciešamo resursu iepirkumi, piegāde, ieviešana, sistēmu un to drošības testēšana (tostarp, simulējot krīzes scenārijus);
- nodrošināta atbilstība visām kiberdrošības jomā noteiktajām prasībām.

1.2.2 Programmatūras dzīves cikla nodrošināšana

Programmatūras dzīves cikls ir procesu un pasākumu kopums, kas nodrošina valsts pārvaldes informācijas sistēmām nepieciešamās programmatūras un tās izpildvides sagādi un uzturēšanu ievērojot izstrāddarbināšanas (ang.val. “DevOps”) principus.

Tas ietver:

- programmatūras sagāde;
- programmatūras uzstādīšana;
- programmatūras darbināšana;
- programmatūras jaunināšana;
- programmatūras noņemšana;
- kvalitatīvo un kvantitatīvo ekspluatācijas datu uzkrāšana dzīves cikla laikā;

- tehniskā atbalsta pieejamību un nepieciešamos kiberdrošības pasākumus gan programmatūras, gan platformas līmenī.

Programmatūras sagādi jāveic atbilstoši normatīvajiem aktiem par iepirkumu procedūrām. Programmatūras uzstādīšana sākas ar tās pirmkoda (ja pieejams) un uzstādīšanas izpildprogrammas izvietošanu mākoņdatošanas pakalpojuma sniedzēja repozitorijā, kas dublēts pie citiem mākoņdatošanas pakalpojuma sniedzējiem Valsts vienotā datu apstrādes mākoņa ietvaros.

Sasniedzamie rezultāti:

- jaunveidotajām programmatūrām vai programmatūrām, kas tiek būtiski pārstrādātas, ir jānodrošina, lai tās spēj darboties, izmantojot standartizētus infrastruktūras virtualizācijas resursus;
- vienots repozitorijs programmu kodiem – attīstot risinājumus un to komponentes par publisku finansējumu, ir jānodrošina, lai izstrādes rezultāti, tostarp programmatūras pirmkods un tā dokumentācija, ir pieejami pēc iespējas plašākam potenciālo izmantotāju lokam. Funkcionalitātes pieejamības analīze ir obligāta prasība lietojumprogrammatūras risinājumu attīstības projektiem. Repozitorijā programmatūrām jānorāda piederība noteiktai funkcionālajai klase, lai atvieglotu pārizmantošanu noteiktā jomā.
- Valsts vienotā datu apstrādes mākoņa pakalpojuma sniedzēji nodrošina savā pārziņā esošo repozitoriju un katra no pārējiem mākoņpakalpojumu sniedzēju repozitoriju kopiju sinhronizāciju un pastāvīgu pieejamību sava mākoņa ietvaros.
- tiek nodrošināts programmatūras dzīves cikla pārvaldība atbilstoši industrijas labajai praksei;
- tiek ievērotas kiberdrošības jomas prasības programmatūras sagādes un darbināšanas laikā;
- tiek nodrošināts, ka programmatūras sagāde neizvirza īpašas prasības gala iekārtām, pieļaujot to efektīvu darbību pēc iespējas daudzveidīgās gala iekārtās;
- izveidots Centralizēts process drošo sertifikātu un domēnu vārdu dzīvescikla pārvaldībai, kas ietver savlaicīgus atgādinājumus par derīgumu termiņu beigām ar iespēju tos pagarināt.

Paredzēts ieviest Programmatūras dzīves cikla nodrošināšanas (DevOps) platformu, kas sastāv no vairākiem būtiskām komponentēm, kas palīdz organizēt un pārvaldīt programmatūras izstrādi. Galvenie elementi ir:

- Versiju kontroles sistēma (VCS);
- Failu un direktoriju struktūra;
- Apstiprinājumu (*Commit*) vēsture un zaru (*branch*) struktūra;
- Platforma nodrošina tehniskos līdzekļus CI/CD (Nepārtraukta integrācija un piegāde) realizācijai;
- Piekļuves kontrole un sadarbība;
- Kodu repozitorijs.

Jomas arhitektūras ietvarā veicamās aktivitātes:

- jāizstrādā izstrāddarbināšanas (ang.val. “DevOps”) vadlīnijas, kas apraksta programmatūras izstrādes un piegādes vēlamos procesus, ar mērķi centralizēt un automatizēt konfigurācijas vienumu (ang.val. “configuration item”) lietojamību un izmaiņu pārvaldības procesus.

Programmatūras sagādes un darbināšanas pamatprincipus paskaidro vadlīnijas "Valsts pārvaldes rīcībā esošo datu apstrādei nepieciešamas specializētas lietojumprogrammatūras sagādes modeļi"[1].

1.2.3 Datorizētās darba vietas un tīkli

Datorizētā darba vieta un tīkli – darba vides sastāvdaļa, kas nodrošina darbiniekiem iespēju strādāt efektīvi, izmantot nepieciešamos IKT resursus un veikt darbu gan lokāli, gan attālināti, izmantojot drošu datu

[1] https://www.varam.gov.lv/lv/media/37737/download?attachment

pārraides tīklu un uzticamu autentifikāciju.

Sasniedzamie rezultāti:

- izveidota Centralizēta tehnoloģiskā platforma valsts pārvaldes darbinieku darbvirsmu un mobilo ierīču darbības un apkalpošanas nodrošināšanai, darba vieta ietver standartizētu programmatūras komplektu;
- drošs datu pārraides tīkls starp datorizētajām darba vietām un IS darbību nodrošinošajiem resursiem;
- realizēta institūciju IKT ekspertu kompetenču konsolidāciju, specializāciju un attīstību datorizēto darba vietu un tīkla darbības nodrošināšanai;
- izpildītas valsts kiberdrošības likumā noteiktās prasības valsts pārvaldes darbinieku standartizēto darbvirsmu pieejamībai un drošībai;
- ieviestas minimālās kiberdrošības prasības attālinātā darba organizēšanai;
- izveidota divu faktoru autentifikācija, izmantojot SSO (Single sign-on);
- ieviesta obligāta un Centralizēta gala iekārtu aizsardzība pret datorvīrusiem un ļaunatūru.

Jomas arhitektūras ietvarā veicamās aktivitātes:

- Valsts vienotā datorlietotāju autorizācijas un pieejas tiesību pārvaldības risinājuma izveide, kas ietver:
    - federatīva, Centralizēti pārvaldāma valsts pārvaldes darbinieku un darbvirsmu kontu direktorija izveide ar automātisku izmaiņu sinhronizāciju;
    - nodrošina lomās balstītu autorizāciju un piekļuvi;
    - valsts pārvaldes darbinieku un darbvirsmu kontu Centralizētas pārvaldības procesu;
    - kiberdrošības uzlabojumus;
    - lietošanas ērtības uzlabojumus;
    - integrāciju ar personāla pārvaldības risinājumiem.
- Valsts pārvaldes darbinieku darbvirsmu sadarbspējas uzlabošana, kas ietver:
    - Centralizētu VPN risinājumu, individuālu lietotāju attālināta darba nodrošināšanai;
    - programmdefinēta teritoriālā datortīkla (Software-Defined WAN) risinājumu darba nodrošināšanai ēkās ar mazu darbinieku skaitu;
    - lokālo datu pārraides tīklu pieslēguma ar Centralizētu ugunsmūri risinājuma izveidi ēkās ar lielu darbinieku skaitu;
    - Centralizēta ugunsmūra risinājuma izveidi valsts datu apstrādes mākoņa datu centros pieslēgumu nodrošināšanai ar lietotāju darbvirsmām.
- Valsts pārvaldes darbinieku darbvirsmu un mobilo ierīču pārvaldības uzlabošana, kas ietver:
    - Centralizētas paroļu, lietotāju tiesību un digitālo sertifikātu pārvaldības risinājuma izveidi kiberdrošības paaugstināšanai lietotāju darbā ar informācijas sistēmām;
    - standartizēta piekļuves risinājuma lietotāju darbvirsmai attālināta atbalsta sniegšanai izveidi;
    - Centralizēta lietotāju darbvirsmu un mobilo iekārtu uzraudzības, konfigurēšanas un programatūras atjaunojumu piegādes risinājuma ieviešanu.
- Mākslīgā intelekta risinājumu ieviešana biroja darba efektivitātes paaugstināšanai.

1.2.4 Datu dublēšana un sistēmu pieejamība ārpus Latvijas teritorijas (turpmāk – Datu vēstniecība)

Datu dublēšana un aizsardzība citā valstī nodrošinot informācijas drošību un pieejamību ārkārtas situācijās. Paredzētais risinājums ir Datu vēstniecība, kas ir ārpus Latvijas teritorijas izmitināta IKT infrastruktūra, kas atbilst noteiktiem drošības un pieejamības kritērijiem un garantē spēju nacionāla mēroga krīzes gadījumā nodrošināt publiskās pārvaldes informācijas sistēmu pilnu atkopi un iedarbināšanu pakalpojumu pilnvērtīgai nodrošināšanai. Datu vēstniecības infrastruktūrā ietilpst fiziski izolēti izmitināšanas resursi – statnes, serveri tīkla iekārtas un datu glabātuves, kuras pastāvīgi sinhronizētas ar primārajām datu glabātuvēm Latvijā. Lai arī

šie IKT resursi fiziski atrodas citā valstī vai valstīs, tie ir un paliek Latvijas Republikas īpašumā un jurisdikcijā ar piekļuvi, kas ierobežota tikai deleģētam personālam. Datu vēstniecības pakalpojuma ieviešanas plānošana un realizācija tiek uzsākta, tikai tad, kad izmitināšanas pakalpojuma drošības, nepārtrauktības un uzticamības garantijas ir nostiprinātas starpvalstu sadarbības vienošanās līmenī.

Sasniedzamie rezultāti:

- jāatrodas ārpus Latvijas teritorijas ES vai NATO dalībvalstī (vismaz 1 000 km attālumā no Krievijas Federācijas un Baltkrievijas rietumu robežām) un izmitināšana jānodrošina Uptime Institute sertificētā TIER3 vai augstāka drošības līmeņa datu centrā;
- uzturēšanas personāla piekļuvei infrastruktūrai jāparedz četru acu autorizēšanas princips;
- publiskās pārvaldes funkcionēšanai kritiski svarīgajiem datiem jānodrošina replikācija karsto (pastāvīgi) un auksto (periodiski) dublējumkopiju izveidei;
- skaitļošanas un datu pārraides joslas resursiem jābūt pietiekamiem, lai nodrošinātu informācijas sistēmu pilnas atkopes, iedarbināšanas un pilnvērtīgas lietošanas spēju gan no Latvijas teritorijas, gan ārvalstīs;
- datu sinhronizēšana ar primārajām datu glabātuvēm jāveic virzienā uz Datu vēstniecību ar replikāciju datus pārraidot šifrētā veidā (in-transit);
- sensitīvajiem datiem Datu vēstniecībā jānodrošina to šifrēšana mērķa datu glabātuvēs (at-rest);
- Datu vēstniecības uzturēšanai jānodrošina;
- kontrole pakalpojuma līmeņa vienošanās izpildei no izmitināšanas pakalpojumu sniedzēja puses;
- uzticama deleģēta personāla ar autorizētu piekļuvi Datu vēstniecības resursiem un atbilstošu tehnisko kompetenci pastāvīga pieejamība dežūras režīmā;
- pastāvīgs datu replikācijas procesa un resursu kapacitātes monitorings;
- periodiska atkopes spēju testēšana.

Jomas arhitektūras ietvarā veicamās aktivitātes:

- noteikt Datu vēstniecībā izmitināmās IS atbilstoši normatīvajos aktos noteiktajām drošības kategoriju prasībām;
- apzināt Datu vēstniecību izveidei nepieciešamos papildus datu centru, datu pārraides tīklu, skaitļošanas, datu glabātuvju, mākoņdatošanas resursus un to pārvaldības rīkus Latvijas teritorijā un ārpus tās;
- iepazīt un izvērtēt citu ES valstu pieredzi valsts pārvaldes mākoņdatošanas un datu vēstniecību risinājumu ieviešanā;
- izstrādāt katrai Datu vēstniecībā dublējamajai IS optimālu Datu vēstniecības risinājumu;
- balstoties izstrādātajā Datu vēstniecības risinājumā katrai IS izstrādāt individuālo pilnas avārijas atkopes Datu vēstniecībā plānu;
- risinājuma, tostarp, datu vēstniecību darbības un nepārtrauktības krīzes scenārijos nodrošināšanai nepieciešamās pārvaldības un reglamentu dokumentācijas izstrāde un speciālistu apmācība.

1.2.5 Visaptverošā kiberdrošība

1.2.5.1 Esošās situācijas novērtējums un izmaiņu nepieciešamība

01.09.2024. stājās spēkā Nacionālās Kiberdrošības likums, kas nosaka prasības būtisko un svarīgo pakalpojumu sniegšanai un saņemšanai, kā arī informācijas un komunikācijas tehnoloģiju darbībai. Sagatavošanā ir MK normatīvais akts "Noteikumi par minimālajām kiberdrošības prasībām" (iepriekš - MK 442. noteikumi).Kopumā esošās un plānotās likumdošanas izmaiņas paredz striktākas prasības visās kiberdrošības dimensijās. Atbilstoši NIS2 klasifikācijai tās ir: pieejamība, autentiskums, integritāte un konfidencialitāte.
Lielākā atbildība subjektiem – būtisko un svarīgo pakalpojumu sniedzējiem ir par aizsardzības jomas

sistēmu, kritiskās infrastruktūras un A kategorijas informācijas sistēmu drošību, kuru kiberdrošības tehnisko un organizatorisko resursu un procesu atbilstība kvalificēšanās prasībām ir prioritāte. Līdztekus tam, arī B un C kategorijas informācijas sistēmu kiberdrošību ir nepieciešams pilnveidot.
Saistībā ar šīm izmaiņām paredzami būs nepieciešams investēt:

- kvalificēta personāla piesaistē un esošā personāla kvalifikācijas celšanā;
- kiberdrošības atbalsta rīku un procesu modernizēšanā;
- autentifikācijas, autorizēšanas un piekļuves kontroles līdzekļu un metožu uzlabošanā;
- kriptogrāfijas modernizēšanā datu uzglabāšanā un pārraidē;
- sistēmu un datu dublēšanā un darbības nepārtrauktībā, lai uzlabotu pieejamību;
- resursu un sistēmu konsolidācijā un integrācijā mākoņdatošanas platformās;
- kiberuzbrukumu atpazīšanas un novēršanas rīkos;
- datu un informācijas autentiskuma pārbaudes rīkos.

1.2.5.2 Priekšnoteikumi

Kiberdrošības pakalpojumu ieviešanas plānošanu un realizāciju var veikt kā publiskā, tā privātā sektora iestādes un uzņēmumi, ja tie atbilst likumdošanā noteiktajiem kritērijiem.

Sasniedzamie rezultāti:

- Uzlabots kiberdrošības kontroles process realizējot šādus pasākumus:
  - noteikts minimālais laiks kiberdrošības draudu avota un mērķa sistēmas noteikšanai un CERT.LV informēšanai;
  - iespējota kiberdrošības personāla 100% aizvietojamība Nacionālās kiberdrošības likuma funkciju izpildei katras institūcijas ietvaros.
  - kiberdrošības personāla kvalifikācija ir nodrošināta nepieciešamajā līmenī.
- Lietotāju un datoru kontu kiberdrošības pārvaldība ir standartizēta un Centralizēta;
- Pilnveidots un standartizēts mākoņdatošanas datu centru un mākoņdatošanas pakalpojumu iepirkumu process, iekļaujot minimāli nodrošināmās kiberdrošības prasības;
- Kiberdrošības prasību izpildes kontrole ir nodalīta no pamatpakalpojumu sniegšanas, ieviešot neatkarīgu kiberdrošības pakalpojumu;
- Aprobēts kvantu atslēgu izplatīšanas tīkls (QKDN) drošu kriptogrāfijas atslēgu ģenerēšanai;
- Sniegts atbalsts Datu vēstniecību projektu realizācijai;
- VARAM ciešā sadarbībā ar VDAA, Aizsardzības ministriju un mākoņdatošanas pakalpojumu sniedzējiem izstrādā grozījumus kiberdrošības jomā attiecināmajos normatīvajos aktos.

1.2.6 Jomā līdzdarbojas šādas iestādes:

- Viedās administrācijas un reģionālās attīstības ministrija – nozares ministrija, kas atbild par digitālās transformācijas politikas izstrādi un īstenošanu;
- Nacionālo kiberdrošības centrs (Aizsardzības ministrija, CERT.LV) – vienotais kontaktpunkts kiberdrošības jautājumos, veic nacionālo kiberdrošības prasību ieviešanas pārraudzību, izstrādā nacionālās kiberdrošības rīcībpolitikas iniciatīvas;
- Valsts digitālās attīstības aģentūra – digitālā aģentūra, kas atbild par valsts pārvaldes koplietošanas IKT risinājumiem;
- Valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs” - valsts datu apstrādes mākoņa, mākoņdatošanas platformu pārzinis;
- Latvijas Nacionālā bibliotēka – valsts datu apstrādes mākoņa, mākoņdatošanas platformu pārzinis;
- Zemkopības ministrijas Lauksaimniecības datu centrs (no 2025.gada Lauksaimniecības datu centru aizstās LAD (Lauku atbalsta dienests)) – valsts datu apstrādes mākoņa, mākoņdatošanas platformu pārzinis;

- Iekšlietu ministrijas Informācijas centrs – valsts datu apstrādes mākoņa, mākoņdatošanas platformu pārzinis;
- Valsts tiešās pārvaldes iestādes2 (Ministrijas un to iestādes, tostarp valsts aģentūras, dienesti, biroji, administrācijas, inspekcijas, pārvaldes, muzeji, Valsts kanceleja, Centrālā vēlēšanu komisija (koleģiāla institūcija), Datu valsts inspekcija, Tiesībsarga birojs, Valsts administrācijas skola, Valsts kontrole).

1.3 Termini un saīsinājumi

Dokumentā izmantotie termini un saīsinājumi sniegti 1.tabulā.

1. tabula. Dokumentā izmantotie termini un saīsinājumi.

Termins, saīsinājums	Skaidrojums
ANM	Atveseļošanas un noturības mehānisms.
Arhitektūras joma	Arhitektūras joma (domēns) ir arhitektūras strukturējums, kas tipiski tiek iedalīts pēc darbības virzieniem (angl. – Architecture Domain).
BaaS	Rezerves kopija kā pakalpojums mākoņdatošanas pakalpojumu modelis, kurā dati tiek glabāti drošā, hibrīdā mākoņa vai mākoņa repozitorijā ārpus vietnes - drošībā pret nesankcionētu piekļuvi, bojājumiem, uzlaušanu vai zādzību.
Centralizēts	Risinājums, funkcija vai pakalpojums, kas tiek nodrošināts centralizēti federētā veidā.
CI/CD	DevOps metode: Nepārtraukta integrācija un nepārtrauktas piegādes (angļu val. – Continuous Integration/Continuous Deployment).
DC	Datu centrs.
DevOps	Izstrāddarbināšana. Metodoloģija, kas integrē un automatizē programmatūras izstrādes (Dev angļu val. - Development) un informācijas tehnoloģiju operāciju (Ops angļu val. - Operations) darbu. Tā kalpo kā līdzeklis sistēmu izstrādes dzīves cikla uzlabošanai un saīsināšanai.
DevSecOps	DevOps paplašinājums, kas iekļauj drošību (angļu val. - Security).
ERAF	Eiropas Reģionālās attīstības fonds.
Federatīvs risinājums	Vairāku nesaistītu platformu savienošana caur ātrgaitais tīklu un vienotu pakalpojumu pieteikšanas vienotā piekļuves risinājumu, nodrošinot federatīvu modeli un iespēju robežās arī savstarpējo aizvietojamību sistēmu izmitināšanā.
IaaS	Infrastruktūra kā pakalpojums ir mākoņdatošanas pakalpojumu modelis, kurā mākoņpakalpojumu pārdevējs nodrošina tādus skaitļošanas resursus kā krātuve, tīkls, serveri un virtualizācija (kas imitē datora aparatūru). Šis pakalpojums atbrīvo lietotājus no sava datu centra uzturēšanas, taču viņiem ir jāinstalē un jāuztur operētājsistēma un lietojumprogrammatūra.
IeM IC	Iekšlietu ministrijas Informācijas centrs.
Iestāde/Institūcija	Publiska persona, tās institūcija vai amatpersona, kā arī persona, kas īsteno tai deleģētos valsts pārvaldes uzdevumus, ja šī persona informācijas apritē ir saistīta ar attiecīgo uzdevumu izpildi.
IKT	Informācijas un komunikāciju tehnoloģija.
IS	Informācijas sistēmas.
IT	Informācijas tehnoloģija.
LAD	Lauku atbalsta dienests.

[2] Izņemot Nacionālie bruņotie spēki, Zemessardze un Valsts drošības dienests.

