Valstybės hibridinės debesijos modelis

2024-05-17

Turinys

Versijavimas

Versija	Data (įsigalioja)	Pakeitimo aprašymas	Rengėjas
1.0	2024-05-17	Naujas dokumentas	Informacinės visuomenės plėtros komiteto direktorius Tomas Misevičius

Dokumento suderinimo istorija

Data	Aprašymas	Rengėjas
2024-05-09	Lietuvos Respublikos ekonomikos ir inovacijų ministerija 2024-05-09 raštu Nr. 3-1640 (2024-05-09 reg.G-402(2024)), atsakydami į Informacinės visuomenės plėtros komiteto (toliau – IVPK) 2024-05-03 raštą Nr. S-153(2024), pritarė parengtam Valstybės hibridinės debesijos modeliui.	Lietuvos Respublikos ekonomikos ir inovacijų ministerija

1. Dokumento paskirtis

Šio dokumento paskirtis – aprašyti valstybės hibridinės debesijos modelį, kaip valstybės debesijos platformos vystymo kryptį bei pagrindinius reikalavimus modelio realizacijai, sudarant sąlygas naudoti viešosios debesijos paslaugas valstybės informacinių išteklių plėtrai, rezervinėms kopijoms bei valstybės informacinių sistemų ir registrų nepertraukiamos veiklos užtikrinimui arba veiklos tęstinumo užtikrinimui.

Suderinus valstybės hibridinės debesijos modelį su EIM bei patvirtinus IVPK vidiniu tvirtinimu:

- Bus sukurta detali valstybės hibridinės debesijos realizacijos architektūra ir įgyvendinimo planas.
- IVPK įstaigos organizacinėje struktūroje bei biudžete bus suplanuoti valstybės hibridinės debesijos modelio ir paslaugų vystymui ir priežiūrai reikalingi žmogiškieji ištekliai, atlikti organizaciniai pokyčiai bei atnaujinti paslaugų valdymo procesai.
- Valstybės hibridinės debesijos modelis, architektūra, įgyvendinimo planas bei planuojamos paslaugos bus pristatytos valstybės institucijoms, kurios jau konsolidavo arba dar tik planuoja konsoliduoti savo IT infrastruktūrą į valstybės debesijos platformą.
- Valstybės hibridinės debesijos paslaugų vystymas bus derinamas atsižvelgiant į įstaigų IT migravimo į valstybės debesijos platformą poreikius.

Modelio diegimo prioritetai ir uždaviniai – skyriuje „6. Hibridinės debesijos modelio įgyvendinimas: prioritetai ir pagrindiniai uždaviniai“.

2. Įžanga ir esama situacija

Informacinės visuomenės plėtros komitetas (toliau – IVPK) vykdydamas Lietuvos Respublikos Vyriausybės 2015 m. gegužės 13 d. nutarimą Nr. 498 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo ir jos valdymo optimizavimo“ (aktuali redakcija), įgyvendina(-o) žemiau išvardintus projektus:

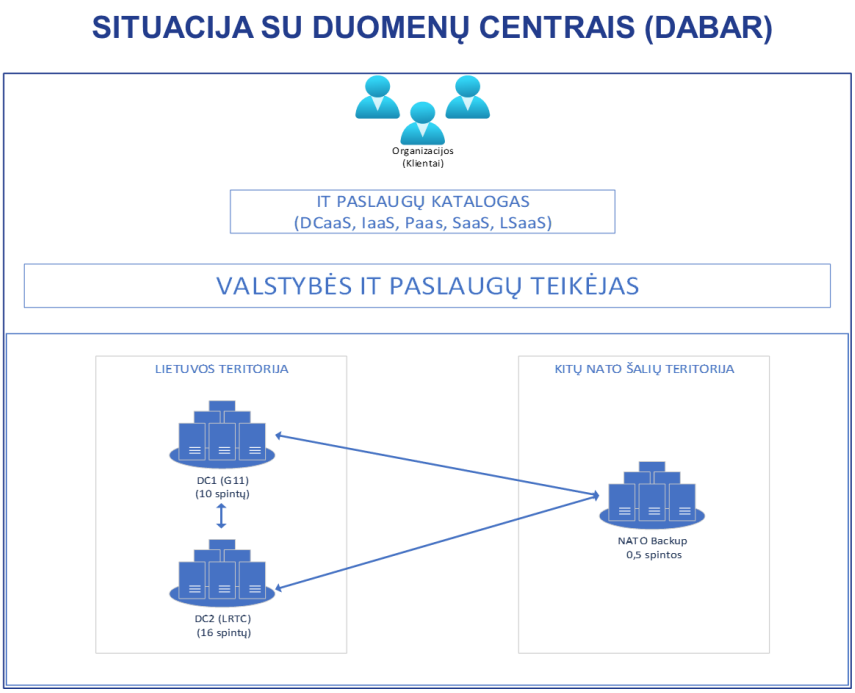
1. **Projektas.** Įgyvendintas Europos Sąjungos 2 prioriteto lėšomis finansuotas projektas Nr. J06-CPVA-V „Valstybės debesijos paslaugų teikimo infrastruktūros sukūrimas“. Projekto tikslas – sukurti ir įdiegti valstybės debesijos paslaugų teikimo veiklai reikalingą informacinių ir ryšių technologijų (IRT) infrastruktūrą ir suformuoti žmogiškuosius išteklius, reikalingus valstybės debesijos paslaugoms teikti.
   Projekto pagrindiniai uždaviniai:
   - sukurti ir įdiegti valstybės debesijos paslaugų teikimo veiklai reikalingą IRT infrastruktūrą;
   - talpinti/migruoti Valstybės informacinių išteklių infrastruktūrą sukurtoje debesijos paslaugų teikimo infrastruktūroje, įgalinant jų veikimą ir tvarkymą naudojant Debesijos paslaugas;
   - sukurti valstybės debesijos paslaugų teikimo organizacijos veiklos planavimo ir valdymo reglamentavimą ir įgyvendinimo priemones bei užtikrinti tinkamą valstybės debesijos paslaugų teikimo organizacijos veikimą.

2. **Projektas.** Šiuo metu vykdomas Europos Sąjungos RRF lėšomis finansuojamas projektas Nr. EIM-V-001-0001 „Valstybės informacinių technologijų valdymo pertvarka“. Pagrindinis projekto tikslas - **Error! Reference source not found.**saugumą, kompleksiškai įvykdant Valstybės informacinių t echnologijų valdymo pertvarką, užtikrinant konsoliduotos IRT infrastruktūros tolimesnę plėtrą ir naujų IT pertvarkos veiklų įgyvendinimą.
   Projekto pagrindiniai uždaviniai:

   - Centralizuotai atnaujinti valstybės biudžetinių įstaigų naudojamą IRT infrastruktūrą, užtikrinant esamos debesijos informacinių ir ryšių technologijų infrastruktūros praplėtimą iki visoms Valstybės biudžetinėms įstaigoms reikalingos apimties;

- Valstybės biudžetinių įstaigų pasenusios bei saugumo reikalavimų neatitinkančios IRT infrastruktūros migravimas į centralizuotai valdomą debesijos informacinių ir ryšių technologijų infrastruktūrą;
- Valstybės biudžetinių įstaigų pasenusių bei saugumo reikalavimų neatitinkančių lokalių duomenų perdavimo tinklų techninės ir sisteminės programinės įrangos kompleksinis atnaujinimas ir pertvarka, saugaus centralizuoto valdymo sprendimo įdiegimas (4000 KDV);
- Valstybės biudžetinių įstaigų pasenusios bei saugumo reikalavimų neatitinkančios kompiuterinių darbo vietų techninės ir sisteminės programinės įrangos kompleksinis atnaujinimas ir pertvarka, saugaus centralizuoto valdymo sprendimo įdiegimas (4000 KDV).

Įgyvendinant aukščiau išvardintus projektus bei pagal Loginėje debesijos paslaugų teikimo IT infrastruktūros architektūroje (toliau – Detali architektūra) numatytus principus, šiuo metu yra naudojami du valstybiniai duomenų centrai Lietuvos Respublikos teritorijoje ir papildomai daromos kritinių valstybės informacinių sistemų ir registrų rezervinės kopijos į NATO (Briuselyje) esantį duomenų centrą (Krašto apsaugos ministerijos išduotos patalpos, kuriose patalpinta IVPK rezervinio kopijavimo specializuota įranga). Pažymėtina, kad KAM išduotos patalpos šiuo metu nėra įtrauktos į Valstybinių duomenų centrų sąrašą. Žemiau pateikta šiuo metu naudojamų valstybinių duomenų centrų principinė schema.



Brėžinys 1 Esama duomenų centrų situacija

2.1. Valstybinių duomenų centrų plėtra

Didėjant konsoliduotos IRT infrastruktūros apimtims, padidėjo ir valstybinių duomenų centrų papildomų patalpų poreikis, todėl nuo 2024 m. I-II ketv. numatoma pradėti naudoti 2 (du) naujai įrengtus valstybinius duomenų centrus (toliau – VDC), turinčius pakankamą kiekį spintų ir elektros energijos galios. Numatoma per 2024-2025 m. į naujas VDC patalpas sumigruoti esamą konsoliduotos IRT infrastruktūros platformą bei juose vykdyti tolimesnę platformos plėtrą. Pagal šiuo metu numatyta koncepciją, konsoliduota IRT infrastruktūra ir toliau funkcionuos 2 (dviejose) valstybinių duomenų centrų patalpose, esančiuose Lietuvos Respublikos teritorijoje, o šiuo metu naudojamos valstybinių duomenų patalpos bus atlaisvintos ir naudojamos pagal poreikį (pvz. papildomoms duomenų rezervinėms kopijoms saugoti ir pan.).

2.2. Rezervinio kopijavimo poreikiai

Vadovaujantis Lietuvos Respublikos Vyriausybės 2022 m. liepos 11 d. patvirtinto nutarimo Nr. 739 „Dėl valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties,

ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašo patvirtinimo“ nuostatomis (https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/779cbbc401a711edbfe9c72e552dd5bd?jfwid=-3xe81ejhb), šiuo metu rezervinės duomenų kopijos saugomos viename arba dviejuose Lietuvos Respublikos teritorijoje esančiose duomenų centruose, o kritinių valstybės informacinių sistemų ir registrų papildomos rezervinės kopijos yra saugomos NATO (Briuselyje) esančiame duomenų centre.

