PATVIRTINTA
NEO Finance, AB
Valdybos 2025-05-21 d.
sprendimu

VEIKLOS TĘSTINUMO PLANAS

TURINYS

BENDROSIOS NUOSTATOS

NEO Finance, AB, veiklos tęstinumo planas (toliau – Planas) nustato NEO Finance, AB (toliau - Bendrovė) taikomas priemones ir procedūras, skirtas užtikrinti, kad Bendrovės veiklos būtų vykdomos nuolat ir nenutrūkstamai, nepertraukiamas sutartinių įsipareigojimų vykdymas nenumatytų aplinkybių atvejais vyktų sklandžiai.

Veiklos tęstinumo planas - tai planas, kuris užtikrina savalaikį ir organizuotą tęstinumą ar greitą veiklos atkūrimą po ekstremaliosios situacijos. Šis procesas apima metodus ir priemones, kurie užtikrina, kad tiek ekstremaliosios situacijos metu, tiek po jos pagrindinė Bendrovės veikla išliktų pastovi bei nenutrūktų.

Planas yra reguliariai testuojamas ir bent kartą per metus, siekiant užtikrinti Bendrovės gebėjimą nuolat vykdyti veiklą ir apriboti nuostolius veiklai sutrikus. Visi sunkumai ar trikdžiai vykdant testavimus yra dokumentuojami ir vertinami atitinkamai tikslinant veiklos tęstinumo planą.

Už Plano įgyvendinimą yra atsakingas Bendrovės vadovas ar jo įgaliotas administracijos vadovo pavaduotojas. Tuo atveju, jeigu Bendrovės vadovas dėl objektyvių priežasčių negali atlikti savo funkcijų (atostogauja, serga ir pan.), Bendrovės vadovas iš anksto paskiria Bendrovės darbuotoją, atsakingą už visų šiame Plane numatytų funkcijų įgyvendinimą.

Bendrovės Valdyba bent kartą per metus arba pagal poreikį peržiūri ir susipažįsta su Planu.

NAUDOJAMOS SĄVOKOS

ABD – Neopay atvirosios bankininkystės departamentas.

ABĮ – Lietuvos Respublikos akcinių bendrovių įstatymas.

Akcininkas – UAB „ERA Capital“, įmonės kodas 300638657, buveinė Ulonų g. 5, Vilnius. Akcininkui priklauso pagrindinis Bendrovės akcijų paketas.

AML - pinigų plovimo, teroristų finansavimo ir sukčiavimo prevencija.

BDAR (Bendrasis duomenų apsaugos reglamentas) – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB.

Bendrovė – NEO Finance, AB, įmonės kodas 303225546, buveinė Ukmergės g. 126, Vilnius. Bendrovė veikia kaip Elektroninių pinigų įstaiga, Vartojimo kredito davėjas ir Tarpusavio skolinimo platformos operatorius.

Bendrovės dukterinė įmonė – UAB Finomark, įmonės kodas 305538582, buveinė Ukmergės g. 126, Vilnius. Bendrovės dukterinė įmonė veikia kaip Sutelktinio finansavimo platformos operatorius.

Bendrovės – Bendrovė ir Bendrovės dukterinė įmonė.

Bendrovių krizių valdymo grupė – nestruktūrinis Bendrovių organas, atsakingas už sprendimų priėmimą, kai visos Bendrovės veiklą veikia incidentas ar krizė. Organas yra neformalus ir sudaromas Bendrovių vadovų nuostata.

EPĮ – elektroninių pinigų įstaiga, kurią apibrėžia Lietuvos Respublikos Elektroninių pinigų ir elektroninių pinigų įstaigų įstatymas.

Finomark – Bendrovės dukterinės įmonės valdoma sistema, kurioje yra saugomi ir kaupiami visi duomenys, susiję su tarpusavio skolinimo operatoriaus veikla. Bendrovės dukterinės įmonės klientams sistema pasiekiama internete adresu: https://www.finomark.lt/.

Incidentas – bet kokia esama ar neišvengiama situacija, kuri gali turėti trikdantį poveikį įprastai Bendrovių veikla ir turėti neigiamą poveikį paslaugų teikimui. Verslo tęstinumo požiūriu bet koks incidentas gali tapti krize, jei poveikis būtų didelis arba ilgalaikis.

Klientas – bent viena Sistema besinaudojantis fizinis arba juridinis asmuo.

KYB - Kliento pažinimo procesas, juridiniams asmenims.

KYC - Kliento pažinimo procesas, fiziniams asmenims.

Licencija – Lietuvos banko Bendrovei 2017-01-05 išduota elektroninių pinigų įstaigos licencija Nr. 7 (licencija buvo atnaujinta: 2018-10-30 – leidimu teikti mokėjimo inicijavimo paslaugas; 2020-05-14 – leidimu teikti sąskaitos informacijos paslaugas).

MIP – mokėjimo inicijavimo paslauga, kaip tai apibrėžia Lietuvos Respublikos mokėjimų įstatymas.

„Neopay" – tai MIP / SIP ir kitų atvirosios bankininkystės paslaugų teikimo sistema, kuri pasiekiama internete adresu: https://mano.neopay.lt.

Paskolos davėjas – fizinis arba juridinis asmuo, skolinantis per Sistemą, kaip tai apibrėžia VKĮ.

Priežiūros institucija – Lietuvos bankas ir / arba kita LR institucija, atliekanti Bendrovės reguliacinę priežiūrą.

„Paskolų klubas" – Bendrovės valdoma sistema, kurioje yra saugomi ir kaupiami visi duomenys, susiję su Bendrovės vykdoma elektroninių pinigų leidimo veikla, tarpusavio skolinimo operatoriaus veikla, mokėjimo paslaugų veikla, išskyrus mokėjimo inicijavimo ir sąskaitos informacijos paslaugas. Bendrovės klientams Sistema pasiekiama internete adresu: https://www.paskoluklubas.lt/prisijungti.

Rizikos pareigūnas – asmuo, atsakingas už vidinių rizikos valdymo modelių kūrimą, bendrą Bendrovės rizikos valdymo sistemos priežiūrą.

SIP – sąskaitos informacijos paslauga, kaip tai apibrėžia Lietuvos Respublikos mokėjimų įstatymas.

SFPO – sutelktinio finansavimo platformos operatorius

Sistema – Tarpusavio skolinimo platformos „Paskolų klubas" sistema, Sutelktinio finansavimo platformos "Finomark" sistema, Elektroninių pinigų ir mokėjimų sistema, ir MIP/SIP „Neopay" sistema toliau tekste kartu vadinamos Sistemomis.

TSPO – tarpusavio skolinimo platformos operatorius, kaip tai apibrėžia VKĮ.