Termins, saīsinājums	Skaidrojums
LDC	Lauksaimniecības datu centrs.
LNB	Latvijas Nacionālā bibliotēka.
LVRTC	Valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs".
MK	Ministru kabinets.
PaaS	Platforma kā pakalpojums vai uz platformu balstīts pakalpojums ir mākoņdatošanas pakalpojumu modelis, kurā lietotāji nodrošina, instalē, palaiž un pārvalda modulāru skaitļošanas platformas un lietojumprogrammu kopumu bez sarežģītas infrastruktūras izveides un uzturēšanas.
SaaS	Programmatūra kā pakalpojums ir mākoņdatošanas pakalpojuma modelis, kurā pakalpojumu sniedzējs piedāvā klientam izmantot lietojumprogrammatūru un pārvalda visus nepieciešamos fiziskos un programmatūras resursus. Atšķirībā no citiem programmatūras piegādes modeļiem tas nodala "programmatūras valdījumu un īpašumtiesības uz to no tās izmantošanas".
SIEM	Drošības informācijas un notikumu pārvaldība (angļu val. – Security Information and Event Management) ir risinājums, kas palīdz organizācijām noteikt, analizēt drošības apdraudējumus un reaģēt uz tiem.
SOC	Drošības operāciju centrs (SOC angļu val. – Security Operations Center) ir atbildīgs par organizācijas aizsardzību pret kiberdraudiem.
VARAM	Viedās administrācijas un reģionālās attīstības ministrija.
VDAA	Valsts digitālās attīstības aģentūra.
VIRSIS	Valsts informācijas resursu, sistēmu un sadarbspējas informācijas sistēma.
ZM	Zemkopības ministrija.

1.4 Saistītie dokumenti

Jomas mērķarhitektūru aprakstošie saistītie dokumenti uzskaitīti 2.tabulā.

2. tabula. Saistītie dokumenti

Nr.	Dokuments, dokumenta kods	Saistība ar šo dokumentu
1.	Ministru kabineta rīkojums "Digitālās transformācijas pamatnostādnes 2021.-2027. gadam" [DTP]. Par Digitālās transformācijas pamatnostādnēm 2021.–2027. gadam	Nosaka Latvijas digitālās transformācijas politiku, aptverot laika periodu no 2021.gada līdz 2027.gadam ar mērķi identificēt jomas, kurās nepieciešama un tiek plānota rīcība, kā arī iezīmēt turpmāk nepieciešamo rīcību, kuras realizēšana ir atkarīga no iespējām to veikt, balstoties uz turpmākajām budžeta un citu finanšu instrumentu izmantošanas iespējām.
2.	Digitālās transformācijas pamatnostādņu 2021.–2027. gadam ieviešanas plāns 2023.–2027. gadam [DTPIP]. Par Digitālās transformācijas pamatnostādņu 2021.–2027. gadam ieviešanas plānu 2023.–2027. gadam (likumi.lv)	Definē un apkopo pasākumus 2023.-2027.gadam Digitālās transformācijas pamatnostādnēs 2021. – 2027. gadam noteikto mērķu sasniegšanai.
3.	Valsts pārvaldes iekārtas likums. Valsts pārvaldes iekārtas likums (likumi.lv)	Nosaka Ministru kabinetam padotās valsts pārvaldes institucionālo sistēmu un valsts pārvaldes darbības pamatnoteikumus, kā arī nosaka, ka iestādes sadarbojas, lai veiktu savas funkcijas un uzdevumus.
4.	Ministru kabineta rīkojums Nr. 55 "Par Valdības rīcības plānu Deklarācijas par Evikas Siliņas vadītā Ministru kabineta	Nosaka rīcības plānu, kas izstrādāts, lai īstenotu valdības deklarācijā noteiktos mērķus un prioritātes. Politikas mērķu un uzdevumu noteikšana tai skaitā

Nr.	Dokuments, dokumenta kods	Saistība ar šo dokumentu
	iecerēto darbību īstenošanai”. Par Valdības rīcības plānu Deklarācijas par Evikas Siliņas vadītā Ministru kabineta iecerēto darbību īstenošanai (likumi.lv)	IKT un kiberdrošības jomās. Ietver Digitālās transformācijas veicināšanu, lai uzlabotu valsts IKT infrastruktūru, attīstītus mākoņdatošanas risinājumus un kiberdrošības stiprināšana, kā arī ietver Valsts IT resursu centralizāciju un efektivitātes celšanu.
5.	Valsts informācijas sistēmu likums. Valsts informācijas sistēmu likums (likumi.lv)	Nosaka tiesiskos pamatprincipus un prasības, kas saistītas ar valsts informācijas sistēmu izveidi, pārvaldību, uzturēšanu, darbību, un drošību. Nosaka datu apstrādes un drošības prasības, kas veido pamatu infrastruktūras un kiberdrošības principiem un risinājumiem.
6.	Fizisko personu datu apstrādes likums. Fizisko personu datu apstrādes likums (likumi.lv)	Likuma mērķis ir radīt tiesiskus priekšnoteikumus fiziskās personas datu (turpmāk — dati) aizsardzības sistēmas izveidošanai nacionālajā līmenī, paredzot šim nolūkam nepieciešamās institūcijas, nosakot to kompetenci un darbības pamatprincipus, kā arī reglamentējot datu aizsardzības speciālistu darbību un datu apstrādes un brīvas aprites noteikumus.
7.	Informatīvais ziņojums “Par valsts informācijas un komunikācijas tehnoloģiju resursu un kompetenču konsolidāciju”, pieņemts 2021.gada 19.oktobra MK sēdē, prot. Nr.70, 34.§,). Par valsts informācijas un komunikācijas tehnoloģiju resursu un kompetenču konsolidāciju	Apraksta, kā optimizēt IKT infrastruktūru un pārvaldību apvienojot valsts pārvaldes iestāžu IKT resursus un kompetences, kā arī uzlabojot efektivitāti un kiberdrošību. Ziņojumā noteiktā kārtība, kas paredz IKT infrastruktūras pakalpojumu attīstības un izmantošanas plānu.
8.	Informatīvais ziņojums “Par valsts pārvaldes informācijas un komunikācijas tehnoloģiju koplietošanas pakalpojumu attīstības plānošanu un finansēšanu”, pieņemts 2022. gada 7. jūnija MK sēdē, prot. Nr. 30, 29.§”. Informatīvais ziņojums „Par valsts pārvaldes informācijas un komunikācijas tehnoloģiju koplietošanas pakalpojumu attīstības plānošanu un finansēšanu”	Apraksta, kā plānot, attīstīt un finansēt koplietojamus IKT pakalpojumus valsts pārvaldes iestādēm. Vērsts uz efektīvas koplietojamo IKT resursu izmantošanu.
9.	MK 2022.gada 14.jūlija noteikumi Nr.435 “Eiropas Savienības Atveseļošanas un noturības mehānisma plāna 2.komponentes "Digitālā transformācija" 2.1.reformu un investīciju virziena "Valsts pārvaldes, tai skaitā pašvaldību, digitālā transformācija" īstenošanas noteikumi”). Eiropas Savienības Atveseļošanas un noturības mehānisma plāna 2. komponentes "Digitālā transformācija" 2.1. reformu un	Noteikumi nosaka reformu un investīciju projektu īstenošanas nosacījumus (t. sk. 2.1.2.2.i.investīcijas “Latvijas nacionālais federētais mākonis”, kas paredzēta datu centru un mākoņdatošanas platformas attīstībai). Noteikumi atbalsta publiskā sektora modernizāciju un digitālo tehnoloģiju izmantošanu efektīvākai pārvaldībai.

Nr.	Dokuments, dokumenta kods	Saistība ar šo dokumentu
	investīciju virziena "Valsts pārvaldes, tai skaitā pašvaldību, digitālā transformācija" īstenošanas noteikumi	
10.	Informatīvais ziņojums "Mākoņdatošanas pakalpojumu izmantošana valsts pārvaldē", pieņemts 2018.gada 20.augusta MK sēdē, prot.Nr.11, 30.§. Latvijas Republikas Ministru Kabinets: Tiesību aktu projekti (līdz 08.09.2021)	Apraksta un veicina mākoņdatošanas pakalpojumu izmantošanu valsts pārvaldes iestādēs, izvērtējot arī kiberdrošības aspektus. Valsts datu apstrādes mākoņa attīstības plāns ir skatāms arī saistībā ar mākoņdatošanas pakalpojumu izmantošanas politiku, kas tika noteikta informatīvajā ziņojumā.
11.	MK 2022.gada 8.novembra instrukcija Nr.5 "Valsts elektronisko sakaru pakalpojumu centra nodrošināšanas kārtība". Valsts elektronisko sakaru pakalpojumu centra nodrošināšanas kārtība	Apraksta kārtību kādā valsts pārvaldes iestādes var pieteikties VESPC mākoņdatošanas pakalpojumiem un kādus pakalpojums sniedz VESPC ietvaros.
12.	Informatīvais ziņojums "Par valsts kiberdrošības pārvaldības uzlabošanu", pieņemts 2022.gada 7.jūnija MK sēdē, prot. Nr.30, 4.§. Par valsts kiberdrošības pārvaldības uzlabošanu	2024. gadā izveidojamais Nacionālais kiberdrošības centrs cieši sadarbosies ar valsts pārvaldes IKT infrastruktūras koplietošanas pakalpojumu sniedzējiem, tajā skaitā izveidojot CERT.LV drošības operāciju centrus IKT resursu koplietošanas specializētajos kompetenču centros – t.i. pie valsts datu apstrādes mākoņa pakalpojumu sniedzējiem.
13.	Svarīgi kopīgu Eiropas interešu projekti – nākošās paaudzes mākoņa infrastruktūra un pakalpojumi. *(angļu val. - Important Projects of Common European Interest on Next Generation Cloud Infrastructure and Services (IPCEI CIS)).* Cloud - European Commission IPCEI - European Commission	IPCEI CIS *(angļu val. - Important Projects of Common European Interest on Cloud Infrastructure and Services)* ir Eiropas Savienības iniciatīva, kas veicina lielus, stratēģiskus projektus mākoņdatošanas infrastruktūras un pakalpojumu jomā. IPCEI CIS projekti koncentrējas uz pētniecību un attīstību, radot jaunus mākoņpakalpojumus, datu pārvaldības risinājumus un drošības standartus.
14.	MK 2023. gada 4. jūlija noteikumu Nr.368 "Informācijas sistēmu un to darbībai nepieciešamo informācijas un komunikācijas tehnoloģiju resursu un pakalpojumu attīstības aktivitāšu un likvidēšanas uzraudzības kārtība" Informācijas sistēmu un to darbībai nepieciešamo informācijas un komunikācijas tehnoloģiju resursu un pakalpojumu attīstības aktivitāšu un likvidēšanas uzraudzības kārtība	Nosaka informācijas sistēmu un to darbībai nepieciešamo informācijas un komunikācijas tehnoloģiju resursu un pakalpojumu attīstības aktivitāšu un likvidēšanas uzraudzības kārtību atbilstoši Valsts informācijas sistēmu likuma (turpmāk - VISL) 4. panta otrajai daļai. Visu datu apstrādes mākoņa attīstības projektu īstenošana notiek šo noteikumu noteiktajā kārtībā.
15.	Eiropas Savienības mākoņdatošanas platformām atbilstoši Eiropas mākoņdatošanas iniciatīvas mērķiem un	Iniciatīva izklāsta mērķus un pasākumus, lai veicinātu mākoņdatošanas un lielo datu izmantošanu Eiropā. Iniciatīvas viens no mērķiem ir radīt vienotu Eiropas

Nr.	Dokuments, dokumenta kods	Saistība ar šo dokumentu
	vadlīnijām. 2016.gada 19.aprīļa Eiropas Komisijas paziņojumu "Eiropas mākoņdatošanas iniciatīva: konkurētspējīgas datu un zināšanu ekonomikas veidošana Eiropā". EU Cloud post ISC	datu mākoņinfrastruktūru, kas nodrošinātu piekļuvi lieliem datu kopumiem un skaitļošanas jaudai pētniecības, zinātnes un inovāciju vajadzībām. Iniciatīva arī uzsver nepieciešamību pēc drošiem mākoņrisinājumiem un datu aizsardzības pasākumiem. Nosaka stratēģiju, lai attīstītu mākoņdatošanu un lielo datu infrastruktūru, veicinot zinātnes, pētniecības un inovāciju jomu digitālo transformāciju.
16.	MK 2023.gada 31.oktobra sēdes protokollēmuma (Nr.54, 22.§). Ministru kabineta 31.10.2023. sēdes protokols Nr. 54	Protokollēmuma 5. punkts paredz VARAM sadarbībā ar Satiksmes ministriju, Kultūras ministriju, Iekšlietu ministriju un Zemkopības ministriju līdz 2024.gada 1.martam izstrādāt un Vides aizsardzības un reģionālās attīstības ministram iesniegt izskatīšanai MK noteikumu projektu, kurā noteikt: 1) valsts datu apstrādes mākoni veidojošo valsts platformu pārziņus, to pienākumus un atbildību, kā arī funkcijas un uzdevumus, kuru izpildei nepieciešama valsts platformas izmantošana; 2) valsts datu apstrādes mākoni veidojošo valsts platformu darbības, finansēšanas un izmantošanas kārtību. Patreiz izstrādē ir Valsts datu apstrādes mākoņa noteikumi (24-TA-1050).
17.	MK 2015.gada 28.jūlija noteikumus Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām". Zaudējis spēku - Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām	(Zaudē spēku 18.10.2024) Noteikumi nosaka, kā valsts un pašvaldību iestādes, kā arī privātie uzņēmumi, kas apstrādā valsts informāciju, nodrošina savu IKT sistēmu atbilstību minimālajām drošības prasībām. Noteikumi ir būtiski IKT infrastruktūras aizsardzībai pret kiberdraudiem. Patreiz izstrādē ir Noteikumi par minimālajām kiberdrošības prasībām (22-TA-3183)
18.	Ministru kabineta 2011. gada 1. februāra noteikumi Nr. 100 "Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība". Zaudējis spēku - Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība	(Zaudē spēku 18.10.2024) Nosaka, kā jāplāno un jāīsteno drošības pasākumi, lai aizsargātu kritiskās informācijas tehnoloģiju infrastruktūras valsts pārvaldē un citās nozīmīgās jomās.
19.	Ministru kabineta 2021. gada 6. jūlija noteikumi Nr. 508 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības	Nosaka procedūras un prasības, lai identificētu, aizsargātu un nodrošinātu kritiskās infrastruktūras (t.sk. IKT infrastruktūra), tai skaitā Eiropas kritiskās infrastruktūras drošību un nepārtrauktību.

Nr.	Dokuments, dokumenta kods	Saistība ar šo dokumentu
	plānošanas un īstenošanas kārtība". Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtība	
20.	Nacionālais kiberdrošības likums. Nacionālās kiberdrošības likums	Nosaka tiesisko regulējumu lai nodrošinātu kiberdrošību valstī. Likums ietver kiberdrošības pārvaldību un atbildību, kritiskās infrastruktūras aizsardzību un minimālās drošības prasības IKT sistēmām.
21.	Patreiz izstrādē ir Informācijas sistēmu izvietošanas un datu centru drošības prasības (24-TA-3243).=	Noteikumu mērķis ir noteikt kārtību informācijas sistēmas uzturēt atbilstošā un drošā infrastruktūrā, ja nolemts tās uzturēt datu centros, kā arī noteikt kārtību, kā tiek veikta un uzraudzīta datu centru drošības atbilstība, kā arī noteikt drošības operāciju centru (SOC) darbību datu centros, tai skaitā telemetrijas datu uzraudzību.
22.	Latvijas Nacionālais attīstības plāns 2021.-2027.gadam. Par Latvijas Nacionālo attīstības plānu 2021.–2027. gadam (NAP2027)	Nosaka valsts attīstības prioritātes, tostarp digitālās transformācijas un kiberdrošības jomās. Izvirzītais mērķis ir paātrināt digitālo transformāciju valsts pārvaldē tieši ietekmē IKT infrastruktūras attīstību, kā arī nepieciešamību modernizēt datu centrus, darba vietas un datu pārraides tīklu risinājumus.
23.	Eiropas Parlamenta un Padomes Direktīva 2016/1148 (NIS direktīva) "Par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā". Direktīva - 2016/1148 - LV - EUR-Lex	Nosaka pasākumus, lai uzlabotu tīklu un informācijas sistēmu drošību visā Eiropas Savienībā. Direktīvas mērķis ir veidot vienoti augstu drošības līmeni būtisko pakalpojumu un digitālo pakalpojumu sniedzējiem, lai mazinātu kiberdrošības incidentu ietekmi un novērstu kiberdraudus.
24.	Eiropas Komisijas COM(2016) 178 "Eiropas mākoņdatošanas iniciatīva". EUR-Lex - 52016AE2740 - LV - EUR-Lex	Veicina Eiropas datu un mākoņdatošanas pakalpojumu attīstību. Nodrošina vadlīnijas mākoņdatošanas attīstībai, ko valsts var integrēt savā IKT infrastruktūrā.
25.	Regula (ES) 2016/679 (GDPR). Regula - 2016/679 - LV - GDPR - EUR-Lex	Attiecas uz personas datu aizsardzību datu centros un mākoņdatošanā. Mākoņdatošanā glabātie dati jāaizsargā saskaņā ar GDPR prasībām.
26.	Ministru kabineta 2023. gada 28. marta noteikumi Nr. 158 "Par Latvijas kiberdrošības stratēģiju 2023.–2026. gadam". Par Latvijas kiberdrošības stratēģiju 2023.–2026. gadam	Nosaka Latvijas valsts kiberdrošības stratēģijas pamatprincipus un mērķus. Izstrādāta, lai stiprinātu valsts spējas novērst, atklāt un reaģēt uz kiberdrošības incidentiem, uzlabotu digitālo infrastruktūru aizsardzību.
27.	2015.gada 27.janvāra Informatīvais	Ziņojums uzsver standartizētu risinājumu un IKT

Nr.	Dokuments, dokumenta kods	Saistība ar šo dokumentu
	ziņojums "Par publiskās pārvaldes informācijas sistēmu konceptuālo arhitektūru". Informatīvais ziņojums "Par publiskās pārvaldes informācijas sistēmu konceptuālo arhitektūru"	tehnoloģiju izmantošanu. Nosaka pamata principus, struktūru un vadlīnijas, kas regulē publiskās pārvaldes informācijas sistēmu attīstību un savstarpējo sadarbspēju Latvijā. Ziņojumā uzsvērtie drošības standarti un vadlīnijas palīdz veidot konsekventu kiberdrošības pieeju visā publiskajā pārvaldē, samazinot ievainojamību riskus.
28.	2023.gada 29.decembra informatīvai ziņojums "Valsts pārvaldes rīcībā esošo datu apstrādei nepieciešamas specializētas lietojumprogrammatūras sagādes modeļi". IKT arhitektūras vadlīnijas | Viedās administrācijas un reģionālās attīstības ministrija	Nosaka vadlīnijas valsts pārvaldes specializētu programmatūras risinājumu iegādes un izmantošanas modelim. Tajā tiek analizēti dažādi sagādes modeļi, piemēram, programmatūras iegāde, licencēšana un pielāgošana. Palīdz definēt pārvaldes iestāžu vajadzības un risinājumu pieejamību, kas ir kritiski svarīgi, lai nodrošinātu valsts sistēmu atbilstību drošības un efektivitātes standartiem.

1.5 Jomas esošās arhitektūras novērtējums

Arhitektūras novērtējumā gūtie galvenie secinājumi apkopoti SVID analīzē (3.tabula), kurā iekļautas jomas arhitektūras tvēruma sadaļas - Datu vēstniecība, Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana un Datorizētās darba vietas un tīkli, lai plānojot mērķarhitektūru:

- maksimāli izmantotu **stiprās puses** esošajā situācijā;
- novērstu vai ierobežotu **vājās puses**;
- izmantotu **iespējas**;
- mazinātu draudu iestāšanās varbūtību vai **draudu** iestāšanās sekas.

3. tabula. Jomas esošās arhitektūras novērtējums

STIPRĀS PUSES	VĀJĀS PUSES
Datu centri un mākoņdatošana Atsevišķi, nedaudzi publiskās pārvaldes datu centri ir sasnieguši tehnoloģisku briedumu un ievērojamu skaitļošanas, datu pārraides tīklu un datu glabātuvju kapacitāti, kā arī sniedz daudzpusīgus mākoņdatošanas pakalpojumus, nodarbinot kvalificētu personālu. Segmentēti iekšējie, perimetra un ārējie datu centru pārraides tīkli. Mākoņdatošanas platformās realizēta segmentācija starp nomniekiem.	***Datu centri un mākoņdatošana*** Daudzi, mazāki publiskās pārvaldes datu centri veido sadrumstalotu un neefektīvi pārvaldītu kopējās infrastruktūras daļu. Savi mākoņdatošanas pakalpojumi nav ieviesti, tiek izmantota virtualizācija un savrupi serveri un datu glabātuves. Personāls nereti ir pārslogots, jo tam ir pārāk plašas, vāji specializētas atbildības. Pakalpojumu pieteikšana datu centros, lielākoties veidojot līgumu katrreiz no jauna, kas procesu padara pārāk birokrātisku. Sadrumstalotība neveicina kiberdrošības prasību efektīvu izpildi un pieejamības uzraudzību. Patreiz sniegtie kiberdrošības pakalpojumi pašlaik nav salīdzināmi, ieskaitot saturiski līdzīgus pakalpojumus, starp datu centriem, nav vienoti kritēriji. Esošie SIEM netiek pilnvērtīgi kompetenti ekspluatēti, trūkst kompetentu speciālistu, SIEM kā rīks nav iekļauts SOC ietvarā (incidentu gadījumā nenotiek pilnvērtīga operatīva izmeklēšana un novēršana).

