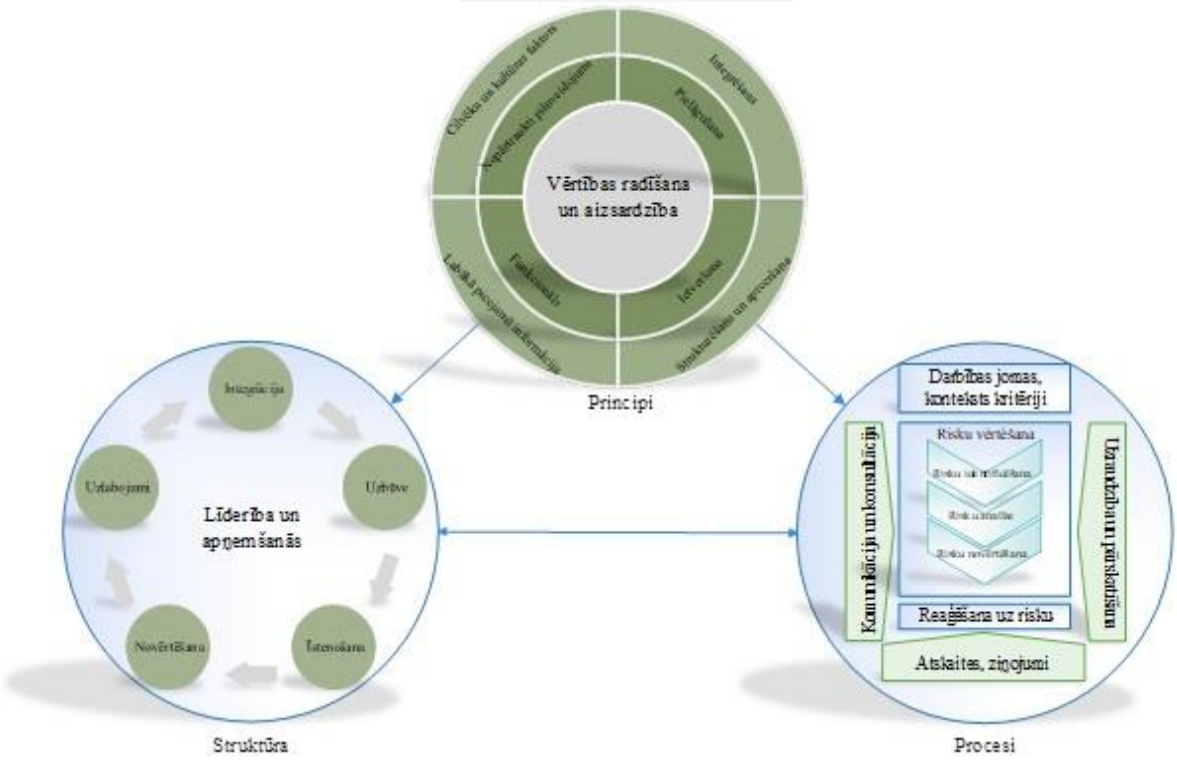
APSTIPRINĀTA
ar VAS "Ceļu satiksmes drošības direkcija"
2024.gada 18. janvārī
padomes lēmumu (prot. Nr.1 , 7.1.§)

Risku vadības politika

I. Risku vadības politikas mērķis

1. Risku vadības politikas mērķis ir piemērot risku vadības labo praksi visā organizācijā, lai līdzsvarotu riskus, iekļaujot risku vadības praksi vadības un plānošanas aktivitātēs. Risku vadība ietver sekojošus principus, struktūru, procesu:



