Finanšu ministrija

Institute of Internal Auditors Latvia

Risku vadības ieviešanas rokasgrāmata

RĪGA 2023

Risku vadības ieviešanas rokasgrāmatu izstrādājusi biedrība “Iekšējo auditoru institūts” pēc Finanšu ministrijas pasūtījuma. Šīs rokasgrāmatas autortiesības pieder Finanšu ministrijai. Pievienojot norādi uz rokasgrāmatu, atļauta rokasgrāmatā iekļautās informācijas citēšana.

SATURS

IEVADS

Veiksmīgas iestādes risku vadība sekmē mērķu sasniegšanu, veicina stratēģisko vadību, darbību prioritizēšanu, uzlabo procesu un funkciju īstenošanu, pakalpojumu sniegšanu, kā arī stiprina institūcijas spēju elastīgi reaģēt uz riskiem un izmaiņām. Lai institūcijas ieviestu efektīvu risku vadību un to attīstītu, nepieciešams pārzināt un piemērot starptautiskos modeļus, standartus un vadlīnijas, kuri apkopo starptautisko labo praksi.

Risku vadības ieviešanas rokasgrāmata (turpmāk – Rokasgrāmata) izstrādāta, izmantojot Eiropas Savienības dalībvalstu un citu valstu atzīto praksi, starptautiskos standartus un vispārpieņemtās risku vadības metodoloģijas, kā arī praksē pārbaudīto risku vadības pieredzi.

Rokasgrāmatā iekļauta informācija par risku vadības ieviešanas, uzturēšanas un pilnveidošanas starptautisko labo praksi. Praktisko piemēru un ieteikumu kopums, kas iekļauts Rokasgrāmatā, var atvieglot risku vadības ieviešanas nepieciešamības pamatošanu un radīt pārliecību par risku vadības ieviešanas iespējamību un izaicinājumu pārvarēšanu.

Rokasgrāmatas galvenais mērķis ir palīdzēt Latvijas publiskās pārvaldes iestādēm (turpmāk – iestādes) izvēlēties vajadzībām un iespējām piemērotu un visaptverošu risku pārvaldības modeli un nodrošināt izvēlētā modeļa ieviešanu un sistemātisku pilnveidošanu, sekmējot vienotas izpratnes par risku vadības nepieciešamību un ieguvumiem rašanos iestādēs.

Rokasgrāmatas mērķim pakārtotie mērķi ir:

- veicināt vienotas izpratnes rašanos par risku kultūras izveides nepieciešamību;
- pilnveidot izpratni par risku vadības procesu integrācijas nepieciešamību ar citiem pārvaldības procesiem;
- stiprināt risku vadības procesa dalībnieku pārliecību par nepieciešamību paaugstināt risku vadības brieduma līmeni (1.pielikums);
- stiprināt risku vadības procesā iesaistīto dalībnieku pārliecību par viņu spēju pārvarēt risku vadības ieviešanas un pilnveidošanas izaicinājumus un šķēršļus.

Rokasgrāmatas pielietojums:

Rokasgrāmata ir pielietojama iestādēs, neatkarīgi no brieduma līmeņa. Rokasgrāmatas būtiska sastāvdaļa ir praktiskie piemēri un ieteikumi.

Rokasgrāmatu var pielietot:

- risku vadības brieduma līmeņa, tostarp esošās situācijas novērtēšanai (2. pielikums), iestādes risku vadības stipro un vājo pušu novērtēšanai;
- iestādes vienotu risku vadības prasību izstrādei;
- risku vadības ieviešanas un pilnveidošanas/efektivizēšanas plānošanai un organizēšanai;
- risku vadības brieduma līmeņa paaugstināšanas plānošanai un organizēšanai;
- risku vadības procesa dalībnieku kvalifikācijas paaugstināšanai un mācību plānošanai;
- risku vadības procesa integrācijas ar citiem pārvaldības procesiem plānošanai un organizēšanai, visaptveroša risku vadības modeļa izveidei;
- risku vadības sinhronizēšanai ar iestādes vajadzībām, lielumu un darbības specifiku.

Rokasgrāmatas mērķauditorija:

- augstākā vadība (ministriju valsts sekretāri, iestāžu vadītāji, pašvaldību vadītāji) – risku vadības nepieciešamības apzināšanas un risku vadības ieviešanas un pilnveidošanas pārvaldība;
- risku vadības speciālisti – risku vadības pārvaldības plānošana un nodrošināšana, sadarbības organizēšana ar augstāko vadību un risku vadības procesa dalībniekiem;
- risku vadības procesa dalībnieki – risku vadības nepieciešamības un savas lomas risku vadības procesā apzināšanās;
- kvalitātes vadītāji – neatbilstību apzināšana, novēršana un procesu nepārtrauktas pilnveidošanas nodrošināšana;
- procesu vadītāji – procesu integrācijas ar risku vadības procesu nepieciešamības apzināšanās, visaptverošas risku vadības nepieciešamības izpratne;
- iestādes darbinieki – risku vadības nepieciešamības un savas lomas risku vadības procesā apzināšanās;
- iekšējie auditori – informācijas avots par risku vadības ietvaru, procesu un tā elementiem, lomu sadalījumu, kā arī nozīmi un pievienoto vērtību iestādes pārvaldībā.

Rokasgrāmatas attiecīgās nodaļas ir iespējams lietderīgi izmantot, pieņemot lēmumus par rīcību, kas nepieciešama, lai iestādē pilnveidotu risku vadību:

- lai organizētu iestādes vadības komandu esošā risku vadības brieduma līmeņa novērtējumā, veicot vērtēšanu un koordinējot rezultātu apkopojumu;
- organizējot iestādes vadības komandas diskusijas par vēlamo brieduma līmeni iestādes mērķu sasniegšanai. Caurskatot, vai iestādes mērķi visos līmeņos ir definēti, kaskadēti un mērāmi, vai ir skaidri definēti procesi;
- lai labāk izprastu un plānotu risku vadības ieviešanu un pilnveidošanu/efektivizēšanu, izmantojot piemērus un ieteikumus;
- risku vadības iekšējā normatīvā regulējuma izstrādei, tai skaitā pilnveidojot iestādes risku vadības metodiku, izmantojot Rokasgrāmatas pielikumus;
- lai sadarbotos ar citu iestāžu pārstāvjiem risku vadības jautājumos;
- iestādes vadības komandas, kas jāiesaista risku vadībā, izveides organizēšanā (tai skaitā galveno procesu/struktūrvienību vadītājus, kā arī koordinatorus, kuriem jānodrošina iestādes mērķu sasniegšana un kuriem nepieciešama informācija argumentētu lēmumu pieņemšanai);
- iestādes vadības komandu mācību plānošanā un organizēšanā, lai iepazītos ar labāko pieredzi un praksi un veidotu vienotu risku vadības informācijas struktūru mācību materiāliem;
- veicot iestādes risku uzraudzību, tai skaitā incidentu un notikumu reģistrāciju, pārskatu sagatavošanu, vērtējot, vai riski attīstās atbilstoši plānotajam, un pieņemot lēmumus;
- veicot risku identificēšanu un novērtēšanu katrā iestādes struktūrvienībā;
- iestādes galveno struktūrvienību risku apkopošanā un risku novērtēšanā risku vadības darba grupā, pasākumu noteikšanā risku optimizēšanai un ietveršanai iestādes gada plānos un stratēģijās.

Lai ieviestu iestādēs risku vadību, Rokasgrāmatas 3. pielikumā ir pievienotas "Ceļa kartes", kas, ņemot vērā iestādes risku vadības brieduma līmeni un lielumu, sniedz stratēģiskas norādes par risku vadības ieviešanas/ attīstības iespējām un rīcību, lai pilnveidotu/paaugstinātu brieduma pakāpi un sasniegtu iecerēto risku vadības attīstības mērķi. Savukārt, lai veiksmīgi uzsāktu "Ceļa

kartēs" paredzēto risku vadības ieviešanas un uzturēšanas darbību īstenošanu, iestādei nepieciešams veikt esošās situācijas novērtējumu, ņemot vērā atsevišķus risku vadības pamatnosacījumus un pamatelementus. "Ceļa kartēs" attēlotie risku vadības brieduma līmeņi var atšķirties no kritērijiem Finanšu ministrijas izstrādātajā risku vadības sistēmas brieduma līmeņa novērtēšanas modelī (1. pielikums).

Kā strādāt ar Rokasgrāmatu:

Rokasgrāmatas pirmajās divās nodaļās iespējams iegūt informāciju par risku vadības pamatiem - standartiem, regulējumu un terminoloģiju, kā arī risku vadības lomu un nozīmi iestādes darbībā, tostarp "Ceļa kartēm", kas palīdz ieviest risku vadību iestādēs. Pēc tam nākamajās nodaļās tiek sniegta informāciju par risku kultūru, risku vadības pārvaldību un risku vadības procesu. Savukārt noslēgumā iekļauta informācija par publiskajam sektoram raksturīgākajiem jeb tipiskākajiem riskiem un iekšējā audita lomu risku vadībā.

Katras nodaļas beigās iekļauts kopsavilkums par tajā pieejamo svarīgāko informāciju.

Lai pievērstu Rokasgrāmatas lietotāja uzmanību būtiskai informācijai par risku vadību, Rokasgrāmatā izmantoti šādi simboli un apzīmējumi:

 **Padoms** vai **Svarīgi**:
Veicot novērtējumu, pievērsiet uzmanību ….

 **Piemērs**:
Projekta riskam varbūtības vērtējums ….

1. STANDARTI, REGULĒJUMI un TERMINOLOĢIJA

1.1. Standarti

Labās prakses prasības risku vadības ieviešanai noteiktas vairākos starptautiskajos standartos un modeļos, piemēram, COSO Uzņēmumu risku vadības ietvars – integrēšana ar stratēģiju un sniegumu (*COSO Enterprise Risk Management Framework - Integrating with Strategy and Performance*) (2017) (turpmāk – COSO ERM), COSO Iekšējā kontrole – Integrētais ietvars (*COSO Internal Control - Integrated Framework*) (2013), ISO 31 000:2018 standarti, Amerikas Savienoto Valstu Nacionālā standartu un tehnoloģijas institūta (*The National Institute of Standards and Technology*) (NIST) izdotie standarti, Lielbritānijas Valsts kases izdotā Oranžā grāmata (*The Orange Book*) (2020) (4. pielikums), kā arī Korporatīvās pārvaldības kodekss, kura ieviešana noteikta ar Ministru kabineta (turpmāk – MK) 15.03.2022. noteikumiem Nr. 175 "Noteikumi par publiskas personas kapitālsabiedrībā un publiski privātā kapitālsabiedrībā piemērojamajiem korporatīvās pārvaldības ieteikumiem".

Ieviešot risku vadību un izvēloties kādu no iepriekšminētajiem standartiem vai modeļiem, sākotnēji iestādei jāizvērtē, kurš no tiem ir iestādes darbības specifikai, lielumam, struktūrai un vajadzībām vispiemērotākais. Šajā nodaļā tiek aprakstīti atsevišķi risku vadības standarti. Skaidru priekšstatu par risku vadības principiem un procesu sniedz, piemēram, ISO 31 000:2018 standarts un Lielbritānijas Valsts kases izdotā Oranžā grāmata[1].

Salīdzinājumā ar ISO 31 000:2018 standartu modeļos COSO ERM un COSO Iekšējā kontrole – Integrētais ietvars iekļauta detalizētāka, sarežģītāka un teorētiskāka informācija par risku vadības sistēmas pamatkomponentēm, piemēram, risku apetīti, risku toleranci un risku kapacitāti, kas iestādēm, kurām atbilstoši risku vadības sistēmas brieduma novērtējumam ir pirmais vai otrais risku vadības brieduma līmenis[2], būtu šķietami sarežģītāk uztverama.

Savukārt, iestādēm, kuras ir sasniegušas vismaz trešo risku vadības brieduma līmeni, būtu iespējams vairāk attīstīt un stiprināt jau ieviesto risku vadību, ņemot vērā iepriekšminētajos modeļos iekļauto risku vadības teorijas un prakses apkopojumu.

Spēcīga iekšējā kontrole var palīdzēt mazināt daudzus sarežģītus riskus. COSO Iekšējā kontrole – Integrētais ietvars var uzskatīt par "Ceļa karti" iekšējās kontroles un risku vadības izveidē, lai nodrošinātu, ka riski tiek uzraudzīti un mazināti lēmumu pieņemšanas procesā. COSO ERM ir plašāk vērsts uz iestādes darbības uzraudzību, ne tikai risku vadības procesa uzraudzību.

Izdoti arī specifiski standarti noteiktās specifiskās jomās. Piemēram, Amerikas Savienoto Valstu Nacionālā standartu un tehnoloģijas institūta izdotie standarti un ISO 27 001:2022 standarti[3] ir izdoti, lai stiprinātu kiberdrošību, ieviestu informāciju sistēmu un to drošības risku vadību. ISO 27 001:2022 standarts ir starptautiski pazīstamākais informācijas drošības pārvaldības sistēmu

[1] Orange Book (2023. gada versija). Pieejama šeit: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154709/HMT_Orange_Book_May_2023.pdf

[2] Finanšu ministrijas izstrādātais risku vadības sistēmas brieduma līmeņa novērtēšanas modelis paredz un skaidro piecus brieduma līmeņus (1.pielikums).

[3] Informācijas drošības vadības sistēma (*Information Security Management System*)

izveides, ieviešanas, uzturēšanu un nepārtrauktas uzlabošanas, kā arī kibernoturības, tostarp kiberrisku apzināšanas standarts.

Atbilstība ISO 27 001:2022 standartam nozīmē, ka iestāde ieviesusi sistēmu, lai vadītu riskus, kas saistīti ar iestādei piederošo vai apstrādāto datu drošību, un ka šī iestāde ievēro visu šajā starptautiskajā standartā ietverto labāko praksi un principus. Kiberdrošības risku vadība aptver visu informācijas tehnoloģiju aizsardzībai veikto darbību klāstu no nesankcionētas piekļuves līdz pat sociālās inženierijas apdraudējumiem un citiem kiberdraudiem.

Papildus iepriekšminētajam, ir arī dažādi nozares standartu ietvari un metodoloģijas, piemēram, projektu vadības, tostarp projektu risku vadības jomā (*Project Management Book of Knowledge (PMBOK)*), kas integrē risku vadību ar projektu vadību. Iestādes risku vadības procesu parasti sinhronizē ar projektu risku vadības procesu, lai veidotu vienotu risku pārvaldības sistēmu. *PMBOK* sniedz detalizētu projektu vadības procesa aprakstu, kā arī vadlīnijas, kas palīdz projektu vadītājiem pieņemt projektu vadības lēmumus, uzlabot savas prasmes izmaksu vadībā, cilvēkresursu un kvalitātes vadībā.

ISO 31 000:2018 standarts sniedz detalizētas vadlīnijas par risku vadības sistēmas plānošanu un īstenošanu, bet mazāk skaidro risku vadības sistēmas ietvaru (kontekstu) un līderību.

Ņemot vērā iepriekšminētos apsvērumus, ISO 31 000:2018 standartā paredzēto risku vadības procesu iespējams kombinēt ar COSO ERM modelī un citos standartos un modeļos iekļauto risku vadības labo praksi, tādējādi radot padziļinātāku izpratni par risku vadības ieviešanu iestādē un veicinot risku vadības brieduma līmeņa paaugstināšanu.

Kombinējot strukturētu un proaktīvu risku vadības pieeju, iestādēm būs iespējams nepārtraukti pilnveidot, piemēram, šādas jomas:

- stratēģisko vadību, jo tiks analizēti ar stratēģiskajiem mērķiem un darbības virzieniem saistītie riski, kā arī pieņemti kvalitatīvāki stratēģiskie lēmumi;
- taktikas īstenošanu, jo tiks ņemta vērā iespējamo alternatīvu izvēle un ar to saistītie riski;
- operacionālās darbības nodrošināšanu, jo tiks identificēti risku notikumi, kas var izraisīt iestādēm darbības traucējumus/pārtraukumus, kā arī tiks ieviesti pasākumi, lai samazinātu šo notikumu iespējamību, ierobežotu negatīvās sekas un to izraisītos finansiālos zaudējumus;
- finanšu vadību, jo tiks nodrošināta uzticama, savlaicīga un precīza finanšu un vadības ziņošanas sistēma, apzinot un mazinot finanšu vadības, tostarp pārskatu sagatavošanas riskus;
- atbilstības nodrošināšanu, jo tiks novērtēti riski, kas saistīti ar Latvijas Republikas, Eiropas Savienības u.c. saistošo tiesību aktos, kā arī iestāžu iekšējos normatīvajos aktos paredzēto prasību ievērošanu. Izvērtējot atbilstības jomas, tiks mazinātas krāpšanas iespējas un aizsargāti informācijas resursi.

Visiem iepriekšminētajiem standartiem un modeļiem ir tikai rekomendējošs raksturs un neviens no tiem nenosaka precīzas visu risku vadības procesa soļu prasības un aprakstus, metodiku un risku vadībā izmantojamās veidlapas. Risku vadības ieviešanas izaicinājums ir sinhronizēt iepriekšminēto modeļu/ standartu prasības ar labo praksi un faktisko rīcību risku vadībā.

1.2. Regulējums

Risku vadības prasības ir noteiktas tiesību aktos, kā arī papildus iespējams ņemt vērā starptautiskās labās prakses piemērus, lai veicinātu risku vadības ieviešanu. 1. tabulā tiek

analizēti tiesību akti, tostarp nacionālie normatīvie akti, kuros iekļautas prasības par risku vadību, kā arī citu valstu labās prakses piemēri, kurus iespējams izmantot risku vadībā.

1. tabula. Tiesību akti

Tiesību akta/starptautiskās iestādes nosaukums	Īss raksturojums
Latvijas Republikas tiesību akti	
MK 08.05.2012. noteikumi Nr.326 "Noteikumi par iekšējās kontroles sistēmu tiešās pārvaldes iestādēs"	Iekšējās kontroles elementi, izveidošana, kontroles pasākumu īstenošana un risku vadības atsevišķi pamatelementi. Tiek izmantots iekšējās kontroles sistēmas izveidei vai atbilstības normatīvajam regulējumam novērtēšanai. Informācija par riskiem ir nepietiekama, lai risku vadību izveidotu kā iekšējās kontroles sastāvdaļu vai lai novērtētu risku vadības procesu. Noteikumos nav iekļauta pietiekama informācija, ir tikai vispārīgs ietvars iekšējās kontroles sistēmai.
MK 17.10.2017. noteikumi Nr.630 "Noteikumi par iekšējās kontroles sistēmas pamatprasībām korupcijas un interešu konflikta riska novēršanai publiskas personas institūcijā"	Iekšējās kontroles sistēmas pamatprasības korupcijas un interešu konflikta riska novēršanai publiskas personas institūcijā. Papildina MK 08.05.2012. noteikumus Nr.326 "Noteikumi par iekšējās kontroles sistēmu tiešās pārvaldes iestādēs". Tiek izmantots iekšējās kontroles sistēmas korupcijas un interešu konflikta risku vadībai. Noteikumos nav iekļauta pietiekama informācija par korupcijas un interešu konflikta risku vadību, tāpēc ieteicams izmantot kopā ar likumu "Par interešu konflikta novēršanu valsts amatpersonu darbībā" un KNAB vadlīnijām.
Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums	Noziedzīgi iegūtu līdzekļu legalizāciju un terorisma un proliferācijas finansēšanas novēršana. Var izmantot iestādēs noziedzīgi iegūtu līdzekļu legalizāciju un terorisma un proliferācijas risku vadībai, papildinot iestādes izveidoto risku vadību.
Starptautisko un Latvijas Republikas nacionālo sankciju likums	Sankciju riska novērtējums un sankciju riska pārvaldīšanas iekšējās kontroles sistēmas izveidošana. Tiek izmantots likumā noteiktajās iestādēs, lai veiktu un dokumentētu starptautisko un nacionālo sankciju riska novērtējumu un vienlaikus noskaidrotu, novērtētu, izprastu un pārvaldītu savai darbībai vai klientiem noteikto starptautisko un nacionālo sankciju neizpildes riskus.
Darba aizsardzības likums	Nodarbināto un pašnodarbināto drošība un veselības aizsardzība darbā, nosakot darba devēju, nodarbināto un viņu pārstāvju, pašnodarbināto, kā arī valsts institūciju pienākumus, tiesības un savstarpējās attiecības darba aizsardzībā. Var izmantot iestādēs, lai veidotu visaptverošu risku vadību, ietverot dažādu kategoriju riskus, kuru vadībai ir atšķirīgs normatīvais regulējums un novērtēšanas metodika, analogi MK 19.04.2016. noteikumiem Nr. 238 "Ugunsdrošības noteikumi".
Eiropas Savienības tiesību akti un citi dokumenti	
Eiropas Parlamenta un Padomes direktīva (ES) 2022/2557	Var izmantot iestādēs, lai risku vadība būtu viens no iestādes darbības nepārtrauktības nepieciešamības un izveides atbalsta nosacījumiem.
Eiropas Regulas un inovāciju foruma (*The European*	Eiropas Regulas un inovāciju forums (ERIF) ir neatkarīga, bezpeļņas ideju grupa Briselē, kuras mērķis ir veicināt ES institūciju regulatīvo lēmumu pieņemšanas standartu izstrādi, kas ietver pārvaldību,

Tiesību akta/starptautiskās iestādes nosaukums	Īss raksturojums
Regulation and Innovation Forum (ERIF)) publikācijas	zinātnisko integritāti un lēmumu pieņemšanu, lai veiktu *ex-post* novērtējumu. Piemēram, 21. piezīme. Jaunas regulēšanas filozofijas — nākotnes virzieni un ietekme uz riska pārvaldību (*Note 21: Novel Regulatory Philosophies – Future Directions and Implications for Risk Management*)[4].
Eiropas Risku vadītāju asociācijas federācija *(The Federation of European Risk Management Associations (FERMA))*	FERMA publicē informāciju par risku vadību, kuru var izmantot iestādes risku vadības efektivitātes novērtēšanā un pārvaldības pilnveidošanā. Piemēram, Eiropas riska pārvaldības ziņojums Nr. 2022 (*European Risk Management Report 2022*)[5].
Citu valstu normatīvie akti	
ASV Kongress	ASV Kongress publicē informāciju par risku vadību, kuru var izmantot iestādes risku vadības pilnveidošanā. Piemēram, Katastrofu seku novēršanas plānošanas likums, Kvantu skaitļošanas kiberdrošības gatavības likums, Iekšzemes bērnu drošības akts (*Disaster Resiliency Planning Act, Quantum Computing Cybersecurity Preparedness Act, Homeland Security for Children Act*).
Federālais normatīvā regulējuma reģistrs (*The Federal Register of legislation*)	Austrālijas parlamenta informācija par risku vadību, kuru var izmantot iestādes risku vadības pilnveidošanā. Piemēram, Kritiskās infrastruktūras drošība (Kritiskās infrastruktūras riska pārvaldības programmas noteikumi) (BEAR 23/006) 2023 (*Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*).