Verslo tęstinumo sutrikimas (krizė) - neplanuotas ir nepageidaujamas Bendrovių veiklos sutrikimas tam tikroje srityje, kuris gali sutrikdyti Bendrovių veiklos veikimą ar nutraukti jos veiklos tęstinumą, t.y. bet kokia nestandartinė situacija, kelianti rizikos grėsmę. Paprastai prasideda kaip incidentas.

VK – vartojimo kreditas, kaip tai apibrėžia VKĮ.

VKD – vartojimo kredito davėjas.

VKG – vartojimo kredito gavėjas, kai VK suteikiamas per Sistemą, kaip tai apibrėžia VKĮ.

VKĮ - Lietuvos Respublikos vartojimo kredito įstatymas.

Vyriausiasis informacijos saugos pareigūnas (angl. *CISO*) - atsakingas už informacinių ir ryšių technologijų rizikos ir saugumo rizikos valdymą.

Visos sąvokos, Plane vartojamos vienaskaita, priklausomai nuo konteksto gali būti suprantamos ir kaip naudojamos daugiskaita, ir atvirkščiai.

VEIKLOS RIZIKOS

Verslo tęstinumo plano esmę sudaro šie elementai:

- Svarbiausių veiklos sričių nustatymas;
- Bendrųjų rizikų nustatymas;
- Kiekvienos rizikos poveikio veiklai analizė;
- Esamų kontrolės priemonių nustatymas ir likutinės rizikos nustatymas;
- Reikalingų kontrolės priemonių planavimas.

Bendrovė siekia, jog finansinių arba reguliuojamų paslaugų teikimas nenutrūktų daugiau nei 2 valandoms arba neperžengtų kitų sutartinių arba reguliacinių ribų.

Bendrovės nuostoliai matuojami eurais, kai lėšų suma yra reikalinga padengti atsiradusius nuostolius, atstatyti bendrovės infrastruktūrą reputaciją ir kitą būklę į anksčiau buvusį lygį.

VEIKLOS SRITYS IR PALAIKANTYS IŠTEKLIAI

Bendrovės yra identifikavusios šias veiklos sritis, kurios papuola į šio Plano apimtį:

- Elektroninių pinigų įstaigos veikla;
- MIP;
- SIP;
- Tarpusavio skolinimo platformos operatoriaus veikla;
- Sutelktinio finansavimo platformos operatoriaus veikla;

- Vartojimo kredito davėjo veikla.

1. Funkcijas palaiko šie ištekliai ir tiekėjai: [KONFIDENCIALU].
2. Elektroninių pinigų įstaigos veikla / Tarpusavio skolinimo platformos operatoriaus veikla / Vartojimo kredito davėjo veikla: [KONFIDENCIALU].
3. Sutelktinio finansavimo platformos operatoriaus veikla: [KONFIDENCIALU].

RIZIKOS SCENARIJAI

Bendrovės yra identifikavusios ir vertina šias bendrąsias rizikas, kurios gali daryti neigiamą poveikį veiklos tęstinumui:

- Geopolitinė rizika
- Gamtos stichijos
- Duomenų centro gedimas / netektis
    - Duomenų centro gedimas gali būti susijęs su kibernetinėmis atakomis, kenkėjiška veikla, DDoS atakomis ir pan.
- Duomenų perdavimo sutrikimai
    - Duomenų perdavimo sutrikimai gali būti susiję su masiniais gedimais, kurie paliestų ne tik Bendrovę, bet ir sukeltų didensį poveikį. Tai taip pat gali būti susiję su ryšio tiekėjų sutrikimais, DDoS atakomis.
- Elektros tiekimo nutraukimas
- Personalo netektis
- Įrangos netektis arba gedimas
- Neopay sistemos netektis
    - Sistemos netektis gali įvykti dėl daugelio scenarijų, įskaitant kibernetines atakas, rizikas, gedimus ir pan.
- Paskolų Klubas sistemos netektis
    - Sistemos netektis gali įvykti dėl daugelio scenarijų, įskaitant kibernetines atakas, rizikas, gedimus ir pan.
- Finomark sistemos netektis
    - Sistemos netektis gali įvykti dėl daugelio scenarijų, įskaitant kibernetines atakas, rizikas, gedimus ir pan.
- Neopay sistemos programavimo klaida – gedimas
- Paskolų Klubas sistemos programavimo klaida – gedimas
- Finomark sistemos programavimo klaida – gedimas
- Ofiso patalpų neprieinamumas
- Neopay duomenų bazės netektis
    - Duomenų bazės netektis gali įvykti dėl daugelio scenarijų, įskaitant kibernetines atakas, rizikas, gedimus kenkėjišką veiklą ir pan.
- Paskolų Klubas duomenų bazės netektis
    - Duomenų bazės netektis gali įvykti dėl daugelio scenarijų, įskaitant kibernetines atakas, rizikas, gedimus kenkėjišką veiklą ir pan.
- Finomark duomenų bazės netektis
    - Duomenų bazės netektis gali įvykti dėl daugelio scenarijų, įskaitant kibernetines atakas, rizikas, gedimus kenkėjišką veiklą ir pan.
- AML tiekėjo sutrikimai
- KYC / KYB tiekėjo sutrikimai
- Kitų kritinių paslaugų teikėjų sutrikimai arba pasitraukimas

POVEIKIO VEIKLAI ANALIZĖS METODOLOGIJA

Bendrovių veiklos tęstinumo planavimas grindžiamas galimo rizikos scenarijaus poveikio Bendrovių verslo procesams vertinimu ir jo analize. Verslo procesai turi būti vertinami pagal:

- Galimos grėsmės poveikį finansams ir reputacijai.
- Verslo procesų kritiškumą, atsižvelgiant į poveikio vertes atitinkamo verslo proceso užtikrinimui.

- Atkūrimo laikotarpį (angl. *Recovery Time Objective - RTO*) ir ilgiausio laikotarpio, per kurį dėl incidento duomenų praradimas laikomas priimtinu (angl. *Recovery Point Objective - RPO*), nustatomą IT sistemoms ir duomenims, būtiniems verslo procesų palaikymui.
- Dabartinį Bendrovių pasirengimą veikti nenumatytomis aplinkybėmis.
- Organizacinius ir technologinius reikalavimus Bendrovių veiklai ir informacinių technologijų veiklai atkurti.
- Toliau apibrėžtą verslo procesų kritiškumo vertinimo metodiką.