2. Politika ir izstrādāta, lai nodrošinātu:
   2.1. vienotu risku vadības sistēmu CSDD;
   2.2. augstākās vadības uz zināšanām par riskiem un prioritātēm balstītu aktīvu un strukturētu rīcību, lai radītu pārliecību par organizācijas mērķu sasniegšanu;
   2.3. visu līmeņu vadītāju aktīvu un mērķtiecīgu rīcību, izplatot izpratni par riskiem un to prioritātēm visā organizācijā;
   2.4. organizācijas darbības plānošanas un risku vadības sistēmas lietderīgu un efektīvu darbību;
   2.5. noteiktu atbildību un atbilstošas pilnvaras risku vadības realizēšanai;
   2.6. optimāli izmantotus resursus risku vadībai;
   2.7. specifisko risku vadības jomu uzskaiti, normatīvos dokumentus šo risku pārvaldībā un rezultātu ietveršanu kopējā iestādes risku sarakstā;

2.8. kontroles mehānismus risku ierobežošanā uzskaiti, normatīvos dokumentus kontroļu efektivitātes izvērtēšanā.

II. Organizācijas risku vadība

3. **Risks** ir tāda notikuma vai apstākļu iespējamība, kas radītu negatīvu ietekmi uz CSDD mērķu sasniegšanu (jo īpaši, zaudējumus CSDD vai negatīvu ietekmi uz CSDD funkciju veikšanu/pakalpojumu sniegšanu), risku vērtē ietekmes un varbūtības izteiksmē. Riski tiek reģistrēti CSDD risku reģistrā.

4. **Riska avots** ir elements, kurš atsevišķi vai kombinācijā ar citiem rada risku vai potenciālu riska pieaugumu.

5. **Riska notikums** ir specifisku apstākļu atgadījums ar ietekmi uz CSDD mērķu sasniegšanu:

5.1. notikums var būt viens vai virkne atgadījumu un tam var būt dažādi cēloņi;

5.2. notikums var būt kaut kas, kas nenotiek, bet būtu jānotiek (t.sk. novirzes procesu vai procedūru izpildē);

5.3. riska notikums var tikt nosaukts par "notikumu", "incidentu" vai "negadījumu". Notikumiem var būt gan pozitīva, gan negatīva ietekme uz CSDD mērķu sasniegšanu, savukārt incidenti ir negatīvi notikumi. Atsevišķām risku grupām var tikt piemērotas specifiskas riska notikuma un/vai incidenta definīcijas, piemēram, terminu "informācijas tehnoloģiju drošības incidents" definē Informācijas tehnoloģiju drošības likums;

5.4. noteiktiem riskiem (risku apakšgrupām un/vai risku grupām) var tikt noteikta prasība visus notikušos (riska) notikumus un/vai incidentus reģistrēt, klasificēt (pēc to cēloņiem, jomām, ietekmes smaguma u.tml.), nodot atbildīgajiem darbiniekiem rīcībām noviržu novēršanai, tālākai analīzei, korektīvām un preventīvām darbībām. Atsevišķiem riskiem (risku apakšgrupām un/vai risku grupām) var būt noteiktas specifiskas vai papildus prasības attiecībā uz rīcību risku notikumu un/vai incidentu gadījumā, piemēram, Informācijas tehnoloģiju drošības likums nosaka rīcību informācijas tehnoloģiju drošības incidenta gadījumā. Gadījumos, kad ir noteikta prasība reģistrēt riska notikumus, riska īpašnieks nosaka formu un nodrošina informācijas resursus notikumu un/vai incidentu reģistrācijai un apstrādei, nosaka par riska notikumu reģistrēšanu (un apstrādi) atbildīgo darbinieku/-us un kārtību kādā tiek apkopota informācija par notikušajiem riska notikumiem un tās izmantošanu atbilstošā riska analīzei (analīzes aktualizēšanai).

6. **Risku apetīte** ir risku apjoms, ko CSDD ir gatava pieņemt, lai sasniegtu tās stratēģiskos mērķus. CSDD apzinās, ka ne visus riskus ir iespējams mazināt un ka noteiktu risku tālāka mazināšana var nebūt lietderīga.