Pagal Detalioje architektūroje numatytus principus NATO papildomas rezervinis kopijavimo sprendimas buvo suprojektuotas tik konsoliduotoje IRT infrastruktūroje talpinamoms valstybės informacinėms sistemoms ir registrams, tačiau atsižvelgiant į 2022 m. susiklosčiusią geopolitinę situaciją pasaulyje, atsirado poreikis atlikti ir kitų valstybės kritinių informacinių sistemų ir registrų (veikiančių ne konsoliduotoje IRT infrastruktūroje, o pvz. Registrų centro, Informatikos ir ryšių departamento ir kitų valstybės institucijų IRT infrastruktūrose) papildomą rezervinį kopijavimą, todėl NATO DC įdiegtos rezervinio kopijavimo saugyklos buvo pilnai užpildytos padengiant tik apie 30-40 proc. valstybės mastu reikalingo poreikio. Taip pat, vadovaujantis Lietuvos Respublikos Vyriausybės 2022 m. liepos 11 d. patvirtinto nutarimo Nr. 739 „Dėl valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašo patvirtinimo“ nuostatomis, atsirado papildomas reikalavimas “Karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais Lietuvos teritorijoje praradus prieigą prie VII ar sutrikus jų veiklai ir nesant galimybės jos atkurti, turi būti inicijuojamas šių VII atkūrimas iš VII atsarginės kopijos, laikomos užsienio teritorijose esančiuose duomenų centruose”, kas reiškia, kad turi būti įsigyta IRT infrastruktūra (fiziškai arba kaip paslauga), įdiegta už Lietuvos Respublikos teritorijos ribų ir nuolat parengta darbui nenumatytų situacijų atveju (*angl. Disaster Recovery*), **kas keičia ir papildo esamą konsoliduotos IRT infrastruktūros architektūrą, kurioje buvo numatytas tik rezervinis kopijavimas ir kopijų saugojimas.**

Esamą konsoliduotos IRT infrastruktūros architektūrą papildo ir nuo 2024 m. sausio 1 d. įsigaliojanti Valstybės informacinių išteklių valdymo įstatymo 45 (2) straipsnio nuostata, kuri leidžia institucijoms savo valdomus mažos ir vidutinės svarbos VII išteklius laikyti privačiuose duomenų centruose, jų kopijas saugant VDC.

2.3. Sistemų vystymo poreikiai

Dalis valstybės informacinių sistemų yra monolitinio tipo. Tokių sistemų vystymas yra sudėtingesnis ir lėtesnis, ribotos galimybės plėsti individualių komponentų ar funkcionalumų našumą, monolitinių sistemų kompleksiškumas mažina sistemos patikimumą. Vykdant tokių sistemų pakeitimus, neįmanoma pritaikyti modernių technologijų atskiriems funkcionalumams ar moduliams nekeičiant visos informacinės sistemos architektūros. Net ir maži valstybės informacinių sistemų pakeitimai dažniausiai yra brangūs ir lėti. Todėl yra būtina keisti naujų valstybės informacinių sistemų kūrimo ir senųjų sistemų modernizavimo principus (architektūros, įrankių ir procesų, infrastruktūros naudojimo), kurie užtikrintų greitesnį sistemų pateikimą naudojimui, efektyvų sistemų veikimą ir priežiūrą, saugumą bei efektyvų valstybės biudžeto lėšų panaudojimą.

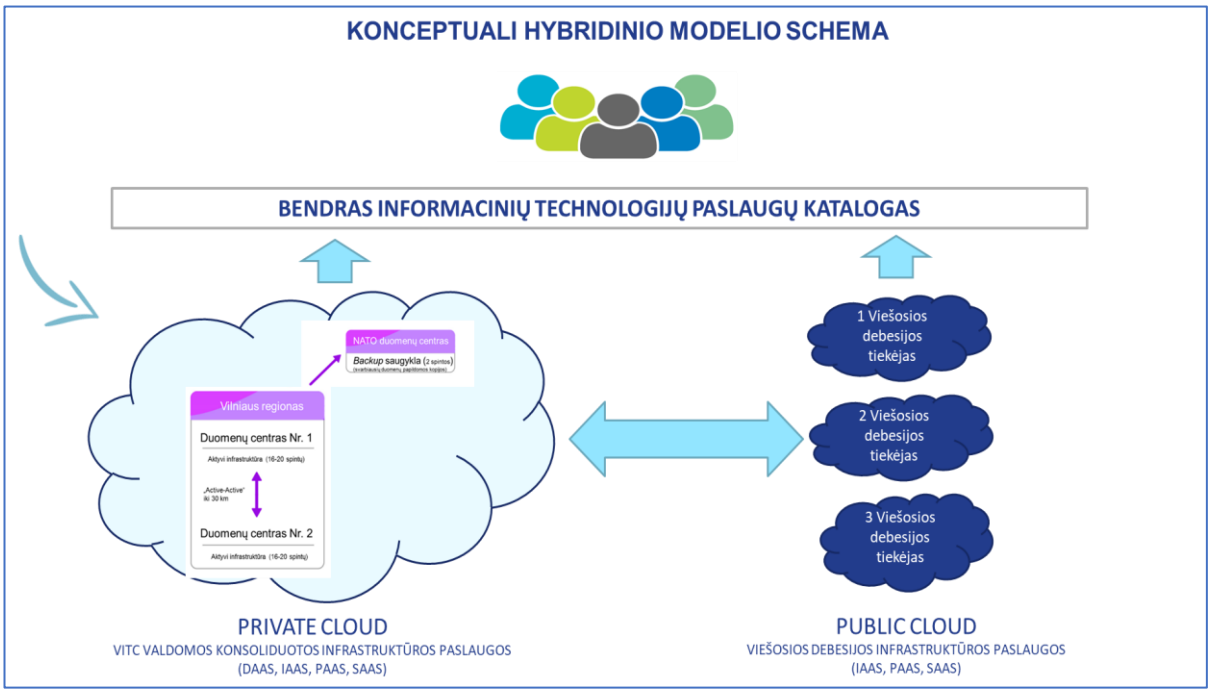
Nauja valstybės hibridinės debesijos platformos architektūra turi:

- palaikyti viešajai debesijai pritaikytų (*angl. Cloud Ready*) informacinių sistemų veikimą;
- neapriboti galimybes kurti valstybės informacines sistemas moderniais įrankiais ir procesais (CI/CD);
- sudaryti galimybes pilnai automatizuoti sistemų vystymą ir priežiūros procesus (DevOps);
- gebėti greitai reaguoti į IS našumo poreikius.

Siekiant sudaryti galimybes efektyviau kurti ir modernizuoti valstybės informacines sistemas, reikalinga vystyti valstybės debesijos platformos architektūrą, sudarant technologines prielaidas diegti inovatyvias ir modernias IS vystymo ir priežiūros technologijas.

2.4. Esamos situacijos analizė ir siūlymai

Atsižvelgiant į atnaujintą teisinį reglamentavimą, naujai atsiradusius poreikius ir reikalavimus valstybės informacinių sistemų kūrimui ir senųjų modernizavimui, o taip pat siekiant išnaudoti viešosios debesijos teikiamų pažangiausių sprendimų potencialą (kuriant naujas informacines sistemas ir sprendimus), buvo atlikta papildoma analizė ir pateikti pasiūlymai įdiegti valstybės hibridinės debesijos modelį (toliau – hibridinė debesija *angl. Hybrid Cloud*) sujungiant esamos konsoliduotos IRT infrastruktūros sprendimą (*angl. Private Cloud*) su viešosios debesijos (*angl. Public Cloud*) teikiamomis paslaugomis. Žemiau pateikiamas aukšto lygio Hybrid Cloud siūlomas koncepcinis modelis[1].



Brėžinys 2 Konceptuali hibridinio modelio schema

Analizės metu identifikuota, kad šiuo metu didžiosios dalies valstybės informacinių sistemų ir registrų IRT infrastruktūros yra decentralizuotos, o aplikacijos yra monolitinio tipo. Nemaža dalis valstybės informacinių sistemų ir registrų realizuotos naudojant klasikines technologijas (Oracle, MS SQL ir pan. duomenų bazes, aplikacijų komponentai įdiegti virtualiuose arba fiziniuose serveriuose, aukšto patikimo sprendimai realizuoti infrastruktūros lygyje ir t.t.)., todėl diegiant hibridinės debesijos sprendimą, **būtina užtikrinti, kad visos naujos ir modernizuojamos valstybės informacinės sistemos ir registrai būtų kuriamos taip, jog veiktų naudojant viešosios debesijos technologijas (*angl. Cloud Ready*)**.

3. Teisinė aplinka

Hibridinė debesija turi būti diegiama ir naudojama vadovaujantis Lietuvos Respublikoje galiojančiais teisės aktais. Žemiau pateikiami pagrindiniai teisės aktai, kurie įgalina hibridinės debesijos diegimą ir nustato hibridinės debesijos pagrindinius reikalavimus ir panaudojimo principus (įskaitant, bet neapsiribojant):

1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (*aktuali redakcija*);
2. Lietuvos Respublikos kibernetinio saugumo įstatymas (*aktuali redakcija*);
3. Lietuvos Respublikos Vyriausybės 2015 m. gegužės 13 d. nutarimas Nr. 498 „Dėl valstybės informacinių technologijų infrastruktūros konsolidavimo ir jos valdymo optimizavimo“ (*aktuali redakcija*);

[1] Hibridinio valstybės debesijos modelio įgyvendinimo pradžioje, numatoma naudotis 3-jų viešosios debesijos tiekėjų paslaugas. Vėliau numatoma prijungti daugiau viešosios debesijos paslaugų teikėjų.

4. Lietuvos Respublikos Vyriausybės 2022 m. liepos 11 d. nutarimas Nr. 739 „Dėl valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašo patvirtinimo“ (*aktuali redakcija*);
5. Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. gegužės 10 d. įsakymas Nr. 4-249 „Dėl techninių ir organizacinių reikalavimų, taikomų valstybiniams duomenų centrams ir Lietuvos Respublikoje ar kitose Europos sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (ar) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esantiems duomenų centrams, kuriuose laikomi valstybės informaciniai ištekliai, aprašo ir valstybinių duomenų centrų sąrašo patvirtinimo” (*aktuali redakcija*);
6. Lietuvos Respublikos ekonomikos ir inovacijų ministro 2020 m. balandžio 20 d. įsakymas Nr. 4-241 „Dėl informacinių technologijų paslaugų teikėjo centralizuotai teikiamų informacinių technologijų paslaugų katalogo patvirtinimo“ (*aktuali redakcija*);
7. Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimas Nr. 576 “Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo” (*aktuali redakcija*);
8. Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymas Nr. 4-418 “Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“ *(aktuali redakcija)*;
9. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 “Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir saugos dokumentų turinio gairių aprašo patvirtinimo” (*aktuali redakcija*);
10. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (*aktuali redakcija*);
11. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“ (*aktuali redakcija*);
12. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1807 „Dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų“ (*aktuali redakcija*);
13. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 “Dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti“ (*aktuali redakcija*).