1, 2 lentelės. Verslo procesų poveikio klasifikavimo vertės (kokybinės ir kiekybinės):

Poveikio lentelė					
		Žemas	**Vidutinis**	**Aukštas**	**Labai aukštas**
Finansinis poveikis EUR		<20 000	20 000 - 50 000	50 000 - 100 000	>100 000
Klientų praradimas		<5%	5% - 20%	20% - 30%	>30%
Poveikis reputacijai		Neigiamo komentaro grėsmė vietinėje žemo rakto žiniasklaidoje. Neigiami socialinių tinklų komentarai.	Faktinis neigiamas komentaras vietinėje žemo rakto žiniasklaidoje. Neigiami įrašai socialinėje žiniasklaidoje.	Individualūs spaudos pranešimai nusistovėjusioje žiniasklaidoje, neigiamas socialinių tinklų nuomonės formuotojų turinys. Tai gali pasikartoti.	Suderintas, plačiai paplitęs ir pasikartojantis kritinis konkretaus susijusio įvykio nušvietimas. Paremtas neigiamu nuomonės formuotojų, ekspertų ar reguliuotojų komentarų.
Darbuotojų praradimas	**Vadovybė**	<10%	10% - 20%	20% - 30%	>30%
	Ne vadovybė	<10%	10% - 20%	20% - 30%	>30%
Reguliacinis poveikis		Jokio poveikio	Įspėjimas, blogas teisės pažeidimo viešinimas, patikrinimas.	Bauda, įspėjimas ir teisinio pažeidimo paviešinimas.	Licencijų praradimas, bauda. BDAR bauda. Pašalinimas iš mokėjimo schemų.
IT infrastruktūra		Nedidelės klaidos.	Daugumos darbo vietų praradimas. Žinių bazės praradimas. Didelio masto sutrikimas, trunkantis mažiau nei 24 valandas.	Ribotas finansinių arba asmens duomenų duomenų praradimas arba pažeidimas. Didelio masto sutrikimas, trunkantis mažiau nei 72 valandas.	Didelės apimties finansinių arba asmens duomenų praradimas arba pažeidimas. Didelio masto sutrikimas, trunkantis ilgiau nei 72 valandas.

Tikimybės lentelė				
	Žemas	**Vidutinis**	**Aukštas**	**Labai aukštas**
Tikimybė	Mažai tikėtina, kad įvyks	Pagrįsta tikimybė, kad įvyks	Tikėtina, kad įvyks	Beveik tikra tikimybė atsirasti
Paveldimumas	Rizikos šaltinis yra nemotyvuotas ir mažai tikėtina, kad rizika atsiras.	Rizikos šaltinis yra arba nemotyvuotas, arba mažai tikėtina, kad rizika kils.	Rizikos šaltinis yra arba motyvuotas, arba natūraliai tikėtina, kad rizika atsiras.	Rizikos šaltinis yra motyvuotas ir rizika natūraliai gali atsirasti.
Kontrolės priemonės	Yra keli kombinuotos techninės ir administracinės kontrolės lygmenys. Kontrolės priemonės yra reguliariai peržiūrimos ir išbandomos.	Yra daugiau nei du techniniai kontrolė, derinama su administracine kontrole, ir ji laikoma veiksminga.	Yra dvi techninės kontrolės priemonės arba vienas techninių ir administracinių kontrolės priemonių rinkinys.	Nėra jokių riziką mažinančių kontrolės priemonių.

3. lentelė. Proceso kritiškumo vertė apskaičiuojama sudauginus poveikio ir tikimybės vertes. Proceso kritiškumo balai (kiekybiniai ir kokybiniai):

		Probability			
		L	ML	MH	H
Impact	H	MH	MH	H	H
	MH	ML	ML	MH	H
	ML	L	ML	ML	MH
	L	L	L	ML	MH

L vertė yra 1; ML vertė yra 2; MH vertė yra 3; H vertė yra 4. Pvz. L x H yra 1 x 4 = 4.