Lai arī Korporatīvās pārvaldības kodekss[6] ir saistošs valsts kapitālsabiedrībām, tā sadaļā "Iekšējās kontroles sistēma, risku vadība un iekšējais audits" iekļautais risku vadības mērķis un koncepts ir piemērojams arī citām publiskā sektora, tai skaitā valsts pārvaldes iestādēm.

1.3. Terminoloģija

Rokasgrāmatā izmantotā terminoloģija veicina vienotas "risku valodas" veidošanu. Terminu sarakstā iekļautas vairākas viena termina definīcijas un trīs kolonnas ar termina definīcijas lietošanas ieteikumiem. Vairākas terminu definīcijas ir piedāvātas ar mērķi ļaut iestādei izvēlēties tās brieduma pakāpei un iekšējai videi, kā arī citiem nosacījumiem atbilstošāko definīciju.

Piemērotas terminu definīcijas izvēle sekmē risku vadības brieduma līmenim atbilstošāka iekšējā normatīvā akta, kas reglamentē risku vadību, izstrādi, labāku risku vadības procesa dalībnieku izpratni par risku vadības procesu, tai skaitā par risku identificēšanu un risku analīzi. Iestādēm, kurām jau ir ieviests otrais vai par to augstāks risku vadības brieduma līmenis, varētu novērtēt terminu atbilstību iepriekšminētajam brieduma līmenim un plānot tā paaugstināšanu.

[4] https://www.eriforum.eu/uploads/2/5/7/1/25710097/erif_highlights_21_-_nrps_final.pdf
[5] https://www.ferma.eu/publication/european-risk-manager-report-2022/
[6] Apstiprināts ar MK 15.03.2023. noteikumiem Nr. 175 "Noteikumi par publiskas personas kapitālsabiedrībā un publiski privātā kapitālsabiedrībā piemērojamajiem korporatīvās pārvaldības ieteikumiem".

Viena no termina definīcijām svarīgāko terminu sarakstā ir izcelta treknrakstā. Izceltais termins tiks turpmāk izmantots Rokasgrāmatā. Iestādēm iespējams pašām definēt terminus, izmantojot starptautiskās labās prakses un risku vadības standartos/ modeļos iekļautās definīcijas.

Terminu un to skaidrojumu izvēle un pietiekamība, ņemot vērā iestādes risku vadības brieduma līmeni un risku vadības veidu, var ietekmēt risku vadības efektivitāti, jo, skaidrojot terminus, tiek nodrošināta visu risku vadības procesā iesaistīto dalībnieku vienota izpratne par risku vadību un līdz ar to produktīvāka iesaiste risku vadības procesā (2. tabula).

2. tabula. Risku vadības svarīgākie termini

Termins ***Termins angļu valodā***	**Definīcija** **Avots**	**Lietošanas ieteikumi**		
		Brieduma līmenis	**Saistītie termini, kuru definīcijas ir nepieciešamas**	**Ieteicamais izmantošanas veids**
Risks	Nenoteiktības ietekme uz mērķiem. ISO Guide 31000:2018	Ne mazāks par 2. līmeni	Nenoteiktība Ietekme	Risku vadības normatīvajos aktos Risku identificēšanas procesā Risku analīzes procesā
	Iespēja, ka notikumi notiks un ietekmēs stratēģijas un biznesa mērķu sasniegšanu. **COSO ERM**	Jebkurā līmenī	Notikums Iespēja Ietekme	Risku vadības normatīvajos aktos Risku identificēšanas procesā Risku mazinošo pasākumu plānošanā Stratēģijas izstrādē
	Nenoteikts notikums vai nosacījums, kam, īstenojoties, ir pozitīva vai negatīva ietekme uz projekta mērķi. Practise Standart for Project Risk Management, Project Management Institute	Jebkurā līmenī	Nenoteiktība Ietekme	Risku vadības normatīvajos aktos Projektu vadības normatīvajos aktos Projektu dokumentācijā Projektu risku identificēšanas procesā Projektu risku analīzes procesā

Termins *Termins angļu valodā*	Definīcija Avots	Lietošanas ieteikumi		
		Brieduma līmenis	**Saistītie termini, kuru definīcijas ir nepieciešamas**	**Ieteicamais izmantošanas veids**
				Projekta vadības procesā
	Mērījums, kas atklāj, cik lielā mērā uzņēmumu apdraud potenciāls apstāklis vai notikums, un parasti tas ir atkarīgs no: i) nelabvēlīgās ietekmes, kas rastos, ja īstenotos kāds apstāklis vai notikums; un ii) notikuma iespējamības. NIST, [FIPS 200, Adapted]	Ne mazāks par 2. līmeni	Apstāklis Notikums Apdraudējums Ietekme Iespējamība	Stratēģijas izstrādē Darbības vērtēšanā
	Iespējamība, ka kāds notikums negatīvi ietekmēs iestādes mērķu sasniegšanu. MK 08.05.2012. noteikumi Nr.326 "Noteikumi par iekšējās kontroles sistēmu tiešās pārvaldes iestādēs"	Ne mazāks par 2. līmeni	Notikums Ietekme	Risku vadības normatīvajos aktos Risku identificēšanas procesā Risku mazinošo pasākumu plānošanā Stratēģijas izstrādē
Risku vadība	**Koordinētas darbības, lai vadītu un kontrolētu organizāciju attiecībā uz risku.** ISO Guide 73:2009	Jebkurā līmenī	Nav nepieciešami	Risku vadības normatīvajos aktos Risku identificēšanas procesā Risku analīzes procesā
	Kultūra, iespējas un prakse, kas integrēta ar stratēģijas noteikšanu un izpildi, uz ko organizācijas paļaujas, lai pārvaldītu risku, radot, saglabājot un realizējot vērtību. COSO ERM			
	Projektu risku vadība ietver procesus, kas saistīti ar risku vadības plānošanu, identificēšanu, analīzi, reakciju (*responses*), kā arī projektu uzraudzību un kontroli. Projektu risku vadības mērķis ir palielināt pozitīvu notikumu iespējamību un ietekmi, kā arī samazināt	Jebkurā līmenī	Risku vadības/risku vadības procesu definīcijas Ieteicams definēt arī:	Risku vadības normatīvajos aktos Projektu vadības normatīvajos aktos

Termins *Termins angļu valodā*	Definīcija Avots	Lietošanas ieteikumi		
		Brieduma līmenis	**Saistītie termini, kuru definīcijas ir nepieciešamas**	**Ieteicamais izmantošanas veids**
	projektu mērķiem nelabvēlīgu notikumu iespējamību un ietekmi. Practise Standart for Project Risk Management, Project Management Institute		Pozitīvs notikums Nelabvēlīgs notikums	Projektu dokumentācijā Projektu risku identificēšanas procesā Projektu risku analīzes procesā Projekta vadības procesā
	Programma un atbalsta procesi, lai pārvaldītu aģentūras riskus operācijās (tostarp misija, funkcijas, tēls, reputācija), aģentūras aktīvus, personas, citas organizācijas un nāciju, ietver: konteksta izveidi ar risku saistītām darbībām, riska novērtēšanu, reaģēšanu uz risku, kad tas ir noteikts un riska uzraudzību laika gaitā. NIST, NIST Special Publication 800-37, Revision 2	Ne mazāks par 2. līmeni	Nav nepieciešams	Risku vadības normatīvajos aktos Stratēģijas izstrādē Valsts institūcijas darbības vērtēšanā
Notikums ***Event***	Noteikta apstākļu kopuma īstenošanās vai maiņa. ISO Guide 31000:2018	Jebkurā līmenī	Nav nepieciešams	Risku vadības normatīvajos aktos Risku identificēšanas procesā Stratēģijas izstrādē
	Atgadījums vai gadījumu kopa. COSO ERM			
	Notikums netiek definēts, eksistē notikumu sadalījums negatīvajos notikumos. Practise Standart for Project Risk Management, Project Management Institute			
	Jebkurš novērojams notikums tīklā vai informācijas sistēmā. NIST, NIST Special Publication 800-37, Revision 2	Nevar attiecināt	Atbilstoši informācijas tehnoloģiju normatīvajam regulējumam	Atbilstoši informācijas tehnoloģiju normatīvajam regulējumam

Turpinājumā uzskaitīti citi Rokasgrāmatā izmantoti risku vadības termini (3. tabula).

3. tabula. Citi risku vadības termini

Termins, tai skaitā angļu valodā	Definīcija	Avots
Riska avots/riska cēlonis ***Risk source***	Elements, kas atsevišķi vai kopā var radīt risku.	ISO 31000:2018 Risk management — Guidelines
Riska kategorija/veids	Risku grupējums atbilstoši noteiktai pazīmju kopai.	Rokasgrāmatā lietots termins
Būtisks risks	Risks, kura sekas vai varbūtība, vai vērtība apdraudēs iestādes mērķu sasniegšanu vai izraisīs situāciju, ka mērķu sasniegšana nav iespējama.	Rokasgrāmatā lietots termins
Īpaši riski ***Key risk***	Risku kopums, kuriem ir vislielākā ietekme uz projekta izmaksām un laika grafiku.	U.S. Department of Energy
Apdraudējums ***Threat***	Jebkurš apstāklis vai notikums, kas var negatīvi ietekmēt organizatoriskās darbības (tostarp misiju, funkcijas, iestādes tēlu vai reputāciju), organizācijas aktīvus vai personas, izmantojot informācijas sistēmu, nesankcionēti piekļūstot, iznīcinot, izpaužot, mainot informāciju un/vai pārtraucot pakalpojumu sniegšanu.	The National Institute of Standards and Technology, Computer Security Resource Center
Incidents ***Incident***	Īstenojies risks, kas radījis iestādei materiālus vai nemateriālus zaudējumus vai negatīvi ietekmējis iestādes reputāciju, finanses, mērķus.	Rokasgrāmatā lietots termins
Informācijas sistēmas incidents *Information system incident*	Notikums, kas faktiski vai potenciāli apdraud informācijas sistēmas vai informācijas, ko sistēma apstrādā, glabā vai pārraida, konfidencialitāti, integritāti vai pieejamību; vai notikums, kas ir drošības politiku, drošības procedūru vai lietošanas politiku pārkāpums, vai arī tiešs pārkāpuma apdraudējums.	The National Institute of Standards and Technology, Computer Security Resource Center
Informācijas drošības incidents *Information security incident*	Identificēts informācijas sistēmas, pakalpojuma vai tīkla stāvoklis, kas norāda uz iespējamu informācijas drošības politikas pārkāpumu vai kontroļu trūkumiem, vai arī kas liecina par iepriekš nezināmu situāciju, kas var būt būtiska drošībai.	ISO 27 000:2022
Nenoteiktība ***Uncertainty***	Situācija, daļējs informācijas, zināšanu vai izpratnes trūkums saistībā ar notikumu, tā sekām vai iespējamību.	ISO Guide 73:2009
Riska sekas/ ietekme ***Risk consequence***	Notikuma, kas ietekmē mērķus, iznākums.	ISO 31000:2018
Riska ietekme ***Risk impact***	Notikuma, kas negatīvi ietekmē mērķus, īstenošanās rezultāta radītais kaitējums, kas var tikt izteikts kvalitatīvi vai kvantitatīvi.	Rokasgrāmatā lietots termins
Riska varbūtība/ iespējamība ***Risk likelihood/ probability***	Iespēja, ka kaut kas notiks.	ISO 31000:2018

Termins, tai skaitā angļu valodā	Definīcija	Avots
Riska avots ***Risk source***	Elements, kas atsevišķi vai kombinācijā ar citiem elementiem var izraisīt risku.	ISO 31000:2018
Riska vērtība ***Risk value***	Riska kvantitatīvs vai kvalitatīvs mērījums, kuru iegūst, reizinot riska ietekmi ar riska varbūtību.	Rokasgrāmatā lietots termins
Risku indikators ***Key risk indicator***	Risku mērījums, ko izmanto, lai iegūtu agrīnus brīdinājuma signālus par risku palielināšanos dažādās jomās.	COSO ERM
Risku apetīte/ Gatavība riskēt/ Attieksme pret risku/ Riska nepieņemšana	Risku apjoms/vērtība un veids, ko organizācija/iestāde vēlas uzņemties vai saglabāt.	ISO 31000:2018
Risku tolerance/ risku iecietība	Maksimālais riska apjoms, ko iestāde ir gatava uzņemties, ņemot vērā risku veidu un risku apetīti vai novirze no riska apetītes, kas pieļauj mērķu sasniegšanu.	Rokasgrāmatā lietots termins
Sākotnējais risks/sākotnējā riska vērtība/svars ***Inherent risk***	Organizācijas/iestādes riska līmeņa vērtība, ja vadība neveic nekādas tiešas vai mērķtiecīgas darbības, lai mainītu tā vērtību.	COSO ERM
Atlikušais risks/atlikušā riska vērtība/svars ***Residual risk***	Riska līmenis, kas saglabājas pēc tam, kad vadība ir veikusi skaidru vai mērķtiecīgu darbību, lai mainītu riska vērtību.	COSO ERM
Risku profils ***Risk Profile***	Jebkura risku kopuma apraksts.	ISO 31000:2018
Risku izmaksas/Risku seku izmaksas/Risku vadīšanas izmaksas	Risku notikumu paredzamās finansiālās (vai monetizētās) vērtības mērs.	Rokasgrāmatā lietots termins
Riska scenārijs	Hipotētiski riska notikuma vai riska notikumu kombināciju iespējamie iznākumi, kas ietver virkni pieņēmumu, mainīgo lielumu un iespējamību.	Rokasgrāmatā lietots termins
Risku vadības process ***Risk management process***	Sistemātiska vadības politikas, procedūru un prakses piemērošana, komunikācijas, konsultācijas, konteksta noteikšana un risku identificēšana, analīze, novērtēšana, reaģēšana uz riskiem, uzraudzība un pārskatīšanas darbības.	ISO Guide 73:2009
Risku identificēšana	Risku apzināšanas, atpazīšanas un aprakstīšanas process.	ISO Guide 73:2009
Risku analīze	Process, lai izprastu riska būtību un noteiktu riska vērtību/ līmeni.	ISO Guide 73:2009
Risku novērtējums ***Risk evaluation***	Risku analīzes rezultātu salīdzināšanas process ar riska kritērijiem, lai noteiktu, vai risks un/vai tā lielums ir pieņemams vai pieļaujams.	ISO Guide 73:2009
Risku mazināšana/riska apstrādāšana ***Risk treatment***	Risku mainīšanas process.	ISO Guide 73:2009

Termins, tai skaitā angļu valodā	Definīcija	Avots
Visaptveroša risku vadīšana/pārvaldība ***Enterprise risk management***	Kultūra, spējas un prakse, integrēta ar stratēģijas noteikšanu un tā veiktspēju, uz ko organizācijas/iestādes paļaujas, lai pārvaldītu risku, veidojot, saglabājot un realizējot vērtību (organizācijas/iestādes).	COSO ERM
Risku kultūra/ risku pārvaldības kultūra	Vērtības, uzskati, zināšanas, attieksme un izpratne par risku, kas piemīt cilvēku grupai ar kopīgu mērķi.	Institute of Risk Management
Risku saraksts/reģistrs/datu bāze/profils/riska kartiņa	Informācija par identificētajiem riskiem.	ISO 31000:2018
Risku karte	Vienots iestādes visu risku novērtējuma vizuālais attēlojums uz varbūtības un ietekmes asīm, kas sniedz informāciju par riskiem un to profilu.	Rokasgrāmatā lietots termins
Risku matrica	Risku analīzes rezultātā iegūta risku līmeņa vizualizācija, ņemot vērā risku ietekmi un varbūtību.	Rokasgrāmatā lietots termins
Risku ziņošana/ atskaitīšanās	Regulārs mehānisms/process, kas tiek īstenots, lai nosūtītu atjauninājumus galvenajām ieinteresētajām personām, nodrošinot, ka pareizā informācija tiek sniegta īstajiem cilvēkiem pareizajā līmenī un īstajā laikā.	Government Finance Function, Good Practice Guide: Risk Reporting
Risku mazināšanas pasākumu plāns	Organizācijas/iestādes vadības apstiprināts dokuments, kurā apkopota informācija par tām papildu darbībām, ko iestādes vadība un risku īpašnieki ir nolēmuši veikt, lai vēl vairāk samazinātu risku atlikušo līmeni.	Rokasgrāmatā lietots termins
Kontroles/riska kontroles/ iekšējās kontroles	Pasākums, kas uztur un/ vai maina risku.	ISO 31000:2018
	Process, kuru ietekmē iestādes augstākā vadība un citi darbinieki, kas paredzēts, lai sniegtu pamatotu pārliecību par mērķu sasniegšanu šādās kategorijās: • darbību efektivitāte un lietderība; • ziņošanas uzticamība; • atbilstība tiesību aktiem, tai skaitā normatīvajiem aktiem.	COSO Iekšējā kontrole – Integrētais ietvars
Riska kapacitāte ***Risk Capacity***	Maksimālā riska summa/ vērtība, ko organizācija/ iestāde spēj uzņemties, īstenojot stratēģiju un mērķus.	COSO ERM
Risku mazinošie pasākumi/risku mazināšanas pasākumi ***Risk Mitigation measures***	Prioritātes noteikšana, novērtēšana un atbilstošo risku samazināšanas kontroles/ pretpasākumu, kas noteikti risku vadības procesā, ieviešana.	The National Institute of Standards and Technology, Computer Security Resource Center
Risku vadības politika	Dokuments, kuru apstiprina iestādes vadība un kas nosaka galvenos risku vadības uzstādījumus.	Rokasgrāmatā lietots termins

Termins, tai skaitā angļu valodā	Definīcija	Avots
Risku vadītājs	Risku vadības procesa dalībnieks ar noteiktu lomu un atbildību risku vadībā.	Rokasgrāmatā lietots termins
Riska īpašnieks ***Risk owner***	Persona vai organizācija, kas ir atbildīga par apdraudējumu un ievainojamību vadību, ko tie varētu izmantot.	ISO 27001:2013
	Persona/ struktūrvienība, kurai ir iespējams ietekmēt riska līmeni, un kura nodrošina riska mazinošo pasākumu ieviešanu un riska līmeņa izmaiņu uzraudzību.	Rokasgrāmatā lietots termins

KOPSAVILKUMS

Risku vadības prasības ir noteiktas Latvijas Republikas normatīvajos aktos, Eiropas Savienības, ASV un Austrālijas normatīvajos aktos (1. tabula), kā arī dažādos standartos (skat. 1.nodaļu "Standarti, regulējums un terminoloģija").