4. Galimos alternatyvos ir pasirenkama kryptis

Šiame skyriuje analizuojamos šios pagrindinės alternatyvos anksčiau įvardintos problematikos sprendimui:

1. Nieko nekeisti ir prisiimti rizikas;
2. Užsienyje nuomoti papildomas duomenų centro patalpas ir įdiegti dedikuotą sprendimą sistemų veikimui už Lietuvos ribų;
3. Realizuoti hibridinės debesijos sprendimą apjungiant šiuo metu naudojamą Valstybės debesijos platformą su viešosios debesijos platformomis.

4.1. Alternatyvų palyginimas

Sprendimas	**Palikti *AS-IS***	**Dedikuota platforma už Lietuvos ribų**	**Hibridinės debesijos sprendimas**
Infrastruktūros paruošimas Disaster recovery (toliau – DR) sprendimų diegimui	Neaktualu, nes nediegiame DR sprendimų	8-12 mėn. įvertinat sprendimo projektavimą, įrangos ir paslaugų pirkimo bei pristatymo terminus	6-12 mėn., įvertinant, kad reikia įsigyti resursus jau veikiančiose platformose ir juos sujungti

Galimybė naudoti modernias technologijas IS kūrimui	Ribotos, nes dalis modernių technologijų veikia tik debesijos sprendimuose	Ribotos, nes dalis modernių technologijų veikia tik debesijos sprendimuose	Maksimalios, nes praktiškai visos modernios technologijos pradedamos diegti viešosios debesijos sprendimuose
Galimybė operatyviai plėsti resursus	Ribotos, nes reikalingi viešieji pirkimai, įrangos pristatymas, diegimas ir t.t.	Ribotos, nes reikalingi viešieji pirkimai, įrangos pristatymas, diegimas ir t.t.	Maksimalios, nes viešosios debesijos sprendimų esmė – klientai moka už tiek resursų kiek naudoja
Programinės įrangos licencijavimas	Sudėtingas, nes esant poreikiui reikia įsigyti papildomas licencijas	Sudėtingas, nes esant poreikiui reikia įsigyti papildomas licencijas	Viešosios debesijos tiekėjai leidžia naudoti daugumos gamintojų programinę įrangą mokant už licencijas tą laikotarpį kai jos naudojamos
Saugumo sprendimai	Sudėtinga realizacija, didelės investicijos, ribotas produktų funkcionalumas, sąlyginai dideli priežiūros kaštai	Sudėtinga realizacija, didelės investicijos, ribotas produktų funkcionalumas, sąlyginai dideli priežiūros kaštai	Labai didelės viešosios debesijos tiekėjų investicijos, moderniausiomis technologijomis (AI/ML) grįsti sprendimai, sąlyginai lengvas sprendimų aktyvavimas
Kaina	Ilgalaikės investicijos, fiksuota sprendimų kaina	Ilgalaikės investicijos, fiksuota sprendimų kaina	Mėnesiniai mokesčiai už išnaudotus resursus; atsiranda paslėpti kaštai, kuriuos sunku apskaičiuoti prognozuojant sprendimo kainą; neteisingai priimti sprendimai gali sugeneruoti ženklias nenumatytas išlaidas
Ryšys	Naudojami egzistuojantys sprendimai	Reikalingi papildomi sujungimai, didelis vėlinimas tinkle	Reikalingi papildomi sujungimai, didelis vėlinimas tinkle

Lentelė 1 Alternatyvos ir jų palyginimas

Įvertinus galimas alternatyvas, esamą problematiką ir keliamus tikslus, darytina išvada jog **priimtiniausia naudoti hibridinės debesijos sprendimą** t. y. šiuo metų naudojamų techninių paslaugų ir IT Infrastruktūros sprendimų plėtimas prijungiant viešosios debesijos sprendimus.

5. Hibridinės debesijos modelio teikiami privalumai

Pasirinkus hibridinės debesijos modelį ir esamas valstybės IT paslaugų teikėjo teikiamas paslaugas išplečiant viešosios debesijos paslaugomis tikėtinos šios esminės naudos:

1. Viešosios debesijos infrastruktūros techniniai pajėgumai yra praktiškai neriboti ir paruošti plėtrai. Debesijos tiekėjo uždavinys planuoti ir investuoti į infrastruktūros pajėgumų plėtrą.
2. Optimizuojami kaštai išnaudojant debesijos privalumus mokant tik už realiai panaudotas technines paslaugas ir jų pajėgumus. Tai suteikia galimybę išvengti išankstinių investicijų į techninę infrastruktūrą kai IS reikalingi pajėgumai tik kritiniais laikais.
3. Technologijų ir duomenų sauga vienas iš kertinių viešosios debesijos aspektų, kur viešosios debesijos tiekėjai skiria ypatingą dėmesį nuolat vykdydami saugos stebėsenas, teikdami naujinimus. Išnaudojamos pasaulinės saugos užtikrinimo praktikos.

4. Viešosios debesijos tiekėjų duomenų centrų išdėstymas skirtingose valstybėse ir technologijų modernumas leidžia įgyvendinti realius DR ir rezervinių kopijų kūrimo scenarijus.
5. Išnaudojant viešosios debesijos teikiamas paslaugas (PaaS) dėmesys skiriamas veiklos poreikiams ir IS vystymui. Viešosios debesijos paslaugų tiekėjas atsakingas už techninių paslaugų vystymą ir reguliarų naujinimą.
6. Greitas naujų, modernių paslaugų pateikimas IS valdytojams ir tvarkytojams. Viešosios debesijos paslaugų tiekėjai teikia visas reikalingas modernias technines paslaugas.
7. Viešosios debesijos paslaugos įgalins kurti lankstesnes, efektyvesnes, patikimesnes, labiau prieinamas ir saugesnes valstybės IS, išnaudojant modernius viešosios debesijos sistemų vystymo ir palaikymo procesus, įrankius, technologijas ir paslaugas.

Žemiau pateikiamas hibridinės debesijos naudų grafiniai atvaizdai:

Brėžinys 3 Viešosios debesijos teikiamos naudos

6. Hibridinės debesijos modelio įgyvendinimas: prioritetai ir pagrindiniai uždaviniai

Atsižvelgiant į valstybės funkcijų vykdymo priklausomybę nuo duomenų prieinamumo ir šiems duomenims tvarkyti naudojamų priemonių patikimo veikimo, technologijų poreikį, jų teikiamų galimybių panaudojimą ir aktualų teisinį reguliavimą, perėjimas prie hibridinės debesijos architektūros įgyvendinamas vadovaujantis šiais principais:

1. Nacionalinio saugumo interesų ir kibernetinio saugumo užtikrinimo;
2. Technologinės nepriklausomybės ir nepriklausomumo nuo atskirų tiekėjų išlaikymo;
3. Duomenų kontrolės ir prieinamumo užtikrinimo;
4. Infrastruktūros ir IT paslaugų pasiūlos, įgalinančios taikyti modernius valstybės IS kūrimo metodus, suformavimo.

Įvertinus teisės aktų reikalavimus ir anksčiau minėtą informaciją valstybės informacinių sistemų ir registrų architektūroms keliami šie ilgalaikiai uždaviniai, kurie nustato strategines gaires hibridinės debesijos modelio diegimui ir vystymui:

- **Uždavinys/Etapas Nr. 1** – kritinių valstybės informacinių sistemų ir registrų papildomų rezervinių duomenų kopijų **(*angl. Backup*)** už Lietuvos Respublikos ribų užtikrinimas. Atsižvelgiant į tai, kad papildomų rezervinių duomenų kopijų saugojimas už Lietuvos Respublikos ribų yra prioritetinė kryptis - šią užduotį numatoma pradėti vykdyti I etapu (nuo 2024 m.);
- **Uždavinys/Etapas Nr. 2 -** kritinių valstybės informacinių sistemų ir registrų nepertraukiamos veiklos užtikrinimas arba veiklos tęstinumo užtikrinimas karo, nepaprastos padėties ir kitų ekstremalių situacijų atveju, užtikrinant susietų IT paslaugų atstatymą **(*angl. Disaster Recovery*)**. Atsižvelgiant į tai, kad šios užduoties įgyvendinimui būtina daugiau laiko, papildomų techninių sprendimų bei aplikacijų modifikavimo *(angl. Refactoring)* – šią užduotį numatoma pradėti vykdyti II etapu (nuo 2025 m.);
- **Uždavinys/Etapas Nr. 3 -** VIIVĮ nuostatų, leidžiančių institucijoms savo valdomus mažos ir vidutinės svarbos VII laikyti privačiuose duomenų centruose, įgyvendinimas. Viešosios debesijos inovatyvių ir modernių technologijų naudojimas kuriant naujas ir modernizuojant esamas Valstybės informacines sistemas ir registrus **(*angl. Cloud Ready*).**

Atsižvelgiant į tai, kad ilgalaikėje perspektyvoje numatoma valstybės mastu pereiti prie Cloud Ready informacinių sistemų kūrimo, 3 uždavinį numatoma pradėti vykdyti lygiagrečiai I ir II etapams (nuo 2024 m. arba iš karto po hibridinės debesijos modelio patvirtinimo), patvirtinus naujų ir modifikuojamų informacinių sistemų Cloud Ready reikalavimus, suprojektavus ir įdiegus būtinus techninius įrankius (pvz. Git programinio kodo centralizuoto valdymo platformą, automatizacijos įrankius aplikacijų ir infrastruktūros valdymui ir pan.), debesijos paslaugų ir infrastruktūros valdymo bei DevOps procesus, suformavus debesijos paslaugų vystymo ir priežiūros struktūrinius padalinius, atrinkus reikalingos kompetencijos žmogiškuosius išteklius (DevOps).. Pastebėtina, kad nuo 2024 m. įsigaliojus VIIVĮ naujai redakcijai, visos mažos ir vidutinės svarbos informacinės sistemos (atitinkančios Cloud Ready reikalavimus) galės būti iš karto diegiamos viešosios debesijos platformose ir/arba migruojamos iš IRT konsoliduotos infrastruktūros (tokių informacinių sistemų papildomos rezervinės kopijos privalo būti saugomos Valstybiniame duomenų centre, esančiame Lietuvos Respublikos teritorijoje).