Programmatūras dzīves cikla nodrošināšana Daļa IS jau ir izveidotas atbilstoši jaunākās paaudzes arhitektūrai un izmanto konteinerizāciju, objektu krātuvi un citas modernas tehnoloģijas, kā arī DevOps vai DevSecOps dzīves cikla pārvaldības modeli.	***Programmatūras dzīves cikla nodrošināšana*** Aizvien daudzas IS balstās novecojošās tehnoloģijās. Atsevišķām IS vairs nav pieejams platformas ražotāja atbalsts. Atsevišķām IS aparatūras un programmatūras arhitektūra nav savietojama ar izmitināšanu mākoņdatošanas vidē, tādējādi ierobežojot mērogojamības, pārvaldības, kiberdrošības un starpplatformu pārnesamības iespējas. Daudzās IS netiek plaši pielietotas Agile metodoloģijas, kā arī DevOps un DevSecOps pārvaldības modeļi, kas samazina pielietojuma efektivitāti, valsts pārvaldes procesu automatizēšanas elastīgumu un var radīt nevēlamas papildus izmaksas sistēmu uzturēšanā.
Datorizētās darba vietas un tīkli Atsevišķos resoros un iestādēs ir realizētas kvalitatīva datorizētās darba vietas un tīklu pārvaldība, kas paredz to standartizētu uzstādīšanu, aizsardzību pret ļaunatūru, kā arī regulāru apkopju un programmatūras atjaunošanas procesu. Datu plūsmas kiberdrošības higiēnas kontrolei ir uzstādīti notikumu reģistratori un datubāzes (SIEM) draudu savlaicīgai identificēšanai. Valsts pārvaldē darba stacijas ir pietiekoši drošas, lai varētu strādāt ar tām publiskajā tīklā.	***Datorizētās darba vietas un tīkli*** Aizvien daudzos resoros un iestādēs trūkst visaptveroša risinājuma kiberdrošības higiēnas kontrolei un datorizēto darba vietu, to programmatūras un tīklu standartizētai pārvaldībai. Lietotāju kontu direktoriji ir savrupi un decentralizēti.
Datu vēstniecības Atsevišķām IS Datu vēstniecības ir izveidotas ārpus Latvijas teritorijas.	***Datu vēstniecības*** Lielākajai daļai IS Datu vēstniecības nav izveidotas, jo nav atbilstoša regulējuma, kas to paredz (regulējumu izstrāde ir procesā).
IESPĒJAS	**DRAUDI**
Datu centri un mākoņdatošana Konsolidēt mazos datu centrus vairākos lielākos, saglabājot aizvietojamību federatīvā mākoņdatošanas infrastruktūrā. Atslogot iestāžu administratorus no virtualizācijas platformu un serveru administrēšanas. Uz atbrīvoto resursu pamata varētu attīstīt citas funkcijas kā lietotāju atbalstu, lietojumu pārvaldību, pamatdarbības procesu optimizēšanai nepieciešamu jaunu tehnoloģiju izpēti un ieviešanu, un paaugstināt specializācijas pakāpi un uzlabot kiberdrošības kontroli. Izveidot vienas pieturas resursu pieteikšanas un līgumu slēgšanas punktu caur brokera pakalpojumu, ar iespēju saņemt arī konsultatīvu atbalstu kiberdrošībā, sistēmu darbināšanai un migrācijai. Standartizētā un konsolidētā vidē ir vieglāk realizēt kiberdrošības prasību efektīvu izpildi.	***Datu centri un mākoņdatošana*** Kiberuzbrukumi, sistēmu ievainojamības un neatbilstoša personāla kvalifikācija var izraisīt sistēmu dīkstāvi, datu konfidencialitātes, integritātes vai autentiskuma zudumu. Pārāk lēni pakalpojumu pieteikšanas procesi kavē IS ieviešanu un esošo sistēmu atjaunināšanu, kas negatīvi atsaucas uz valsts ekonomiskās attīstības dinamiku un uz publiskā sektora reputāciju.
Programmatūras dzīves cikla nodrošināšana Veikt novecojošu IS koda atjaunošanu uz jaunākām izstrādes platformu, paredzot savietojamību ar mākoņdatošanas platformām,	***Programmatūras dzīves cikla nodrošināšana*** Risks laika gaitā būtiski palielināties uzturēšanas izmaksām novecojušās arhitektūras sistēmām, kā arī, izbeidzoties platformu dzīves ciklam un ražotāja

uzlabojot koda pārizmantojamību, pieejamā atvērtā koda bāzes elementus, tostarp no EU Cloud ekosistēmas, kā arī ieviešot centralizēti pārvaldītu koda repozitoriju. Pakāpeniski pāriet uz Agile metodoloģijas un DevOps un DevSecOps pārvaldības modeļu plašāku pielietojumu.	atbalstam, būtiski palielinās ievainojamību ļaunprātīgas izmantošanas iespējamība.
Datorizētās darba vietas un tīkli Ieviest programmatūras un aparatūras līmeņa risinājumus datorizētas darba vietas un tīklu iekārtu efektīvai pārvaldībai, un uzskaitei. Izveidot federatīvi savienotus, resoru līmeņos centralizētus kontu direktorijus un piekļuves tiesību pārvaldības mehānismus. Ieviest un nodrošināt visaptverošu risinājumu kiberdrošības higiēnas kontrolei, datorizēto darba vietu, to programmatūras un tīklu standartizētai pārvaldībai, nodrošinot iespēju droši strādāt jebkurā tīklā. Ieviest lokālā tīkla segmentēšanu darba stacijām, kas strādā ar konfidenciāliem dokumentiem.	***Datorizētās darba vietas un tīkli*** Savlaicīgi neatjaunojot darbstaciju un tīklu iekārtu programmatūru un mikrokodu, būtiski palielinās ievainojamību ļaunprātīgas izmantošanas iespējamība. Sadrumstaloti kontu direktoriji apgrūtina IS integrāciju, kā arī pazemina noturību pret kiberuzbrukumiem un konfidenciālu datu noplūdi. Tīklos, kuros nepieciešama augstāka konfidencialitātes pakāpe var nebūta ieviesta segmentācija, tādejādi pieļaujot datu noplūdes riskus.
Datu vēstniecības Atbilstoši regulējumam izveidot Datu vēstniecības visām attiecināmajām IS. Paredzēt iespēju veikt pilnu sistēmu atkopi un iedarbināšanu uz resursiem kas ir ārpus Latvijas Republikas teritorijas un atrodas ES vai NATO dalībvalstī (vismaz 1000 km attālumā no Krievijas Federācijas un Baltkrievijas rietumu robežām). Papildus kritēriji: • Ārpus Latvijas; • Tīkla latentums no Latvijas; • Politiski un ekonomiski stabila valsts; • Ar zemu dabas katastrofu un terorisma risku; • Valsts teritorijā nenotiek karadarbība; • Ir NATO dalībvalsts; • Ievēro Eiropas datu regulu (GDPR).	***Datu vēstniecības*** Datu vēstniecības neesamība visaptverošas krīzes situācijās var paralizēt valsts pārvaldes funkcijas, liegt iedzīvotājiem izmantot eksistenciāli nepieciešamus publiskās pārvaldes elektroniskos pakalpojumus, kā arī negatīvi ietekmēt ārkārtas dienestu spējas mazināt krīzi, kā arī izraisīt citas negatīvas sekas.

2 Jomas attīstības mērķi un principi

Jomas attīstību nosaka tā attīstības mērķi un principi. **Mērķi nosaka pārskata periodā sasniedzamos galvenos rezultātus.** Arhitektūras principi definē IKT risinājumu arhitektūras izstrādē piemērojamās vadlīnijas ar mērķi veicināt arhitektūras komponentu sadarbspēju, atbilstību labākajai praksei un sniegt atbalstu lēmumu pieņemšanai.

2.1 Jomas attīstības mērķi

Jomas attīstības mērķi ir izvirzīti saskaņā ar Latvijas politikas plānošanas dokumentā “Par Digitālās

transformācijas pamatnostādnēm 2021.–2027. gadam" noteikto attīstības vīziju[3]: "Koplietojam skaitļošanas un datu glabāšanas resursus, veidojot Latvijas mākoņdatošanas federēto infrastruktūru, kas ir ES mākoņdatošanas federētās infrastruktūras būtisks dalībnieks." un "Valsts pārvaldes iestādēm un privātajam sektoram ir attīstīta noturība pret kibervides draudiem un tā tiek pastāvīgi pilnveidota reaģējot uz jauniem apdraudējumiem un tehnoloģiskajām iespējām".
No dokumenta "Par Digitālās transformācijas pamatnostādnēm 2021.–2027. gadam" izriet jomas attīstības virsmērķi[2]:

- Izveidot Latvijas valsts mākoņdatošanas federēto infrastruktūru un ieviest ar to saistītos pakalpojumus, vismaz 10 valsts platformām un IS pārejot uz šo pakalpojumu pilnvērtīgu un efektīvu izmantošanu;
- Pilnveidot valsts pārvaldes datorizēto darba vietu pārvaldību, vismaz 70% no tiešās pārvaldes institūciju datorizētajām darba vietām izmantojot unificētus koplietošanas vai ārpakalpojumus;
- Valsts pārvaldes "Nākotnes biroja" un digitālās darba vides koncepcijas un tās ieviešanas plāna izstrāde, nodrošinot ka 80% darbinieku ir iespēja to izmantot;
- Izveidot politiku un normatīvo regulējumu IKT koplietošanas pakalpojumu sniedzēju attīstībai. Izveidot un īstenot plānu IKT koplietošanas pakalpojumu sniedzēju attīstībai;
- Nozaru kiberdrošības jautājumu identificēšana un analīze, digitālās drošības aspektu iekļaušana nozaru politikas plānošanas dokumentos un Latvijas kiberdrošības stratēģijā;
- Pāriet uz elastīgo, t.sk attālināto un aktivitātēs balstīto darba organizāciju valsts pārvaldē.

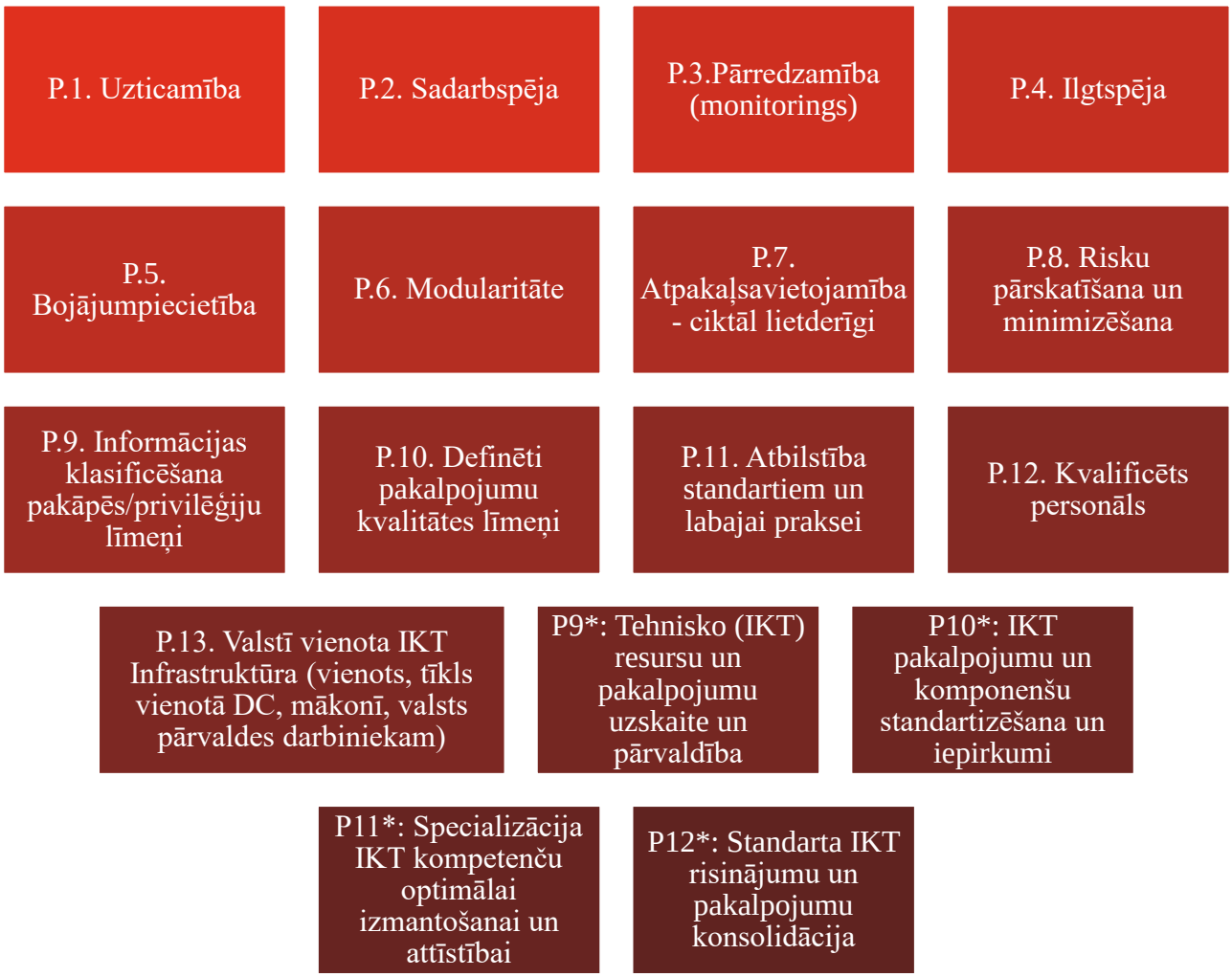
Pārskata periodam no 2024.gada līdz 2029.gadam IKT Infrastruktūras un kiberdrošības jomā tiek izvirzīti šādi specifiskie attīstības mērķi:
M.1. IKT Infrastruktūras resursu konsolidācija – Valsts datu centru apvienošana vienotā valsts datu apstrādes mākonī, centralizētu mākoņpakalpojumu izmantošana, vienotā datu pārraides tīkla infrastruktūrā (WAN, perimetra un LAN), kas atbilst noteiktajām prasībām kiberdrošības jomā.
M.2. Datu centri un mākoņdatošanas risinājumu paplašināšana un pilnveidošana – Būtiski samazināt valsts vienotā datu apstrādes mākoņa darbības pārtraukumu un datu zuduma riskus viena vai vairāku datu centru un citu IKT infrastruktūras būtisko elementu vienlaicīgas atteices scenārijos. Valsts pārvaldes IS un reģistri ir dublēti atbilstoši prasībām kiberdrošības jomā noteiktajam.
M.3. Tiklu attīstība un pilnveidošana – Drošs ātrgaitas datu pārraides tīkls starp mākoņdatošanas pakalpojuma sniedzējiem, datu vēstniecību, privātā sektora mākoņdatošanas pakalpojumu sniedzējiem, tostarp hiperskeileriem, un stabils, drošs datu pārraides tīkls līdz gala lietotāju datorizētajām darba vietām.
M.4. Datu vēstniecības izveide un uzturēšana – Ārpus Latvijas teritorijas izmitināta kiberdrošības prasībām atbilstoša IKT infrastruktūra valsts pārvaldes kritisko funkciju nodrošinošo IS darbināšanai. Starp Datu vēstniecību un valsts vienotajiem datu centriem ir drošs datu pārraides tīkls.
M.5. Kiberdrošības prasībām atbilstoša datorizētās darbavietas attīstība – Tehnoloģiskā platformā valsts pārvaldes darbinieku darbvirsmu, mobilo ierīču un datu pārraides tīklu centralizētas darbības nodrošināšana, apkalpošanas funkciju Centralizācija nodrošinot IKT ekspertu konsolidāciju, specializāciju un attīstību.
M.6. Programatūras sagādes un darbināšanas pilnveidošana – vienotā programmatūras koda repozitorija principa pielietošana attīstot lietojumprogrammatūras risinājumus un to komponentes par publisku finansējumu, nodrošinot, lai izstrādes rezultāti (tajā skaitā programmatūras pirmkods un tā dokumentācija) ir pieejami pēc iespējas plašākam potenciālo izmantotāju lokam. Iegādājoties jaunu programmatūru tā atbilst noteiktajām minimālajām prasībām.
M.7. Droša IKT infrastruktūra – nodrošināt valsts IKT sistēmu, datu pārraides tīkla un datu drošību, integritāti, pieejamību un noturību pret kiberuzbrukumiem, sniegto pakalpojumu ietvaros.

2.2 Jomas attīstības principi

[3] Par Digitālās transformācijas pamatnostādnēm 2021.–2027. gadam

Mērķu īstenošanai definēti vairāki jomas attīstības principi. Principi ir izmantojami jomas risinājumu un projektu attīstības plānošanai un risinājumu arhitektūras izveidei. Principi balstīti uz valsts IKT arhitektūras vadlīnijām[4], Eiropas sadarbspējas ietvara rekomendācijām[5], kā arī nozares standartiem[6] un labāko praksi.

2.2.1 Visām apakš jomam kopīgie principi:



1. Attēls. Visām apakš jomām kopīgie principi.

P.1. Uzticamība – Risinājumu uzticamība ir jomas arhitektūras pamatprincips. Risinājumiem ir jābūt drošiem, uzticamiem un jānodrošina atbilstība normatīvo aktu prasībām. Klientiem ir jājūtas droši, izmantojot jebkuru valsts pārvaldes risinājumu.
P.2. Sadarbspēja – Risinājumos jānodrošina informācijas sistēmu, tehnoloģiju un datu

[4] IKT arhitektūras vadlīnijas | Viedās administrācijas un reģionālās attīstības ministrija (varam.gov.lv). Avots: https://www.varam.gov.lv/lv/ikt-arhitekturas-vadlinijas
[5] European Interoperability Framework | Joinup (europa.eu). Avots: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework
[6] Architecture Principles (opengroup.org). Avots: https://pubs.opengroup.org/architecture/togaf8-doc/arch/chap29.html

sadarbspēja[7]. Sadarbspējas nodrošināšanai būtiski izvēlēties standartizētus un tehnoloģiski neitrālus risinājumus, kā arī atvērtos standartus un specifikācijas. Risinājumiem jānodrošina atvērtas saskarnes un tiem ir jābūt sadarbspējīgiem gan nacionālā, gan ES kontekstā.

P.3. Pārredzamība (monitorings) – Stiprina sistēmu drošību un uzticamību, palīdzot valsts IKT infrastruktūrai un kiberdrošības arhitektūrai ātri reaģēt uz draudiem un nodrošināt stabilu un drošu darbību ilgtermiņā. Nodrošina pastāvīgu un pārskatāmu sistēmu darbības uzraudzību, kas ļauj savlaicīgi identificēt problēmas, traucējumus vai drošības incidentus, kā arī nodrošina atbildību un uzticēšanos starp iesaistītajām pusēm.

P.4. Ilgstspēja – Risinājumi un infrastruktūra ir izstrādāti un pārvaldīti tā, lai spētu darboties efektīvi un droši ilgtermiņā. Risinājumi ir tehnoloģiski noturīgi un resursu ziņā efektīvi, atbilst nākotnes vajadzībām un ir droši ilgtermiņa perspektīvā.

P.5. Bojājumpiecietība – IKT infrastruktūra ir noturīga pret traucējumiem un drošības incidentiem, nodrošinot gan nepārtrauktus pakalpojumus, gan ātru atjaunošanos pēc incidentiem.

P.6. Modularitāte – Vienota elastīga un vieglāka pārvaldība sistēmu un risinājumu struktūra, kas veidota no neatkarīgiem un savstarpēji aizvietojamiem moduļiem. Modularitāte padara IKT infrastruktūru un kiberdrošību daudz elastīgāku, pielāgojamāku, vairākkārt izmantojamu un uzturēšanai draudzīgāku, kas palīdz veidot ilgtermiņā ilgtspējīgus un drošus risinājumus.

P.7. Atpakaļsavietojamība, ciktāl lietderīgi – Saglabāt esošo sistēmu darbības nepārtrauktību, pakāpeniski pārejot uz jaunām tehnoloģijām. Nodrošināt spēju darboties kopā ar vecākām versijām vai tehnoloģijām, kad tas ir praktiski un izdevīgi. Pakāpeniska migrācija ļaus veikt sistēmu modernizāciju pakāpeniski, vienlaikus saglabājot darbību ar vecākām tehnoloģijām, līdz tās tiek aizstātas vai modernizētas.

P.8. Risku pārskatīšana un minimizēšana – Princips veicina IKT infrastruktūras un kiberdrošības risinājumu noturību, pielāgojamību un spēju efektīvi reaģēt uz dažādiem draudiem, nodrošinot valsts pārvaldes sistēmu nepārtrauktību un drošību. Skaidrs ieskats IKT risinājumu darbībā, savlaicīgu draudu un traucējumu atklāšana, kā arī proaktīvu drošības risku pārvaldība. Ieviests nepārtraukts un sistemātisks process risku identificēšanai, novērtēšanai un mazināšanai.