Iestādei, ieviešot risku vadību, nepieciešams izvēlēties kādu no standartiem vai modeļiem, kurš no tiem būs vispiemērotākais tās darbības specifikai, lielumam, struktūrai un vajadzībām. Atbilstoši izvēlētajam standartam un/vai modelim, iestāde veido un īsteno risku vadību.

Lai iestādei būtu iespējams veicināt darbiniekiem vienotu izpratni risku vadības procesā, Rokasgrāmatā definēta vienota terminoloģija jeb "risku valoda", taču iestādēm ir iespējams patstāvīgi definēt terminus, izmantojot starptautiskās prakses definīcijas.

2. RISKU VADĪBAS LOMA UN NOZĪME IESTĀDES DARBĪBĀ

Risku vadība ir viens no labas iestādes pārvaldības prakses stūrakmeņiem. Tas ir pasākumu kopums, kas iestādei ļauj mazināt negatīvu notikumu vai incidentu sekas un ietekmi, aizsargāt iestādes resursus, kā arī atbalstīt un veicināt tās mērķu sasniegšanu. Risku vadība gan privātajā, gan publiskajā sektorā ir kļuvusi arvien nozīmīgāka pēc pēdējās desmitgadēs piedzīvotajām finanšu un ekonomiskajām krīzēm, kā arī tā kļūst arvien izplatītāka prasība normatīvajos aktos. Papildu tam pēdējos gados piedzīvotie globālie izaicinājumi veselības, piegādes ķēžu, kā arī ģeopolitiskajos aspektos, risku vadību padara arvien aktuālāku tām iestādēm, kas grib būt sagatavotas dažādiem scenārijiem un apzināti pārvaldīt savus izaicinājumus.

Ja iestādes vadība ir ieinteresēta stabilā mērķu sasniegšanā, iestādes efektivitātes paaugstināšanā, pārliecinātā un pilnvērtīgi izsvērtā lēmumu pieņemšanā, tad praksē ieviesta un aktīva, elastīga risku vadība noteikti ir viens no priekšnosacījumiem, kas palīdz sasniegt šos mērķus.

Risku vadība ir un būtu jāuztver kā viens no iestādes vadības rīkiem, līdzīgi, kā iekšējās komunikācijas un darbinieku attiecību uzturēšanas, procesu uzraudzības, finanšu vadības, iekšējās kontroles sistēmas uzturēšanas un daudzas citas aktivitātes, kas tiek uztvertas par pašsaprotamām un ir neatņemama katras iestādes pārvaldības sastāvdaļa.

Dažādas ieinteresētās puses, ārējie sadarbības partneri, uzraugošās un kontrolējošās iestādes, klienti, sabiedrība kopumā arvien vairāk arī no iestādēm sagaida kvalitatīvu un atbildīgu pārvaldību, kas ietver risku vadību un arī līdzsvaru ar pietiekami izaicinošu un uz attīstību vērstu iestāžu sasniedzamo mērķu un darbības plānu noteikšanu. Gan Latvijā, gan ārvalstīs jebkurš iestāžu incidents, laicīgi nenovērsts risks rada negatīvu publisku rezonansi un šādas situācijas tiek tolerētas arvien mazāk, jo tiek sagaidīts, ka iestādes atbildīgi un pilnvērtīgi apzinās savus būtiskos riskus un efektīvi tos vada.

Turpmāk šajā nodaļā aprakstīta risku vadības saistība ar citiem iestādes pārvaldības procesiem, kā arī aprakstīti visaptverošas risku vadības modeļi un pamatprincipi.

2.1. Ieguvumi no risku vadības

Iestādēm, kurās ieviesta risku vadība, galvenie ieguvumi no tās uzturēšanas un attīstīšanas ir, piemēram, šādi:

- konsekventa, strukturēta pieeja risku identificēšanai un vadībai;
- tiek atbalstīta iestādes stratēģisko un darbības mērķu sasniegšana, vadot riskus, kas var kavēt sasniegumus;
- tiek veicināta atvērta un pārredzama risku kultūra, kuras ietvaros tiek atbalstīta izpratne par riskiem un to vadību;
- tiek veidota lēmumu pieņemšanas prakse, kas balstīta uz risku pamatotu novērtējumu, nosakot darbību prioritāti;
- tiek noteikti alternatīvi rīcības veidi, ņemot vērā risku scenārijus;
- tiek veicināta izpratne par vidi, kurā iestādes darbojas;
- tiek sniegta pārliecība iestādes vidējā līmeņa un augstākajai vadībai, ka tiek identificēti nozīmīgākie riski un ka tie tiek vadīti efektīvi.

Turpmāk 4. tabulā minēti daži būtiskākie ieguvumi no risku vadības ieviešanas un uzturēšanas publiskās pārvaldes iestādēs, pretstatā aprakstot situāciju bez risku vadības. Šis uzskaitījums nav izsmeļošs un katrai iestādei, atkarībā no tās vispārējās pārvaldības prakses un kultūras, kā arī no

tās vadītāju un darbinieku pieredzes, attieksmes un darba pieejas, var pastāvēt arī citi ieguvumi no risku vadības.

Ieguvumi aprakstīti, ņemot vērā COSO ERM, ISO 31 0000:2018, Oranžo grāmatu *(The Orange Book*) risku vadības standartu labo praksi un citu organizāciju pieredzi, ieviešot šos standartus.

4. tabula. Ieguvumi no risku vadības

Iestādes darbības nodrošināšanas būtiskākie pamatelementi	Ar risku vadību	Bez risku vadības
Stratēģiskā plānošana, mērķi	Stratēģiskie mērķi noteikti, pilnvērtīgi izvērtējot iestādes iekšējo un ārējo vidi un darbības sfēru (kontekstu). Iespējams noteikt izaicinošus un uz attīstību vērstus mērķus, kā arī veiksmīgi virzīties uz to sasniegšanu, jo risku vadība sniedz atbalstu risku mazināšanas pasākumu noteikšanā un ieviešanā. Risku vadība atbalsta iestādes mērķu sasniegšanu, jo ļauj novērst vai mazināt šķēršļus vēlamo rezultātu sasniegšanai.	Stratēģiskie mērķi ir noteikti, bet nav pārdomāti un noformulēti scenāriji, gadījumā, ja tie netiktu sasniegti, iestāde nav sagatavojusies neplānotiem, negatīviem attīstības scenārijiem, kā arī negatīviem iekšējiem vai ārējiem faktoriem. Riski, kurus būtu iespējams paredzēt, mazināt un atbildīgi pārvaldīt, pārsteidz iestādes darbiniekus un vadību spēji un "negaidīti", un nav iespējams operatīvi atbilstoši reaģēt. Tā vietā tiek pielāgoti stratēģiskie mērķi, lai nerastos iespaids, ka tie netiks sasniegti.
Lēmumu pieņemšanas process	Pieņemot lēmumus dažādos vadības līmeņos, tiek apsvērti un ņemti vērā dažādi faktori, tai skaitā riski, nepieciešamības gadījumā paredzot un uzdodot īstenot risku mazināšanas pasākumus, lai nodrošinātu, ka lēmumi tiek pieņemti pamatoti un tiek demonstrēta atbildīga attieksme pret iestādes resursiem un iekšējiem un ārējiem klientiem, ievērojot iekšējos un ārējos normatīvos aktus.	Lēmumu pieņemšanas procesā netiek apsvērti riski un tiem īstenojoties, nav izprotama pieņemto lēmumu pamatotība, jo sevišķi situācijās, kad riskus varēja paredzēt un savlaicīgi mazināt. Tiek reaģēts uz incidentiem pēc tam, kad tie īstenojušies, kā rezultātā tiek izlietots daudz vairāk finanšu, personāla un laika resursu, salīdzinājumā ar situāciju, ja riski tiktu savlaicīgi pārvaldīti pirms tie īstenojas.
Reputācija	Iestāde apzinās savus būtiskākos riskus, un, paaugstinoties to līmenim vai tiem īstenojoties, var savlaicīgi komunicēt ar iekšējām un ārējām ieinteresētajām, tostarp ietekmētajām pusēm, pierādot, kā iestāde ir sagatavojusies, lai mazinātu riskus un plāno arī turpmāk mazināt to varbūtību un/ vai ietekmi. Tādējādi ietekme uz iestādes reputāciju ir mazāk negatīva.	Riskiem īstenojoties vai paaugstinoties to līmenim, iestāde komunicējot ar ieinteresētajām un ietekmētajām pusēm, nevar demonstrēt, kā riski tika pārvaldīti līdz šim un kā varētu mazināt to ietekmi. Iestādes reakcija notiek pēc incidenta, nevis atbilstoši labas pārvaldības praksei, savlaicīgi un preventīvi tam gatavojoties. Līdz ar to tiek radīta negatīva reputācija iestādei un tās vidēja līmeņa un augstākajai vadībai.

Iestādes darbības nodrošināšanas būtiskākie pamatelementi	Ar risku vadību	Bez risku vadības
Sadarbība ar citām iestādēm, partneriem	Sadarbojoties ar ieinteresētajām pusēm (piemēram, darījumu partneriem, uzraugošajām iestādēm, citām valsts iestādēm, ar kurām ir kopīgi procesi un politikas mērķi, valdības noteiktās prioritātes), iestāde var laicīgi komunicēt par gaidāmajiem riskiem, it īpaši tādiem, kuru mazināšanai un vadībai nepieciešama ārējo pušu iesaiste. Tas veicina sadarbību un uzlabo darbības efektivitāti valsts iestāžu kopējos procesos, veido stabilas un pozitīvas attiecības ar iestādes partneriem. Risku vadība uzlabo iestādes vadības dialoga un lēmumu kvalitāti ar uzraugošajām iestādēm un sadarbības partneriem.	Sadarbojoties ar trešajām pusēm, iestāde var nonākt situācijā, kad iepriekš paredzamie riski nav pārrunāti, tie var būtiski aizkavēt kādu kopīgu projektu vai procesu un negatīvi ietekmēt vēlamo rezultātu sasniegšanu. Laicīga informācijas neatklāšana par gaidāmajiem riskiem mazina ieinteresēto pušu uzticību un sadarbības pamatus starp iestādēm, uzraugošajām iestādēm, sadarbības partneriem un tamlīdzīgi. Iepriekšminētais apgrūtina incidentu novēršanu jeb risku, kas ir īstenojušies, mazināšanu, (nepieciešams ieguldīt daudz vairāk resursus, tostarp finanšu un laika resursus).
Klientu apmierinātība	Ieinteresētās puses, tostarp iekšējie un ārējie klienti var gūt pārliecību par iestādes efektīvu risku vadību, ja iestāde demonstrē, ka tā apzina savus riskus un uz tiem pastāvīgi reaģē. Līdz ar to ieinteresētās puses ir apmierinātākas ar iestādes darbību un pozitīvāk novērtē tās sniegumu.	Ieinteresētās puses, tostarp iekšējie un ārējie klienti var negūt pārliecību par efektīvu risku vadību, ja iestāde nav savlaicīgi apzinājusi riskus un iespēju robežās tos mazinājusi. Līdz ar to ieinteresētās puses var būt neapmierinātas ar iestādes darbību, negatīvi novērtēt tās sniegumu, kā arī negatīvi ietekmēt tās reputāciju, publicējot plašsaziņas līdzekļos, tostarp sociālajos medijos negatīvu informāciju par iestādes neveiksmēm un problēmām.
Iekšējo vai ārējo pakalpojumu kvalitāte	Iestādē, kurā tiek apzināti un pārvaldīti riski, ir iespējams uzlabot pakalpojumu/ funkciju/ procesu kvalitāti, jo risku vadība palīdz savlaicīgi identificēt iespējamos apdraudējumus/potenciālos incidentus vai apstākļus, kas varētu negatīvi ietekmēt iestādes funkciju/ procesu/ pakalpojumu norisi. Tas attiecināms gan uz iestādēm, kam ir gan iekšējie, gan ārējie klienti tostarp, piemēram, kad iestādes struktūrvienības kāda procesa ietvaros saņem pakalpojumu no citas struktūrvienības.	Iestādē, kurā nav ieviesta risku vadība, var rasties atkārtotas un ilgstoši neatrisinātas kvalitātes problēmas vai attīstības kavējumi funkcijās/procesos/pakalpojumos, kas kopumā pasliktina to kvalitāti.

Iestādes darbības nodrošināšanas būtiskākie pamatelementi	Ar risku vadību	Bez risku vadības
Darbības nepārtrauktības incidenti, krīzes situācijas	Risku vadība ļauj apzināt darbības nepārtrauktības scenārijus, to potenciālo ietekmi, kā arī veicina iestādes gatavību reaģēt uz darbības nepārtrauktības incidentiem, ņemot vērā izstrādātos darbības nepārtrauktības plānus. Identificējot darbības nepārtrauktības riskus, iestādei ir iespēja savlaicīgi apzināt pagaidu jeb alternatīvos risinājumus incidentu un krīzes gadījumos, kā arī plānot un ieviest jau preventīvi šo risku mazināšanas pasākumus. Iestāde, kurā ir ieviesta risku vadība, ir labāk sagatavojusies negaidītiem pavērsieniem un krīzēm, kā arī plāno un ievieš pasākumus, lai incidenti un krīzes neatkārtotos. Risku vadība sagatavo iestādi ne tikai krīzes un ārkārtas situācijām, bet gan arī pārmaiņu vadībai kopumā.	Nevērtējot riskus, darbības nepārtrauktības scenāriji, kas apdraud iestādes darbību, tiem īstenojoties, iestāde nebūs sagatavojusies, lai uz tiem reaģētu tā, lai rastos pēc iespējas mazāk zaudējumu, kā arī tā nenodrošinās darbību, izmantojot alternatīvus risinājumus, un tiks ievērojami apgrūtināta atgriešanās iepriekšējā darbības režīmā atbilstoši normatīvajos aktos noteiktajām prasībām. Tāpat nereaģējot uz darbības nepārtrauktības incidentiem jeb darbības nepārtrauktības riskiem, kas ir īstenojušies, iestādes var izraisīt valsts mēroga krīzes situācijas. Negaidītas krīzes situācijas iestādēs, kurās nav risku vadības, var radīt haotisku un nekoordinētu pieeju incidentu un krīžu novēršanai, kā arī pieļaut to regulāru atkārtošanos.
Iekšējā komunikācija, sadarbība	Risku vadība veicina iestādes struktūrvienību sadarbību un saliedēšanos, ieviešot kopīgus risinājumus risku mazināšanā un veicot pieredzes apmaiņu par risku vadības labo praksi. Risku vadība ļauj risināt neskaidrības savstarpējo procesu saskares/ mijiedarbības punktos, tas ir, kad atbildība par kādu procesu ir dalīta, saistīta vai pat neskaidra. Kopīga un mērķtiecīga risku vadība uzlabo iestādes iekšējo sadarbības mikroklimatu. Darbinieki un vadītāji jūtas uzklausīti un novērtēti, ja to idejas, kā mazināt riskus un uzlabot iestādes darbību, tiek praktiski pielietotas.	Iestādēs, kurās risku vadība nav ieviesta, var būt neatrisinātas problēmas un nevadīti riski, kas rada neapmierinātību iestādes struktūrvienībās un pasliktina to savstarpējo mijiedarbību. Iekšējā komunikācija par riskiem un ar tiem saistītajām tēmām var būt neefektīva, nepietiekami atklāta un ierobežota. Pat ja atsevišķiem iestādes darbiniekiem ir izveidojies viedoklis par riskiem un iespējām, kā tos mazināt, iestādē, kurā nav ieviesta risku vadība, šādi viedokļi un pieredze netiek izmantota praksē, kā rezultātā darbinieki var nejusties uzklausīti un pietiekami novērtēti.
Ārējā komunikācija	Iestāde, kurā ieviesta risku vadība, risku īstenošanās gadījumā var laicīgi komunicēt ar sabiedrību un citām ārējām pusēm (piemēram, darījumu partneriem, uzraugošajām iestādēm) un tādējādi demonstrēt, ka neskatoties uz to, ka riski īstenojas, vai būtiski pieaug to līmenis, iestāde ir tos apzinājusi un gatavojusies. Kopumā sabiedrība un ārējās ieinteresētās	Iestāde, kurā nav ieviesta risku vadība, risku rašanās gadījumā nevar demonstrēt sabiedrībai vai citām ārējām pusēm, ka tā bija gatavojusies risku līmeņu paaugstināšanās gadījumiem vai nozīmīgiem incidentiem, kā arī krīzēm. Tas neliecina par labas pārvaldības principu ievērošanu un mazina uzticību iestādes darbībai kopumā.

Iestādes darbības nodrošināšanas būtiskākie pamatelementi	Ar risku vadību	Bez risku vadības
	puses sagaida no iestādēm šādu atbildīgu pieeju un rīcību.	
Iestādes resursu un vērtību aizsardzība	Risku vadību var izmantot, lai strukturēti reaģētu uz sarežģītiem ārējiem draudiem, meklētu risinājumus iestādes resursu, aktīvu un vērtību aizsardzībai. Risku vadība veicina vienmērīgāku un stabilāku iestādes darbības sniegumu, kā rezultātā ir mazāka iespēja piedzīvot negaidītas būtiskas novirzes no plāna un izpildāmajiem rādītājiem/ uzdevumiem.	Iestādē, kurā nav ieviesta risku vadība, ārējo draudu vai negatīvu apstākļu ietekmē var pietrūkt risinājumu, lai aizsargātu resursus, aktīvus un vērtības (gan materiālā, gan nemateriālā veidā).

⚠ **Svarīgi**: Risku vadībai jābūt integrētai iestādes ikdienas operacionālajos procesos - risku vadība nedrīkst kļūt par formalitāti vai administratīvo slogu!

2.2. Risku vadība un iekšējās kontroles sistēma

Iekšējās kontroles sistēma (turpmāk - IKS) ir iestādes pārvaldības elementu kopums - procedūras, procesi, noteikumi, kas nodrošina mērķu sasniegšanu, sniedz norādes, optimizē resursu izmantošanu un uzlabo efektivitāti, stiprina atbilstību iekšējām un ārējām prasībām.

Efektīva IKS darbība iestādei ļauj nodrošināt paredzamu un nepārtrauktu darbību, novērst rīcības un darbības, kas tiek uzskatītas par iestādei nevēlamām, kā arī savlaicīgi paredzēt un mazināt iespējamos riskus iestādē, tostarp tās struktūrvienību un procesu līmenī.

Publiski pieejamās COSO Iekšējā kontroles sistēma – Integrētais ietvars (COSO *Internal Control – Integrated Framework*) vadlīnijas[7] apraksta IKS un piecus to veidojošos pamatelementus. 5. tabulā aprakstīti IKS pamatelementi.

