Veiklos rizikos

Operacinė rizika – tai rizika patirti nuostolių dėl netinkamų arba neįgyvendintų Bendrovės vidaus kontrolės procesų, darbuotojų klaidų ir neteisėtų veiksmų bei informacinių sistemų veiklos sutrikimų arba dėl išorės įvykių įtakos. Pagrindiniai operacinės rizikos šaltiniai: informacinės sistemos (techninės ir programinės įrangos, telekomunikacinių sistemų sutrikimai ir kt.); žmogaus įtaka (Bendrovės darbuotojų ir ne Bendrovės darbuotojų neteisėti veiksmai); darbo sąlygos (saugių darbo sąlygų pažeidimas ir kt.); klaidos (neteisingų duomenų įvedimas, netinkami teisiniai dokumentai ir kt.).

Virtualių duomenų netekimo rizika – tai rizika, kad Bendrovės sistemose saugomi duomenys bus prarasti ar kitaip paveikti, kad nebebūtų galima jų atkurti.

Fizinio pavojaus rizika – tai rizika, kad Bendrovės arba trečiųjų šalių, kurioms Bendrovė yra perdavusi vykdyti savo funkcijas, turtui bus padaryta fizinė žala (sužalojant, sunaikinant arba pagrobiant turtą), ir dėl to Bendrovės veikla bus sutrikdyta.

Likvidumo rizika – tai rizika, kad Bendrovė nesugebės laiku įvykdyti finansinių įsipareigojimų, pasireiškianti laikinu arba nuolatiniu Bendrovės nemokumu ir kraštutiniu atveju – bankroto bylos Bendrovei iškėlimu.

Valdymo rizika – tai rizika, kad dėl netinkamo Bendrovės ar atskirų jos vykdomų projektų valdymo Bendrovei ar tretiesiems asmenims bus padaryta žala.

Reputacijos rizika – tai rizika, galinti neigiamai paveikti Bendrovės pajamas ir kapitalą dėl nepalankios klientų, sandorio šalių, investuotojų nuomonės apie Bendrovės reputaciją.

Licencijų netekimo arba veiklos apribojimo rizika – tai rizika, kad Bendrovė neteks elektroninių pinigų įstaigos licencijos, suteikiančios teisę verstis elektroninių pinigų įstaigos veikla; bus išbraukta iš viešojo vartojimo kredito davėjų ir viešojo tarpusavio skolinimo platformos operatorių sąrašų, suteikiančių teises verstis TSPO ir vartojimo kreditų teikimo veiklomis; bus apribota Bendrovės teisė teikti paslaugas aukščiau nurodytais pagrindais ir dėl to Bendrovė nebegalės tinkamai administruoti sudarytų VK sutarčių ir Klientų mokėjimų pagal šias sutartis, laikinai leisti elektroninių pinigų arba teikti vieną ar kelias mokėjimo paslaugas.

Strateginė rizika – tai rizika, kylanti dėl išorės ir vidaus aplinkos veiksnių, galinčių turėti neigiamą įtaką įgyvendinant Bendrovės tikslus, užtikrinant veiklos nuoseklumą ir tęstinumą dėl klaidingo vertinimo arba jo nebuvimo.

Veiklos rizikų valdymo būdai

Ši plano dalis nustato procesus, priemones ir procedūras, kurios taikomos siekiant išvengti arba sumažinti Plano– punktuose nurodytų rizikų pasireiškimą Bendrovės veikloje.

Operacinė rizika yra valdoma žemiau išvardintais būdais.

Parengiant ir su Priežiūros institucija suderinant Bendrovės vidaus kontrolės ir operacinės rizikos valdymo taisykles bei aprašus (Bendrovė atliko tai prieš gaudama Licenciją).

Bendrovės sistemos yra suprogramuotos ir veikiančios taip, kad šiomis sistemomis besinaudojantis darbuotojas negalėtų atlikti tyčinių ar netyčinių apgaulės veiksmų, pavyzdžiui, sukurti fiktyvių Klientų, sudaryti fiktyvių VK (verslo kreditų) sutarčių ir kt. Informacinės sistemos aprašas yra pateiktas Priežiūros institucijai prieš gaunant Licenciją.

Užtikrinant, kad Bendrovės sistemos ir kita Bendrovės veikloje naudojama programinė bei tinklo ir ryšio įranga yra apsaugota nuo programinių virusų, kibernetinių atakų bei kitų nefizinių žalos šaltinių.