POVEIKIO VEIKLAI ANALIZĖ

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
Geopolitinė rizika				
MIP	Dėl geopolitinių įvykių sutrinka MIP veikla. Kyla panika ir sutrinka MIP paslauga. Toks scenarijus yra menkai tikėtinas, nes tai yra automatizuota veikla su minimaliu žmogaus įsikišimu. Papildomai, manoma, jog geopolitinių neramumų atveju, MIP veikla nebūtų itin aktuali.	ML	L	L
SIP	Dėl geopolitinių įvykių sutrinka SIP veikla. Kyla panika ir sutrinka SIP paslauga. Toks scenarijus yra menkai tikėtinas, nes tai yra automatizuota veikla su minimaliu žmogaus įsikišimu. Papildomai, manoma, jog geopolitinių neramumų atveju, SIP veikla nebūtų itin aktuali.	ML	L	L
TSPO veikla SFPO veikla VKD veikla	Tikėtina, kad geopolitinių neramumų metu būtų apribotas paskolų išdavimas.	ML	L	L
EPĮ veikla	Dėl geopolitinių įvykių sutrinka CENTROlink veikla. Toks scenarijus yra menkai tikėtinas, nes tai yra automatizuota veikla su minimaliu žmogaus įsikišimu. Daroma prielaida, kad LB yra numatęs CENTROlink veiklos tęstinumą saugioje teritorijoje ir paslaugų teikimas nesutriktų.	ML	L	L
AML atitiktis	Geopolitinių neramumų metu padidėja sankcionuotų asmenų kiekis, sukčiavimo atvejų, plečiasi sankcijų taikomumas, todėl AML sutrikimas gali turėti neigiamų pasekmių organizacijos reputacijai, lėšoms ir kt.	MH	MH	MH
KYC / KYB	Tikėtina, jog geopolitinių neramumų metu Bendrovė nesulauktų didelio paraiškų kiekio iš naujų klientų.	ML	L	L
Gamtos stichijos				
MIP	Menkai tikėtina, kad Lietuvos Respublikoje gamtos stichijos sutrikdytų mokėjimo paslaugų ir duomenų centrų veikimą.	ML	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
SIP	Menkai tikėtina, kad Lietuvos Respublikoje gamtos stichijos sutrikdytų mokėjimo paslaugų ir duomenų centrų veikimą.	ML	L	L
TSPO veikla SFPO veikla VKD veikla	Menkai tikėtina, kad Lietuvos Respublikoje gamtos stichijos sutrikdytų mokėjimo paslaugų ir duomenų centrų veikimą.	L	L	L
EPĮ veikla	Menkai tikėtina, kad Lietuvos Respublikoje gamtos stichijos sutrikdytų mokėjimo paslaugų ir duomenų centrų veikimą.	L	L	L
AML atitiktis	Menkai tikėtina, kad Lietuvos Respublikoje gamtos stichijos sutrikdytų mokėjimo paslaugų ir duomenų centrų veikimą.	L	L	L
KYC / KYB	Menkai tikėtina, kad Lietuvos Respublikoje gamtos stichijos sutrikdytų mokėjimo paslaugų ir duomenų centrų veikimą.	L	L	L
Duomenų centro gedimas / netektis				
MIP	MIP paslaugos servisas veikia viename duomenų centre, tačiau atsarginės kopijos gali būti atstatomos antrame itin greitai. Duomenų praradimas nesutrikdytų paslaugos veikimo.	MH	L	ML
SIP	SIP paslaugos servisas veikia viename duomenų centre, tačiau atsarginės kopijos gali būti atstatomos antrame itin greitai. Duomenų praradimas nesutrikdytų paslaugos veikimo.	MH	L	ML
TSPO veikla SFPO veikla VKD veikla	Sistemos veikia [KONFIDENCIALU] duomenų centre, kuris yra Tier 3 design sertifikuotas. Atsarginės kopijos yra saugomos nutolusiame duomenų centre. Toks sutrikimas turėtų didelį finansinį ir reputacinį poveikį. Duomenų praradimas taip pat gali turėti nemenką poveikį.	MH	L	ML
EPĮ veikla	Sistema veikia [KONFIDENCIALU] duomenų centre, kuris yra Tier 3 design sertifikuotas. Atsarginės kopijos yra saugomos nutolusiame duomenų centre. Toks sutrikimas turėtų didelį finansinį ir reputacinį poveikį. Duomenų praradimas taip pat gali turėti nemenką poveikį.	MH	L	ML
AML atitiktis	AML atitiktis yra perduota trečiajai šaliai, kuri užtikrina apsaugą nuo sutrikimų. Daroma prielaida, jog vieno duomenų centro gedimo atveju, įsijungtų atsarginė versija (backup site). Visiškai sutrikus veiklai, sutriktų mokėjimo paslaugos.	ML	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
KYC / KYB	KYC / KYB yra perduota trečiajai šaliai, kuri užtikrina apsaugą nuo sutrikimų. Daroma prielaida, jog vieno duomenų centro gedimo atveju, įsijungtų atsarginė versija (backup site). Visiškai sutrikus veiklai, sutriktų naujų klientų atpažinimas.	L	L	L
Duomenų perdavimo sutrikimai				
MIP	Menkai tikėtinas scenarijus dėl duomenų centro naudojamų skirtingų ryšio tiekėjų. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	L	L	L
SIP	Menkai tikėtinas scenarijus dėl duomenų centro naudojamų skirtingų ryšio tiekėjų. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Menkai tikėtinas scenarijus dėl duomenų centro naudojamų skirtingų ryšio tiekėjų. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	L	L	L
EPĮ veikla	Menkai tikėtinas scenarijus dėl duomenų centro naudojamų skirtingų ryšio tiekėjų. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	L	L	L
AML atitiktis	Menkai tikėtinas scenarijus dėl duomenų centro naudojamų skirtingų ryšio tiekėjų. Ilgalaikis sutrikimas sustabdytų kitų finansinių paslaugų teikimą.	ML	ML	ML
KYC / KYB	Menkai tikėtinas scenarijus dėl duomenų centro naudojamų skirtingų ryšio tiekėjų. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	L	L	L
Elektros tiekimo sutrikimai				
MIP	Menkai tikėtinas scenarijus dėl duomenų centro turimų atsarginių energijos šaltinių. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	ML	L	L
SIP	Menkai tikėtinas scenarijus dėl duomenų centro turimų atsarginių energijos šaltinių. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	ML	L	L
TSPO veikla	Menkai tikėtinas scenarijus dėl duomenų centro turimų atsarginių energijos šaltinių. Ilgalaikis	ML	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
SFPO veikla VKD veikla	sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.			
EPĮ veikla	Menkai tikėtinas scenarijus dėl duomenų centro turimų atsarginių energijos šaltinių. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	ML	L	L
AML atitiktis	Menkai tikėtinas scenarijus dėl duomenų centro turimų atsarginių energijos šaltinių. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	ML	L	L
KYC / KYB	Menkai tikėtinas scenarijus dėl duomenų centro turimų atsarginių energijos šaltinių. Ilgalaikis sutrikimas neturėtų didelių pasekmių, nes tikėtina, jog tai būtų nacionalinis incidentas.	ML	L	L
Personalo netektis				
MIP	MIP servisas yra automatizuotas, todėl personalo netektis nesukeltų staigių ir didelio poveikio pasekmių.	ML	L	L
SIP	SIP servisas yra automatizuotas, todėl personalo netektis nesukeltų staigių ir didelio poveikio pasekmių.	ML	L	L
TSPO veikla SFPO veikla VKD veikla	Paskolos išdavimas yra pusiau automatizuotas ir standartizuotas procesas. Ribota personalo netektis yra lengvai pakeičiama ir nesukeltų didelio sutrikimo ar nuostolio.	ML	L	L
EPĮ veikla	EPĮ veikla yra automatizuotas ir standartizuotas procesas. Ribota personalo netektis yra lengvai pakeičiama ir nesukeltų didelio sutrikimo ar nuostolio.	ML	L	L
AML atitiktis	AML funkcija yra pusiau automatizuota, todėl personalo netektis nesukeltų staigių ir didelio poveikio pasekmių.	ML	L	L
KYC / KYB	KYC / KYB funkcija yra pusiau automatizuota, todėl personalo netektis nesukeltų staigių ir didelio poveikio pasekmių.	ML	L	L
Įrangos netektis arba gedimas				