Tam, kad operatyviau ir sklandžiau įdiegti hibridinės debesijos modelį ir užtikrinti aukščiau išvardintų prioritetinių užduočių įgyvendinimą, nuo 2024 m. II-III ketv. numatoma valstybės institucijų atstovams organizuoti viešosios debesijos mokymus, o taip pat suteikti viešosios debesijos teikiamų paslaugų išbandymo aplinką (smėliadėžę), prie kurios galės prisijungti valstybės institucijų atsakingi darbuotojai ir saugiai išbandyti viešosios debesijos teikiamas paslaugas bei galimybes.

7. Pagrindiniai parametrai ir reikalavimai

Šiame skyriuje pateikiami minimalūs parametrai ir reikalavimai valstybės informacinių sistemų ir registrų veiklos užtikrinimui, kuriais remiantis bus kuriama valstybės hibridinės debesijos architektūra.

Eil. Nr.	Reikalavimas	Komentaras
DISASTER RECOVERY IR BACKUP SĄLYGOS		
DR-KRIT	Kritinių valstybės informacinių sistemų ir Registrų veiklos atstatymas (ypatingos svarbos duomenų pasiekiamumo užtikrinamas) už LT ribų kritinių situacijų (angl. *Disaster Recovery*) atveju. Užtikrinant esminių sistemos naudotojų prisijungimą prie IS ar Registro alternatyviu saugiu ryšiu.	Kritinių valstybės informacinių sistemų ir Registrų darbingumo atstatymo ir leistino duomenų praradimo sąlygos turi būti apibrėžtos valstybės hibridinės debesijos architektūroje. **DR scenarijų numatoma įgyvendinti II etape (nuo 2025 m.)**

	PASTABA: Kiekvienos valstybės informacinės sistemos ir/arba registro konkretūs RTO ir RPO reikalavimai nustatomi atsižvelgiant į sąlygas nustatytas valstybės hibridinės debesijos architektūroje.	
BCKP-KRIT BCKP-VID BCKP-MAŽ	Kritinių valstybės informacinių sistemų ir Registrų veiklos atstatymas (ypatingos svarbos duomenų pasiekiamumo užtikrinamas) atstatant iš rezervinių duomenų kopijų (angl. *Backup*) atveju. PASTABA: Kiekvienos valstybės informacinės sistemos ir/arba registro konkretūs RTO ir RPO reikalavimai nustatomi atsižvelgiant į sąlygas nustatytas valstybės hibridinės debesijos architektūroje.	Kritinių valstybės informacinių sistemų ir Registrų darbingumo atstatymo ir leistino duomenų praradimo sąlygos turi būti apibrėžtos valstybės hibridinės debesijos architektūroje. **BACKUP scenarijų numatoma įgyvendinti I etape (nuo 2024 m.)**
BENDRIEJI REIKALAVIMAI		
R-001	Viešosios debesijos paslaugos teikiamos tik iš Europoje esančių duomenų centrų.	Viešosios debesijos paslaugos teikiamos tik iš Europoje esančių duomenų centrų, kurie yra valstybėse, neturinčiose sienų su nedraugiškomis valstybėmis.
R-002	Suprojektuoti sprendimai turi užtikrinti saugų modernių viešosios debesijos paslaugų naudojimą ir techninės kontrolės priemones asmens duomenų apsaugai	Duomenų saugos incidentų didžioji tikimybė kyla iš viešos debesijos paslaugų, kurių nustatymai suteikia nesankcionuotas prieigas prie duomenų ir/arba duomenų šifravimas perduodant ar saugant duomenis (in tranist/ on rest) yra nepakankamas. Siekiant suvaldyti šias rizikas, viešosios debesijos techninės paslaugos užsakomos pasitelkiant centralizuotą sprendimą, kuris garantuotų minimalų nustatytą kiekvienos techninės paslaugos saugumo parametrų rinkinį.
R-003	Įgyvendinama centralizuota stebėsena ir procedūrų testavimas užtikrinant sprendimų pilnavertį veikimą visuose Duomenų centruose	Pasitelkiant viešos debesijos paslaugas rezervinių kopijų kūrimo nustatymai yra dalis nustatymų, už kuriuos atsakingas klientas. Tačiau vertinant duomenų praradimo riziką, vykdoma visų duomenų saugyklų ir duomenų bazių rezervinių kopijų kūrimo nustatymų centralizuota stebėsena.
R-004	Sprendimas projektuojamas taip, kad būtų centralizuotai valdomos techninės ir organizacinės priemonės užtikrinančias duomenų apsaugą	Vykdyti centralizuotas technines ir organizacines priemones užtikrinančias atitiktį duomenų apsaugos reglamentams. Ypatingą dėmesį skiriant duomenų šifravimo sprendimams, duomenų saugojimo ir perdavimo geografijos valdyti.

Lentelė 2 Reikalavimų sąrašas

8. Siekiama situacija įgyvendinus reikalavimus

Įgyvendinus šiame dokumente aprašytą hibridinę architektūrą siekiama žemiau išvardintų rezultatų (įskaitant, bet neapsiribojant):

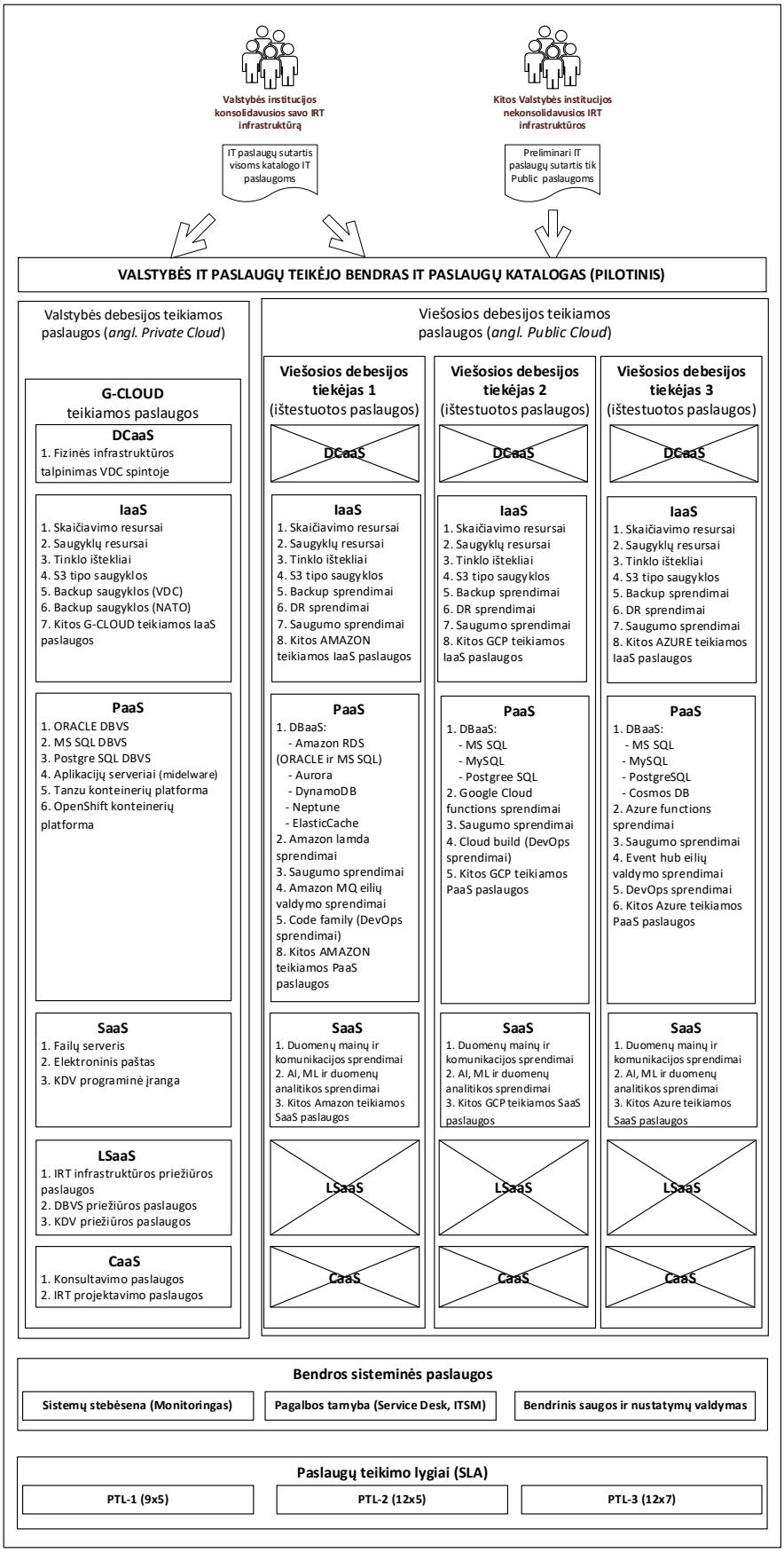
1. Pagal kritinių valstybės informacinių sistemų ir registrų (kurių papildomos rezervinės duomenų kopijos turi būti saugomos už Lietuvos Respublikos ribų) sąrašą, papildomos rezervinės kopijos saugomos už Lietuvos Respublikos ribų ir, prireikus, gali būti operatyviai atstatytos pagal patvirtintus reikalavimus.
2. Pagal kritinių valstybės informacinių sistemų ir registrų (kurių papildomos rezervinės duomenų kopijos turi būti saugomos už Lietuvos Respublikos ribų) sąrašą, sistemos ir registrai, kurių veiklos tęstinumo plane yra numatyta užtikrinti veiklos tęstinumą užsienio valstybėse, turi veikiantį DR sprendimą ir, prireikus, gali tęsti darbą iš už Lietuvos Respublikos teritorijos esančios IRT infrastruktūros (atjungus valstybinius duomenų centrus).
3. Visos naujos ir/arba modernizuojamos valstybės informacinės sistemos pagal nutylėjimą (*angl. By Design*) yra pritaikytos naujausiems viešosios debesijos sprendimams (*angl. Cloud Ready*) ir veikia hibridinės debesijos infrastruktūroje.
4. IT paslaugų gavėjai gali užsakyti modernias ir saugias naudoti viešos debesijos paslaugas savo valdomų IS vystymui;
5. IVPK valdo saugos nustatymus viešos debesijos paslaugose ir, situacijoje kai klientas neatitinka saugos parametrų, sugeba pastebėti parametrų neatitikimą ir pradėti korekcijų veiksmus bei tyrimą;
6. Sudaromos galimybės valstybės informacinėms sistemoms elastingai naudoti viešosios debesijos paslaugas.