5. tabula. IKS pamatelementi

IKS pamatelements	IKS pamatelementa skaidrojums
1. Iekšējās kontroles vide	Vadības nostāja un uzstādījumi attiecībā uz kontroles vidi, ņemot vērā iestādes kultūru un attiecināmās ētikas normas. Kontroles vidi veido tās ietvars, tas ir, iekšējo normatīvo aktu un procesu kopums. Kontroles vide ir pamats pārējiem IKS pamatelementiem. Efektīvu IKS veido,

[7] COSO vadlīnijas https://www.coso.org/sitepages/internal-control.aspx?web=1, https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf

IKS pamatelements	IKS pamatelementa skaidrojums
	skaidri nosakot konkrētu atbildības un pienākumu sadalījumu IKS ieviešanā un pārraudzībā, ievērojot iestāžu darbības ētikas pamatprincipus un labo praksi. Papildu tam būtiski IKS kontroles vides elementi ir iestādes stratēģisko, darbības mērķu un darbinieku pienākumu noteikšana, piemēram, iestādes darbības stratēģija, darbības plāns, Ētikas kodekss un darbinieku amatu apraksti.
2. Risku novērtēšana	Riski, kas apdraud iestādes mērķu sasniegšanu un dažādi kontroļu veidi risku mazināšanai. Risku vadības un efektīvas IKS ietvaros jāvērtē iestādes iekšējā un ārējā vide, lai identificētu risku tendences, tostarp risku līmeņu izmaiņas. Piemēram, izstrādājot iestādes darbības stratēģiju, veic SVID analīzi, kas ir situācijas analīze visās nozares jomās, lai izvērtētu iekšējās un ārējās vides faktorus, nosakot iestādes stiprās puses, vājās puses, iespējas un draudus. Šo analīzi izmanto, lai novērtētu četrus dažādus faktorus, kas saistīti ar jebkuru situāciju. Tāpat iespējams izmantot PESTLE analīzi, kuras ietvaros tiek noteikti politiskie, ekonomiskie, sociālie, tehnoloģiskie, juridiskie un vides ietekmes faktori, kuri jāņem vērā, plānojot iestādes attīstību. Tās ietvaros svarīgi atbildēt uz šādiem jautājumiem: • kāda ir valsts politiskā situācija un kā tā var ietekmēt nozari; • kādi ir dominējošie ekonomiskie faktori; • cik liela nozīme ir saskarsmes vai klientu apkalpošanas kultūrai un kādi ir tās noteicošie faktori; • kādi tehnoloģiskie jauninājumi, visticamāk, tuvākajā laikā radīsies un ietekmēs nozari; • vai var rasties izmaiņas nozari reglamentējošajos tiesību aktos, kas skars iestādes darbību; • kādas ir vides problēmas nozarē. Ievērojot iepriekšminēto analīžu rezultātus, iespējams labāk izprast riskus, ar kādiem iestāde var saskarties, īstenojot darbības stratēģiju.
3. Kontroles	Efektīvai IKS ir vienlīdz svarīgas esošās kontroles, kā arī papildu vai jauni ieviešamie risku mazināšanas pasākumi, kas vērsti uz risku cēloņu novēršanu. Zināmā mērā kontroles var būt ieviestas jebkurā iestādē, neatkarīgi no tā, vai ir ieviesta risku vadība (piemēram, pienākumu nodalīšana, procedūru, amatu pienākumu dokumentācija, drošības risinājumi, lēmumu pieņemšanas un autorizācijas līmeņi, neatkarīga uzraudzība, "četru acu princips"). Iekšējās kontroles var būt digitalizētas jeb automatizētas, piemēram, informācijas sistēmās ieprogrammēti algoritmi vai formulas, kas nodrošina korektus aprēķinus, loģiskās pārbaudes un kļūdu novēršanu. Efektīvai IKS nepieciešamas samērojamas ar riskiem/ optimālas, skaidri saprotamas un noteiktas kontroles. Kontroles ir elementi, kas kopīgi COSO ERM.
4. Informācija un komunikācija	Atbilstoša informācija īstajā laikā un vietā, ko nodrošina gan iekšējā, gan ārējā komunikācija. Ļoti būtisks risku vadības ieviešanas priekšnosacījums un IKS elements ir regulāra, atbilstošām mērķauditorijām paredzēta komunikācija un informācijas apmaiņa par: • riskiem, to līmeņiem, tendencēm, potenciālajām sekām;

IKS pamatelements	IKS pamatelementa skaidrojums
	• iespējamajiem risinājumiem risku mazināšanai; • IKS darbību, un tās iespējamiem nepieciešamajiem pilnveidojumiem. Piemēram, regulāras vadības sanāksmes, kuru darba kārtībā iekļauts jautājums par riskiem, to vadību, iestādes iekšējās komunikācijas aktivitātes un regulāra informēšana par risku vadību (piemēram, intranets).
5. Uzraudzība	IKS elementu pārskatīšana un efektivitāte. Regulāra IKS novērtēšana, lai nodrošinātu, ka ikviens no pieciem tās pamatelementiem ir ieviests un atbilstoši funkcionē. Šī pamatelementa īstenošanā būtiska loma ir iekšējam auditam vai ārējiem neatkarīgajiem ekspertiem, kurus var piesaistīt IKS novērtēšanā (iekšējā audita vai ārējās pārbaudes rezultātā saņemot ziņojumu ar novērtējumu par IKS darbības efektivitāti un iespējamiem uzlabojumiem).

IKS mērķi:

- aizsargāt iestādes resursus un vērtības;
- nodrošināt darbību efektivitāti;
- atbalstīt iestādes pārskatu un atskaišu uzticamību;
- nepieļaut dažādu līmeņu iestādes darbinieku un vadītāju rīcības, kas neatbilst iekšējiem normatīvajiem aktiem un tiesību aktiem kopumā.

Līdz ar to secināms, ka risku vadība ir viens no IKS elementiem, ņemot vērā COSO Iekšējās kontroles sistēma – Integrētais ietvars vadlīnijas. Lai risku vadība veiksmīgi un rezultatīvi darbotos, ir jābūt ieviestiem un attīstītiem arī pārējiem IKS elementiem.

Svarīgi: IKS un risku vadība negarantē visu iestādes mērķu izpildi un nenovērš visu risku varbūtību un ietekmi, taču abas šīs jomas ir būtiski vadības rīki un iestādes pārvaldības elementi, kuru iedzīvināšanai un uzturēšanai ir svarīga augstākās vadības attieksme un kopējā pārvaldības, kontroļu un risku kultūra iestādē.

2.3. Risku vadības sistēmas ietvars

Risku vadības sistēma ir vadības noteiktais procesu, struktūras un pasākumu kopums, ko vadība sistemātiski īsteno, lai identificētu, novērtētu, vadītu un kontrolētu potenciālos notikumus vai situācijas, kas apdraud iestādes mērķu sasniegšanu.

Pasaulē ir izstrādātas neskaitāmi daudz risku vadības pieejas, metodikas, vadlīnijas, ietvari un standarti (skat. 1.nodaļu), kas sniedz padomus, kā iestādes vadībai labāk organizēt un vadīt riskus. Latvijā visvairāk atzītākie un izmantotākie ir, piemēram:

- ISO 31000:2018 (skat. 2.3.1. nodaļu);
- COSO ERM (skat. 2.3.2. nodaļu).

Tāpat atsevišķās valstīs, kā, piemēram, Apvienotajā Karalistē, populāra ir arī Oranžā grāmata (*The Orange Book*) (skat. 2.3.3. nodaļu).

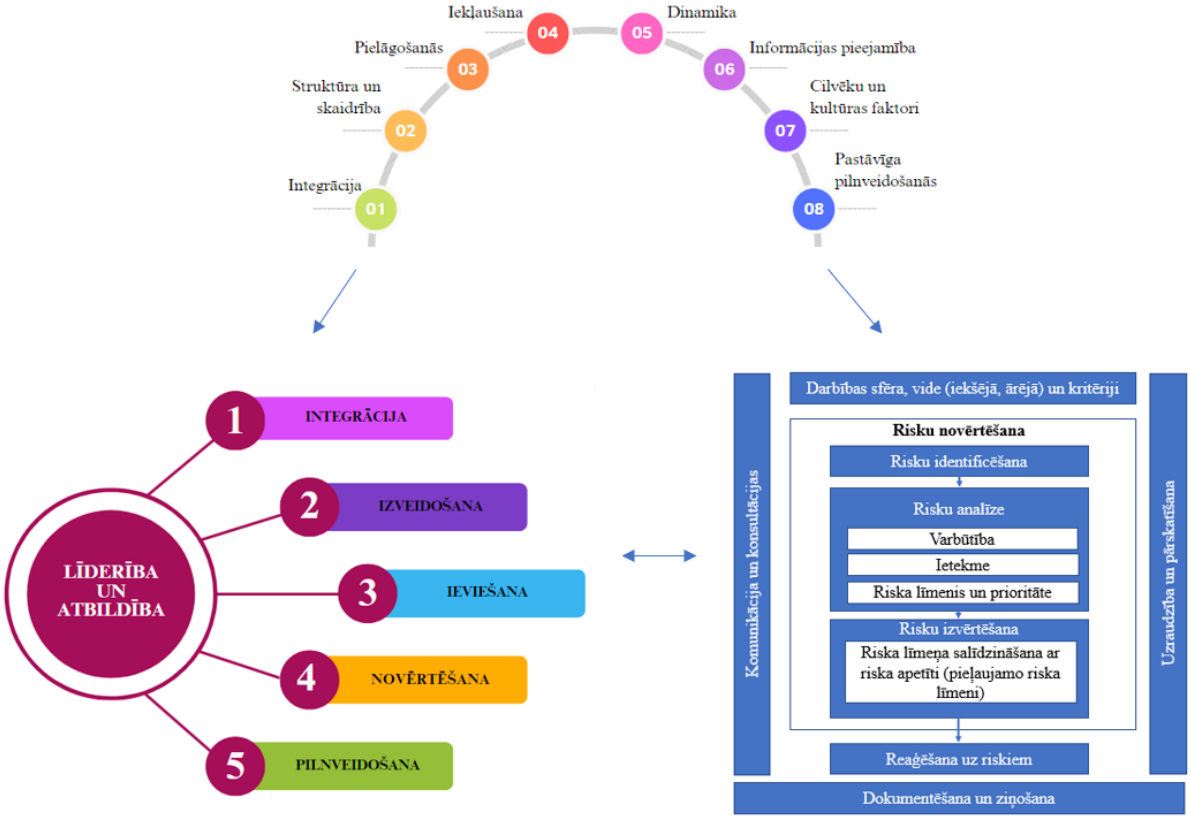
Lai praksē ieviestu labās starptautiskās prakses modeļus, standartus, vadlīnijas, tostarp to principus, iestādē ir nepieciešams izstrādāt un apstiprināt risku vadības politiku un risku vadības politikas ieviešanu skaidrojošos normatīvos aktos, piemēram, risku vadības kārtību/ instrukciju/ procedūru, kuru saturs aprakstīts 4.2. nodaļā.

2.3.1. ISO 31000:2018 "Risku vadība – Vadlīnijas"

ISO 31000:2018 ir Starptautiskās sertifikācijas organizācijas (ISO) izdotais standarts, kas pēdējo reizi atjaunināts 2018.gadā un sniedz vadlīnijas organizācijām labākas riska pārvaldības nodrošināšanai.

ISO 31000:2018 risku vadības standarts apraksta risku vadības principus, ietvaru un procesu, kuru ieviešot var panākt efektīvu, produktīvu un konsekventu risku vadību. Standarts ir piemērojams neatkarīgi no nozares, darbības veida un iestādes lieluma (1.attēls).

1. attēls. Risku vadības principi, ietvars un process[8]



ISO 31000:2018 standartā iekļauti 8 **pamatprincipi**:

- integrācija – risku vadībai jābūt ietvertai visās iestādes darbībās kā neatņemamai sastāvdaļai (t.i. risku vadība ir daļa no iestādes esošajiem pārvaldības procesiem, uzraudzības un komunikācijas procesiem un risku informācija tiek izmantota mijiedarbībā un kopumā ar iestādes darbības rezultātiem);
- struktūra un skaidrība – strukturēta un skaidra pieeja risku vadībā palīdz sasniegt sagaidāmus un salīdzināmus rezultātus;

[8] ISO 31000:2018 standarts

- pielāgošanās – jāizveido un jāpielāgo samērīgs risku vadības ietvars un process, kas būtu piemērots iestādes ārējai un iekšējai darbības videi, vienlaikus, ņemot vērā tās mērķus;
- iekļaušana – pietiekama un savlaicīga visu ieinteresēto pušu iesaiste ļauj ņemt vērā viņu zināšanas, viedokļus un priekšstatus, kas uzlabo izpratni un pārdomātāku lēmumu pieņemšanu risku vadībā;
- dinamika – mainoties iestādes ārējai un iekšējai videi, rodas, mainās un pārstāj eksistēt arī riski, tāpēc risku vadībai jāspēj tos paredzēt, atklāt, apzināt un vadīt pietiekami un savlaicīgi;
- informācijas pieejamība – risku vadībā tiek izmantota vēsturiska un aktuālā informācija, kā arī nākotnes prognozes, taču jāapzinās šādas informācijas ierobežojumi un ticamība. Ieinteresētajām pusēm jānodrošina savlaicīgi labākā pieejamā informācija.
- cilvēku un kultūras faktori – būtiski ietekmē visus risku vadības aspektus visos tās līmeņos un posmos.
- pastāvīga pilnveidošanās – risku vadība pastāvīgi un nepārtraukti jāpilnveido, apgūstot jaunas zināšanas un pieredzi.

Piemērs: Publiski pieejamajās valsts kapitālsabiedrību Risku pārvaldības politikās iekļauti, piemēram, šādi risku vadības principi:

- risku vadība tiek plānota, ieviesta un pilnveidota atbilstoši Valdošā uzņēmuma, kā arī Atkarīgo sabiedrību vidēja termiņa darbības stratēģijai[9];
- risku vadības process ir nepārtraukts un regulārs stratēģiskas nozīmes process Koncernā[10].
- risku pārvaldība paredzēta, lai apzinātu prioritāri risināmos un pārvaldāmos riskus un attiecīgi prioritāros uzdevumus to mazināšanai[11];
- risku pārvaldības procesā iesaistās visi LVM vadītāji un citi darbinieki, lai veicinātu izpratni par risku ietekmi un sadarbotos risku mazināšanas pasākumu ieviešanā[12].

ISO 31000:2018 standarts apraksta risku vadības ietvaru ar šādiem 6 **elementiem**:

- vadības loma – iestādes vadībai jādemonstrē atbildības uzņemšanās un iniciatīva pielāgot un ieviest risku vadības ietvara visus elementus, kā arī noteikt risku vadības politiku un nodrošināt tās ievērošanu, piešķirt nepieciešamos resursus un noteikt pienākumu un atbildības sadalījumu risku vadībā;
- integrācija – lai arī ir svarīgi mazināt risku ietekmi un integrēt risku mazinošos pasākumus iestādes darbības procesos, tomēr ir svarīgi neradīt būtiskus šķēršļus vai kavējumus operacionālo procesu norisei;
- izveidošana – iestādei jāpielāgo risku vadība atbilstoši tās ārējai un iekšējai darbības videi, uzņemoties risku vadību integrēt visos procesos, nosakot pienākumu un atbildības sadalījumu, piešķirot resursus, paredzot komunikācijas un konsultēšanās procesus;

[9] VAS "Latvijas Dzelzceļš" risku vadības principi pieejami šeit: https://www.ldz.lv/lv/risku-vadibas-politika
[10] VAS "Latvijas Dzelzceļš" risku vadības principi pieejami šeit: https://www.ldz.lv/lv/risku-vadibas-politika
[11] VAS "Latvijas Valsts meži" risku vadības principi pieejami šeit: https://www.lvm.lv/images/lvm/Par_mums/risku_vadibas_politika.pdf
[12] VAS "Latvijas Valsts meži" risku vadības principi pieejami šeit: https://www.lvm.lv/images/lvm/Par_mums/risku_vadibas_politika.pdf

- ieviešana – risku vadība jāievieš plānveidīgi, un paredzot risku vadības ieviešanas plāna īstenošanai pietiekamus resursus, tostarp laika resursus, ņemot vērā lēmumu pieņemšanas procesus iestādē, kā arī pārliecinoties, ka visām iesaistītajām pusēm ir skaidra viņu loma;
- novērtēšana – periodiski jāmēra risku vadības rezultāti salīdzinājumā ar risku vadības mērķi, ieviešanas plāniem, rādītājiem un sagaidāmo rīcību. Tāpat jāizprot, vai risku vadība joprojām palīdz uzlabot iestādes mērķu sasniegšanu;
- pilnveidošana – iestādei pastāvīgi jāpilnveido risku vadība, ņemot vērā mainīgo ārējo un iekšējo vidi, kā arī jānosaka pasākumi risku vadības pilnveidošanai.

ISO 31000:2018 iesaka risku vadības ieviešanu veikt **secīgos posmos** un tos secīgi un pastāvīgi atkārtot:

- komunikācija un konsultēšana – šī posma mērķis ir apkopot risku vadībā iesaistīto pušu zināšanas, viedokļus, informāciju, lai veidotu vienotu izpratni par riskiem un to vadību, nodrošinātu pietiekamu un piemērotu informāciju lēmumu pieņemšanai visos risku vadības posmos un veicinātu atbildības uzņemšanos par risku mazināšanu (piemēram, iekšējā komunikācija par iestādes risku vadības metodiku un risku analīzes rezultātiem, konsultācijas par risku vadības principiem iestādes darbiniekiem, vidējā un augstākā līmeņa vadībai);
- darbības sfēra, vide (iekšējā un ārējā), kritēriji – risku vadības pielāgošana iestādes darbības specifikai un vajadzībām (piemēram, noteikt, uz kuriem procesiem un iestādes funkcijām risku vadība attiecas);
- risku novērtēšana – secīgi veicot šādus apakšposmus:
  - risku identificēšana – meklējot iestādes mērķu sasniegšanu ietekmējošos draudus (skat. 5.4. nodaļu);
  - risku analīze – veicot risku izpēti par dažādiem risku parametriem, tai skaitā risku līmeni, sarežģītību, cēloņiem, varbūtību, apstākļiem un iespējām tos kontrolēt (skat. 5.5. nodaļu);
  - risku izvērtēšana – salīdzināt risku analīzes rezultātus ar noteiktiem kritērijiem un saprast, vai ir nepieciešamas papildus darbības (skat. 5.5. un 5.6. nodaļu);
- reaģēšana uz riskiem – izvēlēties, plānot un piemērot risku mazināšanas pasākumus (skat. 5.7. nodaļu);
- uzraudzība un pārskatīšana – nodrošināt un uzlabot risku vadības procesa izveides, ieviešanas un rezultātu kvalitāti un efektivitāti (skat. 5.12. nodaļu);
- dokumentēšana un ziņošana – dokumentēt risku vadības procesu un sniegt informāciju par risku vadības aktivitātēm un to rezultātiem (skat. 5.13. nodaļu).

2.3.2. COSO ERM: Organizācijas riska pārvaldība - risku iekļaušana stratēģijā un darbības vadīšanā

COSO ERM - risku iekļaušana stratēģijā un darbības vadīšanā ir Amerikas Savienoto Valstu piecu lielāko grāmatvežu asociāciju un institūtu dibinātās Trīdveja komisijas sponsorējošās organizācijas komitejas (*Committee of Sponsoring Organizations of the Treadway Commission*) izdots labākās prakses risku vadībā apkopojums, kura jaunākā versija publicēta 2017.gadā.

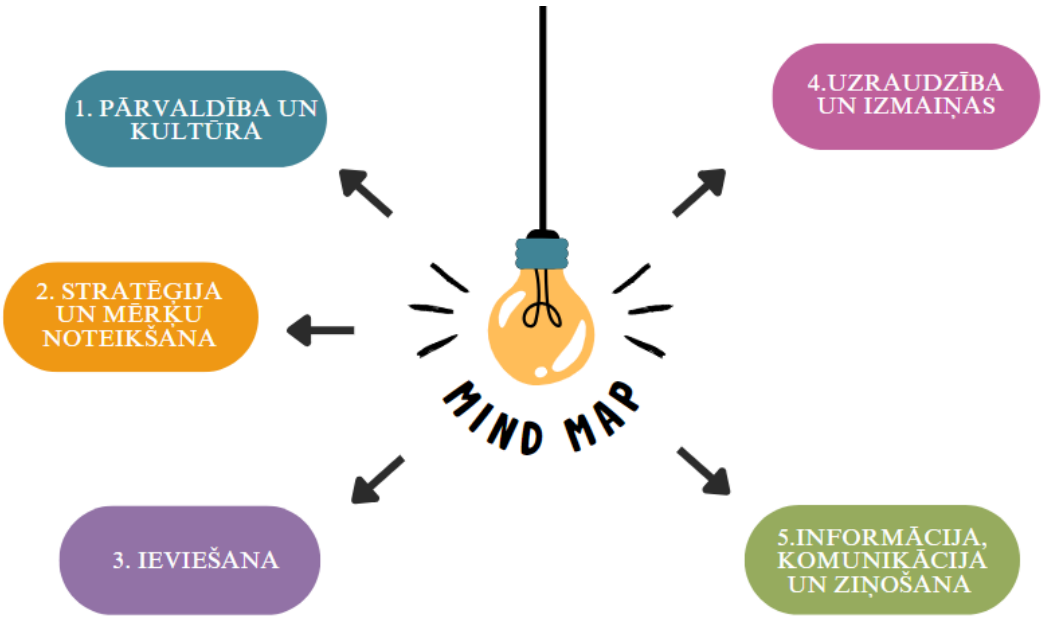
COSO ERM risku vadības ietvara pēdējā publicētajā versijā tiek uzsvērta risku vadības būtiskā nozīme stratēģiskās plānošanas procesā (2. attēls) un iekļaušana visu iestādes procesu izpildē visos organizatoriskajos līmeņos, kas skaidrota principu veidā. Ietvars ir principu kopums, kas sakārtots piecos savstarpēji saistītos komponentos.