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
MIP	Įrangos netektis nepaveiktų paslaugos, nes ji veikia virtualizuotoje aplinkoje. Sutrikus duomenų centro įrangai, MIP servisas gali būti greitai atstatytas.	ML	L	L
SIP	Įrangos netektis nepaveiktų paslaugos, nes ji veikia virtualizuotoje aplinkoje. Sutrikus duomenų centro įrangai, SIP servisas gali būti greitai atstatytas.	ML	L	L
TSPO veikla SFPO veikla VKD veikla	Įrangos gedimas duomenų centre gali sukelti sutrikimą, kuris būtų lėtai atstatomas dėl monolitinės infrastruktūros. Retas duomenų bazės dublikavimas gali reikšti didelius duomenų praradimus, reputacinę žalą.	MH	ML	ML
EPĮ veikla	Įrangos gedimas duomenų centre gali sukelti sutrikimą, kuris būtų lėtai atstatomas dėl monolitinės infrastruktūros. Retas duomenų bazės dublikavimas gali reikšti didelius duomenų praradimus, reputacinę žalą.	MH	ML	ML
AML atitiktis	Daroma prielaida, kad įrangos netektis nepaveiktų paslaugos, nes ji veikia virtualizuotoje aplinkoje, veidrodiniu režimu.	ML	L	L
KYC / KYB	Daroma prielaida, kad įrangos netektis nepaveiktų paslaugos, nes ji veikia virtualizuotoje aplinkoje, veidrodiniu režimu.	ML	L	L
Neopay sistemos netektis				
MIP	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos.	MH	L	ML
SIP	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos.	MH	L	ML
TSPO veikla SFPO veikla VKD veikla	Nėra poveikio.	L	L	L
EPĮ veikla	Nėra poveikio.	L	L	L
AML atitiktis	Nėra poveikio.	L	L	L
KYC / KYB	Nėra poveikio.	L	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
Paskolų Klubas sistemos netektis				
MIP	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos. Praradus įrašus apie transakcijas ir sutartis, galimi nuostoliai.	MH	L	ML
SIP	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos. Praradus įrašus apie transakcijas ir sutartis, galimi nuostoliai.	MH	L	ML
TSPO veikla SFPO veikla VKD veikla	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos. Praradus įrašus apie transakcijas ir sutartis, galimi nuostoliai.	MH	L	ML
EPĮ veikla	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos. Praradus įrašus apie transakcijas ir sutartis, galimi nuostoliai.	MH	L	ML
AML atitiktis	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos. Praradus įrašus apie transakcijas ir sutartis, galimi nuostoliai.	MH	L	ML
KYC / KYB	Visiškas paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos. Praradus įrašus apie transakcijas ir sutartis, galimi nuostoliai.	MH	L	ML
Finomark sistemos netektis				
MIP	Nėra poveikio.	L	L	L
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Visiškas SFPO paslaugos sutrikimas. Reguliacinės ir komercinės sankcijos. Praradus įrašus apie transakcijas ir sutartis, galimi nuostoliai	MH	L	ML
EPĮ veikla	Nėra poveikio.	L	L	L
AML atitiktis	Nėra poveikio.	L	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
KYC / KYB	Nėra poveikio.	L	L	L
Neopay sistemos programavimo klaida - gedimas				
MIP	Galimas trumpalaikis paslaugos sutrikimas, pranešimai Lietuvos Bankui, reputacinė žala, sutarties nutraukimas kritiniu atveju.	MH	L	ML
SIP	Galimas trumpalaikis paslaugos sutrikimas, pranešimai Lietuvos Bankui, reputacinė žala, sutarties nutraukimas kritiniu atveju.	MH	L	ML
TSPO veikla SFPO veikla VKD veikla	Nėra poveikio	L	L	L
EPĮ veikla	Nėra poveikio	L	L	L
AML atitiktis	Nėra poveikio	L	L	L
KYC / KYB	Nėra poveikio.	L	L	L
Paskolų Klubas sistemos programavimo klaida - gedimas				
MIP	Galimas paslaugos sutrikimas, sankcijų patikra operacijų metu. Tai gali turėti reputacinį arba reguliacin poveikį. Galimas tiesioginis lėšų praradimas.	MH	ML	ML
SIP	Galimas paslaugos sutrikimas, sankcijų patikra operacijų metu. Tai gali turėti reputacinį arba reguliacin poveikį. Galimas tiesioginis lėšų praradimas.	MH	ML	ML
TSPO veikla SFPO veikla VKD veikla	Galimas paslaugos sutrikimas, sankcijų patikra operacijų metu. Tai gali turėti reputacinį arba reguliacin poveikį. Galimas tiesioginis lėšų praradimas.	MH	ML	ML
EPĮ veikla	Galimas paslaugos sutrikimas, sankcijų patikra operacijų metu. Tai gali turėti reputacinį arba reguliacin poveikį. Galimas tiesioginis lėšų praradimas.	MH	ML	ML

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
AML atitiktis	Galimas paslaugos sutrikimas, sankcijų patikra operacijų metu. Tai gali turėti reputacinį arba reguliacin poveikį.	MH	ML	ML
KYC / KYB	Galimas paslaugos sutrikimas, sankcijų patikra operacijų metu. Tai gali turėti reputacinį arba reguliacin poveikį.	MH	ML	ML
Finomark sistemos programavimo klaida - gedimas				
MIP	Nėra poveikio.	L	L	L
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Galimas SFPO paslaugos sutrikimas. Tai gali turėti reputacinį arba reguliacinį poveikį	MH	ML	ML
EPĮ veikla	Nėra poveikio.	L	L	L
AML atitiktis	Nėra poveikio.	L	L	L
KYC / KYB	Nėra poveikio.	L	L	L
Ofiso patalpų neprieinamumas				
MIP	Nėra poveikio.	L	L	L
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Nėra poveikio.	L	L	L
EPĮ veikla	Nėra poveikio.	L	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
AML atitiktis	Nėra poveikio.	L	L	L
KYC / KYB	Nėra poveikio.	L	L	L
Neopay duomenų bazės netektis				
MIP	Nėra poveikio.	L	L	L
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Nėra poveikio.	L	L	L
EPĮ veikla	Nėra poveikio.	L	L	L
AML atitiktis	Nėra poveikio.	L	L	L
KYC / KYB	Nėra poveikio.	L	L	L
Paskolų Klubas duomenų bazės netektis				
MIP	Nėra poveikio.	L	L	L
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Finansinių įrašų praradimas, pilnas paslaugos sutrikimas, reguliaciniai ir finansiniai nuostoliai.	H	M	MH
EPĮ veikla	Finansinių įrašų praradimas, pilnas paslaugos sutrikimas, reguliaciniai ir finansiniai nuostoliai.	H	M	MH
AML atitiktis	Galimas neigiamas poveikis dėl ribotos apimties neatitikties. Daroma prielaida, jog duomenys paraleliai saugomi ir pas tiekėją.	ML	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
KYC / KYB	Galimas neigiamas poveikis dėl ribotos apimties neatitikties. Daroma prielaida, jog duomenys paraleliai saugomi ir pas tiekėją.	L	L	L
Finomark duomenų bazės netektis				
MIP	Nėra poveikio.	L	L	L
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	SFPO finansinių įrašų praradimas, pilnas paslaugos sutrikimas, reguliaciniai ir finansiniai nuostoliai.	H	M	MH
EPĮ veikla	Nėra poveikio.	L	L	L
AML atitiktis	Nėra poveikio.	L	L	L
KYC / KYB	Nėra poveikio.	L	L	L
AML tiekėjo sutrikimai				
MIP	Paslaugos sutrikimas, galima neatitiktis ir reguliacinės pasekmės.	ML	ML	ML
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Paslaugos sutrikimas, galima neatitiktis ir reguliacinės pasekmės.	MH	ML	ML
EPĮ veikla	Paslaugos sutrikimas, galima neatitiktis ir reguliacinės pasekmės.	MH	ML	ML
AML atitiktis.	Paslaugos sutrikimas, kuris sukelia grandininę reakciją. Galimas reguliacinis ir reputacinis poveikis.	MH	ML	ML