7. **Risku vadības grupa** tiek izveidota ar CSDD valdes lēmumu, ar kuru tiek noteikti Risku vadības grupas locekļi. Risku vadības grupa koordinē CSDD riska pārvaldības metodikas izmaiņas un procesus, lai nodrošinātu visaptverošu un homogēnu pieeju un izpratni par risku vadību visās risku grupās un apakšgrupās un kopīgi risinātu risku vadības problēmas.

8. **Riska īpašnieks** ir struktūrvienības vadītājs vai speciāli pilnvarota persona, kas atbild par konkrētā riska analizēšanu, novērtēšanu, kontroles pasākumu un izpildes termiņu noteikšanu, kā arī riska mazinošo pasākumu īstenošanu saskaņā ar valdes pilnvarojumu.

9. **Risku vadības speciālists** ir darbinieks vai speciāli pilnvarota persona, kas koordinē riska vadības aktivitātes struktūrvienībās, saskaņā ar amata aprakstā noteiktajiem darba pienākumiem.

10. **Iekšējā kontrole** ir organizācijas pārvaldības mehānismi, t.sk. politikas, procedūras un procesi, kurus īsteno CSDD vadība un personāls (Risku vadības kontekstā iekšējās kontroles var tikt sauktas arī par riska kontrolēm jeb pasākumiem/aktivitātēm riska vadībai):

10.1. lai nodrošinātu pārliecību par CSDD mērķu sasniegšanu attiecībā uz CSDD darbības efektivitāti un lietderību;

10.2. lai nodrošinātu atskaitīšanos (savlaicīgumu, pilnīgumu un precizitāti);

10.3. lai nodrošinātu atbilstību (normatīvajiem aktiem un citiem saistošajiem dokumentiem);

10.4. lai izmainītu risku.

11. **Risku vadības sistēma** – CSDD izmantotās prakses, rīku un metožu kombinācija, lai identificētu, analizētu, novērtētu, mazinātu un pārvaldītu riskus.

12. **Risku vadības jeb risku pārvaldības process** ir sistēmiska vadības politikas, procedūru un prakses pilnveidošana un pielietošana attiecībā uz saziņu, konsultēšanu, satura noteikšanu un risku identificēšanu, analīzi, novērtēšanu, lēmuma pieņemšanu, uzraudzību, riska pārskatīšanu. Organizācijas risku vadības process ir attiecināms uz visu CSDD darbību:

12.1. **Riska vērtēšana** *(angl. Risk assessment)* ir riska identificēšanas, riska analīzes un riska novērtēšanas process:

12.1.1. **riska identificēšana** ir risku atrašanas, atpazīšanas un pierakstīšanas process;

12.1.2. **riska analīze** ir informācijas sistemātiska pielietojuma process, lai noteiktu riska varbūtību, ietekmi un līmeni (aplēses veidā);

12.1.3. **riska novērtēšana** ir risku analīzes rezultātu un risku apetītes kritēriju salīdzināšanas process, lai noteiktu vai risks ir akceptējams vai maināms.

12.2. **Reaģēšana uz risku** ir veiktās aktivitātes, lai izveidotu situāciju, kurā pakļaušanās riska iedarbībai organizācijai ir pieņemama. Reaģēšana ietver izvairīšanos no riska, riska avota likvidēšanu, riska samazināšanu, izmainot riska varbūtību un/vai ietekmi, riska sadalīšanu, apzinātu riska pieņemšanu:

12.2.1. **izvairīšanās no riska** – parasti ietver atteikšanos no aktivitātes vai izmaiņas funkcijā/procesā, iepirkumu plānošanā, aktivitāšu secībā, kā rezultātā riska avotam vairs nav ietekmes vai arī **riska avots tiek likvidēts**;

12.2.2. **riska samazināšana izmainot riska varbūtību un/vai ietekmi** - piemēram radot un ieviešot piemērotas iekšējās kontroles, izstrādājot alternatīvu rīcības plānu riska iestāšanās gadījumam;

12.2.3. **riska sadalīšana** - *(angl. Risk sharing)* riska nodošana trešajām personām, piemēram, nododot daļu funkcijas/procesa ārpakalpojumā vai risku apdrošināšana;

12.2.4. **apzināta riska pieņemšana** - tiek veikta gadījumos, kad riska mazināšanas pasākumi tiek novērtēti kā ekonomiski neizdevīgi, tādēļ tiek pieņemts lēmums par riska saglabāšanu, turpinot to uzraudzīt un kontrolēt.