P.9. Informācijas klasificēšana pakāpēs/privilēģiju līmeņi – Nodrošināt sistēmu drošību un aizsardzību, efektīvi pārvaldot riskus un piekļuves tiesības atbilstoši informācijas vērtībai, jūtīgumam un normatīvajiem aktiem. Skaidri definēti informācijas pakāpes un lomu privilēģiju līmeņi, kas nosaka, kuri lietotāji vai sistēmas komponentes drīkst piekļūt konkrētajai informācijai vai resursiem.

P.10. Definēti pakalpojumu kvalitātes līmeņi – Pakalpojumi tiek sniegti atbilstoši noteiktiem minimālajiem un kopējiem standartiem, kas garantē to drošību, pieejamību un stabilitāti, uzlabo klientu apmierinātību un efektīvu pakalpojumu pārvaldību. Skaidri definēti un nodrošināti kvalitātes līmeņi IKT pakalpojumu sniedzējiem.

P.11. Atbilstība standartiem un labajai praksei – Princips veicina stabilitāti, drošību un uzticamību IKT infrastruktūrā un kiberdrošībā. Regulāra pārvaldības prakses novērtēšana un uzraudzība, lai atbilstu standartiem un identificētu uzlabojumu nepieciešamību risku samazināšanā, efektivitātes uzlabošanā un standartu un normatīvo aktu ievērošanā.

P.12. Kvalificēts personāls – Tiek nodrošināts, ka visiem procesiem un sistēmām, kas saistītas ar informācijas drošību un tehnoloģiju pārvaldību, ir profesionāli apmācīti, zinoši, prasmīgi un pieredzējuši kvalificēti darbinieki. Regulāri zināšanu un prasmju pilnveidošanas pasākumi, kas ietver sertifikācijas programmas, seminārus un citus izglītības pasākumus nodrošina nemainīgi

[7] IKT arhitektūras vadlīnijas Vides aizsardzības un reģionālās attīstības ministrija (varam.gov.lv). Avots: https://www.varam.gov.lv/lv/ikt-arhitekturas-vadlinijas

augstu kvalitāti.

Sekojošie principi ir pārmantoti no Informatīvais ziņojums par publiskās pārvaldes informācijas sistēmu konceptuālo arhitektūru, 2015[8]*:*

P9: Tehnisko (IKT) resursu un pakalpojumu uzskaite un pārvaldība – Efektīvu IKT uzturēšanas procesu sastāvdaļa ir pieejamo tehnisko resursu uzskaite un pārvaldība. Valsts pārvaldes daļēji centralizētās IKT pārvaldības ietvaros tehnisko resursu uzskaiti veic tehnisko resursu īpašnieki. Tiek nodrošināta programmatūras licenču un to faktiskā izmantojuma precīza uzskaite, lai efektīvi izmantotu esošās licences un lai izvairītos no licencēšanas noteikumu pārkāpumiem.

P10: IKT pakalpojumu un komponenšu standartizēšana un iepirkumi – Nepieciešama elastīga standartizēšana, kas ļautu pārizmantot infrastruktūras risinājumus, rīkus un atbalsta procesus tādējādi ekonomējot infrastruktūras uzturēšanai nepieciešamos resursus un vienkāršojot pārvaldību. Virzība standartizēšanas virzienā ir pieļaujama tikai līdz robežai, kamēr neiestājas bezalternatīvu atkarība no viena ražotāja vai piegādātāja. Infrastruktūras standartizēšana rada papildus iespējas arī lielāku apjomu centralizētiem iepirkumiem.

P11: Specializācija IKT kompetenču optimālai izmantošanai un attīstībai – Nepieciešami kompetenču centri, kas specializējas noteiktu tehnoloģisko risinājumu jomā un/vai orientējas uz noteikta veida pakalpojumu sniegšanu. IKT atbalsta nodrošināšanā ir maksimāli jāveicina un jāizmanto iestāžu sadarbība un IKT koplietošanas risinājumi un pakalpojumi. Ir jāattīsta kompetenču un/vai koplietošanas pakalpojumu centri, kas nodrošina noteiktus pakalpojumus citām iestādēm.

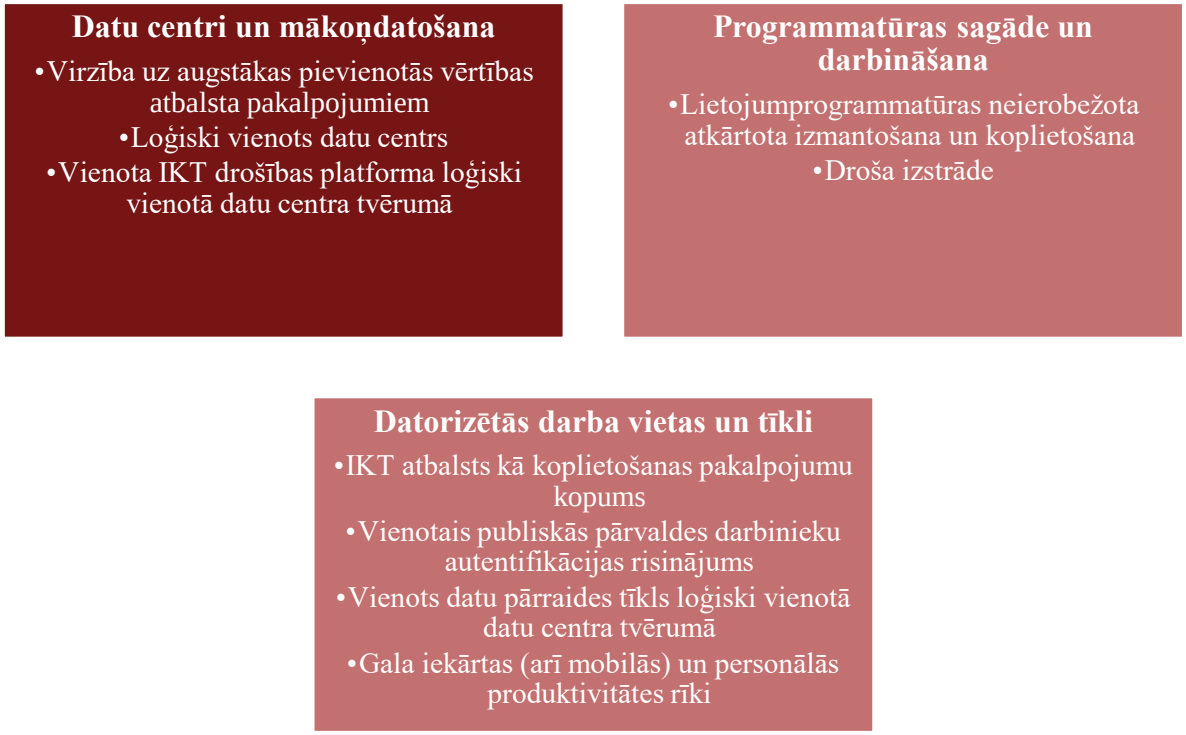
P12: Standarta IKT risinājumu un pakalpojumu konsolidācija – Standarta IKT risinājumu un atbalsta pakalpojumu fragmentācija nav pamatota, un no efektivitātes viedokļa optimāls ir vienotas (centralizētas) pakalpojumu sagādes un pārvaldības modelis. Vienota pakalpojumu centra pieeja ir paplašināma, to piemērojot visiem no nozarēm neatkarīgiem jeb standarta IKT atbalsta pakalpojumiem.

2.2.2 Apakš jomu specifiskie principi

Zemāk esošie principi ir saistoši un aktuāli no koncepcijas 2015.[9]

[8] 2015.gada 27.janvāra Informatīvais ziņojums "Par publiskās pārvaldes informācijas sistēmu konceptuālo arhitektūru"

[9] 2015.gada 27.janvāra Informatīvais ziņojums "Par publiskās pārvaldes informācijas sistēmu konceptuālo arhitektūru"



2. Attēls. Apakš jomu specifiskie principi.

2.2.2.1 Datu centri un mākoņdatošana

P13: Virzība uz augstākas pievienotās vērtības atbalsta pakalpojumiem – IKT atbalsta un pārvaldības resursus var optimizēt pārejot uz pēc iespējas augstākas pievienotās vērtības mākoņdatošanas pakalpojumu izmantošanu, grupējot tos četros līmeņos: SaaS, PaaS, IaaS un fiziskie resursi. (sākot ar fizisko resursu izmitināšanu IaaS PaaS un SaaS).
P37: Loģiski vienots datu centrs – loģiski vienotais publiskās pārvaldes datu centrs, kas veidots no vairākiem datu centriem dažādās atrašanās vietās, izmantojot tās investīcijas datu centru izveidē, kas dažādās valsts nozarēs pēdējā laikā jau veiktas. Infrastruktūras un datu dublēšanai tiks arī izveidota rezervēšana datu vēstniecībā ārvalstīs.
P39: Vienota IKT drošības platforma loģiski vienotā datu centra tvērumā – Datu centri un nozīmīgākās publiskās pārvaldes IKT resursi ir aizsargāti, izmantojot vienotu IKT drošības risinājumu, ielaušanās atklāšanas sistēmu.

2.2.2.2 Programmatūras sagāde un darbināšana

P19: Lietojumprogrammatūras neierobežota atkārtota izmantošana un koplietošana – Attīstot lietojumprogrammatūras risinājumus un to komponentes par publisku finansējumu, ir jānodrošina, lai izstrādes rezultāti (tajā skaitā programmatūras pirmkods un tā dokumentācija) ir pieejami pēc iespējas plašākam potenciālo izmantotāju lokam.
P22: Droša izstrāde – Drošas izstrādes prakses ieviešana būtiski samazina informācijas sistēmu *ievainojamību no drošības apdraudējumiem. Programmatūra jāizstrādā aizsargātā vidē. Izstrādes videi* jānodrošina, ka kiberdrošības prasības nav zemākas kā izstrādājamās sistēmas.

2.2.2.3 Datorizētās darba vietas un tīkli

P8: IKT atbalsts kā koplietošanas pakalpojumu kopums – Vispārpieņemta prakse ir IKT atbalstu nodrošināt kā pakalpojumu (servisu) kopumu, piemērojot tam pakalpojumu pārvaldības labo praksi un principus. Centralizēt IKT atbalsta pakalpojumus, lai nodrošinātu efektīvāku, drošāku un elastīgāku IKT pārvaldību visā valsts pārvaldē, uzlabojot digitālo transformāciju un reaģēšanas spējas uz kiberapdraudējumiem. IKT atbalsts kā centralizēts pakalpojums atvieglos IKT resursu pārvaldību un

administrēšanu nodrošinot vienotus standartus un procedūras.
P31: Vienotais publiskās pārvaldes darbinieku autentifikācijas risinājums – Piekļuve citu iestāžu uzturētām sistēmām nerada papildu apgrūtinājumus lietotāju darbā, kas, savukārt, var ierobežot servisu atkalizmantojamību un apmierinātību ar koplietošanas platformām, valsts pārvaldē nepieciešams vienotās autentifikācijas risinājums (single sign-on).
P38: Vienots datu pārraides tīkls loģiski vienotā datu centra tvērumā – Vienots valsts datu pārraides tīkls, lai nodrošinātu vienotu un drošu datu pārraidi starp institūcijām – datu centru un citu kritisko resursu savienošanai. Tas nodrošina savienojumu starp loģiski vienotā valsts datu centra fiziskajiem centriem, kā arī savienojumus uz ārzemju rezerves datu centriem.
P40: Gala iekārtas (arī mobilās) un personālās produktivitātes rīki – Nodrošināt informāciju sistēmu pieejamību dažādās gala iekārtās. Attiecībā uz informācijas sistēmu izstrādi ir kritiski svarīgi, lai ieviešamie risinājumi neizvirza īpašas prasības gala iekārtām, pieļaujot to efektīvu darbību pēc iespējas daudzveidīgās gala iekārtās.

3 Jomas mērķarhitektūra

Jomas mērķarhitektūra identificē būtiskākās izmaiņas jomas arhitektūras juridiskajā skatā, organizatoriskajā skatā, semantiskajā skatā un tehniskajā skatā. Jomas mērķarhitektūra strukturēta atbilstoši "The Open Group Architecture Framework (TOGAF)[10]" standarta prasībām, ņemot vērā Eiropas sadarbspējas paraugarhitektūras "European Interopability Reference Architecture (EIRA)[11]" rekomendācijas.

3.1 Juridiskais skats

Pārskata periodā ir paredzamas vairākas būtiskas izmaiņas jomas normatīvajā regulējumā, galvenās paredzamās izmaiņas ir aprakstītas 4.tabulā.

4. tabula. Paredzamās izmaiņas jomas juridiskajā skatā

Nr.	Normatīvais akts	Statuss	Izmaiņu apraksts un pamatojums
Datu centri un mākoņdatošana			
1.	Valsts datu apstrādes mākoņa noteikumi.	Izmaiņas	Noteikumu mērķis ir veicināt centralizāciju un vienotu pārvaldību, kas uzlabos efektivitāti, drošāku valsts datu apstrādi kā arī resursu optimizāciju, samazinot individuālos risinājumus un dublēšanos, kas būtiski ietaupīs finanšu resursus un cilvēkresursus. Iekļautas funkcijas, piemēram, integrācija ar Eiropas un Latvijas mākoņiem, izmantojot Eiropas mākoņdatošanas iniciatīvas standartus. Par brokera lomu atbildīgā institūcija (šobrīd – VDAA) nodrošinās valsts datu apstrādes mākoņa atbilstību mūsdienu tehnoloģiskajām prasībām. Brokera pārvaldnieks kļūs par centrālo starpnieku starp pakalpojumu saņēmējiem un pakalpojumu sniedzējiem, koordinējot mākoņpakalpojumu piegādi. Brokera pārvaldnieka loma ietver iepirkumu vadības funkcijas, kas nodrošina līgumu pārvaldību un piekļuves kontroli starp LVRTC, LNB, IeM IC un LDC (LAD) pakalpojumiem. MK noteikumi tiek izstrādāti, balstoties uz informatīvo ziņojuma pamata. Tie precizē un juridiski nostiprina ziņojumā paredzētās funkcijas un mērķus, nosakot atbildīgo iestāžu

[10] TOGAF | The Open Group Website: https://www.opengroup.org/togaf
[11] About European Interoperability Reference Architecture (EIRA): https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/about

Nr.	Normatīvais akts	Statuss	Izmaiņu apraksts un pamatojums
			lomas, pārejas posmus un tehnoloģiskās prasības, lai izveidotu un uzturētu efektīvu un drošu valsts datu apstrādes mākoņa infrastruktūru. MK noteikumi noteiks termiņu līdz kuram iestādēm ir jāsagatavo, jādefinē detalizēts pārejas plāns uz mākoņpakalpojumiem. Noteiks nepieciešamā finansējuma nodrošināšanas kārtību pārejā uz valsts mākoņpakalpojumiem un termiņus decentralizēto, individuālo risinājumu (privātajiem iestādes mākoņiem, serveriem) pakāpeniskai pārtraukšanai.
Programmatūras dzīves cikla nodrošināšana			
2.	MK noteikumi par programmatūras izstrāddarbināšanas platformas nodrošināšanu.	Jauns	Pirms noteikumu izstrādes ir paredzēts izveidot informatīvo ziņojumu, kas noteiktu vienotu pieeju valsts pārvaldes IS programmatūras izstrādes un darbināšanas procesiem ieviešot centralizētu DevOps risinājumu. Noteikumi nepieciešami, lai valsts programmatūras tiktu veidotas un darbinātas atbilstoši pasaulē noteiktajai labajai praksei un veicinātu standartizāciju, iestāžu sadarbību, uzlabotu drošību un optimizētu resursu. Noteikumi nostiprinās informatīvajā ziņojumā izvirzītos mērķus un funkcijas, precizējot atbildīgās iestādes, to lomas, pienākumus un prasības attiecībā uz programmatūras izstrādi, darbināšanu un uzturēšanu, izmantojot centralizētu DevOps risinājumu. Tiks noteikta iestāde vai iestādes, kas uzturēs un pārvaldīs centralizēto DevOps risinājumu, pārējām iestādēm savas programmatūras attīstību un uzturēšanu būs jānodrošina atbilstoši DevOps platformā noteiktajām vadlīnijām. Noteikumi definēs pakāpenisku pāreju uz DevOps risinājumu izmantošanu, nosakot termiņus integrācijai un atbalsta mehānismus (apmācības un tehnisko konsultāciju sniegšana veiksmīgai pārejai). Noteikumi noteiks arī apmaksas kārtību.
Datorizētās darba vietas un tīkli			
3.	Informatīvais ziņojums par centralizētas datorizētās darba vietu un datu pārraides tīklu platformas pārvaldība.	Jauns	Informatīvā ziņojuma mērķis ir uzlabot valsts pārvaldes IKT infrastruktūras efektivitāti, drošību un ilgtspēju, veicot būtiskas reformas darba vietu un tīkla pārvaldības jomā. Izveidot vienotu pieeju, kas standartizē darbvirsmu, mobilo ierīču un datu pārraides tīklu pārvaldību, nodrošinot vienotu un drošu lietotāju pieredzi. Centralizācija samazina tehnoloģiju pārklāšanos un dublēšanos, nodrošinot zemākas kopējās izmaksas.
4.	MK noteikumi par centralizētas datorizētās darba vietu un datu pārraides tīklu platformas pārvaldība.	Jauns	Noteikumu galvenie mērķi ir standartizēt valsts pārvaldes IKT darba vietas un tīklu pārvaldību, samazināt resursu dublēšanos un pārklāšanos, un uzlabot kiberdrošību. Šie MK noteikumi tiks izstrādāti, balstoties uz informatīvo ziņojumu par centralizētas datorizētās darba vietu un datu pārraides tīklu platformas pārvaldību, kura mērķis ir uzlabot valsts pārvaldes IKT infrastruktūras efektivitāti, drošību un ilgtspēju. Noteikumi konkretizē informatīvajā ziņojumā ietverto informāciju un pievieno detalizētus pienākumus, procedūras un atbildīgās iestādes. Noteiks iestādi, kas koordinēs, nodrošinās lietotāju atbalstu un pārvaldīs centralizētās darba vietas un tīklu infrastruktūru. Noteikumi samazinās administratīvās

Nr.	Normatīvais akts	Statuss	Izmaiņu apraksts un pamatojums
			izmaksas un tehnoloģiskos riskus, vienlaikus ieviešot augstākus drošības standartus. Noteikumi noteiks arī apmaksas kārtību.
c			
5.	Koncepcija par Datu vēstniecības izveidi.	Jauns	Koncepcijā tiek ieviests datu vēstniecības risinājums, kas nosaka valsts pārvaldes kritisko datu un sistēmu aizsardzības mehānismu ārpus valsts robežām. Koncepcijā tiek noteikti kritēriji sistēmu un reģistru atjaunošanas termiņiem. Sistēmām un reģistriem, kas ir daļa no kritiskiem pakalpojumiem, Datu vēstniecībā pēc atkopes jādarbojas augstas pieejamības režīmā ar slodzes balansēšanu. Līdz atkopei un arī pēc tās Datu vēstniecībā jānodrošina datu rezerves kopiju droša izveide un glabāšana, kā arī pilnai atkopei nepieciešamie serveru, datu glabātuvju, programmatūras un tīkla iekārtu resursi. Datu vēstniecībā iekļaujamajām valsts pārvaldes sistēmām un reģistriem tiek noteikts izstrādāt un ieviest pilnas avārijas atkopes (*disaster recovery)* ārpus Latvijas Republikas teritorijas plānus, kā pielikumu darbības nepārtrauktības plānam - DNP, kas paredz periodiski atjaunojamas datu un sistēmu atjaunošanas procedūras Datu vēstniecības infrastruktūrā. Šie plāni drošā veidā jāglabā datu vēstniecības teritorijā ar piekļuvi tikai autorizētam personālam. Lai izveidotu un uzturētu Datu vēstniecību, koncepcijā paredz noteikt finansējuma pieprasījumu valsts budžetā. Koncepcija nepieciešama, lai stiprinātu valsts drošību, nodrošinot valsts stratēģisko datu un IS pieejamību un aizsardzību pret dažādiem apdraudējumiem.
6.	MK noteikumi par Datu vēstniecībā izmitināmajām IS.	Jauns	Noteikumu mērķis ir garantēt valsts pārvaldes funkciju un datu pieejamību ārkārtas situācijās. Šie MK noteikumi tiek izstrādāti, pamatojoties uz koncepciju par datu vēstniecības izveidi, kurā aprakstīts datu vēstniecības koncepts, sistēmu atjaunošanas nosacījumi. Noteikumi papildina koncepciju, detalizēti nosakot konkrētas procedūras, atbildīgās iestādes un to pienākumus. Noteikumi precīzi definē kritērijus, kā tiek izvēlētas un klasificētas IS, kuras tiek izvietotas Datu vēstniecībā. Noteikumi noteiks iestādi, kas koordinēs IS izvietošanu datu vēstniecībā, noteiks darbības, kas būs jāveic iestādēm kuru IS jāizvieto Datu vēstniecībā un kādus kiberdrošības standartus jāievēro pašai Datu vēstniecībai un tajā esošajām IS. Noteikumi arī noteiks budžeta piesaisti datu vēstniecības izveidei un tās uzturēšanai.