9. Paslaugų valdymo modelis

Viešosios debesijos paslaugas planuojama teikti analogiškais principais kaip šiuo metu teikiamos Valstybės debesijos platformos (Konsoliduotos IRT infrastruktūros) paslaugos. Esamas paslaugų teikimo procesas ir paslaugų krepšelis bus adaptuotas pagal viešosios debesijos paslaugų specifiką. Numatoma, kad hibridinės debesijos paslaugų naudotojai bus dviejų tipų:

1. **Valstybės institucijos konsolidavusios savo IRT infrastruktūrą** – tai yra valstybės institucijos, kurios yra pasirašiusios su IVPK IT paslaugų teikimo sutartį ir yra konsolidavusios/konsoliduojančios savo IRT infrastruktūrą. Tokio tipo naudotojams IVPK centralizuotai ir pilna apimtimi teiks visas IT paslaugų kataloge numatytas IT paslaugas (tiek konsoliduotos IRT infrastruktūros teikiamas paslaugas, tiek viešosios debesijos teikiamas paslaugas).
2. **Valstybės institucijos, kurios nebuvo įtrauktos į IRT infrastruktūros konsolidavimo apimtį ir nekonsolidavusios savo IRT infrastruktūros –** tai yra Valstybės institucijos, kurios nėra su IVPK pasirašiusios IT paslaugų teikimo sutarties ir nėra konsolidavusios savo IRT infrastruktūros (t.y. naudoja savo dedikuotą IRT infrastruktūrą). Su tokio tipo naudotojais numatoma pasirašyti preliminarias sutartis, kurių pagrindu, suderinus atsiskaitymo už paslaugas viešosios debesijos paslaugų teikėjui tvarką, jie galės užsakyti **tik viešosios debesijos tiekėjų teikiamas paslaugas**. Valstybės IT paslaugų teikėjo teikiamų paslaugų (pvz.: KDV priežiūra, lokalių tinklų priežiūra ir pan.) tokio tipo naudotojai užsisakyti negalės. Institucijos, kurios naudosis viešos debesijos paslaugomis, turi laikytis IVPK nustatytų paslaugų naudojimo taisyklių bei atitikti nustatytus saugumo reikalavimus.

10. Bendras paslaugų katalogas ir paslaugų užsakymas



Brėžinys 4 Bendras IT paslaugų katalogas (pilotinis)

Bendro paslaugų katalogo valdymas:

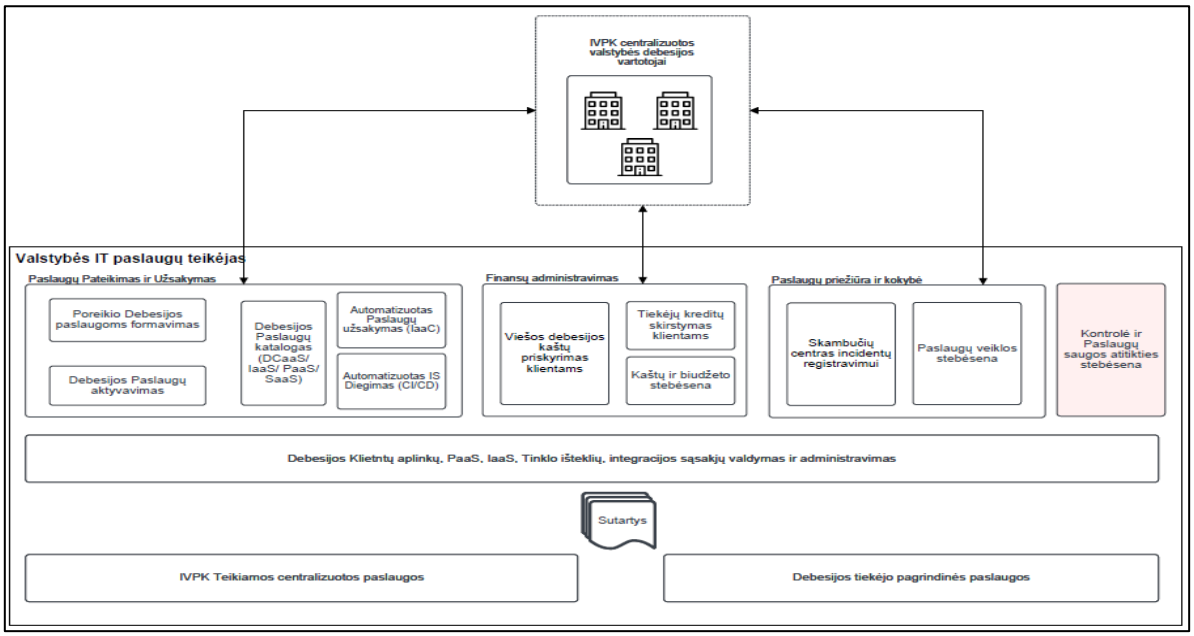
Numatoma, kad paslaugų katalogas bus valdomas pagal žemiau išvardintus principus:

- Paslaugų katalogas valdomas IVPK centralizuotai, atsižvelgiant į strategines kryptis bei, siekiant aiškaus ir paprasto supratimo paslaugų naudotojams.
- Paslaugų kataloge pateikiamos debesijos paslaugos paruoštos naudotis klientams, nurodant paslaugų kokybės ir prieinamumo parametrus (SLA)
- Į viešosios debesijos paslaugų katalogą įtraukiamos tik IVPK ekspertų įvertintos ir paruoštos naudojimui viešos debesijos paslaugos, užtikrinant konkrečios paslaugos minimalius saugos reikalavimus.
- Klientai naudojasi viešos debesijos paslaugomis tik pagal IVPK ekspertų nustatytas taisykles.
- Vertinant, kad viešos debesijos tiekėjų viešas paslaugų katalogas labai platus, klientams suteikiama galimybė pateikti poreikį papildomų IVPK viešos debesijos paslaugų paruošimui.
- Įtraukiant naujas paslaugas ar modifikuojant esamas, bus siekiama maksimalaus paslaugų standartizavimo ir neprisirišimo prie konkretaus viešosios debesijos paslaugų teikėjo ar konkrečios viešosios debesijos paslaugų teikėjo technologijos (*angl. Vendor Lock-in*). Prioritetas bus teikiamas standartinėms paslaugoms, kurios vienodai veiks tiek valstybės duomenų centrų platformoje, tiek viešojoje debesijoje (*angl. Feature Parity*).
- Valstybės institucijos galės rinktis konkrečios viešosios debesijos IVPK paslaugų katalogo paslaugas tik esant techninėms galimybėms, finansiniams bei žmogiškiesiems ištekliams. Tokiais atvejais institucijos pačios atsakingos už atitinkamos viešosios debesijos paslaugų kompetencijos valdymą.
- Esant naujų ar papildomų paslaugų poreikiui IVPK įvertina tokių paslaugų saugumą, rizikas, kaštų valdymą, atitikimą hibridinės debesijos plėtros planams bei teikia argumentuotą ir motyvuotą išvadą dėl tokių paslaugų teikimo galimybės ir (ar) įtraukimo į paslaugų katalogą.

IT paslaugų užsakymas, valdymas ir priežiūra:

Numatoma, kad IT paslaugos bus užsakomos ir valdomos pagal žemiau išvardintus principus:

- Klientas iš paslaugų katalogo užsako sau skirtą aplinką, kurioje diegiama IS ir pateikiamos techninės paslaugos pagal IS architektūrą;
- Klientai turi dvi galimybes techninių paslaugų užsakymui/atsisakymui:
    - Klientas užsako paslaugas per IVPK pagalbos tarnybą;
    - Klientas, taikantis modernias IS kūrimo ir naujinimo metodikas, naudojasi automatizuotu būdu užsakyti ir pateikti paslaugas (angl. *Infrastructure as a Code*). Šis būdas yra rekomenduotinas, nes užtikrina minimalių saugumo reikalavimų pritaikymą automatiniu keliu;
- Klientams, kurie yra pasirašę IT paslaugų teikimo sutartį ir naudojasi IVPK platformos centralizuotai teikiamomis paslaugomis – visų paslaugų veikimą (įskaitant ir viešos debesijos paslaugų veikimą) centralizuotai prižiūri IVPK darbuotojai;
- Klientams, kurie yra pasirašę preliminarią sutartį ir per bendrą IT paslaugų katalogą užsako viešos debesijos paslaugas – IVPK suteikia viešosios debesijos patikrintas aplinkas, tačiau už užsakytų paslaugų veikimo priežiūrą ir už debesijos resursų panaudojimą atsako patys klientai.



Brėžinys 5 Paslaugų teikimo principinė schema

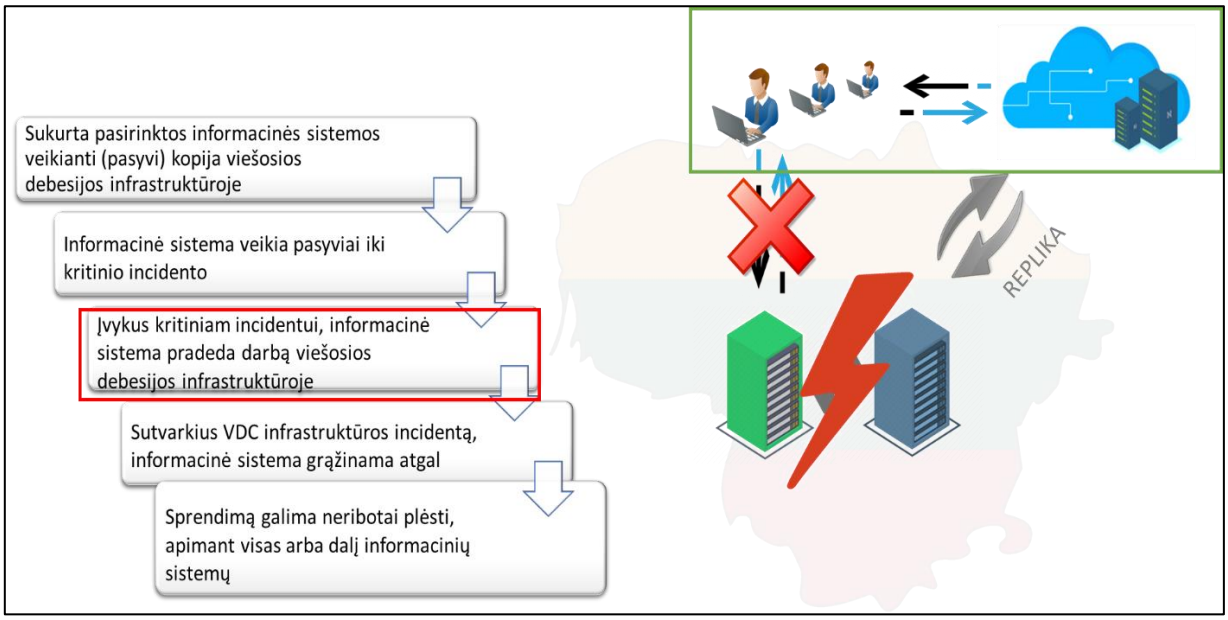
11. Pilotiniai projektai ir išvados

Siekdamas geriau suprasti kaip praktiškai veikia viešosios debesijos rezervinio kopijavimo (*angl. Backup as a Service*) ir IRT infrastruktūros greito atstatymo (*angl. Disaster Recovery as a Service*) paslaugos, Valstybės IT paslaugų teikėjas atliko kelis pilotinius bandymus, pasirinkus vieną iš valstybės informacinių sistemų (ITSM/VIPVIS) ir praktiškai išbandant jos Backup ir Disaster Recovery scenarijus panaudojant viešosios debesijos paslaugas.