Užtikrinant, kad laikinas elektros energijos nepasiekiamumas dėl naudojamų apsaugos priemonių (naudojamų papildomų nenutrūkstamo maitinimo šaltinių) nesukeltų žalos Plane nurodytiems įrenginiams, įrangai ir Serveriams.
Sudarant sutartį su trečiaisiais asmenimis, kurie užtikrina darbo saugą įmonėse. Trečioji šalis parengia tinkamas vidaus taisykles ir procedūras siekiant, kad nebūtų pažeisti tinkamų ir saugių darbo sąlygų reikalavimai ir užtikrinama tinkama ir saugi darbo aplinka.
Su visais Bendrovės darbuotojais pasirašant materialinės atsakomybės sutartis, kuriose numatyta kiekvieno Bendrovės darbuotojo materialinė atsakomybė už jo tyčiniais ar netyčiniais veiksmais sukeltą žalą Bendrovei.
Užtikrinant sudarytų sutarčių saugumą. Visos naudojantis Sistema sudarytos sutartys yra saugomos Sistemoje; sutartys, kurios sudarytos nesinaudojant Sistema, yra saugomos fiziniu pavidalu Bendrovės buveinėje. Sutartims taikomas 10 metų saugojimo senaties terminas, skaičiuojant nuo visiško sutarties įvykdymo dienos.
Reguliariai atliekant operacinės ir saugumo rizikų vidaus auditą, atnaujinant operacinės rizikos valdymą nustatančių taisyklių redakcijas bei patikrinant ir patobulinant Bendrovėje veikiančius operacinę riziką valdančius procesus.
Garantuotos paslaugų kokybės lygis (angl. Service-level agreement (SLA) pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą, nustatomas atskirose sutartyse su paslaugų teikėjais.
Paskiriant duomenų apsaugos pareigūną, kuris atsakingas už asmens duomenų apsaugos reikalavimų laikymąsi pagal Bendrąjį duomenų apsaugos reglamentą.
Paskiriant informacijos saugos specialistą, kuris atsakingas už informacinės saugos programos valdymą ir atnaujinimą, informacijos saugumo ir kibernetinio saugumo rizikų identifikavimą ir jų pašalinimą.
Paskiriant atitikties specialistą, kuris atsakingas už Bendrovės veiklų priežiūrą, vadybą ir organizavimą taip, kad visos Bendrovės veiklos atitiktų galiojančių teisės aktų reikalavimus.

Sistemos virtualių duomenų netekimo rizika eliminuojama žemiau išvardintais būdais:

Patvirtinta 2021-05-20 d. „Procentas“ UAB administracijos vadovo įsakymu Nr. IS2021-5/23
Duomenų kopijos yra daromos naudojant FORGE programinę įrangą, kuri užtikrina naudojamų kopijų integralumą ir kuria automatines duomenų bazės ir serverio failų atsargines kopijas (incremental backups). Duomenų bazių kopijos yra daromos toliau nurodyta tvarka:
kiekvieną naktį 3 valandą daroma virtualios mašinos kopija į dvi lokacijas: (i) lokalią serverio repozitoriją; ii) nutolusį serverių masyvą;
kiekvieną sekmadienį atliekama pilna serverio failų ir duombazes kopija kopija (angl. full copy), kurios yra saugomos nutolusiame serveryje, skirtingame disko masyve, tame pačiame duomenų centro masyve;
kiekvieną dieną Bendrovė duomenis apie visas naudojantis Sistema sudarytas VK sutartis su detalia informacija apie jų vykdymą perduoda UAB „Creditinfo Lietuva“, administruojančiai jungtinę skolininkų ir finansinių įsipareigojimų duomenų rinkmeną ir užtikrinančiai duomenų apie per Sistemą sudarytas ir vykdomas VK sutartis saugumą.
ABD sistemos virtualių duomenų netekimo rizika eliminuojama žemiau išvardintais būdais.
Darant visų ABD sistemos duomenų kopijas remiamasi plačiai paplitusia taisykle „3-2-1“, pagal kurią privaloma turėti bent tris duomenų kopijas, kurios yra laikomos dviejuose skirtinguose

diskų lygiuose, viena duomenų kopija turi būti nutolusi. Duomenų kopijos yra daromas toliau nurodyta tvarka:
kiekvieną kalendorinę dieną yra daromos duomenų bazės kopijos (angl. incremental) ir saugomos pagrindiniame Serveryje;
kiekvieną dieną praėjusios dienos informacija persiunčiama į nutolusį serverį;
paskutinių 30 dienų duomenų kopijos yra saugomos dviejuose atskiruose nuotoliniuose serveriuose.
Visos ABD sistemos duomenų kopijos yra saugomos nuo pagrindinių Serverių [DIGITAL OCEAN] nutolusiuose serveriuose. Tokiu būdu užtikrinama, kad, dėl fizinio poveikio praradus prieigą prie pagrindinių Serverių ar dėl kitų priežasčių negalint atkurti jose esančių duomenų, tas pats fizinis poveikis nepaveiks nutolusių serverių, kuriuose saugomos duomenų kopijos.

Bendorvės mokumo problemų ir bankroto rizika

Jeigu Bendrovė susiduria su nekontroliuojamomis mokumo problemomis, Bendrovei iškyla reali bankroto rizika ar dėl kitų priežasčių atsiranda rizika, kad Bendrovė nebegalės tęsti sutelktinio finansavimo veiklos, Bendrovė imasi sekančių žingsnių:
pirmiausia, Bendrovė apie šią situaciją nedelsiant informuoja Lietuvos banką (priežiūros instituciją), detalizuodama esamus rizikos lygį, pasitelktas ar planuojamas pasitelkti rizikos valdymo priemones bei veiklos tęstinumą užtikrinančias priemones;
antra, Bendrovė nedelsiant apie atitinkamą situaciją informuoja visus savo klientus (Finansuotojus ir Projektų savininkus);
trečia, Bendrovė nedelsiant atšaukia Platformoje paskelbtus Projektus, kuriems renkamas finansavimas, taip pat nebesudaro ir nebesuteikia galimybės sudaryti naujų sutelktinio finansavimo sandorių (tokių Finansuotojų lėšos yra grąžinamos atgal šiems Finansuotojams);
ketvirta, Bendrovė nedelsiant sustabdo Platformoje funkcionuojančią antrinę reikalavimo teisių perleidimo rinką; galiausiai, Platformos administravimas nedelsiant perduodamas kitam platformos operatoriui, kuris galėtų užtikrinti jos veiklos tęstinumą.