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
KYC / KYB	Paslaugos sutrikimas, galima neatitiktis ir reguliacinės pasekmės.	ML	ML	ML
KYC / KYB tiekėjo sutrikimai				
MIP	Nėra poveikio.	L	L	L
SIP	Nėra poveikio.	L	L	L
TSPO veikla SFPO veikla VKD veikla	Menkas sutrikimas.	ML	L	L
EPĮ veikla	Menkas sutrikimas.	ML	L	L
AML atitiktis	KYC sutrikimas gali privesti prie netinkamai atliekamos AML funkcijos ir sankcijų įgyvendinimo labai ribotu mastu.	ML	L	L
KYC / KYB	Sutinka funkcija, negalima sudaryti santykių su nauju klientu, sukeliama grandininė reakcija.	ML	L	L
Kitų kritinių paslaugų teikėjų sutrikimai arba pasitraukimas				
MIP	Mažas poveikis. Paslauga yra vidinė, automatizuota ir mažai priklausoma nuo išorės. Turimi tiekėjai yra globalūs rinkos žaidėjai.	ML	L	L
SIP	Mažas poveikis. Paslauga yra vidinė, automatizuota ir mažai priklausoma nuo išorės. Turimi tiekėjai yra globalūs rinkos žaidėjai.	ML	L	L
TSPO veikla SFPO veikla VKD veikla	Mažas poveikis. Paslauga yra vidinė, automatizuota ir mažai priklausoma nuo išorės. Turimi tiekėjai yra globalūs rinkos žaidėjai.	ML	L	L
EPĮ veikla	Mažas poveikis. Paslauga yra vidinė, automatizuota ir mažai priklausoma nuo išorės. Turimi tiekėjai yra globalūs rinkos žaidėjai.	ML	L	L

Poveikio veiklai analizė				
Pagrindinė funkcija	**Scenarijus**	**Poveikis**	**Tikimybė**	**Rizika**
AML atitiktis	Subtiekėjų valdymas yra patikėtas AML tiekėjams.	ML	L	L
KYC / KYB	Subtiekėjų valdymas yra patikėtas KYC / KYB tiekėjams.	ML	L	L

Atkūrimo laiko tikslai (RTO) ir atkūrimo taško tikslai (RPO) atitinkamiems verslo procesams apibrėžiami toliau pateiktoje lentelėje:

	Verslo procesas	RTO	RPO
1	Neopay MIP	4 val.	4 val.
2	Neopay SIP	24 val.	4 val.
3	EPĮ veikla.	4 val.	4 val.
4	TSPO ir VKD veikla.	48 val.	0
5	SFPO veikla.	48 val.	0
6	AML atitiktis	4 val.	2 val.
7	KYC / KYB	4 val.	4 val.

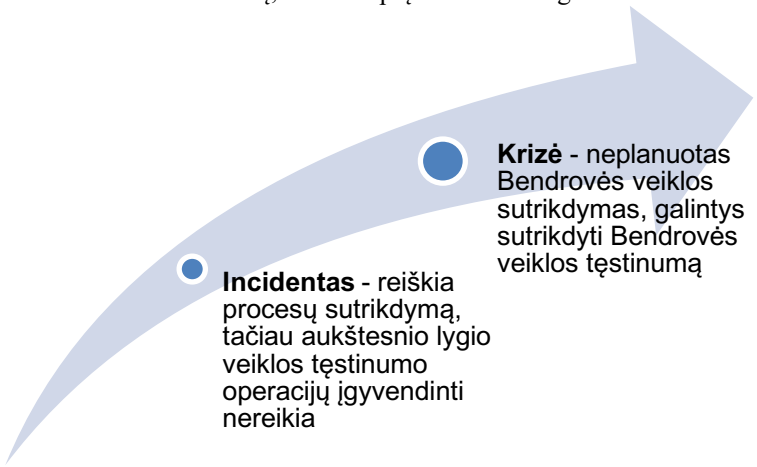
Aplinkybės ir situacijos, susijusios su Bendrovių veiklos rizikų atsiradimu, jų tikimybe, turi būti nuolat analizuojamos, siekiant užtikrinti Bendrovių veiklos tęstinumą.

VERSLO TĘSTINUMO KULTŪRA

Bendrovių veiklos tęstinumo planavimo tikslas – užkirsti kelią Bendrovių veiklos nutraukimui, išvengti ar sumažinti nuostolių, atsiradusių dėl galimų verslo sutrikimų, dydį ir kuo greičiau ir maksimaliai efektyviai atkurti Bendrovių veiklą po incidento ar krizės. Bendrovės siekia:

- Apsaugoti žmonių sveikatą ir gyvybę bei užtikrinti paslaugų tęstinumą;
- Prognozuoti galimus incidentus, krizes ir ekstremalias situacijas ir įvertinti jų poveikį Bendrovių veiklai;
- Nustatyti galimų incidentų ir krizių prevencijos priemones, veiklos tęstinumą užtikrinančias priemones ir tinkamai planuoti įmonės infrastruktūrą;
- Nustatyti alternatyvių procesų valdymo principus;
- Užtikrinti greitą reagavimą incidento ir krizės atveju ir iki minimumo sumažinti jų poveikį Bendrovėms ir klientams;
- Užtikrinti efektyvų dalijimąsi informacija Bendrovėse, su klientais, visuomene, pagrindiniais paslaugų teikėjais ir Lietuvos banku.

Bendrovės supranta kiekvieno incidento svarbą, nes neišspręsti incidentai gali sukelti rimtesnius sutrikimus / krizę.



Planas turi būti pristatytas ir jo turi laikytis visi Bendrovių darbuotojai, taip pat trečiosios šalys, turinčios prieigą prie Bendrovių informacinių sistemų ir informacijos.

INCIDENTŲ VALDYMAS IR RIZIKOS SCENARIJAI

Incidentas ar konkretus rizikos scenarijus gali turėti neigiamą poveikį informacijos prieinamumui, vientisumui ir operacinei saugai; dėl to taip pat gali būti pažeistas arba sutrikdytas veiklos tęstinumas. Bet koks incidentas gali tapti krize, jei poveikis Bendrovių veiklai būtų didelis arba ilgalaikis (ilgesnis nei RTO ir RPO verslo poveikio analizės verslo procesų vertinime).