3.2 Organizācijas skats

Pārskata periodā ir paredzamas vairākas izmaiņas jomas funkcijās, uzdevumos un pakalpojumos, kas galvenokārt saistīti ar funkciju un pakalpojumu Centralizāciju, efektivitātes un kiberdrošības uzlabošanu.

3.2.1 Funkcijas

IKT infrastruktūras un kiberdrošības jomas mērķa funkciju un uzdevumu tabula (5.tabula), definē tā īstenotās funkcijas un uzdevumus līdz 2029. gada sākumā.

5. tabula. Paredzamās izmaiņas jomas funkciju skatā

Esošās funkcijas	Jaunās funkcijas(t.sk., plānotās)
Decentralizēta attālināto lietotāju apkalpošana iestādes vai resora līmenī.	Centralizēta attālināto lietotāju apkalpošana. Vienots palīdzības dienests: • Incidentu reģistrēšana un apstrāde; • Problēmu reģistrācija un risināšanas kontrole; • Lietotāju konsultēšana; • Programmatūras attālināta uzturēšana (instalēšana, atjaunināšana utt.); • Aktīvās direktorijas (Active Directory) lietotāju pārvaldība; • IS lietotāju pārvaldība; • Datu pārraides tīkla, datu centru un informācijas sistēmu pieejamības pārraudzība; • Lokālā atbalsta darbu kontrole; • Lietotāju konsultēšana par kiberdrošības politikas ievērošanu.
Decentralizēts Datortehnikas attālinātais atbalsts.	Centralizēta standartizētās darbavietas programmatūras pārvaldība: • Operētājsistēma; • Biroja programmatūra; • Regulāro atjauninājumu savietojamības testēšana ar izmantojamo programmatūru un uzstādīšana gala iekārtām; • Kiberdrošības programmatūra; • Datora attālinātās vadības programmatūras u.c.
Decentralizēts lokālo lietotāju (onsite support) (t.sk. LAN) un operatīvo, fizisko lietotāju atbalsts.	Centralizēts lokālo lietotāju atbalstu (onsite support) (t.sk. LAN) un operatīvo, fizisko lietotāju atbalsts, tai skaitā: • Lietotāju darba vietu iekārtošana; • Inventāra uzskaiti; • Bojātās tehnikas remonta administrēšana; • LAN krosēšana un slēgkabeļa (patching) pievienošana darbstacijām; • Mikrokoda atjaunināšana datoram, mobilam ierīcēm un perifērijas iekārtām; • SIEM/SOC darbstacijām un iekšējiem datu pārraides tīkliem.
Decentralizēta datortehnikas un sakaru iekārtu un programmatūras sagāde un pārvaldība dzīves cikla laikā.	Centralizēta datortehnikas un sakaru iekārtu un programmatūras sagāde un pārvaldība dzīves cikla laikā: • Datortehnikas un programmatūras vajadzību apkopošana un analīze; • Pieejamās datortehnikas un programmatūras apkopošana un analīze; • Atbilstošā programmatūras komplekta (klona) uzturēšana un uzstādīšana lietotājam; • Dzīves cikla plānošana; • Centralizēta iepirkumu organizēšana; • Drošības prasībām atbilstošas tehnikas sagatavošana darbam, uzstādot nepieciešamo programmatūru; • Sagatavotās tehnikas nogāde lokālajam lietotāju atbalstam; • Inventarizācija; • Novecojošās tehnikas uzglabāšana un utilizācija; • Iekārtu iegādei nepieciešamā finansējuma plānošana.
Decentralizēts, katrai ministrijai/iestādei ir savs WAN.	Centralizēts WAN (Wide Area Network) –Valsts pārvaldē vienots WAN starp iestādēm un datu centriem: • Datu pārraides tīklu plāns; • Datu pārraides tīkla parametru konfigurācijas;

	• Tīkla vadības monitoringa sistēma; • Mobilās tīkla brigādes; • Ugunsmūru konfigurācijas.
Decentralizēta datortehnikas lietotāju funkcijām atbilstošu lomu un politiku pārvaldība.	Centralizēta datortehnikas lietotāju funkcijām atbilstošu lomu un politiku pārvaldība: • Lietotāju nepieciešamo lomu apzināšana; • Lietotāju lomu un politiku veidošana, konfigurēšana un dzēšana aktīvajā direktorijā.
Daļēji decentralizēti mākoņdatošanas pakalpojumi.	Mākoņpakalpojumus nodrošina mākoņdatošanas pakalpojumu sniedzēji: • Apzina vajadzības; • Nodrošina atbilstību Valsts datu apstrādes mākoņa noteikumiem; • Nodrošina atbilstību kiberdrošības jomas normatīvajiem aktiem; • Nodrošina mākoņdatošanas infrastruktūru; • Centralizēta SIEM/SOC pakalpojuma nodrošināšana; • Serveru infrastruktūrai; • Mākoņdatošanas platformai; • Informācijas sistēmām; • Datu pārraides tīklam.
Valsts pārvaldes dati nav izvietoti ārpus Latvijas teritorijas.	Datu vēstniecība: • Nepieciešamo infrastruktūras resursu nodrošināšana; • Datu kopiju izvietošana datu vēstniecībā; • Kritisko IS darbības nodrošināšana. Datu sinhronizēšanas nodrošināšana un automātiskais failover (rezerves darbības aktivizēšana). IS darbības nepārtrauktības nodrošināšana; • Droša datu tīkla nodrošināšana starp Datu vēstniecību un valstī esošajiem Datu centriem.
Decentralizēti DevOps risinājumi.	Centralizēts DevOps risinājums visā valsts pārvaldē: • Resoriem vai iestādēm ir pieejama tikai uz tām attiecināmā DevOps risinājuma aktuālās kopijas daļa; • Koda repozitorijam var piekļūt visas valsts iestādes un izstrādātāji; • Centralizēti pārvaldīts, versionēts un glabāts pasūtītais programmatūras orģinālkods; • Izveidots kontroles process, kas apstrādā iesūtītās un atklātās koda ievainojamības; • Ar automatizētajām plūsmām iespējams veikt testus, drošības pārbaudes, relīžu veidošanu un modernu, mūsdienīgu relīžu izvietošanu produktīvajā vidē.

6.tabulā apkopots funkciju/uzdevumu izmaiņu apraksts.

6. tabula. Paredzamās izmaiņas jomas funkcijās/ uzdevumos

Nr.	Funkcija/uzdevums	Statuss	Izmaiņu apraksts un pamatojums
1.	Centralizēta attālināto lietotāju apkalpošana. Vienots palīdzības dienests.	Jauna/ uzlabota funkcija.	Centralizēta un vienota palīdzības dienesta izveide, kas nodrošinās atbalstu visām iestādēm, izmantojot modernus uzdevumu pārvaldības un monitoringa rīkus. Centralizēta infrastruktūras atbalsts un kopīgs personāls samazina dublēšanos un uzturēšanas izmaksas. Nodrošinās vienotu lietotāju pieredzi neatkarīgi no iestādes vai resora. Centralizētas drošības politikas un instrumenti, piemēram, vienota piekļuves pārvaldība un reāllaika monitorings, mazina ievainojamības riskus.

Nr.	Funkcija/uzdevums	Statuss	Izmaiņu apraksts un pamatojums
			Vienota drošības politika nodrošina labāku risku pārvaldību un atbilstību standartiem. Vienots palīdzības dienests ļauj efektīvāk reaģēt uz incidentiem un ātrāk risināt problēmas.
2.	Centralizēta standartizētās darbavietas programmatūras pārvaldība.	Jauna/ uzlabota funkcija.	Pāreja uz centralizētu modeli, kurā tiek nodrošināta vienota, standartizēta pieeja valsts pārvaldes darbavietu programmatūras pārvaldībai. Centralizēta platforma darbavietu pārvaldībai, izmantojot automatizētus rīkus programmatūras izplatīšanai, konfigurācijai un atjauninājumiem. Vienots programmatūras katalogs, kas nodrošina konsekventu piekļuvi atļautām lietojumprogrammām. Samazinātas uzturēšanas un darbaspēka izmaksas, pateicoties centralizētai vadībai. Konsolidēta drošības politika un vienota ievainojamību pārvaldība. Vienota pārvaldība nozīmē labāku aizsardzību pret kiberdraudiem un datu noplūdēm. Centralizācija samazinās problēmu risināšanas laikus, kas līdz ar to palielina pārvaldes darbības efektivitāti.
3.	Centralizēts lokālo lietotāju atbalstu (onsite support) (t.sk. LAN) un operatīvo, fizisko lietotāju atbalsts.	Jauna/ uzlabota funkcija.	Viens kopējs atbalsta dienests nodrošina lietotāju un LAN infrastruktūras tehnisko atbalstu visā valsts pārvaldes mērogā. Vienots kvalitātes līmenis, kas nodrošināta augsta līmeņa lietotāju atbalsta konsekvence neatkarīgi no iestādes. Lietotāji saņem ātrāku un kvalitatīvāku atbalstu, neatkarīgi no atrašanās vietas. Centralizācija samazina administratīvo un tehnisko personālu nepieciešamību, samazinot izmaksas. Labāka LAN tīklu pārvaldība un monitorings nodrošina augstāku kiberdrošības līmeni. Centralizācija palīdzēs uzlabot vispārējo valsts pārvaldes tehnisko atbalstu un drošību, vienlaikus samazinot dublētās funkcijas un nodrošinot efektīvāku resursu izmantošanu.
4.	Centralizēta datortehnikas un sakaru iekārtu un programmatūras sagāde un pārvaldība dzīves cikla laikā.	Jauna/ uzlabota funkcija.	Centralizēts modelis, kurā valsts līmenī tiek organizēta vienota datortehnikas, sakaru iekārtu un programmatūras sagāde, pārvaldība un dzīves cikla uzturēšana. Centralizācija novedīs pie standartizētas infrastruktūras ar vienotiem tehniskiem risinājumiem un specifikāciju visās valsts iestādēs. Vienoti iepirkumi un standartizācija samazina kopējās izmaksas. Centralizēta dzīves cikla pārvaldība iekļaus vienotu tehnikas uzturēšanu, monitoringu, aizvietošanu un utilizāciju. Centralizācija ļaus īstenot stingrākas kiberdrošības prasības, nodrošinās pārredzamību, efektivitāti datortehnikas un sakaru iekārtu uzraudzībā.
5.	Centralizēts WAN (Wide Area Network) – Valsts pārvaldē vienots WAN starp iestādēm un datu centriem.	Jauna/ uzlabota funkcija.	Centralizēts WAN tīkls valsts pārvaldei, kas savieno visas iestādes un datu centrus vienotā infrastruktūrā. Vienotais WAN ievērojami samazina uzturēšanas, aparatūras un tīkla savienojumu izmaksas. Vienoti drošības standarti un centralizēta uzraudzība samazina iespējamās ievainojamības un kiberdraudus. Vienots WAN tīkls nodrošina ātrāku un vienkāršāku datu apmaiņu starp iestādēm.
6.	Centralizēta datortehnikas lietotāju funkcijām atbilstošu lomu un politiku pārvaldība.	Jauna/ uzlabota funkcija.	Pāreja uz vienotu, centralizētu pieeju lomu un politiku pārvaldībā, kas nodrošina konsekventu un drošu lietotāju piekļuves pārvaldību visā valsts pārvaldē. Samazinās nepieciešamība uzturēt vairākas neatkarīgas piekļuves pārvaldības sistēmas un to atbalsta komandas. Vienota lomu un politiku pārvaldība atvieglo iestāžu sadarbību, datu apmaiņu un resursu koplietošanu. Centralizēta uzraudzība un vienoti drošības standarti samazina riskus un ievainojamības. Vienota sistēma nodrošina konsekventu lietotāju pieredzi neatkarīgi no tā, kurā iestādē lietotājs strādā.
7.	Standartizēti, elastīgi mākoņpakalpojumi ko nodrošina gan publiskā sektora, gan privātie pakalpojumu sniedzēji.	Uzlabota funkcija.	Nodrošinās standartizāciju ar vienotiem tehniskiem un drošības standartiem visiem mākoņpakalpojumu sniedzējiem, nodrošinot konsekvenci un savietojamību. Publiskā un privātā sektora mākoņpakalpojumu izmantošana, pamatojoties uz pakalpojuma veidu un drošības prasībām. Centralizēta pieeja pakalpojumu sniedzēju

Nr.	Funkcija/uzdevums	Statuss	Izmaiņu apraksts un pamatojums
			izvēlei, pārvaldībai un drošības prasību ievērošanai.
8.	Datu vēstniecība.	Jauna.	Izveidota datu vēstniecība, kas ir izveidota IKT infrastruktūra ārpus Latvijas teritorijas, kas nodrošina valsts kritisko datu un sistēmu drošu glabāšanu. Datu vēstniecība garantē nepārtrauktu piekļuvi svarīgākajām datu sistēmām un informācijai, pat ja valstī rodas tehnoloģiskās vai drošības problēmas. Valsts pakalpojumu darbība netiks pārtraukta katastrofu, kara, kiberuzbrukuma vai citu ārkārtas apstākļu gadījumā. Datu vēstniecības izveide iekļaus nepieciešamās IKT infrastruktūras identificēšanu un iegādi, atrašanās vietas izvēli, nepieciešamo datu un IS apzināšanu un iekļaušana Datu vēstniecībā. Datu vēstniecība iekļaus arī drošības pasākumus, kā piekļuves kontroli, šifrēšanas tehnoloģijas un uzraudzības mehānismus, lai novērstu nesankcionētu piekļuvi.
9.	Centralizēts DevOps risinājums visā valsts pārvaldē.	Jauna/ uzlabota funkcija.	Centralizētā pieejā tiek ieviests vienots DevOps risinājums, kas nodrošina saskaņotu platformu visām valsts pārvaldes iestādēm, lai izstrādātu, testētu, izvietotu un uzturētu programmatūras risinājumus. Resursu centralizācija samazina uzturēšanas un operatīvās izmaksas. Vienots kodu repozitorijs, kas būs pieejams visām valsts iestādēm un izstrādātājiem, nodrošinot kodu pārizmantojamību. Centralizācija samazina nevajadzīgu rīku un infrastruktūras dublēšanos dažādās iestādēs. Iebūvētas CI/CD (Continuous Integration/Continuous Deployment) metodes efektīvai programmatūras pārvaldībai.

3.2.2 Pakalpojumi

IKT infrastruktūras un kiberdrošības jomas mērķa pakalpojumi definē domēnā sniegtos pakalpojumus līdz 2029. gada sākumam.
IKT infrastruktūras un kiberdrošības jomā esošo pakalpojumu saraksts redzams 7.tabulā pie katra pakalpojuma noradīts pakalpojuma izmaiņu apraksts. Vēršam uzmanību, ka tabulā norādītais uzskaitījums nav statisks, attīstoties jomām, veidojoties jauniem risinājumiem, šis saraksts tiks atjaunots.

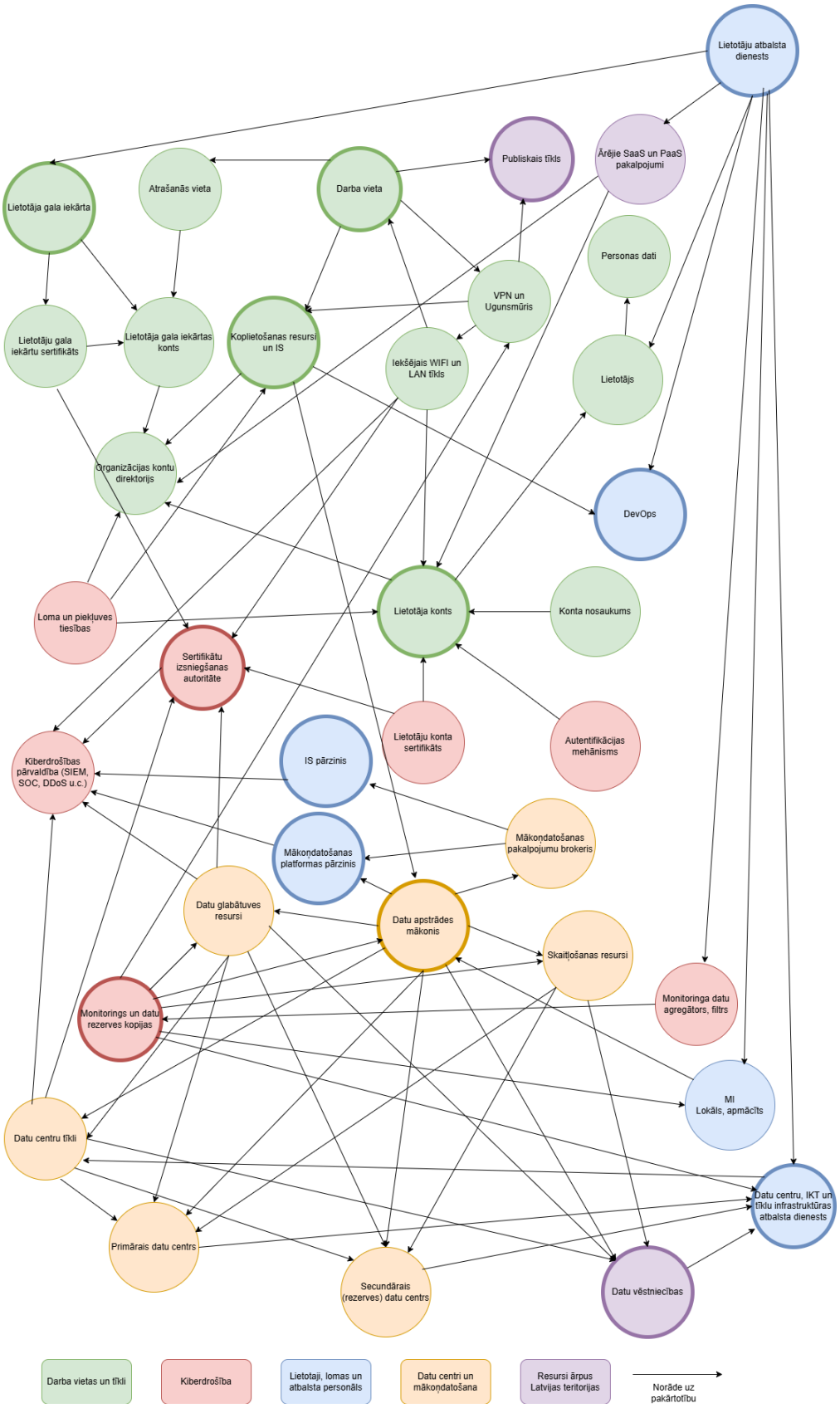
7. tabula. Paredzamās izmaiņas jomas pakalpojumos

Nr.	Pakalpojums	Statuss	Institūcija	Izmaiņu apraksts un pamatojums
1.	Centralizēts datorizētās darba vietas pakalpojums.	Uzlabota, plānots pakalpojums un funkcija.	Noteiks MK noteikumi.	Viena iestāde sniedz Centralizētu pakalpojumu visām citām valsts pārvaldes iestādēm. Pakalpojums sevī iekļaus arī IKT atbalstu kā koplietošanas pakalpojumu, un kontu (lietotāju un datorsistēmu), lietotņu administrēšanu un tehnisko atbalstu. Pakalpojuma ietvaros tiks ievērotas arī kiberdrošības prasības un tiks ieviesta centralizēta gala iekārtu aizsardzība pret datorvīrusiem un ļaunatūru. Pakalpojuma nodrošināšanai tiks izveidota centralizēta tehnoloģiskā platforma valsts pārvaldes darbinieku darbvirsmu un mobilo ierīču darbības un apkalpošanas nodrošināšanai, darba vieta ietvers standartizētu programmatūras komplektu. Pakalpojuma nodrošināšanas ietvaros tiks realizēta institūciju IKT ekspertu kompetenču konsolidācija, specializācija un attīstība datorizēto darba vietu un tīkla darbības nodrošināšanai.