13. Visi CSDD riski tiek sadalīti šādās četrās grupās (pielikums Nr.1):

13.1. **Finanšu risku grupa** ietver iespējas ciest zaudējumus saistībā ar neparedzētām izmaiņām finanšu jomā. Finanšu risks ir saistīts ar finanšu instrumentiem, līgumsaistībām, procentu likmēm, valūtu kursa svārstībām, inflāciju un citiem apstākļiem, kuru dēļ kapitālsabiedrības plānotās izmaksas var būtiski atšķirties no reālajām, kā arī nodokļu riskus;

13.2. **Reputācijas un atbilstības risku grupa** ietver riskus saistībā ar starptautisko, ES un Latvijas normatīvo aktu prasību neizpildi, sabiedrības negatīvu viedokli par CSDD, t.sk. ietver pretkorupcijas un interešu konflikta riskus;

13.3. **Operacionālo risku grupa** ietver riskus ciest zaudējumus no neatbilstošas vai nepilnīgas iekšējo procesu norises, cilvēku un sistēmu darbības vai arī ārējo apstākļu ietekmes dēļ t.sk. Informācijas drošības riskus un Darba vides riskus;

13.4. **Stratēģisko risku grupa** ietver riskus ciest zaudējumus, kas rodas, pieļaujot kļūdas saistībā ar CSDD stratēģisko darbību un attīstību noteicošu lēmumu pieņemšanu, nepareizi vai nepietiekami pamatoti nosakot CSDD darbības perspektīvos virzienus vai nesasniedzot CSDD stratēģiskos mērķus.

III. Organizācijas risku vadība

Atbildība un pilnvaras

14. **CSDD padome**:

14.1. pārrauga risku vadības sistēmas darbību, pārskata tās atbilstību un efektivitāti;

14.2. apstiprina un regulāri pārskata risku vadības politiku;

14.3. pārrauga atbilstību nodrošinošos kontroles pasākumus/sistēmas (sistēmas, kas paredzētas, lai nodrošinātu, ka CSDD ievēro spēkā esošos normatīvos aktus, tai skaitā nodokļu, konkurences, darba, vides, vienādu iespēju, darba un drošības normatīvos aktus);

14.4. izskata valdes iesniegtos ziņojumus par risku vadību.

15. **CSDD valde**:

15.1. regulāri pārskata risku vadības politiku un sagatavo priekšlikumus politikas labojumiem;

15.2. uzrauga galveno risku vadību;

15.3. periodiski pārskata CSDD pieeju risku vadībai;

15.4. novērtē risku vadības atbilstību CSDD mērķiem;

15.5. novērtē līmeni līdz kuram risku vadība tiks iekļauta CSDD procesos un procedūrās;

15.6. apstiprina un regulāri pārskata CSDD risku apetīti;

15.7. novērtē efektivitāti risku vadības pieejai;

15.8. pārliecinās par resursu pietiekamību;

15.9. izskata Risku vadības grupas sagatavoto ziņojumu un regulāri (ne retāk kā divas reizes kalendārajā gadā) sagatavo ziņojumu izskatīšanai padomē. Pēc nepieciešamības ziņo citām ieinteresētajām pusēm par risku vadību.