Toliau aprašyti incidentai – galimi rizikos scenarijai, kurie gali turėti esminį poveikį Bendrovių verslui:

KRIZIŲ VALDYMAS

Krizinių situacijų valdymo tikslas – apibrėžti Bendrovių krizių valdymo ir komunikacijos veiksmus, reikalingus nedelsiant reaguoti į krizines situacijas, valdyti Bendrovių reputaciją, taip pat greitai ir efektyviai atkurti Bendrovių procesų funkcionalumą. Krizių valdymas turi būti eskaluojamas, jei Bendrovių veikla negali būti atkurta per 1 darbo dieną (24 valandas), kaip apibrėžta Poveikio verslui analizėje, taip pat jeigu fiksuojami neplanuotai dideli duomenų praradimai.

Kadangi krizė kelia didelę grėsmę Bendrovių reputacijai ir įsipareigojimams klientams ir kitoms trečiosioms šalims, darbuotojai turi būti pasirengę reaguoti greitai. Siekiant sumažinti krizės poveikį, parengiamas aiškus komunikacijos planas ir alternatyvus Bendrovių veiklos organizavimas.

Bendrovės parengė šį planą, kad išspręstų neatidėliotinus atsakui į krizę reikalavimus, kai reikia imtis specialių priemonių:

- saugoti Bendrovių reputaciją / viešąjį įvaizdį;
- sukurti veiksmingą reagavimo į krizes komandą, įskaitant išorės patarėjus;
- valdyti tiesioginius pranešimus ir informaciją apie alternatyvios Bendrovių veiklos organizavimą;
- efektyviai valdyti Bendrovių išteklius krizinėje situacijoje;
- imtis priemonių, kad kuo greičiau būtų galima atkurti Bendrovių veiklą.

Apie incidentą, kuris sukelia krizę, Verslo procesų savininkas turi pranešti Administracijos vadovui ir Krizių valdymo komitetui.

Krizių valdymo komitetas rengia neatidėliotinus posėdžius krizei įvertinti ir klasifikuoti, bendram reagavimui į krizę valdyti, priimti sprendimą dėl papildomų išteklių gavimo ir patvirtinti komunikacijos planą.

Reagavimo į krizę komandą gali sudaryti viešųjų ryšių agentūra bei tiekėjai, kuriems perduotos vykdyti veiklos funkcijos.
Priklausomai nuo krizės tipo, priskiriamos papildomos funkcinės atsakomybės:

Funkcija	Aprašymas / Užduotis
Saugos	Saugos ekspertizė, priešgaisrinės / darbo apsaugos klausimai
Informacijos sauga	Situacijos poveikio informacijos saugumui vertinimas, Krizių valdymo komiteto konsultavimas, kontaktinis asmuo visais informacijos saugumo klausimais
Technologija	Situacijos poveikio technologijoms vertinimas, Krizių valdymo komiteto konsultavimas, kontaktinis asmuo visais IT klausimais
Finansai	Finansinio poveikio vertinimas, ryšiai su draudimo bendrovėmis, bankais, būtinų finansinių sandorių koordinavimas
Rizika	Rizikos valdymo poveikio vertinimas, bendras Krizių valdymo komiteto sprendimų pasekmių būsimai Bendrovės veiklai įvertinimas
Operacijų	Situacijos poveikio Bendrovės veiklai vertinimas, Krizių valdymo komiteto konsultavimas, kontaktinis asmuo visais veiklos klausimais
Komunikacijos	Trečiųjų šalių atstovai, kurie turėtų būti įtraukti kaip išoriniai patarėjai (t.y. viešųjų ryšių agentūra), yra tiesiogiai atsakingi už incidentų pašalinimą (t.y. IT paslaugų teikėjai)

Krizių valdymo komitetas peržiūrėti paveiktas Bendrovės veiklos sritis, įvertina atsakingų funkcijų pasiūlymus ir patvirtina veiksmų seką.

Pagal krizės tipą turėtų būti priimtas sprendimas dėl alternatyvių Bendrovių veiklos organizavimo būdų.

Turi būti peržiūrimas visų galimų sudedamųjų dalių, kurios turi būti sprendžiamos krizės metu, sąrašas.

KOMUNIKACIJOS ATSAKOMYBĖS

Komunikacijos prioritetai ir atsakomybės yra tokie:

- Kiekvienas darbuotojas - praneša savo tiesioginiam vadovui apie situaciją, pastebėtus sutrikimus. Darbuotojams draudžiama plačiau komunikuoti.
- Skyriaus vadovai - komunikuoja su administracijos vadovu, administracijos vadovo pavaduotoju, pavaldžiu tiekėju, aiškinasi situaciją su kitų skyrių vadovais. Taip pat, esant poreikiui organizuoja alternatyvų skyriaus darbą, krizės sąlygomis.
- Administracijos vadovas ar jo įgaliotas pavaduotojas - komunikuoja su valdyba, išoriniais tiekėjais, valdo išorinę komunikaciją, koordinuoja komunikaciją su reguliatoriumi.
- Marketingo ir komunikacijos skyriaus vadovas (Paskolų klube) / Komercijos vadovas (Neopay) / Direktorius (Finomark) - komunikuoja su paveiktais klientais pagal administracijos vadovo ar jo įgalioto pavaduotojo nurodymus.
- Teisės skyriaus vadovas - komunikuoja su reguliatoriumi, padeda administracijos vadovui ir/ar jo įgaliotam pavaduotojui priimti sprendimą.
- Informacijos saugos pareigūnas - pataria administracijos vadovui ir/ar jo įgaliotam pavaduotojui, konsultuoja problemos sprendimo ir sutrikimų šalinimo klausimais.
- Bendrovės valdyba - yra informuojama apie krizę, sprendimus, komunikaciją.

KOMUNIKACIJA SU LIETUVOS BANKU

Lietuvos Bankas yra informuojamas, jeigu yra pasiekiamos šioje lentelėje esančios sutrikimo reikšmės.

	Didelis MOSRI	
Poveikio lygis	Mažesnis poveikio lygis	Didesnis poveikio lygis
Kriterijų skaičius	**3 ir >**	**1 ir >**
Kriterijai		
1. Paveiktos operacijos	> 10 % mokėjimo paslaugų teikėjo įprasto operacijų lygio (pagal operacijų skaičių) ir MOSRI trukmė > 1 valanda[1] **arba** > 500 000 Eur ir MOSRI trukmė > 1 valanda	> 25 % mokėjimo paslaugų teikėjo įprasto operacijų lygio (pagal operacijų skaičių) **arba** > 15 mln. Eur
2. Paveikti mokėjimo paslaugų vartotojai	> 5 000 ir MOSRI trukmė > 1 valanda **arba** > 10 % mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojų ir MOSRI trukmė > 1 valanda	> 50 000 **arba** > 25 % mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojų
3. Paslaugos neveikimo laikas	> 2 valandos	Netaikoma
4. Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba susiję infrastruktūros objektai	Taip	Netaikoma
5. Poveikis reputacijai	Taip	Netaikoma
6. Ekonominis poveikis	Netaikoma	> Maks. (0,1 % 1 lygio kapitalo[2], 200 000 Eur) **arba** > 5 mln. Eur
7. Aukšto lygio vidinė sklaida	Taip	Taip, ir tikriausiai bus pradėta dirbti kriziniu (arba lygiaverčiu) režimu
8. Tinklų ir informacinių sistemų saugumo pažeidimas	Taip	Netaikoma