Nr.	Pakalpojums	Statuss	Institūcija	Izmaiņu apraksts un pamatojums
2.	Datu centri un mākoņdatošanas pakalpojumi.	Papildināta, Spēkā esošs, Plānots pakalpojums un funkcija.	LNB, LVRTC, ZM LAD, IeM IC un ārpakalpojumi.	Augstas kvalitātes un kiberdrošības valsts mākoņdatošanas platformu pārziņu un privātā sektora mākoņdatošanas pakalpojumi, kas galvenokārt ietvers IaaS, PaaS (ar mākoņdatošanas pakalpojumu nodrošināšanas saistītais PaaS, operētājsistēmu datu bāzu programmatūras licences), SaaS (valsts pārvaldes nespecifisko funkciju aplikāciju darbināšanai), BaaS *(Backup as a Service)*, Datu telpas *(Data spaces)*, nodrošina sistēmu migrācijas pakalpojumu, Privāto mākoņu *(Private cloud)* izmitināšana DC u.c. pakalpojumi. Laika gaitā arī attīstot tādus pakalpojumus kā AIaaS *(AI as a Service)*.
3.	Viens centralizēts DevOps kā pakalpojums.	Jauns, Uzlabots, Plānots pakalpojums un funkcija.	Noteiks MK noteikumi.	Pakalpojumu nodrošinās viena iestāde, kas nodrošinās vienotu Centralizētu DevOps pakalpojumu un sniegs atbalstu visām valsts pārvaldes iestādēm, uzturēs platformu, iekļaujot CI/CD procesus, pārvaldību un automatizāciju, un vienotu DevOps rīku komplektu. Izveidos un uzturēs vienotu kodu repozitoriju, kas nodrošinās centralizētu kodu glabāšanu, piekļuves kontroli un versiju pārvaldību un dalīšanos ar atkārtoti izmantojamiem moduļiem un risinājumiem starp iestādēm. Nodrošinās to, ka centralizētā DevOps vide atbilst kiberdrošības prasībām.
4.	Datu vēstniecības darbības nodrošināšana.	Jauns, Plānots pakalpojums un funkcija.	Noteiks MK noteikumi.	Datu vēstniecība ir kritisks risinājums, kas nodrošina valsts pārvaldes datu un IS nepārtrauktību ārkārtas situācijās, veicinot arī valsts neatkarību no ārējām ietekmēm un nodrošina stratēģisku datu aizsardzību.

3.3 Semantiskais skats

Pārskata periodā ir paredzamas vairākas izmaiņas domēnā radītajos un apstrādātajos informācijas resursos. Jomas resursu un procesu saistību attēls zemāk (3. Attēls. Jomas resursu un procesu saistību mērķa karte).



3. Attēls. Jomas resursu un procesu saistību mērķa karte.

3.Attēlā atspoguļots Jomas resursu un procesu saistību mērķa karte, kur atspoguļoti ar zaļu krāsu atspoguļoti Darba vietas un tīklu elementi, ar sarkanu – kiberdrošības elementi, ar zilu krāsu – Lietotāji, lomas un atbalsta personāla elementi, ar oranžu krāsu – Datu centri un mākoņdatošanas elementi, ar violetu krāsu – Resursi ārpus Latvijas teritorijas un ar bultiņām ir atspoguļota elementu savstarpējā mijiedarbība.

Galvenie arhitektūras elementi ir:

- Lietotājs ir būtisks arhitektūras elements, kur tipiski institūcijas darbinieks vai amatpersona un arhitektūrā ir reprezentēts ar savu digitālo identitāti vai Lietotāja kontu, kas ir daļa no lietotāja digitālās identitātes un personas datiem, kas ļauj to viennozīmīgi identificēt. Lietotāja darba nodrošinājuma un atbalsta procesus realizē Lietotāju atbalsta dienests.
- Lietotāja gala iekārtas ir tehniskais palīglīdzeklis darba pienākumu veikšanai digitālajā vidē. Lietotāju atbalsta dienests veic gala iekārtu reģistrāciju, izsniegšanu, apkopi, atjaunināšanu un utilizāciju. Lietotāju gala iekārtas konts un gala iekārtu sertifikāts ir iekārtas reprezentācija digitālajā vidē, pēc kā tās ir unikāli identificējamas.
- Lietotāju kontu piekļuves tiesības definē un vienlaikus ierobežo lietotāja piekļuvi noteiktiem digitāliem resursiem.
- Organizācijas kontu direktorijs vienuviet satur Lietotāju, gala iekārtu un noteiktu veidu piekļuves tiesību informāciju. Var būt daļa no vienreizējās pieteikšanās sistēmas.
- Datu apstrādes mākonis nodrošina skaitļošanas, datu glabāšanas un apstrādes vidi IS darbināšanai, tas nodrošina daudznomnieku režīmu, mērogojamību un savstarpēji nodalītas drošības zonas jeb segmentus. Tipiski ir izvietots uz IKT resursiem datu centrā.
- Datu apstrādes mākoņa informācijas sistēmu un datu centra IKT resursu pieejamības uzraudzību un dublēšanu nodrošina monitoringa sistēma un datu rezerves kopijas.
- Kiberdrošības pārvaldības būtiskie ir Sertifikātu izsniegšanas autoritāte un Kiberdrošības pārvaldības rīki (SIEM, SOC, DDoS u.c.). Kiberdrošības pārvaldība ir organizatoriski neatkarīga un to veic speciāli pilnvaroti, kvalificēti darbinieki.
- Datu vēstniecība ir svarīgāko IS pilnai atkopei ārpus Latvijas valsts teritorijas nepieciešamo resursu kopums.
- Datu centru, IKT un tīklu infrastruktūras atbalsta dienests ir kvalificēti darbinieki, kas nodrošina datu centru un IKT infrastruktūras dzīves ciklu un pieejamību.
- Lietotājiem izņemot specifiskas lomas tiek nodrošināta droša darba vide neatkarīgi no atrašanās darba vietas, ja ir pieejams interneta pieslēgums, to nodrošina VPN, ugunsmūris un drošie Lietotāju gala iekārtu sertifikāti.
- IS nodrošina institūcijas pamatdarbības funkcijas digitālajā vidē. IS var būt papildus drošības mehānismi piekļuves tiesību definēšanai.
- Mākoņdatošanas platformas un IS pārziņi ir par attiecīgi IS un mākoņdatošanas platformu dzīvesciklu, nodrošinājumu un attīstību. Pārziņi regulāri sadarbojoties ar kiberdrošības pārvaldniekiem analizē risku izvērtējumu un plāno pasākumus kiberdrošības uzlabošanai.

Jomā esošo informācijas resursu katalogs ir skatāms 8.tabulā, kurā apkopotas informācijas resursu izmaiņu apraksts.

8. tabula. Paredzamās izmaiņas jomas informācijas resursos

Nr.	Informācijas resurss	Statuss	Izmaiņu apraksts un pamatojums
1.	Centralizēts tīkla operatoru telekomunikāciju pakalpojumu un	Plānots, uzlabots, jauns.	Reģistrs būs centralizēta datubāze, kas integrē informāciju no dažādām valsts iestādēm un operatoriem, nodrošinot vienotu skatījumu un piekļuvi šiem datiem valsts pārvaldes vajadzībām. Reģistrā tiks apkopota informācija par

Nr.	Informācijas resurss	Statuss	Izmaiņu apraksts un pamatojums
	kvalitatīvo parametru reģistrs.		publiskā tīkla operatoriem (ISP (Interneta pakalpojumu sniedzēji) un citiem elektronisko sakaru pakalpojumu sniedzējiem) kā arī tīkla kvalitātes parametriem, piemēram, interneta ātrumu, latentumu (aizturi), pieejamību, tīkla veiktspēju un citus rādītājus, kas nodrošina pakalpojumu valsts iestādēm. Reģistrs būs būtisks instruments, lai identificētu vājās vietas publiskajā tīklā, nodrošinot datu pārredzamību un ātrāku reaģēšanu uz incidentiem.
2.	Centralizēts lietotāju gala iekārtu reģistrs (Darba vieta).	Plānots, jauns.	Centralizētā lietotāju gala iekārtu reģistrs, kurā tiktu reģistrētas visas valsts pārvaldes darbinieku lietotās gala iekārtas, piemēram: galda datori, portatīvie datori, mobīlās ierīces (viedtālruņi, planšetdatori), papildierīces (printeri, skeneri utt.) un programmatūras licences, kas piešķirtas konkrētajām ierīcēm. Reģistrs nodrošinās vienotu pārskatu par valsts pārvaldes gala iekārtām, to lietotāju piesaisti, ierīču konfigurāciju un atbilstību drošības prasībām.
3.	Centralizēts atbalsta personāla un ārpakalpojuma sniedzēju reģistrs (Lietotāju atbalsta dienests).	Plānots, jauns.	Reģistrs nodrošinās pilnu pārskatu par visu personālu un ārpakalpojumu sniedzējiem, kas iesaistīti lietotāju atbalsta dienestu darbībā visā valsts pārvaldē. Nodrošinās precīzu pārskatu par iesaistītajiem darbiniekiem un ārpakalpojumu sniedzējiem, kas ļaus optimizēt atbalsta darbību un plānot personāla resursu vajadzības. Reģistrā pieejamā informācija par personāla lomām un piekļuves līmeņiem ļaus ātrāk un precīzāk identificēt problēmu risināšanas atbildīgos un uzlabot incidentu vadību. Kiberdrošības likums un datu aizsardzības prasības pieprasa, lai ārpakalpojuma sniedzēju piekļuves un darbības būtu dokumentētas un kontrolētas. Centralizēts reģistrs palīdzēs nodrošināt šo prasību ievērošanu.
4.	Centralizēts koplietošanas resursu un IS reģistrs (VIRSIS), (Koplietošanas resursi un IS).	Esošs, Uzlabots.	Sistēmā VIRSIS jau ir izveidota iespēja iestādēm reģistrēt IS un koplietošanas resursus. Pašlaik ir izveidotas maz saiknes starp IS un tās nodrošināšanai nepieciešamajiem koplietošanas resursiem. Centralizētais reģistrs ieviesīs standartizāciju un caurspīdīgumu veidojot vienotu pieeju IS un koplietošanas resursu dokumentēšanai un pārvaldībai.
5.	Centralizēts lietotāju kontu reģistrs (Lietotāja konts).	Plānots, jauns, uzlabots.	Pašreiz valsts pārvaldes iestāžu lietotāju konti tiek pārvaldīti decentralizēti. Vienots centralizēts lietotāju kontu reģistrs veidos vienotu pieeju lietotāju pārvaldībā, drošības standartos un pieejas kontroles politikā. Centralizēts lietotāju kontu reģistrs nodrošinās lietotāju kontu datu glabāšanu vienā platformā, reģistrā, līdz ar to nodrošinot vienotu konta pieeju (SSO – Single Sign-On) visām valsts pārvaldes IS un resursiem, automatizētu piekļuves tiesību pārvaldību un personas datu aizsardzību atbilstoši GDPR prasībām. Centralizēts reģistrs atvieglos IT personāla darbu un samazinās izmaksas, kas saistītas ar decentralizētu reģistru un sistēmu uzturēšanu un pārvaldību.

Nr.	Informācijas resurss	Statuss	Izmaiņu apraksts un pamatojums
6.	Koda repozitoriju reģistrs (DevOps).	Plānots, jauns, uzlabots.	Centralizēts kodu repozitoriju reģistrs, kas ļaus pārvaldīt visas valsts pārvaldes ietvaros izstrādātos un uzturētos programmatūras projektus. Veicinās koda atkārtotu izmantojamību, samazinot izstrādes laiku un izmaksas līdzīgu risinājumu izveidē. Centralizēts reģistrs nodrošinās efektīvāku DevOps procesu pārvaldību t.sk. CI/CD vienuviet. Centralizēts koda repozitorijs ļaus iestādēm un izstrādātājiem sekot līdzi visiem izmantotajiem repozitorijiem, to versijām un izmaiņām.
7.	Sertifikātu izsniegšanas autoritāšu reģistrs (Sertifikātu izsniegšanas autoritāte).	Plānots, jauns, uzlabots.	Centralizēts sertifikātu izsniegšanas autoritāšu reģistrs, kurā būtu apkopota informācija par visiem valsts pārvaldē izmantotajiem sertifikātiem un sertifikātu izsniegšanas procesiem. Reģistrs kalpotu kā vienots kontroles un pārvaldības mehānisms, veicinot sertifikātu izsekojamību un pārvaldību, nodrošinot standartizētu un drošu sertifikātu izsniegšanu, uzturēšanu un anulēšanu. Reģistrs palīdzēs izsekot sertifikātu dzīves ciklam un nodrošināt to atjaunošanu vai anulēšanu savlaicīgi.
8.	Mākoņpakalpojumu sniedzēju reģistrs (Datu apstrādes mākonis).	Jauns, plānots.	Reģistrs sniegs pārskatu par izmantojamajiem mākoņpakalpojumiem, to sniedzējiem, to sertifikācijām, drošības atbilstības līmeņiem un piegādes nosacījumiem. Reģistra uzturēšanu un aktualitāti nodrošinās mākoņpakalpojumu brokeris. Centralizēts reģistrs, ar brokera palīdzību, palīdzēs valsts iestādēm izvēlēties sev piemērotāko un atbilstošāko mākoņpakalpojumu sniedzēju. Reģistrs arī veicinās vienotu pieeju pakalpojumu iepirkšanai un uzturēšanai.
9.	Centralizēts iepirkumu un līgumu reģistrs.	Plānots, jauns.	Centralizēts iepirkumu un līgumu reģistrs, kurā būs pieejama detalizēta informācija par iepirkumiem, piegādātājiem, līgumu noslēgšanu, nosacījumiem, termiņiem, izmaksām un izpildes statusiem. Atvieglos uzraudzību un novērsīs nelietderīgu resursu izmantošanu un iespējamu dublēšanos. Reģistrs būtiski uzlabos valsts iepirkumu un līgumu pārvaldību, nodrošinot augstāku caurspīdību, atbilstību un efektivitāti.
10.	Centralizēts monitoringu rīku reģistrs (Monitorings un datu rezerves kopijas).	Jauns, plānots.	Centralizēts reģistrs nodrošinās vienotu un detalizētu informāciju par izmantotajiem monitoringa rīkiem, to funkcionalitāti, integrācijas iespējām un pielietojumu. Samazinās izmaksas, optimizējot rīku izmantošanu un izvairoties no dublēšanās. Reģistrs veicinās rīku atbilstību kiberdrošības prasībām.
11.	Datu vēstniecību reģistrs (Datu vēstniecības).	Jauns, plānots.	Izveidot centralizētu datu vēstniecības reģistru, kas apkopo informāciju par visām valsts pārvaldes izmantotajām datu vēstniecībām un to tehniskajām specifikācijām. Datu vēstniecības reģistrā iekļauj arī uzskaiti par līgumiem, izmaksām, drošības sertifikātiem un tehniskajiem standartiem. Reģistrs uzlabos valsts spēju sagatavoties ārkārtas situācijām, nodrošinot pārskatu par drošām un pieejamām datu glabāšanas vietām. Šim reģistram ir jābūt klasificētam.

Nr.	Informācijas resurss	Statuss	Izmaiņu apraksts un pamatojums
12.	Datu centru un tīklu infrastruktūras atbalsta dienestu reģistrs (Datu centru un tīklu infrastruktūras atbalsta dienests).	Jauns, plānots, uzlabots.	Visu datu centru un tīklu infrastruktūras atbalsta dienestu reģistrs apkopos informāciju par visiem atbalsta dienestiem, to personāla kompetencēm un atbildībām, izmantotajiem tehniskajiem risinājumiem un procedūrām, ārpakalpojumu sniedzējiem un līguma detaļām, incidentu un darbības uzraudzības statistiku. Centralizētais reģistrs nodrošinās iespēju iegūt vienotu un aktuālu informāciju par datu centru un tīklu infrastruktūras atbalsta dienestiem visās valsts pārvaldes iestādēs. Reģistrs nodrošinās labāku resursu plānošanu un atbalsta personāla kompetenču izmantošanu. Reģistra ieviešana sekmēs efektīvu valsts pārvaldes infrastruktūras vadību, uzlabos drošību un savstarpējo sadarbību, vienlaikus nodrošinot ilgtspējīgu atbalsta dienestu darbību.
13.	Mākoņdatošanas platformas pārziņu un atbildīgo personu reģistrs (Mākoņdatošanas platformas pārzinis).	Plānots, jauns.	Reģistrs apkopos informāciju par pārziņu sniegtajiem mākoņdatošanas pakalpojumiem un to konfigurācijām, un informāciju par atbildīgajām personām t.sk. mākoņdatošanas platformu administratoriem, pārvaldniekiem un citām atbildīgajām personām, papildus norādot to kompetences, atbildības jomas, piekļuves līmeņus un lomas platformu pārvaldībā. Reģistra ieviešana palīdzēs identificēt piekļuves pārvaldības nepilnības, paaugstināt kiberdrošības prasību izpildi un sekmēs platformu pārvaldības pārskatāmību.
14.	IS pārziņu un atbildīgo personu reģistrs (IS pārzinis).	Esoša (VIRSIS), uzlabota.	Centralizēts reģistrs nodrošinās vienotu pārskatu par valsts pārvaldes IS un atbildīgajām personām, ļaujot efektīvāk organizēt sadarbību un resursu izmantošanu. Reģistrs par visām valsts pārvaldē esošajām IS, to pārziņiem un atbildīgajām personām (vārds, amats un kontaktinformācija. Reģistrs iekļaus informāciju par konkrēto sistēmu, pārzini un atbildīgo personu kompetencēm un lomām (piemēram, sistēmu administratori, drošības eksperti utt.).

3.4 Tehniskais skats

Pārskata periodā ir paredzamas vairākas būtiskas izmaiņas jomas informācijas sistēmās, kas saistītas ar funkciju un pakalpojumu Centralizāciju, efektivitātes un kiberdrošības uzlabošanu.

3.4.1 Informācijas sistēmas

Jomas esošo informācijas sistēmu katalogs ir skatāms 9.tabulā, kurā apkopots informācijas sistēmu izmaiņu apraksts.

9. tabula. Paredzamās izmaiņas jomas informācijas sistēmās

Nr.	Informācijas sistēma	Statuss	Izmaiņu apraksts un pamatojums
1.	Centralizēts Monitoringa risinājums (datu pārraides tīklu un datu centru	Jauna informācijas sistēma, Funkcion	Centralizēta monitoringa sistēma, kas aptver visu valsts pārvaldes datu pārraides tīklu un datu centru infrastruktūru, sadarbojas un integrējas ar esošajām Datu centru un datu pārraides tīklu monitoringa sistēmām. Sistēma nodrošina vienotu pieeju pārraudzībai, drošības analīzei un reakcijai uz incidentiem. Visi

Nr.	Informācijas sistēma	Statuss	Izmaiņu apraksts un pamatojums
	infrastruktūras).	alitātes pārdale un attīstība.	datu pārraides tīklu un datu centru monitoringa procesi tiek pārvaldīti vienā sistēmā, nodrošinot konsekvenci un savstarpēju savietojamību. Monitoringa dati tiek apkopoti, analizēti un interpretēti centralizēti, kas ļauj identificēt plašākus apdraudējumus un izmaiņu tendences.
2.	Centralizēts Aktīvās Direktorijas (AD) risinājums.	Jauna informācij as sistēma, Funkcion alitātes pārdale un attīstība.	Pāreja no decentralizētas AD pārvaldības uz Centralizētu. Risinājums paredz vienotas infrastruktūras ieviešanu visā valsts pārvaldē. Šī pieeja nodrošina vienotu lietotāju autentifikāciju, autorizāciju un piekļuves pārvaldību. Visi valsts pārvaldes lietotāji tiek pārvaldīti Centralizētā sistēmā ar skaidri noteiktām lomām, politiku un piekļuves tiesībām. Centralizēta AD vide atvieglos kopīgu resursu izmantošanu un starpresoru komunikāciju. Centralizēšana samazinās aparatūras, programmatūras licenču un personāla uzturēšanas izmaksas. Centralizēts AD risinājums arī nodrošinās konsekventu un spēcīgu drošības politiku visos pārvaldes tīklos, kā arī ļaus efektīvāk izsekot un novērst kiberapdraudējumus.
3.	Centralizēts Palīdzības dienests (lietotāju apkalpošana, vienota palīdzības dienesta) risinājums (integrācijas ar lokālajām incidentu sistēmām).	Jauna informācij as sistēma, Funkcion alitātes pārdale un attīstība.	Pāreja uz centralizētu Palīdzības dienests risinājumu paredz vienotu palīdzības dienestu visai valsts pārvaldei, kas integrēts ar lokālajām incidentu pārvaldības sistēmām, lai nodrošinātu vienotu piekļuvi atbalsta resursiem un ātrāku problēmu risināšanu. Visi incidenti tiks apkopoti centralizētajā sistēmā, kas nodrošinās vienotu piekļuvi eskalācijas un risinājumu procesiem. Centralizēts Palīdzības dienests samazinās reakcijas laiku un uzlabos lietotāju apkalpošanas kvalitāti, kā arī tiks nodrošināts vienots servisa līmenis visiem valsts pārvaldes lietotājiem, neatkarīgi no iestādes. Risinājums paredzēts vienotajai, centralizētajai valsts Palīdzības dienesta funkcijai, kas savukārt samazinās funkciju dublēšanos, dublējošo sistēmu uzturēšanu, līdz ar to arī samazinot izmaksas.
4.	Datorvadība, *(remote desktop management)* Centralizēta datorsistēmu konfigurācijas un programmatūras pārvaldība.	Jauna informācij as sistēma, Funkcion alitātes pārdale un attīstība.	Pāreja uz Centralizētas sistēmas datoru konfigurācijas pārvaldību, kas integrējas ar Aktīvās direktorijas (AD) risinājumu. Centralizētā pieeja ļauj automatizēt programmatūras instalācijas, atjauninājumus un drošības ielāpus visā valsts pārvaldē. Datori būs konfigurēti pēc vienādiem drošības standartiem un atbilstības prasībām. Centralizēta pieeja uzlabo efektivitāti, ļaujot administratoriem ātrāk un vieglāk veikt uzdevumus, samazinot laiku un resursus, kas nepieciešami vairāku atsevišķu sistēmu pārvaldībai. Centralizēta datorsistēmu pārvaldība ļauj ātrāk ieviest drošības pasākumus un atjauninājumus, tādējādi samazinot kiberdrošības riskus.
5.	Visaptveroša tīklvadība.	Jauna informācij as sistēma, Funkcion alitātes pārdale un attīstība.	Centralizēta pieeja tīklu pārvaldībai, kas ļauj efektīvāk uzraudzīt un pārvaldīt tīkla resursus visā valsts pārvaldē. Incidentus var ātrāk atklāt un novērst, pateicoties vienotai uzraudzības un vadības platformai. Paredzēts, ka visaptveroša tīklvadībai tiks arī nodrošināta sasaiste ar lokālām monitoringa sistēmām. Visaptveroša tīklvadība ietvers monitoringu, analīzi, drošību un citas funkcijas, kas uzlabos tīkla infrastruktūras pārvaldību un efektivitāti.