2. attēls. Risku vadības procesa integrēšana stratēģiskajā vadībā

Iestādes misija, vīzija un pamatvērtības nosaka, kur tā tiecas būt un kā tā vēlas veikt darbību. Lielākajai daļai iestāžu misija, vīzija un pamatvērtības laika gaitā paliek stabilas, un stratēģijas plānošanas laikā tās parasti tiek atkārtoti apstiprinātas. Iestāde, kas definējusi misiju, vīziju un pamatvērtības, var izstrādāt stratēģiju, kā arī noteikt mērķus, ņemot vērā vēlamo riska profilu. Tādējādi risku vadība palīdz iestādei apzināt riskus, kas saistīti ar stratēģiju. Iestādei jāizvērtē, kā izvēlētā stratēģija varētu ietekmēt tās riska profilu, jo īpaši riska veidus un apjomu, kam iestāde tiks pakļauta. Ieviešot stratēģiju, var rasties jauni riski, kurus nebija sākotnēji iespējams paredzēt un kurus nepieciešams ņemt vērā turpmāk. Savukārt, iestādes pievienoto vērtību lielā mērā nosaka vadības pieņemtie lēmumi (vispārējie stratēģiskie lēmumi un ikdienas operacionālie lēmumi). No lēmumu kvalitātes ir atkarīgs, vai pievienotā vērtība tiek radīta, saglabāta, uzlabota vai mazināta. Pievienotā vērtība tiek radīta un saglabāta, ja izlietotie resursi (piemēram, finanses un tehnoloģijas) ir mazāki par ieguvumiem. Piemēram, iestādē vērtība tiek saglabāta un uzlabota, piegādājot tādus produktus un pakalpojumus, kā rezultātā ieinteresētās puses, tai skaitā klienti ir apmierināti, kā arī to apmierinātība palielinās.

COSO ERM risku vadības ietvars iedalīts piecās komponentēs (3. attēls).

3. attēls. COSO ERM ietvara komponentes



COSO ERM piecas komponentes tiek atbalstītas ar 20 principu kopumu. Šie principi aptver komponentes, sākot no pārvaldības līdz pat uzraudzībai, ņemot vērā labo praksi, un ko var piemērot dažādās iestādēs neatkarīgi no lieluma vai nozares. Šo principu ievērošana var nodrošināt, ka iestādē saprot un cenšas vadīt riskus, kas saistīti ar tās stratēģijas ieviešanu un pamatdarbību.

COSO ERM noteiktās komponentes un tām pakārtotie principi ir šādi:

1. **Pārvaldība un kultūra**: Pārvaldība nosaka iestādes attieksmi pret risku vadību un uzsver tās nozīmīgumu, kā arī pārraudzības lomu. Savukārt, kultūra veicina ētisku vērtību noteikšanu un rašanos, atbilstošu uzvedību un izpratni par risku vadību iestādē (skat. 2. un 3.nodaļu).
   - Šajā komponentē paredzētie principi ir:
     - risku pārraudzība no "augšas";
     - operatīvu struktūru izveide;
     - vēlamās kultūras noteikšana;
     - apņemšanās ievērot pamatvērtības;
     - spējīgu indivīdu piesaiste, attīstība un noturēšana.
2. **Stratēģija un mērķu noteikšana**: Iestādes risku vadība, stratēģija un mērķu noteikšana savstarpēji integrējas stratēģiskās plānošanas procesā. Risku apetīti (skat. 4.3. nodaļu) paredz un pielāgo stratēģijai; stratēģiju, nosakot mērķus, pārvērš rīcības plānā, kas vienlaikus palīdz identificēt, novērtēt un mazināt riskus.
   - Šajā komponentē paredzētie principi ir:
     - iestādes darbības vides analīze;
     - risku apetītes definēšana;
     - alternatīvo stratēģiju izvērtēšana;
     - iestādes darbības mērķu noteikšana.
3. **Ieviešana**: Stratēģijas ieviešanu un noteikto mērķu sasniegšanu ietekmējošie riski ir jāidentificē un jānovērtē. Risku līmeni salīdzina ar risku apetīti, un konstatē situācijas, kad tā ir pārsniegta, lai pienācīgi reaģētu, mazinot riska līmeni. Iestāde izvēlas risku vadības, pasākumus, kā arī iekļauj risku kopējā portfelī, riskus, vērtējot portfeļa kopskatu atkarībā no individuālā riska aprēķinātā līmeņa. Šī procesa rezultāti tiek ziņoti galvenajām risku vadībā iesaistītajām pusēm (skat. 5. nodaļu).
   - Šajā komponentē paredzētie principi ir:
     - risku identificēšana;
     - risku ietekmes (*severity*) noteikšana;
     - risku prioritizēšana;
     - reaģēšana uz risku;
     - risku portfeļa skatījuma veidošana.
4. **Uzraudzība un izmaiņas**: Vērtējot iestādes darbības rezultātus, iestāde var vērtēt riska vadības elementu darbības efektivitāti un, būtisku iestādes darbības izmaiņu gadījumā, veikt izmaiņas arī risku vadībā. (skat. 5.12. nodaļu)
   - Šajā komponentē paredzētie principi ir:
     - būtisku izmaiņu novērtēšana;
     - risku un snieguma pārskatīšana;
     - tiekšanās uz risku vadības pilnveidošanu.
5. **Informācija, komunikācija un ziņošana**: Efektīvai riska vadībai nepieciešama pastāvīga informācijas par riskiem iegūšana un apmaiņa no iekšējiem un ārējiem informācijas avotiem, kas tiek virzīta visā iestādes iekšējā darbībā. (skat. 5.13. nodaļu).
   - Šajā komponentē paredzētie principi ir:
     - informācijas un tehnoloģiju lietošana;
     - risku informācijas izplatīšana;
     - ziņošana par risku, kultūru un sniegumu.

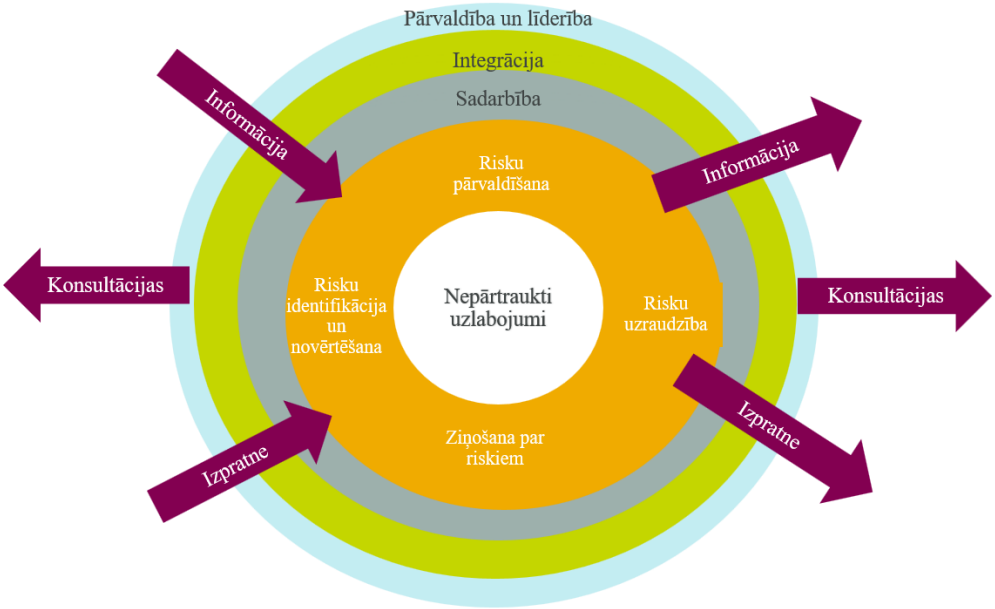
Salīdzinot ISO 31000:2018 standartu un COSO ERM, var konstatēt, ka:

- abi iepriekšminētie ietvari apraksta risku ne tikai kā negatīvu draudu, bet arī mudina uzņemties "apzinātu risku" labāku rezultātu sasniegšanai;
- abi ietvari ir rekomendējoša rakstura un neparedz atbilstības sertificēšanu, kas varētu apliecināt prasību pietiekamu ieviešanu un ievērošanu;
- abi ietvari iesaka risku vadību iekļaut lēmumu pieņemšanas procesos, vadībai uzņemoties riskus samērīgā apjomā;
- ISO 31000:2018 standartā riska apetītes jēdziens netiek izmantots un skaidrots, tā vietā izmantojot līdzvērtīgu jēdzienu – risku kritēriji. Taču COSO ERM risku vadības ietvarā iekļauts garāks apraksts un piemēri par risku apetītes, tolerances un kapacitātes jēdzieniem.

2.3.3. Oranžā grāmata

Oranžā grāmata ("The Orange Book")[13] ir Apvienotās Karalistes valsts pārvaldes un publiskā sektora vajadzībām izstrādāts risku vadības ietvars (4. attēls) kopā ar to skaidrojošajiem dokumentiem (vadlīnijas, rokasgrāmata u.tml.).

4. attēls. Oranžās grāmatas ietvars[14]



Šī ietvara saturs ir līdzīgs ISO 31000:2018 standartam, jo tas paredz, ka:

- **risku vadībai jābūt daļai no iestādes pārvaldības un līderības (vadības)**. Praktiski tas nozīmē, ka risku vadībai ir jābūt tādam pašam risinājumam un procesam, kas tiek izmantots un vērtēts līdzvērtīgā līmenī, kā, piemēram, stratēģiskā plānošana, iekšējais audits, juridiskais atbalsts. Tas nozīmē, ka risku vadības rezultāti jāizvērtē un jāapstiprina tādā pašā līmenī, kā citu pārvaldības funkciju rezultāti un lēmumi. Risku vadībai, tāpat kā, piemēram, budžeta plānošanai un izpildes kontrolei, ir jābūt vienam no kontroles un pārvaldības mehānismiem dažādos iestādes vadības līmeņos. Risku vadībai ir jābūt formāli noteiktai un attiecināmai uz

[13] Orange Book - GOV.UK (www.gov.uk)
[14] Orange Book - GOV.UK (www.gov.uk)

visu iestādi kopumā (skat. 3. nodaļu "Risku kultūra"), tostarp jābūt noteiktām risku vadībā iesaistīto lomām, kā arī jānodrošina informācijas apmaiņa un komunikācija par riskiem;

- **risku vadībai** iespēju robežās jābūt **integrētai lēmumu pieņemšanā dažādos pārvaldības līmeņos**. Piemēram, pirms tiek apstiprināts iestādes vai struktūrvienības gada darbības plāns, jāpārliecinās, ka ir veikta risku analīze. Pirms tiek saskaņots kāds investīciju projekts (piemēram, ārējs projekts iestādes infrastruktūrā vai iekšējs informācijas sistēmas attīstības projekts), jāveic risku analīze un lēmums par projekta īstenošanu jāpieņem, ņemot vērā risku analīzes rezultātus. Iestādes augstākajai vadībai regulāri jāuzrauga vismaz būtiskākie riski un jānosaka pienākumi vidēja līmeņa vadītājiem pārvaldīt to kompetencē esošos riskus.
- **risku vadībai ir jābūt regulāras sadarbības un informācijas apmaiņas rezultātam**. Praksē tas nozīmē, ka iestādē ir noteikta regularitāte un atbildīgie, kā arī sanāksmju veidi vai informācijas kanāli, kuros pastāvīgi tiek nodrošināta risku vadībai nepieciešamā informācija. (skat. Rokasgrāmatas 5.13. nodaļu par risku informācijas apmaiņu un komunikāciju)
- **risku vadībai jāiekļauj visi būtiskie risku vadības posmi**: risku identificēšana un novērtēšana, reaģēšana uz riskiem, risku uzraudzība un risku ziņošana (skat. Rokasgrāmatas 5. nodaļu "Risku vadības process").
- risku vadības funkcija ir periodiski jānovērtē un jānodrošina tās attīstība, piemēram, papildu brieduma modeļa kritēriju ieviešana praksē.

2.4. Risku vadības loma iestādes darbības plānošanā – risku vadības sasaiste ar stratēģisko un operacionālo plānošanu

Viens no stratēģisko un operacionālo mērķu īstenošanas priekšnosacījumiem ir to sasniegšanu apdraudošo risku identificēšana, analīze un pārvaldība.

Risku vadība ir cieši saistīta ar iestādes darbības (mērķu) plānošanu. Iestādei uzsākot ieviest risku vadību, tā atbilst sākotnējam brieduma līmenim, un iestādes darbības un mērķu plānošana eksistē bez risku vadības, bet, iestādei attīstoties un pilnveidojot risku vadību, sasaiste starp šīm jomām kļūst arvien spēcīgāka. Savukārt, risku vadība nevar tikt pilnvērtīgi īstenota, ja iestādē nav ieviesta darbības plānošana, kā arī, ja nav skaidri definēti un izmērāmi mērķi.

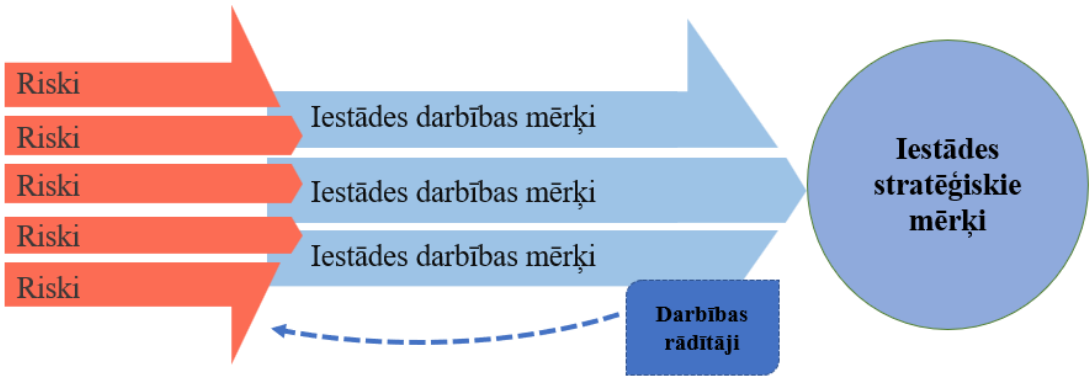
Informācija par potenciālajiem riskiem ir noderīga daudziem procesiem iestādē, jo tā palīdz veidot reālākas nākotnes prognozes, paredzēt pietiekamus resursus un sagatavot rīcības scenārijus gadījumiem, kad riski īstenojas. Iestādes darbības plānošanas ietvaros risku vadītājam un risku īpašniekiem ir iespēja identificēt riskus to sākuma stadijā un pilnvērtīgi vadīt riskus attiecīgajās iestādes darbības jomās.

Risku analīze tiek veikta, lai noteiktu, kuri no darbības plāniem un sasniedzamajiem mērķiem un tiem pakārtotajiem rezultātiem ir apdraudēti, kā arī, kādi riski, kuru līmenis pārsniedz risku pieļaujamo līmeni/ apetīti, ir jāvada, lai šos plānus īstenotu un sasniegtu izvirzītos mērķus. Tas ir, identificētos riskus būtu jāspēj sasaistīt ar konkrētiem mērķiem, kurus tie ietekmē, pat, ja tas būtu netieši, tas ir, ņemot vērā kaskadētos operatīvos darbības plānus un apakšmērķus.

Izstrādājot iestādes darbības plānus, iespējams vērtēt, kādi riski apdraud šo plānu īstenošanu. Tādējādi iestādes darbības plānus un mērķus, kā arī tiem pakārtotos darbības rādītājus var izmantot kā risku identificēšanas avotu. Laicīgi novērtējot riskus, iespējams izstrādāt objektīvākus un kvalitatīvākus darbības plānus, kā arī nepieciešamības gadījumā tos pielāgot faktiskajai situācijai (5. attēls). Ir svarīgi zināt būtiskākās pārmaiņas, kas gaidāmas iestādē vidējā

termiņā, jo arī tās var norādīt uz potenciālajiem riskiem, un tās būtu jāatspoguļo iestādes darbības plānā.

5. attēls. Risku ietekmes novērtēšana



Risku ietekmes novērtēšana

Stratēģiskās plānošanas procesā, plānojot iestādes darbību un attīstību stratēģiskajam periodam, ir svarīgi saprast, cik reāli sasniedzami ir izvēlētie darbības virzieni un sasniedzamie mērķi. Gan SVID analīze, gan konkrētu risku identificēšana stratēģiskās plānošanas procesā palīdz saprast iestādes vadībai, kurus attīstības virzienus un mērķus objektīvi nav iespējams īstenot un sasniegt un tāpēc tie jāizslēdz jau plānošanas procesā. Stratēģiskās plānošanas procesā attīstības virzienu un mērķu izvēlei jānotiek pēc potenciālo risku apzināšanas. Ņemot vērā risku analīzes rezultātus, vadība koriģē mērķus, to ieviešanas plānus, mainot veicamo pasākumu secību, samazinot ieviešamo pasākumu apjomu un mērogus, it īpaši, ja riski iepriekš nav ļāvuši sasniegt kādu no mērķiem.

Operacionālās plānošanas procesā jau ir zināmi sasniedzamie mērķi, piemēram, procesu, struktūrvienību mērķi, bet ir jādefinē plānotās darbības mērķu sasniegšanai un jāpiešķir resursu prioritātes. Risku dēļ iestādes operatīvajā darbībā rodas neplānoti pavērsieni un situācijas, kad vērojama resursu nepietiekamība, tādējādi operacionālās plānošanas procesā ir būtiski apzināt informāciju par riskiem, lai saplānotu nepieciešamās papildu darbības vai resursus gadījumos, kad riski īstenojas un rada ietekmi uz iestādes mērķu sasniegšanu.

Darbības nepārtrauktības plānošanas sākumā tiek izvērtēti risku iestāšanās scenāriji ar dažādu ietekmes mērogu, lai labāk prognozētu, kā un cik lielā mērā riski var pārtraukt iestādes darbības, tās funkcijas/ procesus, tostarp to atbalstošās informācijas sistēmas, citas tehnoloģijas, ja tādas tiek izmantotas. Pēc tam tiek identificēti kritiskie procesi, tostarp iesaistītais personāls un alternatīvie pagaidu risinājumi darbību turpināšanai līdz, kamēr iestādes darbību izdodas atjaunot iepriekšējā līmenī atbilstoši tiesību aktos paredzētajām prasībām. Alternatīvā rīcība, darbības, kas vienlaikus ir arī risku ietekmes mazinošie pasākumi, nepieciešamie resursi tiek aprakstīti iestādes konkrēto risku scenāriju darbības nepārtrauktības plānos, kuru īstenošana atkarīga no risku scenāriju sekām un augstākās vadības pieņemtajiem lēmumiem. Šie pasākumi ir vērsti uz iestādes darbības atjaunošanu ierastajā režīmā pēc iespējas īsākā laikā.

Kā piemēru darbības nepārtrauktībai var minēt Covid – 19 pandēmijas dēļ ieviesto alternatīvu klātienes darbam - attālināto darbu, kad tika nodrošināts risinājums attālināti pieslēgties informācijas sistēmām un veiksmīgi turpināt nodrošināt iestādes funkcijas un īstenot procesus.

Krīžu vadībā risku vadība, galvenokārt, palīdz prognozēt iespējamās krīzes un savlaicīgi sagatavoties to pārvarēšanai. Iestājoties krīzei, iestādes vadība cenšas apzināt riskus, kas ir īstenojušies, to ietekmes apmēru un dinamiku, pieņemt lēmumus par operatīvu rīcību ietekmes

ierobežošanai un mazināšanai, kā arī iekšējai un ārējai komunikācijai. Risku vadība krīzē var palīdzēt sastrukturēt vadības (krīzes vadības darba grupas, ja tāda izveidota) darbu, ievērojot apzinātos riskus, to būtiskumu jeb prioritāti un iepriekš izstrādātos darbības atjaunošanas vai krīzes komunikācijas/ reaģēšanas plānus. Krīzes risināšanas darba grupā (pat, ja tā ir neformāla, un tās sastāvā ir, piemēram, iestādes vadītājs, personāla vadības daļas pārstāvis, komunikācijas daļas pārstāvis u.c. struktūrvienību pārstāvji) risku vadītājam parasti ir darba grupas moderatora un koordinatora loma.