Pilotinio projekto tikslai:

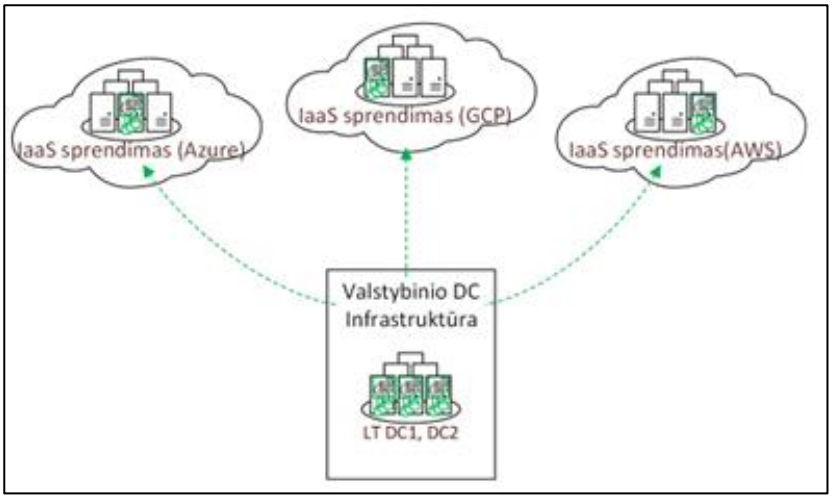
- Įvertinti ir praktiškai išbandyti trijų skirtingų viešosios debesijos tiekėjų (AWS, Google, Azure) siūlomas Backup ir Disaster Recovery paslaugas;
- Įvertinti esamus techninius resursus ir galimas priemones, reikalingas Backup ir Disaster Recovery scenarijams įgyvendinti;
- Panaudojant viešosios debesijos paslaugas, įdiegti numatytus scenarijus, ištestuoti jų realų veikimą ir pateikti išvadas.

Žemiau pateikiamas pilotinio projekto testuojamo scenarijaus grafinis atvaizdas:



Brėžinys 6 Pilotinių projektų scenarijus

Pilotiniams projektams buvo pasirinkti skirtingų viešosios debesijos tiekėjų (*AWS, Google, Azure*) teikiamos paslaugas, sujungiant jas su valstybinių duomenų centrų konsoliduota IRT infrastruktūra ir ištestuojant jų veikimą.



Brėžinys 7 Pilotiniams projektams pasirinkti viešosios debesijos tiekėjai

1. **Azure Site Recovery sprendimas** - projekto metu į Azure Cloud buvo sėkmingai replikuotos informacinės sistemos virtualios mašinos. Pasiektas 3 minučių RPO rezultatas. Failover ir Test failover proceso metu, į Azure Cloud viskas veikė sklandžiai, problemų virtualiose mašinose nepastebėta. Failover procesas testavimo metu truko iki 10 minučių. Sinchronizavimas atgal veikė korektiškai tik „ASR appliance“ išjungus vMotion. Trūkumai: Sinchronizacija atgal iš ASR į konsoliduotą IRT infrastruktūrą periodiškai nutrukdavo ir nuolat teko keisti konfigūracijas pasitelkiant Microsoft techninio palaikymo personalą. Sudėtingas ir ilgai trunkantis kiekvienos sistemos konfigūravimas.

2. **Google Cloud Storage sprendimas** - projekto metu į Google Cloud aplinką buvo sėkmingai padarytos pasirinktų virtualių mašinų rezervinės kopijos (panaudojant Valstybės IT paslaugų teikėjo naudojamą rezervinio kopijavimo įrangą). Atstatymai tiek į konsoliduotą IRT infrastruktūrą, tiek ir į Google Cloud aplinką irgi buvo sėkmingi. Trūkumai: ilgai trunkantis rezervinių kopijų atstatymo procesas. Neveikiant valstybinių duomenų centrų platformai reikia turėti visų virtualių mašinų ir sistemų metaduomenis.

3. **AWS programiškai valdomų duomenų centrų (*angl. SDDC - software-defined data center*) sprendimas -** projekto metu į AWS programiškai valdomą duomenų centrą buvo sėkmingai numigruotos

informacinės sistemos visos virtualios mašinos. Atsižvelgiant į tai, kad tiek konsoliduotos IRT infrastruktūros, tiek AWS programiškai valdomam duomenų centrui naudojama ta pati virtualizacijos valdymo platforma (VMware), migravimas į abi puses įvyko greitai ir sklandžiai. Trūkumai: atsižvelgiant į tai, kad šiam sprendimui viešojoje debesijoje naudojama dedikuota techninė įranga, už kurią reikia mokėti net jos ir nenaudojant, bendra sprendimo kaina kažkiek išbrangsta.

IŠVADOS. Įvertinus pilotinių projektų rezultatus, darytinos išvados:

- tradicinėmis technologijomis realizuotų sistemų (*angl. Legacy*) greitam DR atstatymui labiausiai tinkamas programiškai valdomų duomenų centrų (*angl. SDDC - software-defined data center*) veikiančių viešosios debesijos platformose sprendimas. Šis sprendimas yra brangesnis, tačiau leidžia be didesnių informacinės sistemos pakeitimų, greitai ir sklandžiai replikuoti visus IS komponentus į dedikuotą viešosios debesijos infrastruktūrą ir per trumpą laiką IS iš ten paleisti. Taip pat pažymėtina, kad šiame sprendime naudojama ta pati virtualizacijos platforma, todėl specialistai jau dabar gali ją naudoti be papildomų kompetencijų tobulinimo mokymų;
- naujos kartos informacinėms sistemoms, kurios paruoštos veikti viešosios debesijos platformose, tinka ir efektyviai veikia standartiniai (*angl. Cloud Native*) viešosios debesijos DR ir Backup sprendimai, todėl tokio tipo IS nebūtina naudoti programiškai valdomų duomenų centrų (*angl. SDDC - software-defined data center*), veikiančių viešosios debesijos platformose sprendimų.
- Tam, kad užtikrinti greitą tradicinių informacinių sistemų *(angl. Legacy)* atstatymo (DR) sprendimų realizavimą bei užtikrinti aukščiausius RPO (*angl. Recovery Point Objective*) ir RTO (angl. *Recovery Time Objective*) reikalavimus, pirmuose migravimo į viešąją debesiją etapuose tikslinga išnaudoti viešosios debesijos programiškai valdomų duomenų centrų (*angl. SDDC - software-defined data center*) galimybes, tačiau palaipsniui pritaikant tradicines informacines sistemas (*angl. Legacy*) darbui viešosios debesijos platformose (*angl. Cloud Ready*), tikslinga palaipsniui perkelti ir DR sprendimus iš programiškai valdomų duomenų centrų į standartinius (*angl. Cloud Native*) viešosios debesijos sprendimus (realizuojant HA ir DR sprendimus aplikacijų lygyje, išnaudojant konteinerių technologijų sprendimus ir t.t.).

12. Sprendimo techninė architektūra

Įvertinus anksčiau pateiktą informaciją ir tai, kad planuojama valstybės informacinėms sistemoms ir registrams naudoti hibridinės architektūros modelį, pagrindinius uždavinius galima pasiekti tik projektą įgyvendinant etapais sprendžiant kiekvieną uždavinį atskirai.

Prieš pradedant diegti hibridinės debesijos sprendimus būtina realizuoti sujungimus tarp valstybės duomenų centrų ir viešosios debesijos platformų.

12.1. Tinklų sujungimo architektūra

Įgyvendinant strateginę kryptį, užtikrinančią valstybės informacinių sistemų ir registrų veikimą tiek valstybiniuose duomenų centruose, tiek ir viešosios debesijos platformose esant kritinei situacijai, būtina įgyvendinti sprendimą, užtikrinantį:

a) vartotojų prisijungimą prie IS ir registrų įprastinėmis aplinkybėmis;
b) alternatyvų prisijungimą kritinės situacijos atveju, kuris užtikrintų nepriklausomą prisijungimą prie IS ir registrų veikiančių viešosios debesijos platformose.

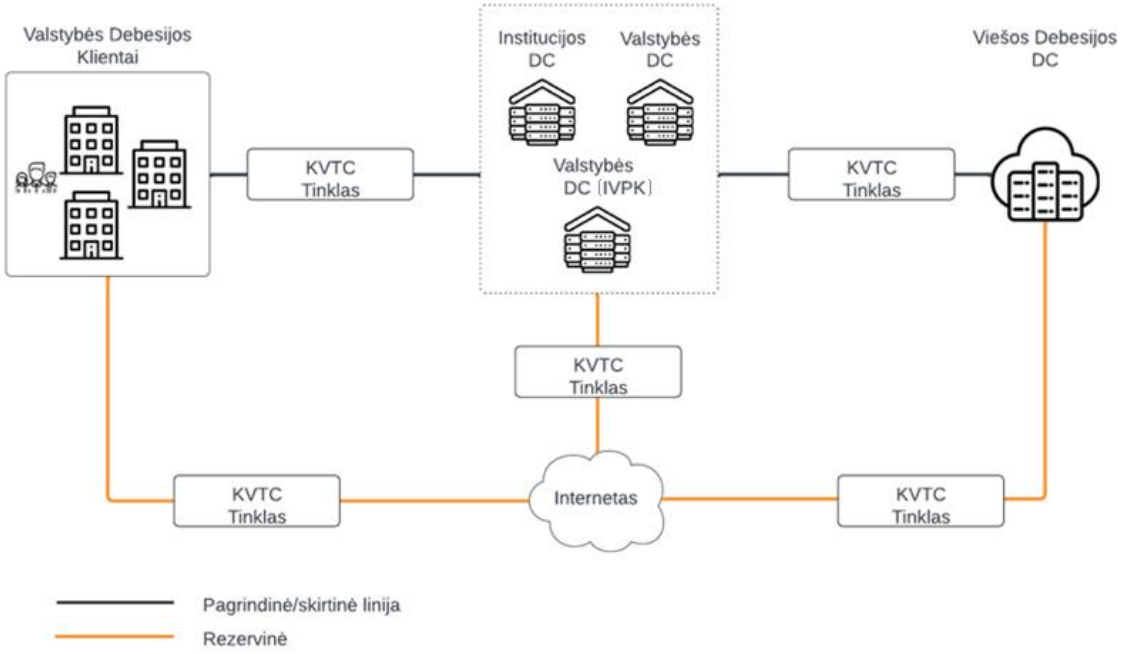
Atsižvelgiant į tai, valstybinių duomenų centrai turi būti sujungiami su viešosios debesijos platformomis dviem būdais:

1. **Skirtosios linijos** – pagrindinis informacijos mainų būdas skirtas užtikrinti pralaidumo reikalavimus;
2. **Saugus sujungimas per viešą internetą** – rezervinis sujungimo būdas naudojamas kritiniu atveju.