Nr.	Informācijas sistēma	Statuss	Izmaiņu apraksts un pamatojums
6.	Centralizēta programmatūras izplatīšanas sistēma.	Jauna informācijas sistēma, Funkcionalitātes pārdale un attīstība.	Pāriešana uz Centralizētu programmatūras izplatīšanas sistēmu paaugstinās efektivitāti, drošību un resursu izmantošanas efektivitāti visā valsts pārvaldē. Samazinās izmaksas, efektīvi pārvaldot licences un uzturēšanas darbus. Programmatūras izplatīšanas process kļūst ātrāks, drošāks un vienkāršāks. Vienota kontrole nodrošina ātru reakciju uz drošības incidentiem un minimizē riskus. Centralizēta sistēma ļaus kontrolēt un standartizēt programmatūras instalācijas visās valsts pārvaldes iestādēs. Atjauninājumi tiks izplatīti automātiski un sinhronizēti, nodrošinot drošību un savlaicīgumu.
7.	Centralizēta attālinātās piekļuves sistēma darba vietām.	Jauna informācijas sistēma, Funkcionalitātes pārdale un attīstība	Centralizētā IT atbalsta personāla Centralizēta attālinātās piekļuves sistēma darba vietām atvieglos atbalsta sniegšanu darbiniekiem neatkarīgi no darbinieku iestādes. Sistēma samazinās IT administratīvos izdevumus (nebūs nepieciešams uzturēt paralēlos risinājumus) un ļaus ātrāk reaģēt uz tehniskām problēmām. Centralizēta attālinātās piekļuves sistēma darba vietām nodrošinās uzticamāku, efektīvāku un drošāku pieeju darba vietu pārvaldībai uzlabojot operatīvo spēju atbalstīt lietotājus neatkarīgi no darbinieku atrašanās vietas.
8.	Centralizētā DevOps platforma	Jauna informācijas sistēma, Funkcionalitātes pārdale un attīstība.	Izveidot Centralizēta DevOps risinājumu visai valsts pārvaldei ar vienotu platformu, kas nodrošina rīkus un procesus programmatūras izstrādei, testēšanai, ieviešanai un uzturēšanai. Platformā esošais vienots kodu repozitorijs, būs pieejams visām valsts iestādēm un programmatūru izstrādātājiem, kas paātrinās programmatūras izstrādes un piegādes procesus, samazinās izmaksas, tai skaitā novērsīs dubultā finansējuma gadījumus, kad pārmaksā par jau esošu kodu repozitorijā esošu kodu, risinājumu.
9.	SIEM/SOC platforma	Jauna informācijas sistēma, Funkcionalitātes pārdale un attīstība.	Tiks ieviesta Centralizēta SIEM/SOC platforma, kas apvienos visu valsts pārvaldes iestāžu drošības notikumu uzraudzību un reakciju vienotā sistēmā. Visi drošības notikumi tiks apkopoti vienotā SIEM/SOC platformā, kas ļaus veikt reāllaika analīzi un uzraudzību. Centralizētā platforma integrēs datus no dažādiem avotiem, piemēram, tīklu infrastruktūras, lietojumprogrammu, serveriem un gala iekārtām. Centralizētā platforma ļauj korelēt drošības notikumus visā valsts pārvaldē, ātrāk identificējot un novēršot potenciālos draudus. Automatizēti procesi samazina reaģēšanas laiku un palielina apdraudējumu pārvaldības precizitāti. Mazāk cilvēkresursu būs jāveltī atsevišķu risinājumu uzturēšanai un uzraudzībai.

3.4.2 Sistēmu sadarbība un integrācija

Iepriekšējā sadaļā aprakstītās IS tiks izstrādātas un darbinātas tā, lai nodrošinātu valsts pārvaldes IS efektīvu, drošu un savietojamu darbību, balstoties uz standartizētām tehnoloģijām, centralizētiem risinājumiem un integrācijas platformām. Plānotās izmaiņas sistēmās ļaus sasniegt augstāku sadarbspējas līmeni starp IS, vienlaikus uzlabojot drošību un darbības nepārtrauktību.

3.4.3 IKT infrastruktūra

IKT infrastruktūra nodrošina stabilu un drošu tehnoloģisko pamatu visām pārējām jomas arhitektūrām, gan

horizontālajām (Valsts digitālie pakalpojumi, Valsts datu apmaiņa un pārvaldība, Datu analīze utt.), gan vertikālajām (Finanses, nodokļi un muita, E-lieta, Kultūra utt.). Tā atbalsta digitālās transformācijas procesu, efektīvu resursu izmantošanu un augstu drošības līmeni.
Datu centri un mākoņdatošana nodrošina drošu datu un IS glabāšanu, augstu pieejamību un nepārtrauktību. Nodrošina, ka tiek izmantoti valsts datu apstrādes mākoņa pakalpojumi un komerciālie pakalpojumi, kas atbilst valsts kiberdrošības prasībām. Mākoņpakalpojumi ir elastīgi mērogojami un to pieejamība atbalsta dažādu nozaru sistēmas. Pakalpojumi nodrošina sistēmu darbības nepārtrauktību pat ārkārtas situācijās, it īpaši IS, kurām to nosaka normatīvie akti kiberdrošības jomā.
Datorizētās darba vietas un tīkli nodrošina standartizētu un drošu darba vidi valsts pārvaldes darbiniekiem, ietverot programmatūras komplektus, drošības pārvaldību un tehnisko atbalstu. Drošs un ātrgaitas tīkls starp iestādēm un datu centriem garantē savienojamību visos valsts līmeņos.
Tiks nodrošināta Programmatūras dzīves cikla, centralizēts DevOps risinājums, kas nodrošinās efektīvu programmatūras izstrādi, testēšanu un uzturēšanas pārvaldību. Vienots kodu repozitorijs nodrošinās atkārtotu kodu izmantošanu un savietojamību starp sistēmām. CI/CD metodoloģija ļaus ātri un droši ieviest izmaiņas dažādās nozarēs.
IKT infrastruktūra atbilst un saskan ar jomu arhitektūras kopējo Tehnisko principu Nr. TP4. Nodrošināt nepārtrauktu darbību:

- "IKT risinājumiem un infrastruktūrai ir jābūt izturīgiem, uzticamiem un spējīgi nodrošināt stabilu darbību pat traucējumu vai drošības incidentu gadījumā. Tas aptver monitoringu, atbilstību standartiem, darbinieku kompetences celšanu un proaktīvu risku pārvaldību, lai saglabātu un uzlabotu valsts IKT sistēmu nepārtrauktību un drošību."

4 Mērķarhitektūras ieviešanas ceļa karte

Mērķarhitektūras ieviešanai ir jāīsteno vairāki savstarpēji saistīti pasākumi. Pasākumu īstenošana ir saistīta ar citu domēnu izmaiņām un to veiksmīgai īstenošanai jāpārvalda izmaiņu riski.

a. Pasākumu plāns

Mērķarhitektūras ieviešanas projekti un aktivitātes uzskaitīti 10.tabulā. Projekti un aktivitātes ietver augsta līmeņa pasākumu kopumu, lai īstenotu izmaiņas jomas juridiskajā, organizācijas, semantiskajā un tehniskajā skatā.
Pasākumu kopums ir informatīvs un apkopo esošos konceptuālos attīstības virzienus, tā izpilde atbildīgajiem nav saistoša.

10. tabula. Mērķarhitektūras ieviešanas pasākumi

Nr.	Projekts / aktivitāte	Apraksts	Termiņš	Prioritāte	Priekšnosacījumi	Atbildīgais, dalībnieki
1. Datu centri un mākoņdatošana						
1.1.	**Mākoņa brokeris**					
1.1.1.	Brokera funkcijas un darbības nepieciešamās platformas izveide un ieviešana.	Brokera funkcijas un darbības nepieciešamās platformas izveide un ieviešana. Risinājuma ieviešana atbilstoši normatīvo aktu prasībām. Nepieciešamo normatīvo aktu izstrāde funkcijas nodrošināšanai.	31.12.2026	Augsta	Ir izveidots normatīvais regulējums, kas nosaka brokera funkcijas un pienākumus. Projekta pase par Mākoņa brokera izvedi.	VARAM, VDAA
1.2.	**Migrācija uz valsts mākoni**					
1.2.1.	Iestāžu migrācijas plānu izstrāde un saskaņošana.	Migrācijas plāni, kas satur informāciju par migrācijas laika plānu, IS migrācijas secību un izmaksām. Migrācijas plānus saskaņo ar mākoņdatošanas pakalpojumu pārziņiem un	31.12.2025	Vidēja	2021.gada Informatīvais ziņojums „Par valsts informācijas un komunikācijas tehnoloģiju resursu un kompetenču konsolidāciju”.	Ministrijas

Nr.	Projekts / aktivitāte	Apraksts	Termiņš	Prioritāte	Priekšnosacījumi	Atbildīgais, dalībnieki
		iesniedz VARAM.				
1.2.2.	Iestāžu migrēšana uz mākoņdatošanas pakalpojumiem.	Iestāžu IS migrēšanas process uz mākoņdatošanas pakalpojumu sniedzējiem.	31.12.2029	Augsta	Projekts Nr.2.1.	Ministrijas
1.2.3	IeM - KRASS migrācija un IeM - FPRIS nepārtrauktība/migrācija	Pabeigta KRASS un FPRIS migrācija	31.12.2027	Augsta	Migrācijas pamatojums un migrācijas plāns (Projekts Nr.2.1.).	IeM IC
1.3.	**Mākoņdatošanas platformu attīstība**					
1.3.1.	KM - LNB mākonis: Paaugstināts LNB datu centra infrastruktūras kapacitāti un uzlabot integrācijas iespējas Valsts federētajā mākonī.	Novecojošu IKT iekārtu aizvietošana ar jaunām iekārtām un integrācija valsts datu apstrādes mākoņa infrastruktūrā.	31.12.2029	Vidēja	ANM 2.1.2.2.i investīciju projekta: Latvijas nacionālais federētais mākonis, izpilde.	KM (LNB)
1.3.2.	SM - LVRTC mākonis: Paaugstināts LNB datu centra infrastruktūras kapacitāti un uzlabot integrācijas iespējas Valsts federētajā mākonī.	Novecojošu IKT iekārtu aizvietošana ar jaunām iekārtām un integrācija valsts datu apstrādes mākoņa infrastruktūrā.	31.12.2029	Vidēja	ANM 2.1.2.2.i investīciju projekta: Latvijas nacionālais federētais mākonis, izpilde.	SM (LVRTC)
1.3.3.	ZM - ZM mākonis: Paaugstināts LNB datu centra infrastruktūras kapacitāti un uzlabot integrācijas iespējas	Novecojošu IKT iekārtu aizvietošana ar jaunām iekārtām un integrācija valsts datu apstrādes mākoņa infrastruktūrā.	31.12.2029	Vidēja	ANM 2.1.2.2.i investīciju projekta: Latvijas nacionālais federētais mākonis, izpilde.	ZM (LDC, LAD)

Nr.	Projekts / aktivitāte	Apraksts	Termiņš	Prioritāte	Priekšnosacījumi	Atbildīgais, dalībnieki
	Valsts federētajā mākonī.					
1.3.4.	IeM – IeM IC mākonis: Paaugstināts LNB datu centra infrastruktūras kapacitāti un uzlabot integrācijas iespējas Valsts federētajā mākonī.	Novecojošu IKT iekārtu aizvietošana ar jaunām iekārtām un integrācija valsts datu apstrādes mākoņa infrastruktūrā.	31.12.2029	Vidēja	ANM 2.1.2.2.i investīciju projekta: Latvijas nacionālais federētais mākonis, izpilde.	IeM (IeM IC)
2. Datorizētās darba vietas un tīkli						
2.1.	**Datorizētā vide**					
2.1.1.	Centralizēta incidentu, problēmu un pakalpojumu pieteikumu sistēmas risinājuma izveide un procesa ieviešana.	Izveidota centralizēta incidentu, problēmu un pakalpojumu sistēma un process, kas nodrošina lietotāju incidentu un problēmu pārvaldību, lietotāju konsultēšanu, kontrolē lokālā lietotāju atbalsta darbu, IS lietotāju pārvaldību, lietotāju konsultēšana par kiberdrošības politikas ievērošanu, kā arī datu pārraides tīkla, datu centru un informācijas sistēmu pieejamības monitorings un citas funkcijas. Izveidots lietotāju gala iekārtu reģistrs.	31.12.2027	Augsta	Informatīvais ziņojums un Juridiskajā skatā minētie MK noteikumi par centralizētas datorizētās darba vietu un datu pārraides tīklu pārvaldība.	Noteiks MK noteikumi.
2.1.2.	Centralizētas tehnoloģiskā platformas izveide un ieviešana	Centralizētā platforma Centralizētas standartizētās darbavietas programmatūras	31.12.2027	Augsta	Informatīvais ziņojums un Juridiskajā skatā minētie MK noteikumi par centralizētas	Noteiks MK noteikumi.

Nr.	Projekts / aktivitāte	Apraksts	Termiņš	Prioritāte	Priekšnosacījumi	Atbildīgais, dalībnieki
	valsts pārvaldes darbinieku darbvirsmu apkalpošanai un darbības nodrošināšanai.	pārvaldībai (t.sk. mobīlo ierīču) apkalpošana un darbības nodrošināšana, kas papildus ietver programmatūras attālināta uzturēšanu (instalēšana, atjaunināšana utt.) un darba vietas standartizētu programmatūras komplektu. Izveidots vai pilnveidots programmatūru un to licenču reģistrs (VIRSIS).			datorizētās darba vietu un datu pārraides tīklu pārvaldība.	
2.1.3.	Centralizētas Aktīvās direktorijas *(Active Directory)* risinājuma izveide un lietotāju pārvaldības procesu ieviešana.	Centralizēts AD risinājums nodrošinās vienotu lietotāju autentifikāciju, autorizāciju un piekļuves pārvaldību. Valsts vienotā datorlietotāju autorizācijas un pieejas tiesību pārvaldības risinājuma izveide.	31.12.2027	Augsts	Informatīvais ziņojums un Juridiskajā skatā minētie MK noteikumi par centralizētas datorizētās darba vietu un datu pārraides tīklu pārvaldība.	Noteiks MK noteikumi.
2.1.4.	Vienots, drošs datu pārraides tīkls starp datorizētajām darba vietām un IS darbību nodrošinošajiem resursiem.	Valsts pārvaldē izveidots vienots datu pārraides tīkls starp iestādēm un datu centriem, kurā ietilpst tīkla vadība, tīkla darbības monitorings, tīkla parametru konfigurācijas, ugunsmūri un mobilās tīkla brigādes pakalpojums, kā arī citas funkcijas. Izveidots tīkla shēmu un tīkla iekārtu reģistrs.	31.12.2027	Augsta	Informatīvais ziņojums un Juridiskajā skatā minētie MK noteikumi par centralizētas datorizētās darba vietu un datu pārraides tīklu pārvaldība.	Noteiks MK noteikumi.
2.1.5.	Centralizēta attālināto lietotāju apkalpošana. Vienots palīdzības	Izveidots palīdzības dienests, lokālais lietotāju atbalsts un IKT infrastruktūras un IS sagādes	31.12.2027	Augsta	Informatīvais ziņojums un Juridiskajā skatā minētie MK noteikumi par centralizētas	Noteiks MK noteikumi.

Nr.	Projekts / aktivitāte	Apraksts	Termiņš	Prioritāte	Priekšnosacījumi	Atbildīgais, dalībnieki
	dienests.	funkcija, kas savu darbību īstenošanai izmanto IS vai platformas, kas minētas 2.1.1.-2.1.4 projektos.			datorizētās darba vietu un datu pārraides tīklu pārvaldība.	
3. Programmatūras dzīves cikla nodrošināšana						
3.1	**Koda repozitorijs**					
3.1.1.	Izveidota kodu repozitorija platforma.	Izveidota vienotu tehnoloģiskā platformu, kas apkopo valsts pārvaldē veidoto tehnoloģisko risinājumu programmatūras kodus no lokālajiem koda repozitorijiem. Koda repozitorijam var piekļūt visas valsts iestādes un izstrādātāji.	31.12.2027	Augsta	Informatīvais ziņojums un Juridiskajā skatā minētie MK noteikumi par programmatūras izstrāddarbināšanas nodrošināšanu.	Noteiks MK noteikumi.
3.1.2.	Izstrādes procesa organizēšana atbilstoši DevOps principiem tai skaitā vienotā koda repozitorija pārraudzība.	Izveidots vienots centralizēts koda repozitorijs ar CI/CD plūsmām, kas nodrošinātu valsts pārvaldē radītā programmatūras koda vienotu pārvaldību, nodrošinot automatizētu plūsmu, testu un drošības pārvaldību.	31.12.2027	Augsta	Informatīvais ziņojums un Juridiskajā skatā minētie MK noteikumi par programmatūras izstrāddarbināšanas nodrošināšanu.	Noteiks MK noteikumi.
4. Datu vēstniecība						
4.1.	**Datu vēstniecības izveide**					
4.1.1.	Valsts kritisko funkciju nodrošināšanai nepieciešamo reģistru, IS un datu identificēšana.	Iegūts saraksts ar valsts kritisko funkciju nodrošināšanai nepieciešamajiem reģistriem, IS un datiem, kurus nepieciešams darbināt datu vēstniecībā.	31.12.2025	Augsta	Juridiskajā skatā minētā Koncepcija un MK noteikumi par Datu vēstniecībā izmitināmajām IS.	Atbildīgo noteiks MK noteikumi.

Nr.	Projekts / aktivitāte	Apraksts	Termiņš	Prioritāte	Priekšnosacījumi	Atbildīgais, dalībnieki
4.1.2.	Datu vēstniecībai piemērota izmitināšanas vieta.	Izmitināšanas vietas noteikšana, lai tā atbilstu datu vēstniecības prasībām. Izmitināšanas līguma sagatavošana un slēgšana.	30.06.2026	Augsta	Juridiskajā skatā minētā Koncepcija un MK noteikumi par Datu vēstniecībā izmitināmajām IS. 4.1.1. projekta izpilde.	Atbildīgo noteiks MK noteikumi.
4.1.3.	Datu vēstniecības platformas un darbības process.	Izveidota platforma vēstniecībā izmitināmo IS darbināšanai, kas nodrošina nepārtrauktu darbību ārkārtas situācijās un atbilstību valsts kiberdrošības prasībām. Platforma integrēta ar valsts kopējo IKT infrastruktūru, nodrošinot datu un IS darbību saskaņotību. Izstrādāts un ieviests datu vēstniecības darbības process.	31.12.2026	Augsta	Juridiskajā skatā minētā Koncepcija un MK noteikumi par Datu vēstniecībā izmitināmajām IS. 4.1.1. un 4.1.2. projekta izpilde.	Atbildīgo noteiks MK noteikumi.
4.1.4.	Datu vēstniecības pārraudzības iestāde.	Datu vēstniecības pārraudzības iestāde nodrošinās datu vēstniecības darbību, nodrošinot tās efektīvu funkcionēšanu, drošību un atbilstību normatīvajiem aktiem. Koordinēs datu vēstniecībā izvietojamo IS migrāciju un uzturēšanu.	31.06.2026	Augsta	Juridiskajā skatā minētā Koncepcija un MK noteikumi par Datu vēstniecībā izmitināmajām IS.	Atbildīgo noteiks MK noteikumi.

a. Mijiedarbība ar citiem domēniem

Jomas mērķarhitektūras ieviešana ir saistīta ar visām jomu arhitektūrām (11.tabula). Kā galvenās komponentes, kas sniedz kopīgu pamatu digitālai transformācijai, uzlabotai pakalpojumu sniegšanai datu drošībai no jomas arhitektūras ir kopīgas un ietekmē arī citas jomu arhitektūras ir:

- **Datu centri un mākoņdatošana** ir nepieciešami visām jomu arhitektūrām un tie veicina centralizētu datu pārvaldību un koplietošanu šajās nozarēs, nodrošinot efektīvāku datu apmaiņu un sadarbību starp iestādēm.
- **Programmatūras dzīves cikla nodrošināšana** ir nepieciešama visām jomu arhitektūrām un tā nodrošina gan koplietojamus risinājumus, gan specializētus risinājumus, kas pielāgoti katrai jomai, ļaujot attīstīt specifiskus digitālos risinājumus.
- **Datorizētās darba vietas un tīkli** nodrošina piekļuvi centralizētiem risinājumiem un datu centriem, lai efektīvi nodrošinātu attiecīgās jomas funkcijas. Nodrošinās Centralizēts datorizētās darba vietas pakalpojums.