ALTERNATYVIOS BENDROVIŲ VEIKLOS ORGANIZAVIMAS

Tais atvejais, kai veiklos tęstinumas esamose Bendrovių patalpose yra laikinai neįmanomas, tačiau bus atkurtas, situacijai spręsti naudojamos šios priemonės:

- Jeigu veiklos susigrąžinimo laikotarpis yra trumpas, t. y. iki 48 valandų, netikslinga skirti lėšų daliniam ar visiškam operacijų perdavimui į alternatyvią infrastruktūrą;
- Tuo atveju, kai esamos patalpos negali būti naudojamos, darbuotojai dirba iš namų.

SUTRIKIMŲ REGISTRAVIMAS IR ATASKAITŲ TEIKIMAS

Visi incidentai turi būti registruojami Bendrovių operacinės ar saugumo rizikos įvykių (incidentų) registre. Darbuotojų veiksmai pranešant apie incidentus, atsitiktines ekstremalias situacijas ir krizes, atkuriant veiklos tęstinumą:

- Incidentų atveju – pranešimo veiksmus atlieka proceso savininkas. Apie sutrikimus pranešama visiems IS naudotojams ir IT projektų vadovui (Paskolų klubas); Produkto vadovui (Neopay) / Direktoriui (Finomark);
- Informaciją apie didelį su mokėjimo paslaugų teikimu susijusį operacinį ar saugumo rizikos incidentą teikiama Administracijos vadovo sprendimu pagal KOMUNIKACIJA SU LIETUVOS BANKU parametrus, naudojant REGATA platformą - https://regata.lb.lt/ .
- Apie incidentus, susijusius su informacijos saugumu, turi būti informuotas CISO.

VEIKLOS TĘSTINUMO PLANO VERTINIMAS IR NUOLATINIS TOBULINIMAS

Kontrolės priemonių, komunikacijos ir kompetencijų veiksmingumas peržiūrimas kartą per metus atliekant plano testavimus. Testavimuose dalyvauja atsakingi darbuotojai, tiekėjai. Testavimo scenarijų organizuoja CISO su Administracijos vadovu ar jo įgaliotu pavaduotoju.

Atliekant testavimus, reikėtų įvertinti komunikacijos efektyvumą, galimybę laiku ir efektyviai koordinuoti veiklą, turimus įrankius ir kompetencijas, ar veiklos procesai ir palaikantys ištekliai gali būti atstatyti per plane numatytą laiką (RTO/RPO).

Vertinimo rezultatai turėtų būti dokumentuojami. Trūkumai turi būti aprašyti kuo konkrečiau, kad prireikus būtų įtraukti sisteminiai patobulinimai. Identifikuotų trūkumų šalinimas turi būti reguliariai stebimas.

Verslo tęstinumo planas turėtų būti tikrinamas bent kartą per metus.

CISO yra atsakingas už veiklos tęstinumo plano rengimą ir periodinę peržiūrą, taip pat už planų testavimo ir bandymų rezultatų dokumentacijos organizavimą.

Atlikus testavimus CISO, administracijos vadovas ir/ar jo įgaliotas pavaduotojas, skyrių vadovai įvertina testavimą ir pateikia jo rezultatus Valdybai ne vėliau kaip per dvidešimt darbo dienų.

GALUTINĖS NUOSTATOS

Planas įsigalioja, kai jį patvirtina Bendrovės valdyba.

Planas tikslinamas atsižvelgiant į teisinio reguliavimo pakeitimus, organizacinius pokyčius, tačiau ne rečiau kaip kartą per metus.

Planas kasmet tikrinamas pagal rizikos scenarijus.

Skyrių vadovai supažindinami su Planu.

Bendrovės vadovas yra atsakingas už bendrą plano įgyvendinimą. Plano nuostatos, susijusios su informacinėmis technologijomis, įgyvendinamos ir atitinkamą kontrolę užtikrina skyrių vadovai, nuostatos, susijusios su informacijos saugumu, įgyvendinamu ir atitinkamą kontrolę užtikrina CISO, su operacine rizika susijusios nuostatos įgyvendinamos, ir atitinkamą kontrolę užtikrina Rizikos pareigūnas.

PRIEDAS NR. 1. KRIZIŲ VALDYMO GRUPĖS NARIŲ STRUKTŪRA IR KONTAKTAI

[KONFIDENCIALU]

PRIEDAS NR. 2. SAUGUMO IR KITŲ SPECIALIŲJŲ TARNYBŲ BEI INSTITUCIJŲ, APIE KURIUOS TURI BŪTI PRANEŠTA APIE INCIDENTUS, KONTAKTAI

Nr.	Institucijos pavadinimas	Kontaktai	Tema
1	Lietuvos bankas	Totorių g. 4, LT-01121 Vilnius Tel.: +370 800 50 500	Pranešimai apie incidentus, dėl kurių sutrikdomos arba nutraukiamos Banko paslaugos
2	Valstybinė duomenų apsauga inspekcija	L. Sapiegos g. 17, 10312 Vilnius Tel.: +370 5 271 2804, +370 5 279 1445 El. paštas ada@ada.lt.	Pranešimas apie incidentus, susijusius su asmens duomenų saugumo pažeidimais
2	Nacionalinis kibernetinio saugumo centras	Gedimino pr. 40, Vilnius Įmonės kodas 191630942 Tel. +370 706 84116 El. paštas: info@nksc.lt Pranešti apie incidentą galima užpildant specialią formą arba rašant el. Pašto adresu cert@nksc.lt, arba skambinant telefonu 1843.	Pranešimas apie incidentus, įvykusius viešųjų elektroninių ryšių kanaluose ir (arba) informacinėse sistemose
3	Reagavimo į ekstremalias situacijas centras	Tel.: 112	Pranešimas apie pažeidimus /incidentus, susijusius su Bendrovės patalpomis, kitus pažeidimus /incidentus, keliančius grėsmę Bendrovės ir jos patalpų darbuotojams ir klientams (policijai, priešgaisrinei saugos ir gelbėjimo tarnybai, Greitosios medicinos pagalbos tarnybai)

PRIEDAS NR. 3. PASLAUGŲ TEIKĖJŲ KONTAKTAI, SVARBIAUSI BENDROVĖS VEIKLOS TĘSTINUMUI
[KONFIDENCIALU].