Įprastomis sąlygomis IS ir registrų vartotojai jungiasi dvejais būdais:

1. Dirbant įstaigų patalpose, jungiamasi skirtosiomis linijomis (schemoje – KVTC tinklas), kurios sujungia įstaigas su valstybiniu duomenų centru;
2. Dirbant nutolusiame režime (*remote connection*) jungiamasi per viešą internetą, naudojant VPN ar analogiškus sprendimus, tiesiogiai į valstybinius duomenų centrus ir (ar) viešos debesijos platformas.

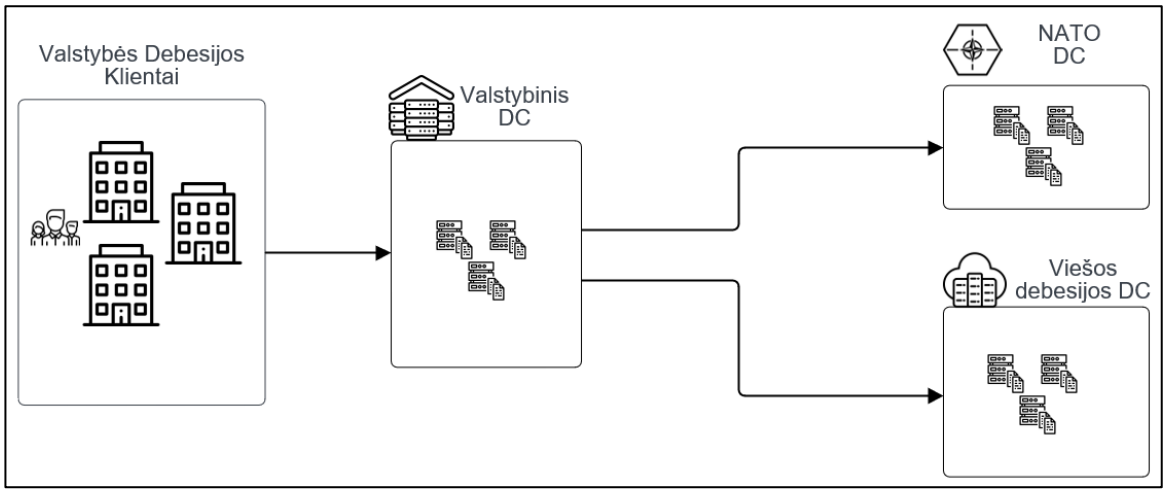
Principinė siūlomo sprendimo architektūra:



Brėžinys 8 Principinė tinklų sujungimo schema

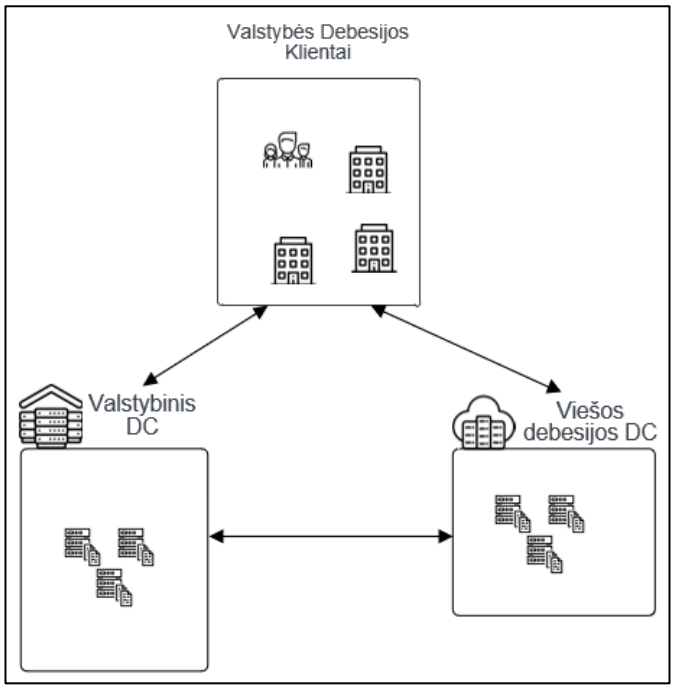
12.2. Pirmasis hibridinės debesijos diegimo etapas

Pirmasis hibridinės debesijos diegimo etapas turėtų būti valstybės informacinių sistemų ir registrų papildomų rezervinių duomenų kopijų (*angl. Backup*) už Lietuvos Respublikos ribų užtikrinimas. Šiuo metu dalinai šis uždavinys sprendžiamas naudojant NATO DC patalpintą įrangą. NATO DC naudojamos įrangos našumo pakanka tik apie 30-40 proc. valstybės informacinių sistemų ir registrų rezervinių kopijų saugojimui. Atsižvelgiant į tai siūlome šį uždavinį spręsti panaudojant viešosios debesijos sprendimus. Kritinės valstybės informacinės sistemos ir registrai normaliu režimu dirba iš valstybinių duomenų centrų. Viešosios debesijos paslaugos naudojamos rezervinių kopijų saugojimui. Principinė sprendimo schema pateikiama žemiau.



Brėžinys 9 Principinė rezervinių kopijų saugojimo schema

Įvertinus strateginį sprendimą naudoti hibridinį debesijos modelį bei tai, kad viešosios debesijos platformų resursai yra praktiškai neriboti, ilgalaikėje perspektyvoje numatoma NATO DC atsisakyti ir rezervines kopijas saugoti tik viešosios debesijos platformose. Principinė sprendimo schema pateikiama žemiau.



Brėžinys 10 Principinė rezervinių kopijų saugojimo schema
atsisakius šiuo metu naudojamų NATO patalpų (KAM laikinai suteiktos patalpos)

12.3. Antrasis hibridinės debesijos diegimo etapas

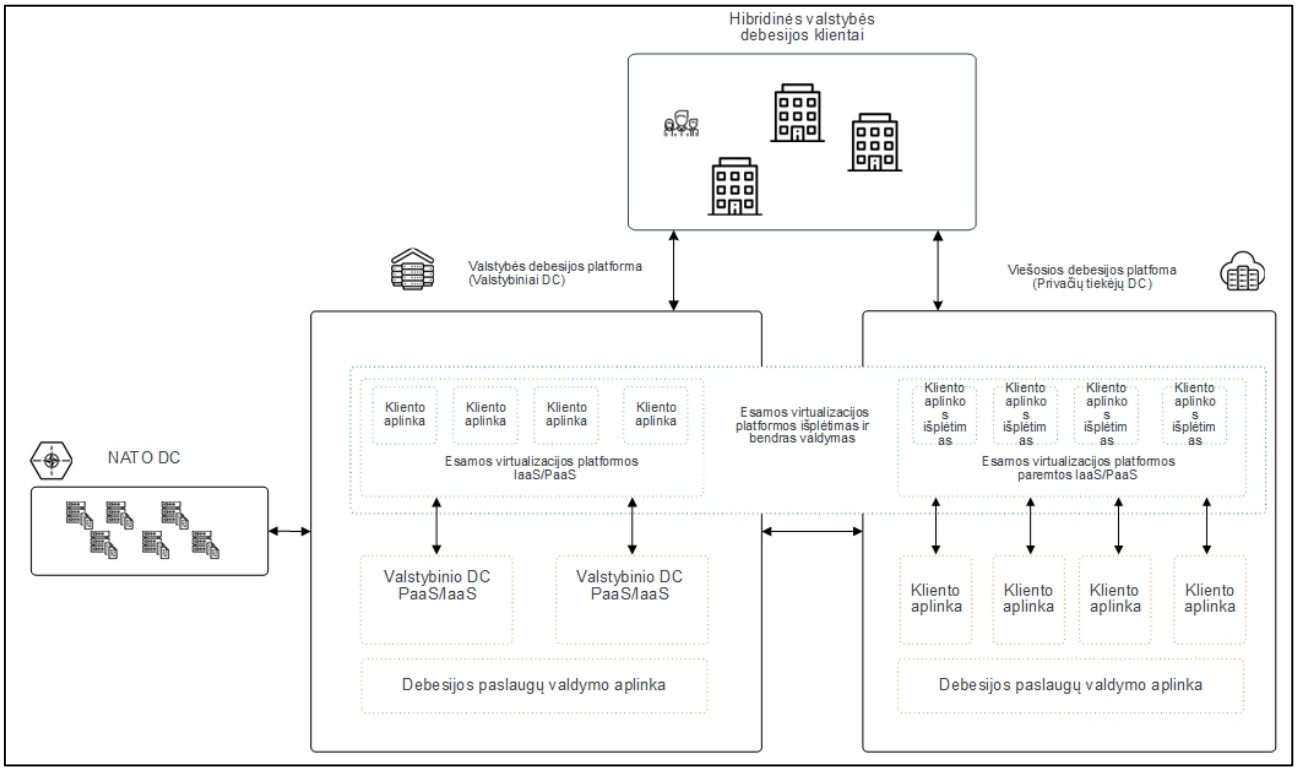
Antrasis hibridinės debesijos diegimo etapas turėtų būti kritinių valstybės informacinių sistemų ir registrų nepertraukiamos veiklos užtikrinimo karo, nepaprastos padėties ir kitų ekstremalių situacijų atveju, užtikrinančių susietų IT paslaugų atstatymą (*angl. Disaster Recovery*) sprendimų diegimas. Atsižvelgiant į tai, kad didžioji dalis kritinių valstybės informacinių sistemų ir registrų infrastruktūros realizuotos naudojant

klasikines technologijas pradiniame etape numatoma bent vienoje iš viešosios debesijos platformų naudoti analogiškas technologijas šiuo metu naudojamoms. Šis etapas gali būti vykdomas lygiagrečiai su pirmuoju etapu.