 **Svarīgi**: Veicot risku analīzi iestādes darbības plānošanā, var šķist, ka risku nav (jo ir plānošanas perioda sākums un iepriekšējā periodā nav īstenojušies riski, kā arī nav bijusi būtiska rādītāju neizpilde un tamlīdzīgi) un var tikt apzināti tikai vispārīgi standarta nenozīmīgi riski. Taču nepieciešams saglabāt objektivitāti un profesionālu skepsi, lai apzinātu specifiskus riskus, kas var apdraudēt iestādes mērķu sasniegšanu, tostarp darbības nepārtrauktības riskus, lai arī to varbūtība ir ļoti zema, bet ietekme katastrofāla.

 **Piemērs**:

Gaidāmo izmaiņu un ar tām saistīto risku atspoguļošana iestādes darbības plānos.

1. Iestāde, kas darbojas gaisa satiksmes jomā, ir informēta, ka pēc pāris gadiem Eiropā tiks aktualizētas gaisa satiksmes drošības prasības, kas ietekmēs tās iekšējās sistēmas un datu atskaišu veidu. Lai šīs izmaiņas laicīgi ieviestu, būs nepieciešami papildu iekšējie resursi izmaiņu prasību definēšanai, testēšanai un ieviešanai, kā arī zināmi ārējo informācijas sistēmu izstrādātāju resursi. Attiecīgie struktūrvienību vadītāji identificē risku par atkarību no informācijas sistēmu izstrādātājiem un to nepieejamību, ja tie netiks savlaicīgi piesaistīti. Šie apstākļi tiek atspoguļoti iestādes vidēja termiņa un ikgadējos darba plānos, paredzot papildu izmaksas informācijas sistēmu izmaiņu ieviešanai, kā arī datu apstrādē iesaistīto darbinieku laika resursus, paredzot, ka būs nepieciešami vismaz trīs mēneši katru gadu prasību izpētei, definēšanai, testēšanai un ieviešanai. Savukārt attiecīgo struktūrvienību citiem uzdevumiem, kas bija noteikti iepriekš, un ir ar zemāku prioritāti, tiek pagarināti to ieviešanas termiņi līdz nākamā gada beigām.

Iepriekšējā perioda darba plānu mērķu neizpilde un tās ietekme uz turpmākajiem plāniem.

2. Iepriekšējā gadā iestāde, kas darbojas būvniecības procesu pārvaldības jomā, neizpildīja dokumentu aprites atvieglošanas un klientu pieteikumu izskatīšanas paātrināšanas mērķus. Analizējot mērķu neizpildi, tika secināts, ka īstenojies un arī turpmāk pastāv risks, ka būs nepietiekama procesu koordinēšana iestādē un, lai sasniegtu vēlamos efektivitātes rādītājus, nepieciešams pielāgot dažus iekšējos procesus, to darbību secību un mainīt atbildīgos par to ieviešanu, kā arī informēt par to darbiniekus. Sagatavojot nākamā perioda plānu, tiek noteikts uzdevums papildu pasākumiem, kas nepieciešami, lai mazinātu identificēto risku un veicinātu efektivitātes mērķu sasniegšanu. Tādējādi efektivitātes mērķi tiek nedaudz

samazināti nākamajam gadam (kamēr tiks ieviestas papildu pasākumi), paredzot to pilnvērtīgu sasniegšanu vidējā termiņā. Iestādes mācību plānā nākamajam gadam tiek iekļautas mācības par gaidāmajām iekšējo procesu izmaiņām un dokumentu apstrādes, kā arī komunikācijas ar klientu tēmām, vienlaikus paredzot termiņus un atbildīgos par iepriekšminēto pasākumu, kas paredzēti riska mazināšanai, ieviešanu.

 **Padoms**: Iesakām identificētos riskus skaidri saistīt ar dažādu līmeņu mērķiem, kas iekļauti iestādes darba plānos, jo tas palīdzēs definēt riskus pēc būtības, vērtējot to sekas un ietekmi. Papildus tas atvieglos un veicinās skaidrāku komunikāciju par riskiem (t.i. kam, kad un par kuriem riskiem ziņot).

2.5. Risku vadības loma iestādes darbības snieguma izpildē

Kad riski ir apzināti iestādes darbības plānošanas procesā, ir tikpat svarīgi sekot līdzi risku tendencēm plānu izpildē, kad tiek praksē pieņemti lēmumi un ieviesti pasākumi mērķu sasniegšanai. Tāpat var veidoties situācijas, kad iestādes plānu īstenošanas laikā radīsies riski, kurus iepriekš nebūtu bijis iespējams identificēt un novērtēt. Turklāt tikai darbības snieguma izpildes laikā iespējams novērtēt, vai sākotnēji (plānošanas stadijā) apzinātie risku mazināšanas pasākumi ir pietiekami un efektīvi.

Iestādes darbības snieguma izpilde ir pastāvīgs process, kad tiek analizēta informācija par iestādes darbības plānu un mērķu izpildes statusu un progresu, iespējams (ja tādi ir noteikti), vērtējot arī darbības rādītājus. Darbības plānu izpildes pārskati ir informācijas avots risku vadītājam un risku īpašniekiem risku identificēšanai, jo mērķu un darbības rezultātu neizpilde norāda uz potenciālajiem riskiem (jebkuri signāli par draudiem, ka mērķi var tikt nesasniegti vai mainīties, ir riski).

Papildus tam, risku vadības sasaiste ar iestādes darbības snieguma izpildes uzraudzību ir laba iespēja risku vadītājam un risku īpašniekiem apzināt dažādus risku mazināšanas pasākumus, jo risku ietekme, iespējams, jau ir jūtama, un iestādes darbiniekiem var rasties vērtīgas idejas par to, kā riskus vadīt.

Saskaņā ar MK 01.02.2022. instrukciju Nr.1 "Kārtība, kādā izstrādā un aktualizē institūcijas darbības stratēģiju un novērtē tās ieviešanu" sagatavo darbības stratēģiju un novērtē tās ieviešanu. Ņemot vērā šīs instrukcijas:

- 5.8. punktu - iestādēm darbības stratēģijā jāiekļauj sasniedzamie rezultāti jeb pārmaiņas, kuras raksturos noteiktā mērķa sasniegšanas pakāpi, un to snieguma rādītāji, tai skaitā tādi, kuri ir kopīgi visām tiešās pārvaldes institūcijām un ir definēti valsts pārvaldes attīstības plānošanas dokumentos;
- 5.9. punktu - galvenie snieguma rādītāji, kuri demonstrēs iestādes darbības progresu un raksturos svarīgākos iestādes sasniedzamos rezultātus.

Piemēram, Tieslietu ministrija ir izstrādājusi darbības stratēģiju, ievērojot šo instrukciju, iekļaujot tajā politikas rezultātus un rezultatīvos rādītājus, kuru noteikšanas principi un kārtība ir paredzēta MK 01.09.2009. noteikumos Nr.979 "Rezultātu un rezultatīvo rādītāju sistēmas darbības kārtība", MK 18.06.2008. rīkojumā Nr.344 "Par Rezultātu un rezultatīvo rādītāju sistēmas pamatnostādnēm 2008.-2013.gadam".

6. tabula. Tieslietu ministrijas tiesu sistēmas politikas rezultātu piemērs

Rezultāts	Rezultatīvais rādītājs	Faktiskā vērtība	Mērķa vērtība (2026)	Politika, kuru ietekmē rādītājs
Uzticama tiesu sistēma	Sabiedrības daļa, kas pilnībā vai daļēji uzticas tiesu sistēmai	34% (2020)	55%	Tiesu sistēmas politika
	Uzņēmēju daļa, kas uzskata, ka tiesu un tiesnešu neatkarība ir ļoti liela vai diezgan liela	53% (2021)	65%	Tiesu sistēmas politika
Efektīva tiesu darba organizācija	Lietu izskatīšanas ilgums rajona (pilsētu) tiesās: • administratīvajās lietās (mēneši) • administratīvo pārkāpumu lietās (mēneši) • civillietās (mēneši) • krimināllietās (mēneši) • ELT piekritīgajās komerclietās (mēneši) • ELT piekritīgajos krimināprocesos (mēneši)	• 9,2 (2021) • 4,3 (2021) • 7,4 (2021) • 6,7 (2021) • 2,5 (2021) • 2,0 (2021)	• 7,0 • 3,0 • 6,0 • 4,7 • 5,7 • 4,5	Tiesu sistēmas politika
	Visa tiesvedības procesa kopējais ilgums (no tiesvedības uzsākšanas līdz galīgajam nolēmumam lietā): • administratīvajās lietās (mēneši) • administratīvo pārkāpumu lietās (mēneši) • civillietās (mēneši) • krimināllietās (mēneši)	• 20,2 (2021) • 6,2 (2021) • 16,3(2021) • 14,1 (2021)	• 20 • 4,6 • 16 • 11,7	Tiesu sistēmas politika

Ņemot vērā Tieslietu ministrijas darbības stratēģijā paredzētos politikas rezultātus (6. tabula), var secināt, ka pastāv, piemēram, šādi riski:

- Tieslietu ministrija var nesasniegt rezultatīvā rādītāja "Sabiedrības daļa, kas pilnībā vai daļēji uzticas tiesu sistēmai" mērķa vērtību, jo lietas izskatīšanas ilgums pārsniedz astoņus mēnešus;
- Tieslietu ministrijai nav iespējams sasniegt politikas rezultāta "Lietas izskatīšanas ilgums rajonu tiesās mērķa vērtību – 7 mēnešus", jo tiesas process pagarinās dēļ atbildētāju un prasības cēlāju pierādījumu vākšanas ieilgšanas un zvērinātu advokātu attaisnotām prombūtnēm.

Iestādes darbības stratēģijā, definējot sasniedzamos rezultātus, būtu ieteicams izmantot vienoto pieeju, ņemot vērā izveidoto rezultātu un rezultatīvo rādītāju sistēmu, kas paredzēta spēkā esošajos MK 01.09.2009. noteikumos Nr.979 "Rezultātu un rezultatīvo rādītāju sistēmas darbības kārtība", MK 17.11.2009. instrukcijā Nr.16 "Ministriju un citu centrālo valsts iestāžu rezultātu un to rezultatīvo rādītāju izstrādes un novērtēšanas metodika", kā arī MK 18.06.2008. rīkojumā Nr.344 "Par rezultātu un rezultatīvo rādītāju sistēmas pamatnostādnēm 2008. – 2013. gadam", lai mazinātu risku izveidot vairākas paralēlas un savstarpēji nesalīdzināmas rezultātu un rezultatīvo rādītāju sistēmas, jo spēkā esošā MK 01.02.2022. instrukcija Nr. 1 "Kārtība, kādā izstrādā un aktualizē institūcijas darbības stratēģiju un novērtē tās ieviešanu" paredz, ka iestādes stratēģijā jāiekļauj sasniedzamie rezultāti jeb pārmaiņas, kuras raksturos noteiktā mērķa sasniegšanas pakāpi, un to snieguma rādītāji, tai skaitā tādi, kuri ir kopīgi visām tiešās pārvaldes institūcijām un ir definēti valsts pārvaldes attīstības plānošanas dokumentos. Attīstības

plānošanas sistēmas likums paredz, ka attīstības plānošanas rezultāti ir attīstības plānošanas dokumentu īstenošanas gaitā iestāžu izstrādātie produkti un pakalpojumi, kā arī sabiedrībā un tautsaimniecībā panāktās pārmaiņas. Rezultātu noteikšanai izmanto rezultatīvos rādītājus. Rezultātu un rezultatīvo rādītāju sistēmu un tās darbības kārtību nosaka MK.

Ņemot vērā stratēģijās noteiktos, piemēram, politikas un darbības rezultātus un rezultatīvos rādītājus, nepieciešams apzināt riskus, kas apdraud šo rādītāju sasniegšanu, kā arī ņemot vērā 5. nodaļā "Risku vadības process" noteikto risku vadības procesu, analizēt, izvērtēt šos riskus, kā arī, ja to līmenis pārsniedz pieļaujamo līmeni/ riska apetīti, noteikt to mazināšanas pasākumus.

Vērtējot riskus iestādes darbības snieguma izpildes posmā, var uzlabot atdevi pret ieguldītajiem resursiem, tas ir, iestādes budžeta un citu resursu pielietojuma lietderību, pakalpojumu kvalitāti un klientu (iekšējo un ārējo) apmierinātību.

Iestādes snieguma izpildē un izpildes vērtēšanā risku vadība palīdz prioritizēt riskus un attiecīgi arī iepriekš noteiktos uzdevumus (mērķus, kas iekļauti plānos), lai laicīgi ieviestu risku mazināšanas pasākumus, reaģējot uz mērķu izpildes progresu un statusu. Tā rezultātā nepieciešamības gadījumā iespējams aktualizēt iestādes darbības plānus, tādējādi tos pielāgojot faktiskajai situācijai.

Lai risku vadība paaugstinātu iestādes darbības sniegumu, informācijas apmaiņai un lēmumiem par riskiem ir jābūt regulāriem un elastīgiem.

Piemērs: Iestādē tiek sagatavoti un iesniegti pusgada pārskati par darbības plānu izpildi. Atbildīgās struktūrvienības vadītājs konstatē, ka ir daži rezultāti un rezultatīvie rādītāji, kuru izpilde pusgadā nedaudz kavējas, jo ir palielinājušies attiecīgo risku līmeņi. Atbildīgās struktūrvienības vadītājs ziņo par rezultātu un rezultatīvo rādītāju (sasniedzamo mērķu) izpildes kavēšanās iemesliem un saistītajiem riskiem. Tā kā risku līmenis divu mēnešu laikā ir palielinājies, attiecīgās struktūrvienības vadītājs ir uzsācis ieviest risku mazināšanas pasākumus, un informē iestādes augstāko vadību arī par tiem un to izpildes progresu. Augstākā vadība pieņem zināšanai informāciju par darbības rezultātu un rezultatīvo rādītāju pagaidu izpildes kavēšanos, saistītajiem riskiem un to vadību. Augstākā vadība lemj par iepriekš noteikto mērķu saglabāšanu sākotnējā apjomā, ņemot vērā, ka tiek sagaidīts, ka risku ietekme tiks mazināta. Tāpat augstākā vadība piedāvā papildu idejas – pasākumus risku mazināšanai un deleģē attiecīgo struktūrvienības vadītāju ieviest iepriekšminētos pasākumus.

Padoms: Izskatiet biežāk nekā vienu reizi gadā risku mazināšanas pasākumu statusu būtiskajiem (prioritārajiem) riskiem, piemēram, reizi pusgadā vai pat ceturksnī, it īpaši, ja ir iespēja to sasaistīt ar iestādes iekšējām pārskatiem par darbības plānu izpildes statusu. Nosakiet risku (jo sevišķi būtisko risku) uzraudzības regularitāti un mazināšanas pasākumu statusa pārskatīšanu iestādes iekšējā normatīvajā dokumentā, kas regulē risku vadības procesu (piemēram, kārtībā, procedūrā, struktūrvienības nolikumā un tamlīdzīgi). Norādiet iesaistītos darbiniekus, kam jāpiedalās risku statusa izmaiņu uzraudzībā.

2.6. Risku vadības saistība ar procesu vadību un kvalitātes vadību

Procesu vadība ir iestādes iekšējo procesu struktūra, organizēšana, aprakstīšana un uzturēšana, tas ir, procesu izveides un uzturēšanas formāts, veids, prasības. Par ieviestu procesu vadību šajā nodaļā tiek uzskatīta situācija, kad iestādē, izmantojot vienotu pieeju, ir aprakstīti, tostarp shematiski var būt attēloti jeb dizainēti iestādes funkcijām pakārtotie procesi, atspoguļojot pamatinformāciju par procesiem: to soļiem, darbībām, secību, atbildīgajiem, sasniedzamajiem rezultātiem, ievades un izvades datiem/ notikumiem, termiņiem, procesu aktualizācijas pieeju, kā arī procesu savstarpējo sasaisti.

Procesu vadību var praktiski pielietot risku vadībā šādos veidos:

- funkciju - procesu katalogs ir piemērots risku identificēšanas avots. Piemēram, procesu uzskaitījums, saraksts un saturs nodrošina pietiekamu informāciju risku vadītājam, lai būtu iespējams iepazīties ar iestādes svarīgākajiem iekšējiem procesiem, to norisi, kā faktiski tiek veiktas funkcijas, kādi amati tajās iesaistīti. Izskatot procesu aprakstus, risku vadītājs var identificēt riskus, ja tiek konstatētas nepietiekamas vai neesošas kontroles vai neskaidra to soļu secība un rezultāti;
- procesu vadība palīdz strukturēt risku vadību un īstenot to pakāpeniski, kā arī pārliecināties, ka risku vadība ir piemērota visos procesos vienlīdzīgi, respektīvi, tā ir visaptveroša;
- procesu darbības var norādīt uz kontrolēm un attiecīgi arī uz riskiem. Piemēram, ja procesā ietilpst darbības, kas paredz informācijas un datu pārbaudes, saskaņojumus, salīdzināšanu – tas nozīmē, ka procesā ir ieviestas kontroles. Savukārt, ja var konstatēt loģisku darbību neesamību procesā, kā arī neskaidru atbildības un pienākumu sadalījumu, neviennozīmīgus procesa rezultātus – tas var liecināt par riskiem konkrētā procesa ietvaros;
- procesu analīze var palīdzēt identificēt risku jomas un uzdot jautājumus, kas palīdzētu rast atbildes, vai procesā ir identificējami riski;
- procesu īpašnieki un atbildīgie par procesa darbībām norāda uz risku īpašniekiem, kuri var ietekmēt riska ierobežošanu;
- ieviešot būtiskas izmaiņas iestādes darbībā, tiek pārskatīti procesi un apzināti riski, kas ietekmē procesu īstenošanu;
- izvērtējot iekšējo un ārējo auditu konstatējumus un ieteikumus par procesiem, var secināt, kādi riski piemīt attiecīgajam procesam;
- procesu pārskatīšanas sistemātiskums, regularitāte, lai aktualizētu procesus. Piemēram, visi procesi tiek pārskatīti vismaz vienu reizi trīs gados, vienlaikus apzinot būtiskākos riskus.

Piemērs: Iestāde izglītības jomā sniedz pakalpojumu ārējiem klientiem, izskatot iesniegumus un izsniedzot sertifikātus, kas ļauj tiem veikt saimniecisko darbību konkrētā nozarē. Lai identificētu riskus, risku vadītājs iepazīstas ar iestādes procesiem. Risku analīzes laikā risku vadītājs un procesa īpašnieks secina, ka procesā atspoguļotā iesniegumu izskatīšana praksē ne vienmēr tiek ievērota, jo viena no ārējām datu bāzēm, kurā tiek veikta klientu iesniegto datu pārbaude, datus apkopo citos periodos un citā detalizācijas pakāpē. Pārrunājot, tiek secināts, ka tas nerada būtiskus riskus iestādes sniegtajiem pakalpojumiem un to kvalitātes nodrošināšanai, taču radies atbilstības risks, jo iestādes faktiskā rīcība atšķiras no procesā noteiktajām prasībām, kā rezultātā tiek plānota šī procesa apraksta aktualizācija.

Kvalitātes vadība ir aktivitāšu un procesu kopums, kas vērsts uz iestādes darbības kvalitātes nodrošināšanu (noteikumi un prasības, lai produkts / pakalpojums atbilstu vēlamajai kvalitātei) un kvalitātes kontroli (vai prasības tiek ievērotas).

Kvalitātes vadība vērsta uz negatīvo iznākumu mazināšanu un kvalitātes uzlabošanu, kas atbilst arī risku vadības mērķiem. Abas iepriekšminētās funkcijas nav savstarpēji pretrunīgas un tās var iegūt viena no otras, ja tiek nodrošināta nepieciešamā informācijas apmaiņa.

Praksē kvalitātes vadība un risku vadība ir saistītas šādos veidos:

- risku novērtēšana un reaģēšana uz tiem ļauj pastāvīgi uzlabot produktu/ pakalpojumu kvalitāti un rast risinājumus risku mazināšanai, izmantojot kvalitātes vadības sistēmas atbalstu;
- kvalitātes vadība norāda uz būtiskākajām jomām, kurās nepieciešams vērtēt riskus un pievērst uzmanību kontroļu pietiekamībai un efektivitātei;
- kvalitātes vadībā izmantotie galvenie kvalitātes rādītāji (piemēram, procesu mērījumi) tiek izmantoti risku analīzē. Piemēram, kvalitātes rādītāju regulāra neizpilde var liecināt par riskiem, kā arī kvalitātes datu neesamība var liecināt par jomu, kurā nepieciešama padziļināta risku analīze.