Zemāk tabulā norādīt visas jomu arhitektūras un to mijiedarbība ar IKT infrastruktūras un kiberdrošības jomas arhitektūru.

11. tabula. Mijiedarbība ar citiem domēniem

Nr.	Joma	Komponentes	Ietekme
1.	Valsts datu apmaiņa un pārvaldība (t.sk. bāzes reģistri, datu izplatīšana).	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Nodrošina efektīvu datu pārvaldību, apstrādi un izplatīšanu, uzlabojot valsts pārvaldes datu pieejamību, drošību un sadarbspēju. Centralizēti datu centri un mākoņpakalpojumi nodrošina vienotu datu uzglabāšanas vidi, kas padara datu pārvaldību un izplatīšanu efektīvāku un drošāku. Izvēloties atbilstošu programmatūru un optimizējot tās lietojumu, var uzlabot datu kvalitāti, pārskatāmību un pieejamību. Darba vietu un tīklu infrastruktūra nodrošina valsts pārvaldes darbiniekiem drošu un ātru piekļuvi datiem.
2.	Datu analīze.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Komponenti veicina ātru, drošu un efektīvu datu apstrādi un analīzi, atvieglojot liela apjoma datu analīzi un pieņemto lēmumu kvalitāti valsts pārvaldē. Tīkli un mākoņdatošana ļauj analītiķiem strādāt attālināti, vienlaikus piekļūstot reāllaika datiem un analīzes rīkiem. Pareiza programmatūras izvēle nodrošina, ka dažādas datu analīzes platformas var integrēties ar valsts IKT infrastruktūru. Mākoņplatformas nodrošina mērogojamas datu analīzes iespējas, īpaši liela apjoma datu kopu apstrādei.
3.	Valsts digitālie pakalpojumi (Pakalpojumu pārvaldība un sniegšana).	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Nodrošina stabilu un efektīvu tehnoloģisko pamatu, uz kura tiek balstīta valsts pārvaldes digitālo pakalpojumu sniegšana. Centralizētie datu centri un mākoņdatošana ļauj ātri apstrādāt un piegādāt pakalpojumus, jo dati un lietojumprogrammas tiek glabāti vienā vietā, padarot pakalpojumu sniegšanas procesu efektīvāku kā arī nodrošina nepārtrauktu pakalpojumu darbību un mērogajamību.

Nr.	Joma	Komponentes	Ietekme
			Nodrošinot datorizētas darba vietas un stabilu tīklu infrastruktūru, valsts pārvaldes darbinieki var sniegt pakalpojumus attālināti un efektīvi.
4.	Uzticamība un elektroniskā identifikācija.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Datu centri, mākoņdatošana, programmatūras dzīves cikla nodrošināšana un datorizētās darba vietas un tīkli ievērojami stiprina uzticamības un elektroniskās identifikācijas sistēmu drošību, pieejamību un efektivitāti. Datu centri un mākoņdatošana nodrošina drošu un nepārtrauktu eID pakalpojumu darbību un uzlabo eID pieejamību, kā arī nodrošina drošu identifikācijas datu glabāšanu. Centralizēts DevOps risinājums nodrošina, ka eID un uzticamības pakalpojumiem izmantotā programmatūra tiek izstrādāta un uzturēta atbilstoši DevOps standartiem un drošības prasībām. Drošs tīkls starp darba vietām un centrālajām eID sistēmām samazina risku piekļuves datu pārtveršanai vai sistēmas kompromitēšanai.
5.	Valsts pārvaldes modernizācija (t.sk.: valsts resursu pārvaldība, pārvaldes caurskatāmība un vēlēšanas, tiesiskā informācija u.c.).	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Nodrošina tehnoloģisko pamatu, kas atbalsta efektivitāti, inovācijas un ilgtspējību publiskajā sektorā. Modernizētās darba vietas un tīkli nodrošina valsts pārvaldes darbiniekiem iespēju drošā veidā strādāt gan attālināti, gan uz vietas un piekļūt sistēmām, to funkcijām un datu kopām atbilstoši no darba pienākumiem izrietošajām pilnvarām. Iegādājot un darbinot standartizētas programmatūras, valsts pārvalde var nodrošināt sistēmu savietojamību un vienotību starp dažādām valsts iestādēm, kas veicina labāku sadarbību un informācijas apmaiņu. Modernizācija ļauj efektīvāk izmantot pieejamos tehniskos resursus, samazinot liekus izdevumus un palielinot pakalpojumu kvalitāti.
6.	Mākslīgā Intelekta pielietojumi valsts pārvaldes produktivitātei.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Mākoņdatošana nodrošina nepieciešamo infrastruktūru lielu datu apjomu glabāšanai un apstrādei, horizontālu mērogojamību un procesēšanas jaudu, kas ir būtisks priekšnosacījums Mākslīgā Intelekta algoritmu apmācībai un pielietošanai. Modernizēta programmatūras ekosistēma, kas iekļauj Mākslīgā Intelekta rīkus un algoritmus, ļauj valsts pārvaldei uzlabot produktivitāti, automatizējot atkārtojamus uzdevumus. Mākslīgā Intelekta pielietojums tīklu un datu drošības pārvaldībā ļauj ātri identificēt anomālijas, potenciālos uzbrukumus un citus drošības incidentus.
7.	Kultūra.	Datu centri un mākoņdatošana, Programmatūras	Nodrošina efektīvu tehnoloģiju izmantošanu kultūras attīstībai, izplatīšanai, pieejamībai un vēsturiskā kultūras mantojuma digitalizācijai.

Nr.	Joma	Komponentes	Ietekme
		dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Nodrošina datu, programmatūras uzglabāšanu, uzturēšanu, piekļuvi un kiberdrošību. Modernizētās darba vietas un droši tīkli ļauj darbiniekiem strādāt efektīvāk, sadarbojoties attālināti un ātri piekļūstot vajadzīgajiem resursiem. Ietekmē kultūras digitalizāciju veicinot kultūras satura saglabāšanu un atvēršanu sabiedrībai.
8.	Izglītība un zinātne.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Centralizēti IKT risinājumi samazina izmaksas un resursu dublēšanos, nodrošinot lielāku piekļuvi izglītības un zinātnes resursiem. IKT infrastruktūra stiprina datu un programmatūras drošību ļaujot efektīvi aizsargāt sensitīvus izglītības un zinātnes datus. Mākoņdatošanas un centralizēto DevOps risinājumu pieejamība veicina zinātniskās inovācijas un jaunu risinājumu izstrādi īsākā laikā. Datorizētās darba vietas un droši tīkli ļauj nozares darbiniekiem strādāt efektīvāk, sadarbojoties attālināti un ātri piekļūstot vajadzīgajiem resursiem.
9.	Labklājība.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Centralizētās un drošās IKT infrastruktūras izmantošana uzlabo labklājības pakalpojumu pieejamību un ļauj ātri reaģēt uz iedzīvotāju vajadzībām. Centralizēts DevOps un kodu repozitorijs, samazina nozares IS izstrādes un uzturēšanas izmaksas, vienlaikus paaugstinot efektivitāti. Datu centri un mākoņdatošanas risinājumi nodrošina augstu sensitīvu datu aizsardzības līmeni, kas ir kritiski sociālās aizsardzības datu apstrādei. Datorizētās darba vietas un tīkli nodrošina nozares darbiniekiem drošas un uzticamas darba vietas ar piekļuvi nepieciešamajiem IT resursiem neatkarīgi no atrašanās vietas, kā arī vienoti tīkli nodrošina savienojamību starp valsts iestādēm, tādejādi uzlabojot pakalpojumu sniegšanas ātrumu un kvalitāti.
10.	Veselība.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Datu centri un mākoņdatošana nodrošina Veselības jomas IS darbību un pieejamību, pacientu un jomas datu drošu glabāšanu. Mākoņdatošana ļauj nodrošināt reāllaika piekļuvi datiem un IS veselības aprūpes speciālistiem neatkarīgi no atrašanās vietas. Centralizēts DevOps risinājums un vienots kodu repozitorijs nodrošina efektīvu medicīniskās programmatūras un attālināto monitoringa rīku, izstrādi, testēšanu, drošību un uzturēšanu. Vienota un droša tīkla infrastruktūra nodrošina ātru datu pārraidi starp valsts iestādēm.

Nr.	Joma	Komponentes	Ietekme
11.	Finanses, nodokļi un muita.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Komponetes būtiski uzlabo finanšu, nodokļu un muitas pakalpojumu kvalitāti, drošību un efektivitāti, stiprinot valsts spējas pārvaldīt savus finanšu resursus un nodrošināt likumu ievērošanu. Centralizēts DevOps un vienots kodu repozitorijs samazina nozares IS izstrādes un uzturēšanas izmaksas, vienlaikus paaugstinot efektivitāti un drošību tādejādi veicina inovāciju ieviešanu, piemēram, mākslīgā intelekta pielietošanu nodokļu analīzē vai riska pārvaldībā muitas procesos. Centralizēti pārvaldītas datorizētās darba vietas nodrošina drošu piekļuvi sensitīviem finanšu un muitas datiem neatkarīgi no darbinieka atrašanās vietas. Vienota un droša tīkla infrastruktūra nodrošina ātru datu pārraidi starp valsts iestādēm.
12.	Transports.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Komponenšu kopīgā ietekme sekmē transporta sistēmu digitalizāciju un inovācijas, uzlabojot transporta pārvaldību, lietotāju pieredzi un valsts transporta infrastruktūras efektivitāti. Datu centri un mākoņdatošana nodrošina drošu Transporta datu glabāšanu un elastīgus, mērogojamus resursus, kas nepieciešami, lai apstrādātu liela apjoma transporta datus, piemēram, no satiksmes monitoringa sistēmām. Centralizēts DevOps risinājums atvieglo transporta pārvaldības sistēmu izstrādi, uzturēšanu un uzlabošanu. Datorizētās darba vietas nodrošina transporta nozares darbiniekiem piekļuvi informācijas sistēmām neatkarīgi no atrašanās vietas. Drošs tīkla savienojums starp dažādām jomas iestādēm un sistēmām uzlabo datu plūsmas efektivitāti un drošību.
13.	E-lieta.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Komponenšu IKT infrastruktūras un procesu kopums būtiski uzlabo E-lietas sistēmas uzticamību, efektivitāti un ilgtspēju, veicinot digitālās transformācijas īstenošanu juridiskajā nozarē. Datu centri un mākoņdatošana nodrošina drošu un nepārtrauktu E-lietas sistēmas darbību, uzlabojot tiesvedības un juridisko pakalpojumu pieejamību. Centralizēts DevOps risinājums ļauj ātri izstrādāt, testēt un ieviest E-lietas programmatūras risinājumus, kā arī vienotais kodu repozitorijs nodrošinās risinājumu versiju pārvaldību un koda atkārtotu izmantojamību. Datorizētās darba vietas nodrošinās juridiskajiem speciālistiem drošu un ērtu piekļuvi E-lietas sistēmām un datiem neatkarīgi no atrašanās vietas.
14.	Būvniecība.	Datu centri un mākoņdatošana, Programmatūras	Komponentes uzlabo būvniecības jomas tehnoloģiju, procesu, pakalpojumu, drošību, pārvaldību un efektivitāti. Datu centri un

Nr.	Joma	Komponentes	Ietekme
		dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	mākoņdatošana nodrošina drošu jomas datu glabāšanu un IS darbību. Centralizēts DevOps risinājums nodrošina efektīvu informācijas sistēmu, piemēram, BIS (Būvniecības informācijas sistēma), projektēšanas rīku un pārvaldības platformu izstrādi, testēšanu un uzturēšanu. Datorizētās darba vietas un tīkli nodrošinās jomas darbiniekiem drošu piekļuvi būvniecības IS un dokumentācijai neatkarīgi no atrašanās vietas.
15.	Vide un reģioni.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Komponentes veicina efektivitāti, ilgtspēju un drošību uzlabojot datu glabāšanu, to pārvaldību un analīzi. Datu centri un mākoņpakalpojumi nodrošina drošu IS darbību, vienotu pieeju vides un reģionālajiem datiem, uzlabojot to izmantojamību un atvieglojot sadarbību starp iesaistītajām pusēm. Centralizēts DevOps risinājums nodrošina efektīvu sistēmu izstrādi un uzturēšanu. Automatizētās testēšanas un drošības pārbaudes garantē šo sistēmu uzticamību un drošību. Vienots kodu repozitorijs veicina koda atkārtotu izmantošanu, ļaujot ieviest inovatīvus risinājumus, piemēram, mākslīgā intelekta izmantošanu vides datu analīzē. Datorizētās darba vietas nodrošina piekļuvi sistēmām, datiem un ļauj jomas darbiniekiem efektīvi strādāt neatkarīgi no atrašanās vietas. Vienots un drošs tīkls nodrošina efektīvu komunikāciju un datu apmaiņu starp DC, dažādām jomas iestādēm un veicina reāllaika datu pārraidi no vides sensoriem un citām vides monitoringa sistēmām.
16.	Zemkopība.	Datu centri un mākoņdatošana, Programmatūras dzīves cikla nodrošināšana, Datorizētās darba vietas un tīkli.	Komponenšu kopīgā ietekme būtiski uzlabo zemkopības jomas pārvaldību, veicina ilgtspējīgu resursu izmantošanu un sekmē nozares digitālo transformāciju. Datu centri un mākoņdatošana nodrošina drošu IS darbību, jomas datu uzglabāšanu un sniedz piekļuvi šiem datiem reāllaikā, uzlabojot resursu pārvaldību un lēmumu pieņemšanas procesus. Centralizēts DevOps risinājums nodrošina Zemkopības jomas IS izstrādi, testēšanu un uzturēšanu. Automatizētās drošības pārbaudes un testēšanas metodes garantē šo sistēmu drošību un uzticamību. Vienots kodu repozitorijs ļauj veicināt koda atkārtotu izmantošanu un jaunu risinājumu ātrāku izstrādi, un CI/CD metodes paātrina jaunu funkcionalitāšu ieviešanu. Datorizētās darba vietas un tīkli nodrošina zemkopības jomas darbiniekiem piekļuvi būtiskajām sistēmām neatkarīgi no to atrašanās vietas. Vienots tīkls nodrošina ātru un drošu datu apmaiņu starp dažādām zemkopības

Nr.	Joma	Komponentes	Ietekme
			nozares iestādēm.

b. Riski

Jomas arhitektūras ieviešanā ir jāņem vērā vairāki riski (12.tabula). Tabulā sniegts izvērtējums par potenciāliem iekšējiem un ārējiem riskiem, ar kuriem ir jārēķinās nākotnes mērķarhitektūras izstrādē, kā arī darbībām, kuras ir veicamas attiecīgo risku pārvaldībai.
Risku matrica tiks periodiski atjaunota.

12. tabula. Mērķarhitektūras ieviešanas riski

Nr.	Risks	Ietekme	Iespējamība	Mazināšanas pasākumi	Īpašnieks
1.	Normatīvo aktu izmaiņu aizkavēšanās laikietilpīgās izstrādes un saskaņošanas dēļ.	Augsta	Vidēja	Izvirzīt normatīvo aktu izmaiņas kā mērķarhitektūras ieviešanas prioritāti. Veikt rūpīgu situācijas analīzi un plānot normatīvo aktu izmaiņu nepieciešamību jau projekta sākumposmā. Izstrādāt prioritāšu sarakstu normatīvajiem aktiem, lai koncentrētos uz būtiskākajām izmaiņām. Laikus konsultēties ar atbildīgajām iestādēm (ministrijām, aģentūrām) un identificēt potenciālos šķēršļus normatīvo aktu izstrādei. Ja nepieciešams, tad izveidot starpinstitūciju darba grupas, lai nodrošinātu efektīvāku saskaņošanu un vienotu pieeju normatīvo aktu izstrādē. Piesaistīt augstāka vadības līmeņa atbalstu.	VARAM, VDAA, Sadarbībā ar visām citām iestādēm.
2.	Nepietiekams finansējums attīstības aktivitāšu ieviešanai un īstenošanai.	Augsta	Vidēja	Izvērtēt attīstības aktivitātes un prioritizēt tās, kas sniedz vislielāko ieguldījumu drošības, efektivitātes un darbības nepārtrauktības uzlabošanā. Veikt izmaksu optimizāciju izmantojot Centralizētus un standartizētus risinājumus. Izstrādāt ilgtermiņa budžetu IKT infrastruktūras un kiberdrošības attīstībai, lai iepriekš sagatavotos nepieciešamajam finansējumam. Prezentēt aktivitāšu izmaksas un sagaidāmos ieguvumus, lai pārliecinātu lēmumu pieņēmējus par projekta vērtību un finansējuma nepieciešamību.	VARAM, VDAA, Sadarbībā ar visām citām iestādēm.
3.	Nepietiekama personāla kapacitāte,	Vidēja	Vidēja	Personāla apmācības un kvalifikācijas celšana, kas aptver jauno funkciju un risinājumu	VARAM, VDAA, Sadarbībā

Nr.	Risks	Ietekme	Iespējamība	Mazināšanas pasākumi	Īpašnieks
	prasmes, kvalifikācija un zināšanas jauno funkciju un risinājumu efektīvai lietošanai.			tehniskos un praktiskos aspektus. Nodrošināt personālam pieeju starptautiski atzītiem sertifikācijas kursiem. Veicināt jaunu IKT profesionāļu piesaisti, nodrošinot konkurētspējīgu atalgojumu un karjeras izaugsmes iespējas valsts sektorā. Sadarboties ar augstskolām un profesionālās izglītības iestādēm, lai veidotu mācību programmas, kas sagatavo speciālistus ar nepieciešamajām zināšanām un prasmēm. Īstermiņā piesaistīt ekspertus no privātā sektora, vienlaikus nodrošinot zināšanu pārnesi uz valsts sektora darbiniekiem. Iestādēs ieviest zināšanu datu bāzes un mentoru programmas. Plānot darba slodzes tā, lai darbiniekiem būtu laiks apgūt jaunas prasmes un risinājumus. Regulāri izvērtēt darbinieku prasmju attīstības progresu un nepieciešamību pēc papildu apmācībām.	ar visām citām iestādēm.
4.	Tehnoloģiskie riski un risinājumu savstarpējā saderība.	Vidēja	Vidēja	Izstrādāt un ieviest vienotu tehnisko standartu kopumu visām jaunajām tehnoloģijām un risinājumiem, lai nodrošinātu savstarpēju saderību. Izmantot atvērtos standartus un protokolus (piemēram, REST API, SAML, OpenID), lai nodrošinātu sistēmu savietojamību neatkarīgi no piegādātāja. Izvēlēties risinājumus, kas ir viegli pielāgojami un spēj apmierināt pieaugošas IKT infrastruktūras, lietotāju un datu plūsmas prasības nākotnē. Regulāri novērtēt tehnoloģiskos riskus un savietojamības problēmas, izstrādājot plānus to novēršanai.	VARAM, VDAA, Sadarbībā ar visām citām iestādēm.
5.	Drošības riski (kiberdrošības uzbrukumi).	Augsts	Augsta	Izstrādāt un ieviest vienotas drošības vadlīnijas, normatīvos noteikumus un prasības, kuras piemēro visām valsts pārvaldes iestādēm un sistēmām. Nodrošināt izstrādāto kiberdrošības jomas normatīvo aktu ievērošanu. Centralizēt drošības notikumu uzraudzību un reaģēšanu, izmantojot SIEM/SOC platformu, lai savlaicīgi atklātu un novērstu	VARAM, VDAA, Sadarbībā ar visām citām iestādēm.

Nr.	Risks	Ietekme	Iespējamība	Mazināšanas pasākumi	Īpašnieks
				apdraudējumus. Ieviest divu vai vairāku faktoru autentifikāciju visās kritiskajās sistēmās, lai samazinātu piekļuves uzlaušanas risku. Nodrošināt, ka visi sensitīvie dati gan tranzītā (in transit), gan atpūtā (at rest) tiek šifrēti. Nodrošināt regulāras apmācības darbiniekiem par kiberdrošības pamatiem, tostarp par paroļu pārvaldību, pikšķerēšanas uzbrukumiem un drošības procedūrām. Izveidot rezerves infrastruktūru (piemēram, Datu vēstniecību/as), kas nodrošina kritisko funkciju darbības nepārtrauktību kiberuzbrukumu gadījumā.	
6.	Konvencionālas karadarbības Latvijas teritorijā risks.	Augsta	Zema	IS un kiberdrošības normatīvo aktu prasību savlaicīga un konsekventa izpilde, Datu vēstniecību izveide. Federatīvas, aizvietojošas un dublējošas arhitektūras izveidi, konsolidējot šobrīd vājāk aizsargātās sistēmas vienotajā datu apstrādes mākonī.	VARAM, VDAA, Sadarbībā ar visām citām iestādēm.