16. **Risku vadības grupa**:

16.1. izskata un apstiprina risku īpašnieku sagatavotos risku vērtēšanas rezultātus, nepieciešamības gadījumā iesakot korekcijas vai papildinājumus risku analīzes rezultātos un/vai risku vadības kontrolēs;

16.2. izstrādā risku vērtēšanas metodiku;

16.3. nodrošina un pārrauga risku vērtēšanas procesu;

16.4. atbild par stratēģisko risku vadību un veic stratēģisko risku un to kontroļu identificēšanu un analīzi;

16.5. regulāri (ne retāk kā divas reizes kalendārajā gadā) ziņo CSDD valdei un padomei:

16.5.1. par situāciju risku vadības jomā;

16.5.2. par risku analīzes un novērtēšanas rezultātiem un galvenajiem riskiem;

16.5.3. par risku vadības problēmām (tikai par būtiskām);

16.6. sagatavo informāciju publiskošanai CSDD mājaslapā internetā par paredzamiem riska faktoriem.

17. **Informācijas sistēmu drošības komiteja**:

17.1. informācijas sistēmu drošības komitejas pamatfunkcijas ir noteiktas CSDD Informācijas drošības politikā, kas nosaka, ka Informācijas sistēmu drošības komiteja pārrauga un nodrošina informācijas drošības risku vadību;

17.2. informācijas sistēmu drošības komiteja sadarbojas ar Risku vadības grupu, lai harmonizētu Informācijas sistēmu drošības jomas CSDD iekšējo normatīvo aktu prasības ar CSDD kopējās risku vadības prasībām, kā arī Informācijas sistēmu drošības komiteja informē Risku vadības grupu par galvenajiem informācijas sistēmu drošības riskiem un to vadības problēmām (tikai par būtiskām).

18. **Iekšējā audita daļa**:

18.1. auditos neatkarīgi vērtē riskus un kontroles;

18.2. par audita rezultātiem ziņo CSDD valdei un padomei.

19. **Riska īpašnieks**:

19.1. veic risku sākotnējo novērtējumu, dokumentējot to CSDD risku reģistrā;

19.2. seko atbilstošu kontroles pasākumu dokumentēšanai, ieviešanai un uzturēšanai (kā arī, ja riska īpašnieka pārziņā esošajai risku grupai nepieciešama (piem. šādu prasību nosaka ārējie normatīvie akti) papildus dokumentācija, iekšējie noteikumi, regulāras apmācības u.tml., nodrošina šādas dokumentācijas izstrādi un uzturēšanu, māca/ organizē mācības darbiniekiem vai veic citas noteiktās aktivitātes);

19.3. uzrauga risku, tā statusa izmaiņas un koordinē kontroles pasākumu izmaiņas;

19.4. ziņo Risku vadības grupai par riska izmaiņām, riska kontroļu efektivitāti un risku vadības problēmām.

20. **Risku vadības speciālists**:

20.1. sniedz konsultācijas CSDD struktūrvienībām risku pārvaldībā un kontrolē;

20.2. izstrādā iekšējo normatīvo aktu risku vadības jomā projektus, seko līdzi CSDD procesu atbilstībai normatīvajiem aktiem;

20.3. nodrošina riska vadības procesu koordinēšanu CSDD un ir kontaktpersona šo jautājumu risināšanai CSDD struktūrvienībās;

20.4. sagatavo pārskatu par risku vadības aktualitātēm projektus izskatīšanai Risku vadības grupā;

20.5. sagatavo informāciju publiskošanai CSDD mājaslapā internetā par paredzamiem riska faktoriem.

21. **Katrs darbinieks**:

21.1. veic noteiktos uzdevumus saskaņā ar normatīvajiem dokumentiem un darba uzdevumiem;

21.2. ziņo tiešajam vadītājam, riska īpašniekam vai attiecīgi nozīmētam darbiniekam par risku notikumiem, incidentiem, konstatētajiem trūkumiem risku kontrolēs un/vai risku vadības procesā.

IV. Noslēguma jautājums

22. Atzīt par spēku zaudējušu ar CSDD 2022.gada 20.jūlija padomes lēmumu Nr.4.1. (protokols Nr.10) apstiprināto CSDD risku vadības politiku.

VALSTS AKCIJU SABIEDRĪBA
CEĻU SATIKSMES DROŠĪBAS DIREKCIJA

Pielikums Nr.1 “Risku klasifikācija”