Padoms: Dažas valsts pārvaldes iestādes darbojas nozarēs, kurās, izmantojot ārējos normatīvos aktus, tiek regulēti kvalitātes standarti. Ja šie kvalitātes standarti tiek ievēroti un ieviesti, iestāde var uzskatīt, ka tai nav būtisku risku, jo netiek pārkāpti kvalitātes standarti un prasības. Iesakām neatkarīgi no dažādu ārējo kvalitātes un citu normatīvu ievērošanas aktīvi un objektīvi vērtēt riskus, jo atbilstība vēl neliecina par risku neesamību. Piemēram, pat, ja tiek ievērotas kvalitātes prasības, iespējams, ka riski piemīt klientu apmierinātības vai iestādes darbības efektivitātes nodrošināšanā.

2.7. Visaptveroša risku pārvaldība: pazīmes, izaicinājumi

Ir vairākas pazīmes, kas liecina par visaptverošu risku vadību:

- **konteksts** - tiek apzināti un ņemti vērā iekšējie un ārējie faktori, iestādes nozares specifika. Risku vadītājam pieejama visa nepieciešamā informācija par iestādes darbību un prasībām, lai pilnvērtīgi vadītu riskus;
- **organizatoriskā struktūra** - risku vadītāja funkcija ir neatkarīga, tas ir, tā nav pakļauta kādai iestādes konkrētai vienai darbības jomai, bet attiecināma uz visu iestādi kopumā. Risku vadītājs ir tiešā pakļautībā iestādes augstākajai vadībai. Risku vadītājs ir vienlīdz pieejams visiem iestādes darbiniekiem un struktūrvienībām;
- **izmērs un tvērums** - risku vadības funkcija un sistēma atbilst iestādes izmēram, organizatoriskajai struktūrai un sarežģītības pakāpei. Iestādes risku vadības pieeja piemērojama dažādām risku grupām, jomām un veidiem;
- **sasaiste ar citiem iestādes pārvaldības procesiem** - risku vadība nav atrauta no citiem iestādes pārvaldības procesiem. Risku vadība integrēta iestādes regulāro lēmumu pieņemšanā un pārvaldības aktivitātēs. Risku vadības principus iestāde pēc iespējas var izmantot dažādās saistītās situācijās (piemēram, krīžu vadība, incidentu izmeklēšana u.tml.);
- **mandāts** - ieviešot risku vadību iestādē, augstākā vadība pieņem skaidru lēmumu par risku vadības funkcijas mērķiem, darbinieku iesaisti un ar risku vadību saistīto atbildības

sadalījumu. Risku vadītājam un citiem struktūrvienību vadītājiem un darbiniekiem (risku īpašnieki) ir skaidri noteikti pienākumi risku vadības procesā;

- **laiks un citi resursi** - risku vadībai ir pieejami laika un citi nepieciešamie resursi, lai risku vadītājs, iestādes augstākā un vidējā līmeņa vadība, kā arī darbinieki spētu iesaistīties un veltīt pienācīgu laiku risku vadības ieviešanai.

Visaptveroša risku vadība nozīmē, ka iestādē ar vienlīdzīgu metodi un pieeju, izmantojot vienotus principus un kārtību, tiek pārvaldīti dažādu līmeņu un veidu riski. 7. tabulā attēloti dažādi aspekti, kas var palīdzēt apzināt, vai iestādē risku vadība ir visaptveroša vai ierobežota (tas ir, ja riski tiek vērtēti kādā atsevišķā jomā vai līmenī).

7. tabula. Visaptveroša risku vadība

Risku līmeņi	Stratēģiskie riski	Operacionālie riski	Ikdienas riski
Struktūrvienības	Iestāde kopumā, augstākā vadība.	Iestādes pamatdarbības funkciju struktūrvienības.	Iestādes atbalsta/centrālo funkciju struktūrvienības.
Risku pārklājums/ ietekme	Visas iestādes risks.	Vairāku struktūrvienību, horizontālais risks.	Vienas struktūrvienības vai procesa/sistēmas risks.
Risku jomas	Personāla, finanšu, IKT, operatīvie, tehniskie, vides, reputācijas, juridiskie, korupcijas un krāpšanas un citi riski. (Riski tiek vērtēti ne tikai reglamentētajās jomās, kur noteiktas specifiskas ārējo normatīvo aktu prasības, piemēram, interešu konflikta un korupcijas novēršanā, ES fondu projektu vadībā, fizisko personu datu aizsardzībā un citās jomās, bet gan tie tiek vadīti visā iestādes darbībā).		
Risku saistība ar iestādes darba plānošanu	Stratēģiskā, operatīvā, finanšu vai cita veida un līmeņa plānošana, lēmumu pieņemšana.	Stratēģisko vai cita līmeņa darbības plānu izpilde un uzraudzība Projektu vai procesu ieviešana, lēmumu izpilde.	Neplānoti pēkšņi identificēti riski, krīzes vai ārkārtas situācijas.
Risku ietekmes sfēra, iesaistītās puses	Iestādi ietekmējošie riski, kas skar iestādes mērķus un to sasniegšanu atbalstošos procesus. Riski, kas skar sabiedrību, ārējos klientus un partnerus. Riski, kas skar citas iestādes, kontrolējošās un uzraugošās iestādes, nozares vai valsts līmeņa sistēmas.	Skar iestādes iekšējos procesus, darbiniekus un darbības nodrošināšanai nepieciešamo aprīkojumu un informācijas un komunikācijas tehnoloģijas.	Skar iestādes darbinieku ikdienas darbības, pienākumu veikšanu.

Bieži pieļauta kļūda ir risku vadības nodalīšana, izolēšana dažādās struktūrvienībās, neveicot analīzi par risku kopsakarībām, mijiedarbību, neapsverot kopīgu lēmumu pieņemšanu. Šādos gadījumos zūd risku vadības un kopīgās lēmumu pieņemšanas un mērķu izpildes pārvaldības konteksts.

Ņemot vērā normatīvo regulējumu vai standartus specifiskās darbības un risku jomās (piemēram, informācijas un komunikāciju tehnoloģiju riski, korupcijas un krāpšanas riski, darba drošības riski), iestādes mēdz ieviest atsevišķus risku vadības posmus vai elementus šajās jomās, taču esošā prakse netiek salāgota vai attīstīta, lai ieviestu risku vadību visā iestādē kopumā, lai pārvaldītu iestādes darbības operatīvos un stratēģiskos riskus. Piemēram, iestādes pārvalda tikai darba aizsardzības, korupcijas un krāpšanas vai ES fondu projektu riskus.

Taču tieši visaptveroša risku vadība ir būtiska risku vadības veiksmīgai ieviešanai, tās optimālajiem rezultātiem un atbalstošas risku kultūras uzturēšanai.

Padoms: neuzskatīt esošo risku vadības praksi iestādē kādā konkrētā risku jomā par šķēršli, nemēģināt to viens pret vienu pielāgot visām risku jomām. Iesakām attīstīt esošo labo praksi, ja tā veiksmīgi darbojas un izveidot tādu risku vadības metodisko pieeju, kas iekļauj jau pastāvošos procesus un risku vadības rezultātus.

2.8. Risku vadības ieviešanas "klupšanas akmeņi" valsts pārvaldes iestādēs

Publiskajā sektorā un valsts iestādēs nereti pret risku vadību ir skepse vai arī tā tiek neatbilstoši, virspusēji piemērota, tādējādi radot šaubas par šīs funkcijas lietderību un pievienoto vērtību. Praksē mēdz pastāvēt dažādi objektīvi iemesli, kas rada šķēršļus risku vadības veiksmīgai ieviešanai, piemēram, resursu ierobežojumi, kā arī atsevišķos gadījumos risku vadības ieviešanu kavē un negatīvu izpratni par to rada vadības un pārējo darbinieku nelabvēlīga attieksme. Šajā nodaļā apkopoti biežākie risku vadības ieviešanas "klupšanas akmeņi" jeb nekorektie priekšstati vai pieejas risku vadības ieviešanai iestādēs, kas bremzē un neveicina šīs funkcijas attīstību:

- nepietiekami un neregulāri, nepilnvērtīgi paredzēti darbinieku resursi, kas darbotos risku vadības jomā;
- risku vadība tiek uztverta kā "atbilstība", nesaistot risku vadību ar lēmumu pieņemšanu un iestādes mērķu noteikšanu. Uzskats, ka, ja iestāde atbilst visiem iekšējiem un ārējiem normatīvajiem aktiem, tad riski faktiski nepastāv vai nav īstenojušies;
- iestādē nav nodefinēti skaidri, mērāmi un pietiekami izaicinoši mērķi, līdz ar to nav iespējams vērtējums par riskiem, kas varētu negatīvi ietekmēt šo mērķu izpildi. Līdzīga kļūda ir arī negatīvajā attieksmē, ka tikai privātajā, tai skaitā finanšu sektorā var būt izvirzāmi konkrēti un pietiekami izaicinoši mērķi, līdz ar to, privātajā sektorā atšķirībā no publiskā sektora arī būtu vairāk jāpielieto risku vadība;
- riski netiek pietiekami precīzi definēti (tas ir, bez cēloņiem un sekām), bet atspoguļo jau esošus / radušos negatīvos apstākļus vai faktus. Negatīvie apstākļi netiek tālāk izvērsti un analizēti, netiek apzināti potenciālie riska scenāriji, kas varētu iestāties un ietekmēt iestādes mērķu sasniegšanu;
- riski tiek definēti pārāk plaši, augstā virsrakstu līmenī un tādējādi nav iespējams tiem identificēt risku mazināšanas pasākumus, kurus konkrētā iestāde, tās struktūrvienība vai kāds no vadītājiem varētu ieviest. Piemēram, "personāla nepietiekamības risks", "kiberdrošības risks" - šādi virsraksti nav uzskatāmi par precīzu riska formulējumu, jo neapraksta konkrētu riska scenāriju, nezināmo negatīvo apstākļu ietekmi un potenciālās sekas. Kā arī tie nav pietiekami konkrēti. Tas ir īpaši raksturīgi valsts iestādēm, kas riskus definē savas nozares politikas mērķu un iespējamo nozares sistēmisko risku līmenī - šādi riski ir pārāk kompleksi, iespējams tie ir valsts līmeņa riski un nav mazināmi vienas iestādes ietvaros;

- iestādes mērķi var būt kompleksi un grūti mērāmi, ja tie definēti plaši un augstā nozares līmenī (piemēram, kādas politikas īstenošana vai apjomīgas funkcijas nodrošināšana) - tas apgrūtina risku identificēšanu, jo dažu iestādes identificēto līmeņu riski var būt mazināmi tikai nozares vai valstiskā līmenī;
- iestādēs risku vadība vai fakts, ka pastāv riski, var tikt uztverti kā vājuma vai "uzdevumu neizpildes" pazīme. Tas apvienojumā ar reizēm nepilnīgi caurskatāmu iekšējo un ārējo komunikāciju var apgrūtināt atklātu un objektīvu risku atzīšanu un vērtēšanu;
- bailes paust viedokli, ka struktūrvienībā ir riski, kas liecinātu par nesakārtotību vai neefektivitāti;
- bažas par to, ka tiks sodīti, ja būs problēmas, identificēti riski, kuru līmenis palielinās vai pat risku īstenošanās gadījumi, tas ir, incidenti;
- risku līmenis tiek nepamatoti novērtēts zemāk nekā faktiski tas ir, piemēram, augsta līmeņa risks kā zema līmeņa risks, tādējādi izvairoties no papildu pasākumu jeb risku mazinošo pasākumu īstenošanas;
- nevēlēšanās atklāt savus riskus uzraugošajām iestādēm, auditoriem, klientiem, sadarbības partneriem, kā rezultātā risku līmenis netiek mazināts.

2.9. Ieteikumi risku vadības ieviešanas izaicinājumu pārvarēšanai

Lai iestādes risku vadību būtu iespējamas veiksmīgi ieviest, nepieciešams:

- iesaistīt iestādes vadību (iestādes vadītājs un tā tiešajā pakļautībā esošie vadītāji) lēmuma pieņemšanā par risku vadības funkcijas un sistēmas ieviešanu;
- noteikt mērķus un rezultātus, ko sagaida no risku vadības (tai skaitā, risku vadītājam un tā tiešajam vadītājam vērtējamos uzdevumus konkrētajā laika periodā);
- skaidri noteikt organizatorisko piederību un hierarhiju risku vadītājam (t.i., kuram vadītājam ir pakļauts);
- nesākt ar pārāk lielu risku vadības procesa apjomu jeb neizvirzīt kā mērķi vidējā vai augstākā risku vadības brieduma līmeņa sasniegšanu sākotnējā risku vadības ieviešanas periodā. Arī risku vadības iekšējos normatīvos dokumentus var izstrādāt pakāpeniski un pilnveidot tos ar laiku, gūstot pieredzi risku vadībā;
- lai demonstrētu un pamatotu risku vadības nepieciešamību un pārliecinātu/ veicinātu iestādes darbiniekus iesaistīties risku vadībā, iespējams sākt risku vadību ar kādu pilotprojektu jeb kādu procesu, kas ir ļoti svarīgs iestādei, vai arī iestādes vai citu iestāžu iepriekš pieļautajām kļūdām vai incidentiem (izmantot risku vadību, lai nepieļautu iepriekš notikušās kļūdas vai incidentus);
- ieteicams mainīt uzskatus, ka iestādēs nav būtisku risku (ir tikai standarta riski, piemēram, personāla, korupcijas un krāpšanas, budžeta nepieejamības riski), izmantojot piemērus no prakses, kad riski ir īstenojušies. Iespējams, ka šim nolūkam nepieciešams piesaistīt ārējos neatkarīgos ekspertus, vismaz sākotnēji, kamēr darbiniekiem izveidojas vienota izpratne par riskiem un to definēšanu;
- iepazīstināt dažādu līmeņu struktūrvienību vadītājus ar risku funkciju, dot mandātu un "zaļo gaismu" abām pusēm sadarboties;
- risku vadības procesa plānošana ir būtiska, skaidrojot izvēlēto risku vadības pieeju risku īpašniekiem un tiem, ar kuriem notiks risku analīzes diskusijas (regulāras darba grupas vai individuāla risku analīze, kas nodrošinātu vienotas izpratnes veidošanu);

- nodrošināt informācijas pieejamību par iestādes procesiem, iesaistīt risku vadītāju regulārajās vadības sanāksmēs un diskusijās;
- vienādi attiekties pret risku rezultātiem neatkarīgi no struktūrvienības profila, vadītāja hierarhijas, lai nodrošinātu atbildīgu attieksmi pret būtisko risku vadību, kā arī, lai mazāku struktūrvienību vadītāji un vidēju/zemāku risku īpašnieki arī praktiski saskatītu ieguvumus no risku vadības un būtu uzklausīti;
- sasaistīt risku vadības procesu un rezultātus ar citiem jau esošiem rīkiem (operacionālā un uzdevumu plānošana, darba plānu rezultātu ziņošana, iekšējā regulārā komunikācija un sanāksmes par aktualitātēm un tamlīdzīgi);
- svarīga ir sistēmisko risku apzināšana un mazināšana, tāpat kā operatīva līmeņa risku vadība, lai nodrošinātu praktiskos ikdienas resursus un rīkus, iestādes veiksmīgai darbībai. Ikdienas operatīvo risku vadībā iespējams ātrāk un praktiskāk sniegt uz pierādījumiem balstītus rezultātus un ieguvumus iestādes darbiniekiem, lai tie novērtētu un uztvertu risku vadību kā atbalstu ikdienā;
- īpaši svarīgi ir precīzi aprakstīt risku (uzdodot jautājumus - "un kas no tā?", "kas negatīvs var notikt šo apstākļu rezultātā?"), skaidri nodefinēt riska cēloni, uz kuru vērst risku mazinošās darbības;
- sākotnēji apzināt dažādus līmeņus, kuros strādās ar riskiem, kā atšķirsies nianses, bet pieejai jābūt līdzīgai metodiski un procesuāli (stratēģiskie, operacionālie, procesu, projektu u.c.);
- lai mazinātu horizontālos starpnozaru nozīmīgos riskus, nepieciešams organizēt nozaru ministriju darba grupas, ņemot vērā normatīvajos aktos noteiktās kompetences un deleģējumus.

KOPSAVILKUMS

Risku vadība ir pasākumu kopums, kas iestādei ļauj mazināt negatīvu notikumu vai incidentu sekas un ietekmi, aizsargāt iestādes resursus, kā arī atbalstīt un veicināt tās mērķu sasniegšanu. Risku vadība ir un būtu jāuztver kā viens no iestādes vadības rīkiem.

Efektīva IKS darbība iestādei ļauj nodrošināt paredzamu un nepārtrauktu darbību, novērst rīcības un darbības, kas tiek uzskatītas par iestādei nevēlamām, kā arī savlaicīgi paredzēt un mazināt iespējamos riskus iestādes, tās struktūrvienību un procesu līmenī.

Risku vadībai iespēju robežās jābūt integrētai lēmumu pieņemšanā dažādos pārvaldības līmeņos. Iestādes augstākajai vadībai regulāri jāuzrauga vismaz būtiskākie riski un jānosaka pienākumi vidēja līmeņu vadītājiem pārvaldīt to pārziņā esošos riskus.

Risku vadība ir cieši saistīta ar iestādes darbības un stratēģisko (mērķu) plānošanu. Risku vadība nevar tikt pilnvērtīgi īstenota, ja iestādē nav ieviesta stratēģiskā un darbības plānošana, kā arī, ja nav skaidri definēti un izmērāmi mērķi.

Izstrādājot iestādes darbības plānus, iespējams vērtēt, kādi riski apdraud šo plānu īstenošanu. Tādējādi iestādes darbības plānu un mērķus var izmantot kā risku identificēšanas avotu. Laicīgi novērtējot riskus, iespējams izstrādāt objektīvākus un kvalitatīvākus darbības plānus, kā arī nepieciešamības gadījumā tos pielāgot faktiskajai situācijai. Ir svarīgi zināt būtiskākās pārmaiņas, kas gaidāmas iestādē vidējā termiņā, jo arī tās var norādīt uz potenciālajiem riskiem un būtu jāatspoguļo iestādes darbības plānā.

Lai labāk prognozētu, kā un cik lielā mērā riski var pārtraukt iestādes darbības, tās funkcijas/ procesus, tostarp to atbalstošās informācijas sistēmas, citas tehnoloģijas, ja tādas tiek izmantotas,

būtiski darbības nepārtrauktības plānošanas sākumā izvērtēt risku iestāšanās scenārijus ar dažādu ietekmes mērogu.

Krīžu vadībā risku vadība, galvenokārt, palīdz prognozēt iespējamās krīzes un savlaicīgi sagatavoties to pārvarēšanai. Iestājoties krīzei, iestādes vadība cenšas apzināt riskus, kas ir īstenojušies, to ietekmes apmēru un dinamiku, pieņemt lēmumus par operatīvu rīcību ietekmes ierobežošanai un mazināšanai, kā arī iekšējai un ārējai komunikācijai.

Procesu vadību var praktiski pielietot risku vadībā, izmantojot procesu sarakstu un procesu saturu, lai būtu iespējams iepazīties ar iestādes svarīgākajiem iekšējiem procesiem, to norisi, un identificēt riskus. Procesu darbības var liecināt, ka procesā ieviestas risku kontroles.

Praksē kvalitātes vadība un risku vadība ir cieši saistītas, jo risku novērtēšana un reaģēšana uz tiem ļauj pastāvīgi uzlabot produktu/ pakalpojumu kvalitāti un rast risinājumus risku mazināšanai, izmantojot kvalitātes vadības sistēmas atbalstu. Kvalitātes vadība norāda uz būtiskākajām jomām, kurās nepieciešams vērtēt riskus un pievērst uzmanību kontroļu pietiekamībai un efektivitātei.

Visaptveroša risku vadība nozīmē, ka iestādē ar vienlīdzīgu metodi un pieeju, izmantojot vienotus principus un kārtību, tiek pārvaldīti dažādu līmeņu un veidu riski.

Lai iestādes risku vadību būtu iespējamas veiksmīgi ieviest, nepieciešams iesaistīt iestādes vadību (iestādes vadītājs un tā tiešajā pakļautībā esošie vadītāji) lēmuma pieņemšanā par risku vadības funkcijas un sistēmas ieviešanu, kā arī noteikt mērķus un rezultātus, ko sagaidīt no risku vadības (tai skaitā, risku vadītājam un tā tiešajam vadītājam vērtējamos uzdevumus konkrētajā laika periodā).