Esminiai siūlomo sprendimo architektūros principai:

1. Esami valstybės duomenų centrai saugiai (naudojant dedikuotus sujungimas) sujungiami su pasirinktais viešos debesijos paslaugų tiekėjais;
2. Operatyviam Kritinių valstybės IS ir registrų darbingumo atstatymui realizuojami DR sprendimai į viešosios debesijos platformas;
3. Kritinėms valstybės IS ir registrams kurie naudoja *legacy* technologijas sudaroma galimybė naudoti šiuo metu Valstybės IT paslaugų teikėjo naudojamos IRT infrastruktūros virtualizacijos platformos pagrindu realizuotą darbingumo atstatymo platformą veikiančią viešosios debesijos tiekėjų duomenų centruose;
4. Modernių IS ir registrų valdytojams/tvarkytojams DR sprendimus numatoma realizuoti kiek įmanoma daugiau naudojant *native* technologijas ir CI/CD procesus.

Atsižvelgiant į anksčiau įvardintus reikalavimus ir principus, žemiau pateikiama numatoma kritinių valstybės informacinių sistemų ir registrų nepertraukiamos veiklos užtikrinimo (*angl. Disaster Recovery*) sprendimo principinė schema:



Brėžinys 11 Disaster Recovery sprendimo principinė schema

Pagal aukščiau pateiktą principinę schemą, tradiciniais principais veikiančių informacinių sistemų (*angl. Legacy*) greitam veiklos atstatymui (*angl. Disaster Recovery*) numatoma naudoti programiškai valdomą duomenų centrą (*angl. SDDC - software-defined data center*), veikiantį viešosiose debesijos platformose ir palaikantį šiuo metu naudojamą konsoliduotos IRT infrastruktūros virtualizacijos platformą (VMware), kuri gali būti bendrai valdoma hibridinio modelio principu (schemoje pavaizduota žalia spalva). Viešosios debesijos platformoms pritaikytų informacinių sistemų (*angl. Cloud Ready*) DR sprendimus numatoma realizuoti naudojant standartinius viešosios debesijos (*angl. Cloud Native)* technologijas ir CI/CD procesus (schemoje pavaizduota geltona spalva).

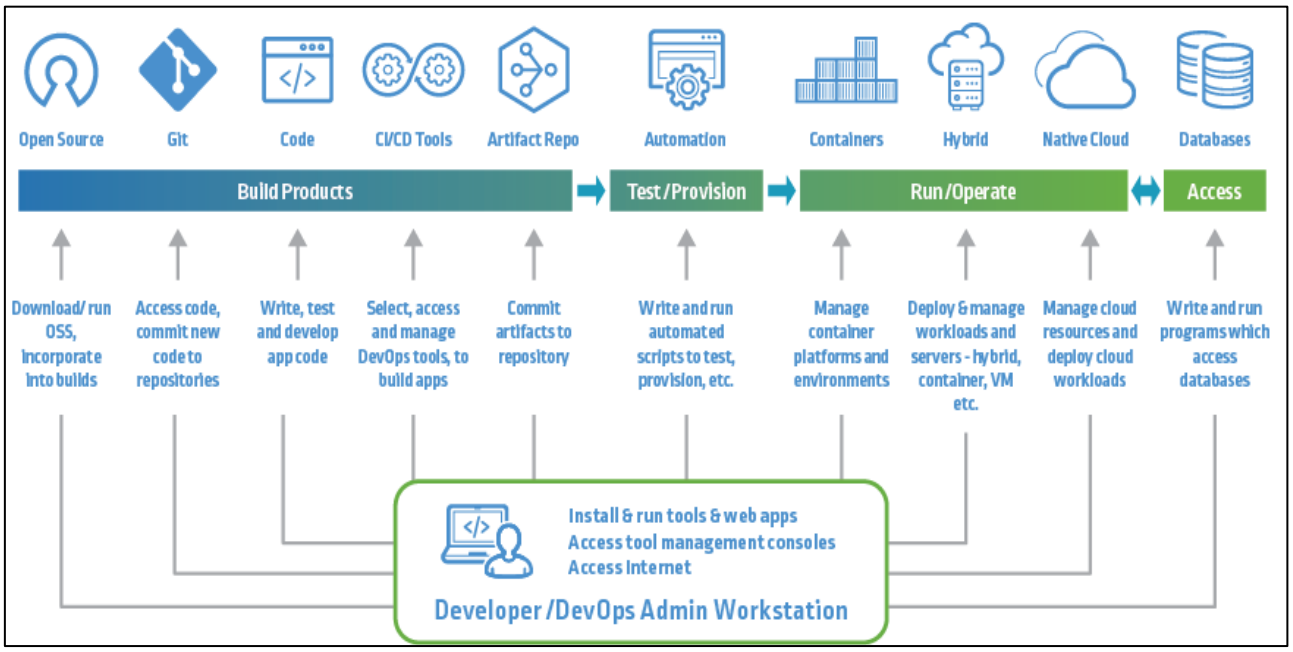
12.4. Trečiasis hibridinės debesijos diegimo etapas

Trečiasis hibridinės debesijos diegimo etapas turėtų būti Viešosios debesijos inovatyvių ir modernių technologijų naudojimas kuriant naujas ir modernizuojant esamas Valstybės informacines sistemas ir registrus (*angl. Cloud Ready*). Šis etapas gali būti vykdomas lygiagrečiai su antruoju ir pirmuoju etapu.

Esminiai siūlomo sprendimo architektūros principai:

1. Dokumentuojami bendrieji reikalavimai Valstybės IS ir registrų kūrimui užtikrinantys inovatyvių ir modernių technologijų naudojimą;
2. Kuriant ar modernizuojant Valstybės IS ir registrus būtina iš karto numatyti DR sprendimus į viešosios debesijos paslaugas;
3. Ilgalaikėje perspektyvoje Vmware technologijų pagrindu veikiantys viešosios debesijos platformos dalis turėtų mažėti, idealiu atveju turėtų būti naudojama tik *native* viešosios debesijos teikiamos paslaugos.
4. Valstybės IS ir registrų valdytojai/tvarkytojai turėtų orientuotis į CI/CD procesus.

Vadovaujantis pasaulio gerosiomis praktikomis, žemiau pateikiamas siūlomas valstybės informacinių sistemų ir registrų kūrimo/modernizavimo proceso organizavimo modelis, panaudojant inovatyvias ir modernias viešosios debesijos technologijas:



Brėžinys 12 Gerosiomis pasaulinėmis praktikomis paremtas informacinių sistemų kūrimo/modifikavimo modelis

13. Rizikos

Pagrindinės rizikos susijusios su šios architektūros ir jai keliamų tikslų įgyvendinimu.

	Rizika	Tikimybė įvykti	Poveikis	Rizikos suvaldymo veiksmai
RI-001	*Viešosios debesijos kompetencijų stygius lėtina projektą.* Viešosios debesijos technologijų ir paslaugų naudojimas skiriasi nuo	Didelė	Didelis	- Trumpalaikėje perspektyvoje pasikliauti partneriais su viešosios debesijos kompetencija - Pasitelkti partnerius viešosios debesijos paslaugų kūrimui/validavimui

	klasikinio DC paslaugų tiekimo, dėl šios priežasties IVPK techninis personalas bei IS valdytojai/tvarkytojai turi turėti atitinkamas kompetencijas.			- IVPK ir susijusiam personalui skirti viešosios debesijos mokymus ir žinių sertifikavimo programas.
RI-002	*Valstybės informacinių sistemų ir Registrų naudojamos technologijos* Didžioji dalis IS ir Registrų realizuoti naudojant klasikines technologijas, kurios ne visada korektiškai veikia debesijos platformose	Didelė	Didelis	- Pradiniame etape planuojama naudoti Vmware technologijų pagrindu veikiančias Viešosios debesijos platformų išplėtimus
RI-003	*Ilgai trunkantis viešos debesijos tiekėjo parinkimas lėtina projekto pradžią* Detali diegimo architektūra priklauso nuo pasirinkto viešosios debesijos tiekėjo. Pastaba: pirminiame etape planuojami keli viešosios debesijos paslaugų tiekėjai	Vidutinė	Didelis	- Parengi technines sąlygas viešosios debesijos tiekėjų parinkimui - Vienu pirmųjų žingsnių pradėti viešosios debesijos tiekėjo parinkimo procesą
RI-003	*Debesijos kaštų valdymas. Išlaidos gali būti ženkliai didesnės nei planuota* Viešosios debesijos paslaugos paremtos Pay-as-you-Go metodu, kas reiškia, kad viešosios debesijos tiekėjui reikia padengti kaštus susijusius su realiu debesijos paslaugų naudojimu. Praktika rodo, jog viešosios debesijos diegimo pradžioje, neturint pakankamų įgūdžių valdyti viešosios debesijos paslaugas, yra sunaudojama neplanuotai daugiau lėšų (dažniausiai dėl žmogiškų klaidų/žinių trūkumo)	Didelė	Vidutinis	- Nuo projekto pradžios vykdyti kasdienį viešosios debesijos kaštų sekimą išnaudojant viešosios debesijos teikiamus įrankius biudžetų stebėjimui ir priimti savalaikius sprendimus - Sutarti su pasirinktais viešosios debesijos tiekėjais projektui skirtą paslaugų kreditų sumą panašių situacijų kompensavimui
RI-004	*IS valdytojai neskiria pakankamo dėmesio savo valdomų Informacinių sistemų ir registrų DR sprendimų perkėlimui į viešąją debesiją*	Vidutinė	Didelis	- Ankstyvoje projekto stadijoje suderinti ir pasitvirtinti planus su IS valdytojais

	DR sprendimų įgyvendinimas nėra įmanomas be IS valdytojo dalyvavimo, nes tik IS valdytojas žino savo valdomos IS techninę architektūrą. IS valdytojo dalyvavimas tiesiogiai įtakoją projekto įgyvendinimo greitį ir sėkmę			
RI-005	*Kibernetinių incidentų rizika naudojant viešąsias debesijos paslaugas*	Didelė	Didelis	- Valstybės hibridinės debesijos kibernetinio saugumo reikalavimus, atsakomybes, sprendimus ir jų apimtis aprašyti detalioje architektūroje, taikant Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatas, ES reguliavimą, ir (ar) tarptautinius informacijos saugumo standartus bei bendradarbiaujant su Lietuvos Respublikos krašto apsaugos ministerijos atstovais. - Kibernetinį saugumą užtikrinti techninėmis ir organizacinėmis priemonėmis, periodiškai vertinant kibernetinių incidentų rizikas, vadovaujantis IVPK Rizikų vertinimo tvarka.

Lentelė 3 Pagrindinių rizikų sąrašas