Lai demonstrētu un pamatotu risku vadības nepieciešamību un pārliecinātu/ veicinātu iestādes darbiniekus, iesaistīties risku vadībā, iespējams sākt risku vadību ar kādu pilotprojektu jeb kādu procesu, kas ir ļoti svarīgs iestādei, vai arī iestādes vai citu iestāžu iepriekš pieļautajām kļūdām vai incidentiem (izmantot risku vadību, lai nepieļautu iepriekš notikušās kļūdas vai incidentus). Tāpat nepieciešams nodrošināt vienlīdzīgu attieksmi pret risku rezultātiem neatkarīgi no struktūrvienības profila, vadītāja hierarhijas, lai nodrošinātu atbildīgu attieksmi pret būtisko risku vadību, kā arī mazāku struktūrvienību vadītāji un vidēju/ zemāku risku īpašnieki arī praktiski saskatītu ieguvumus no risku vadības un būtu uzklausīti.

Lai mazinātu horizontālos starpnozaru nozīmīgus riskus, nepieciešams organizēt nozaru ministriju darba grupas, ņemot vērā normatīvajos aktos noteiktās kompetences un deleģējumus.

3. RISKU KULTŪRA

Viens no svarīgākajiem efektīvas iestādes pārvaldības aspektiem ir risku kultūra un viens no pamatuzdevumiem tās nostiprināšanai un attīstībai ir uz risku orientētas domāšanas ieviešana iestādē, kas veicinātu risku novērtēšanas precizitāti, attīstītu darbinieku kompetenci risku analīzē un lēmumu pieņemšanā.

Risku kultūra ir korporatīvo vērtību, normu, attieksmes, kompetences un uzvedības kopums, kas saistīts ar risku apzināšanos (riska uztveri) un risku uzņemšanos (aktīvu lēmumu pieņemšanu), kas veicina iestādes risku vadību.

Risku kultūra ir vairāk nekā iestādes vērtību noteikšana, jo tā attiecās uz šo vērtību transformēšanu praksē, īstenojot konkrētās rīcības.

3.1. Izpratne par risku kultūru

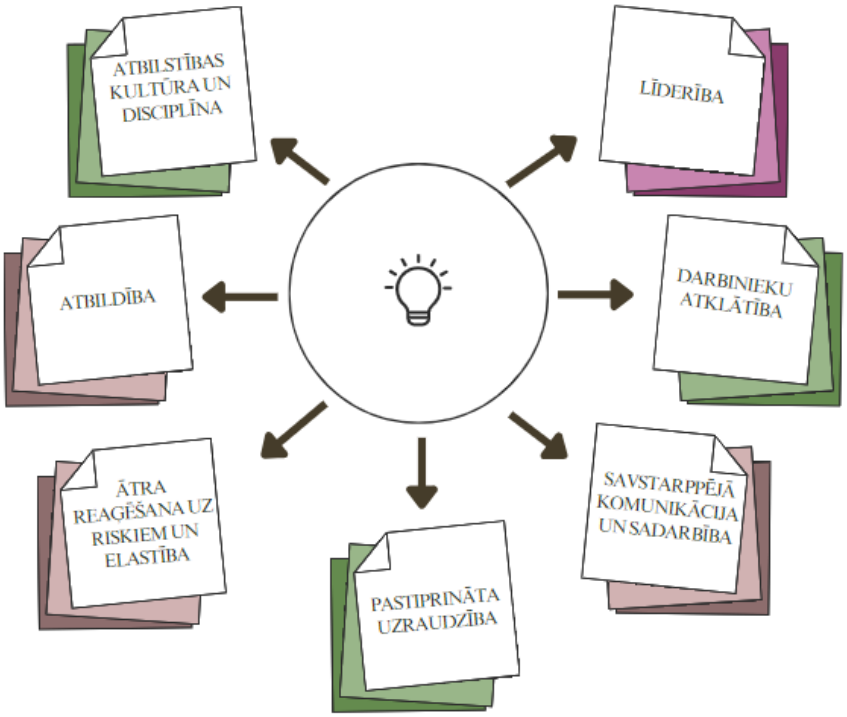
Risku kultūra ir svarīgs stūrakmens veiksmīgai, dzīvai un praktiskai risku vadībai iestādē. Lielākoties, iestādēs risku vadības un risku kultūras ieviešanas motivācija ir tiesību aktu prasības, kas reglamentē risku vadību, kā arī augstākās vadības iesaiste risku vadības ieviešanā.

No risku kultūras viedokļa ir svarīgi, lai risku vadības politika sniedz pārliecību un skaidrību visiem iestādes darbiniekiem par to, kā darbojas risku vadības sistēma un kādā veidā ir vadāmi riski, tai skaitā, nosakot, kādus lēmumus indivīds (darbinieks) var pieņemt un kādus jāpieņem izveidotajai komitejai vai augstākajai vadībai, kāda ir risku apetīte, kādas ir informācijas aprites un ziņošanas prasības.

> **Svarīgi**: Par iestādes kultūru var uzskatīt kopīgu vērtību sistēmu (kas nosaka to, kas ir svarīgs) un normas, kas definē iestādes darbinieku attieksmi un uzvedību (kā justies un reaģēt). Tāpēc risku kultūra ir integrējama iestādes kultūrā un to atspoguļo iestādes kultūras ietekme uz risku vadību. Risku kultūra ir vērtības, pārliecības, praktiskā pieredze un teorētiskās zināšanas risku vadības jomā, kas ir piemērojamas praksē visu organizatorisko līmeņu darbiniekiem ar mērķi efektīvi vadīt riskus. Tāpat par risku kultūru uzskata indivīdu un grupu vērtības, uzskatus, zināšanas, attieksmi un izpratni par riskiem, ar kuriem iestāde saskaras, tāpat arī uzvedības normas un tradīcijas iestādē, kas saistītas ar risku identificēšanu, izpratni, apspriešanu un reaģēšanu uz tiem. Normas un kultūras tradīcijas, kas attiecas uz risku vadību, veidojas, daloties savstarpēji ar pieredzi.

Attīstīta risku kultūra iestādē nodrošina, ka riski tiks savlaicīgi novērtēti un tiks adekvāti reaģēts uz tiem (veikti atbilstoši risku vadības pasākumi), nepieļaujot to īstenošanos. No risku kultūras atkarīgs, kā darbinieki iestādē reaģē uz riskiem, un tāpēc ir nepieciešams izprast būtiskos risku kultūras faktorus un to savstarpējo mijiedarbību, lai paaugstinātu risku kompetenci. Attīstītu risku kultūru raksturo 7 komponentes (6. attēls).

6. attēls. Attīstīta risku kultūra



Attīstītas risku kultūras komponentes ir šādas:

- **līderība** – vadītāja spēja iedvesmot un atbalstīt darbiniekus un viņu centienus. Par līderību var uzskatīt arī iestādes hierarhiski augstāko vadītāju veidoto uzvedības kopumu, kas palīdz darbiniekiem īstenot stratēģiskos plānus un nepārtraukti pilnveidot iestādi;
- **darbinieku atklātība** – darbinieki nebaidās uzdot jautājumus un runāt par identificētajām problēmām, ar kurām tie saskaras ikdienā, kā arī atklāti runāt par savām kļūdām. Piemēram, iespējams organizēt dažādas darbinieku aptaujas un ieviest ziņošanas kanālus, lai dotu iespēju uzklausīt visus viedokļus, lai sliktās ziņas netiktu slēptas vai paliktu nepamanītas. Būtiskākajos iestādes procesos vai projektos iespējams organizēt iegūto mācību (*lessons learned*) apspriešanu, kas ļautu procesa dalībniekiem pašiem novērtēt, kādas ir bijušas problēmas, riski un ko var darīt, lai nākotnē process būtu efektīvāks;
- **savstarpējā komunikācija un sadarbība**– informācija par iespējamiem apdraudējumiem un riskiem brīvi un ātri tiek nodota starp darbiniekiem, struktūrvienībām;
- **pastiprināta uzraudzība** – prasme pievērst uzmanību jauniem apdraudējumiem, pareizi analizēt riskus, tostarp risku līmeņa izmaiņas, kā arī atbilstoši risku līmenim noteikt piemērotākos risku mazinošos pasākumus;
- **ātra reaģēšana uz riskiem un elastība** – iestādes spēja efektīvi reaģēt uz izmaiņām, tiek nodrošināta sistemātiska un ātra reaģēšana uz apdraudējumiem, ātra lēmumu pieņemšana un rīcība. Lai to nodrošinātu, nepieciešams radīt tādu iestādes iekšējo vidi, kas ļauj efektīvi pieņemt lēmumus dažādās, tai skaitā ārējo faktoru izraisītās situācijās, kā arī veicina atklātu un konstruktīvu dialogu starp darbiniekiem;
- **atbildība** – katrs darbinieks jūtas atbildīgs par kvalitatīvu un uz datiem un informāciju balstītu lēmumu pieņemšanu. Darbinieki visos iestādes līmeņos (gan struktūrvienību vadītāji, gan darbinieki) apzinās iestādes pamata vērtības un pieeju risku vadībā, apzinās savu atbildību par darbībām, kas var radīt riskus un savā ikdienā veic pienākumus saskaņā ar iestādes vērtībām;

- **atbilstības kultūra un disciplīna** – darbinieki rīkojas saskaņā ar iekšējo un ārējo normatīvo aktu prasībām, tostarp, izmantojot ikdienā risku vadību. Lai to nodrošinātu, ir svarīgi kopumā no vadības puses informēt darbiniekus, ka no viņiem tiek sagaidīta atbilstoša rīcība.

3.2. Risku kultūras principi

Starptautiskā risku vadības institūta[15] Risku kultūras principi aprakstīti Risku kultūras aspektu modelī (7. attēls), kas identificē astoņus risku kultūras aspektus - galvenos risku kultūras "veselības" rādītājus, kas saskaņoti ar iestādes biznesa modeli un kas sagrupēti četrās tēmās. Šis modelis paredz risku kultūras pakāpenisku pārveidošanas un nepārtrauktas pilnveidošanas pieeju.

7. attēls. Risku kultūras aspektu modelis[16]

Tonis no augšas ietver šādas komponentes:

- **risku līderība jeb virzības skaidrība**. Augstākā līmeņa vadība izvirza skaidras un konsekventas ekspektācijas risku vadībai. Līderi demonstrē uz riskiem balstītu domāšanu un aktīvi apspriež risku vadības jautājumus;
- **saskarsme ar negatīvajām ziņām** – kā iestādē reaģē uz sliktām ziņām. Augstākā vadība aktīvi meklē informāciju par risku notikumiem. Darbinieki, kuri ir atklāti un godīgi pret risku informāciju, iestādē tiek novērtēti.

Pārvaldībā iekļautas šādas komponentes:

- **atbildība** – augstākā līmeņa un vidējā līmeņa vadībai ir skaidra atbildība par pamatdarbības risku vadību. Amatu aprakstos un mērķos ir iekļauta atbildība par riskiem. Jebkuras iestādes viens no būtiskākajiem risku vadības sistēmas aspektiem ir veids, kā tiek sadalīti risku vadības pienākumi, lai šo atbildību spētu īstenot arī praksē. Lai ikvienam darbiniekam ir skaidra atbildība risku vadības procesā, ir svarīgi ne tikai šo atbildību iekļaut amatu aprakstos vai citos iestādes iekšējos normatīvajos dokumentos, bet arī nepieciešams veicināt, lai darbinieki ir ieinteresēti pildīt šos pienākumus un aktīvi iesaistīties risku vadības procesā;

[15] Institute of risk management, https://www.theirm.org/contact-us/
[16] https://www.theirm.org/media/7236/risk-culture-resources-for-practitioners.pdf

- **pārskatāmība** – informācijas par riskiem plūsma. Savlaicīga informācijas par riskiem paziņošana iestādē. Risku notikumi tiek uztverti kā iespēja mācīties.

Kompetence ietver šādas komponentes:

- **risku resursi** – stiprināta risku vadības funkcija. Risku vadības funkcijai ir noteikts uzdevums, un tai ir augstākā līmeņa un vidējā līmeņa vadītāju atbalsts;
- **ar riskiem saistītas prasmes** – risku kompetencē integrētas ar risku vadību saistītās prasmes. Risku "čempioni" (iestādes risku koordinatori, risku vadītāji, kuri ir risku vadības funkcijas paplašinājums, un var sniegt informāciju par risku un ietekmēt riska kultūru un uzvedību) atbalsta tos darbiniekus, kuri vada riskus. Prasmju attīstību veicina arī izstrādāta un īstenota mācību programma un testi par risku vadību visiem iestādes darbiniekiem.

Savukārt, **lēmumu pieņemšanā** ietilpst šādas komponentes:

- **uz informāciju un datiem balstītu lēmumu pieņemšana** – pamatotu un apzinātu lēmumu pieņemšana. Iestādes līderi izmanto informāciju par riskiem lēmumu pieņemšanā. Iestādes vēlme uzņemties riskus tiek izprasta un komunicēta;
- **atlīdzība** – materiāla vai nemateriāla kompensācija - atzinīgi novērtēta pieļaujamo risku uzņemšanās lēmumu pieņemšanā. Snieguma vadība, kas saistīta ar pieļaujamā riska uzņemšanos. Līderi atbalsta darbiniekus, kuri aktīvi cenšas izprast un vadīt riskus.

Efektīvas lēmumu pieņemšanas kultūras rādītājs ir, ka iestādes vadītāji ir izglītoti, aktīvi darbojas un iesaistās risku vadībā, un no saviem darbiniekiem sagaida un pieprasa augstas kvalitātes risku informāciju optimālu lēmumu pieņemšanai. Efektīvas risku informācijas un ziņošanas priekšrocība ir, ka iestāde ir gatava uzņemties risku nenoteiktās situācijās, pamatojoties uz skaidri saprotamu un paziņotu riska informāciju. Viens no būtiskiem ikdienas risku vadības elementiem uz riskiem balstītu lēmumu pieņemšanas nodrošināšanai ir pareizu risku instrumentu izmantošana, kas atbalstītu risku kultūru un uzvedību. Šiem instrumentiem ir jānodrošina caurskatāmība un pieejamība risku informācijai. Atkarībā no nozares šie rīki parasti ietver risku reģistru izveidi (tostarp kontroles novērtējums), risku apetītes noteikšanu, stresa testēšanu, scenāriju analīzi un risku ziņošanas platformas izveidi.

Iestādes vadībai ir jārāda piemērs, ja vadība vēlas, lai ikviens iestādes darbinieks tiem sekotu ar savu rīcību un ievērotu konsekvenci gan rīcībā, gan attieksmē pret risku vadību. Iestādes līderiem jāspēj veidot atklātības un godīguma kultūra iestādē un jāuzklausa iestādes darbinieki, lai saņemtu no tiem informāciju par problēmām un riskiem.

> ⚠ **Svarīgi**: Lai sasniegtu risku vadības brieduma augstākos līmeņus, ir nepieciešams aktīvs iestādes augstākās vadības un pārējās vadības komandas atbalsts, jo viņu attieksme un risku vadības pieeja atspoguļojas iestādes vispārējā kultūrā un pārvaldībā. Iestādes augstākās vadības tonim un risku kultūrai jābūt redzamai, demonstrētai tā, lai tā sasniegtu visu līmeņu iestādes darbiniekus.

Līdz ar to iestādēm jāizvēlas efektīvākais veids, kā nodrošināt atvērtības principu, jebkuram darbiniekam radot iespēju iesaistīties risku vadībā, kā arī sniedzot atgriezenisko saikni par iesaisti.

Svarīgs risku vadības sistēmas elements ir nepieciešamība nodrošināt iestādes augstākajai vadībai pareizu un precīzu informāciju, datus par riskiem. Efektīva risku kultūra nodrošina riska

informācijas un pamatdarbības informācijas integrāciju, kā arī to, ka informācija par galvenajiem riskiem ir sniegta savlaicīgi un atbilstoši, nodrošinātu, ka vadības lēmumi tiek pieņemti, ņemot vērā riska ietekmi.

Jebkuras iestādes kultūra ir sarežģīta, un to ietekmē vairāki faktori. Pirms mēģināt mainīt iestādes kultūru, vispirms ir lietderīgi izprast veidus, kādos darbinieki var tikt ietekmēti.

Piemērs: Pastāv šādi trīs galvenie kanāli, kurus izmantojot indivīdi tiek ietekmēti un uztver iestādes kultūras vēstījumus:

- darbinieks "paraugs", kuram līdzināties. Riska pārvaldības uzvedība, ko demonstrē augstākā un vidējā līmeņa vadītāji, kā arī darbinieki, kuri ir viedokļu līderi iestādē, ietekmēs citus darbiniekus, viņu uzvedību un rīcību risku vadības ietvaros. Darbinieki, kuri ir paraugi citiem darbiniekiem, palīdz ieviest risku vadības vērtības un rāda pareizo piemēru risku vadības procesā, tostarp risku novērtēšanā un reaģēšanā uz riskiem, kas pakāpeniski kļūst par pamata pārliecību, vērtību, kā arī par pieņemamu ikdienas uzvedību;
- ziņošana par risku vadību iestādē. Skaidri vēstījumi par risku vadību ietekmē darbinieku uzvedību, ko nodrošina informācijas par riskiem pieejamība, kas veido vienotu izpratni. Ir arī svarīgi izvērtēt, kā un kādus kanālus izmantojot, informāciju par riskiem un to vadību izplatīt iestādē;
- veicināšana par aktīvu dalību risku vadības procesā. Korekta darbinieka rīcība risku vadībā tiek pienācīgi apbalvota un atzīta, tostarp par ziņošanu par riskiem, kā arī risku mazinošo pasākumu ieviešanas progresu. Darbinieka rīcību var atzinīgi novērtēt un pieminēt operatīvajās vadības sanāksmēs.

3.3. Risku vadības līderība

Risku kultūru rada un attīsta iestādes augstākā vadība, kura atzīst, ka risku kultūras pārmaiņas ir stratēģiska nepieciešamība, nevis tikai ārējo ieinteresēto pušu prasības. Augstākajai vadībai ir jānodrošina, ka tiek sniegta skaidra un nepārprotama informācija par to, kāda rīcība vai uzvedība ir sagaidāma no darbinieka risku vadības ietvaros. Lai vadības sniegtā informācija par risku kultūru tiktu uzklausīta, saprasta, un darbinieki to pielietotu praksē, darbiniekiem ir jāsaprot risku vadības būtība un nozīme, kā arī praktiskie risku piemēri un to īstenošanās sekas, kas apgrūtinās vai pat pārtrauks viņu ikdienas darbības. Komunikācija nav pietiekama, kamēr visi darbinieki nesaprot, kāda ir viņu ietekme un kāda būtu viņu loma risku vadības procesā. Ja iestādes augstākā vadība atbalsta konstruktīvu domstarpību kultūru, tad vadītājiem ir jāspēj uzklausīt darbinieku viedokli, pat ja tas atšķiras no vadītāja viedokļa. Līderiem jāveicina ierastā domāšanas maiņa, ka, īstenojot pienākumus un funkcijas, tiek nodrošināta strukturēta uz riskiem balstīta domāšana, ierobežojot paļaušanos tikai uz intuīciju.

Līdzīgi kā citus principus un praksi, risku vadību veiksmīgi var ieviest un iedzīvināt iestādē tad, ja tās augstākā līmeņa vadība un vidējā līmeņa vadība (struktūrvienību vadītāji) vienlīdzīgi izprot un atbalsta risku vadības funkcijas nepieciešamību un politiku (tas ir, risku vadības funkcijas mērķus, principus un pieeju).

Tas, kā augstākā vadība attiecas pret un reaģē uz riskiem, veido vadības risku kultūru, kam būtu jābūt izjūtamai visiem iestādes darbiniekiem, attiecīgi veidojot līdzīgu risku kultūru visos iestādes organizatoriskās struktūras līmeņos.

Risku kultūras ieviešana ir ilglaicīgs un ne vienmēr vienkāršs process, kam jāsākas no iestādes līderu puses, apzinoties, ka risku vadības process ir kopīgs iestādes uzdevums un atbildība. Ja risku vadībā iesaistītais personāls nerod atbalstu pie iestādes augstākās vadības un līderiem, citu struktūrvienību vadītāji un darbinieki var uztvert risku vadības procesu kā nevajadzīgu un lieku papildus administratīvo slogu, kā rezultātā var iesaistīties risku vadības procesā formāli vai vispār neiesaistīties, noklusējot informāciju par apzinātajiem riskiem, lai, savukārt, izvairītos no atbildības vai soda un papildu īstenojamajiem pasākumiem.

Piemērs: Praksē tiek īstenoti, piemēram, šādi augstākās vadības līderību demonstrēšanas veidi risku kultūrā:

- vienota izpratne par risku vadības nepieciešamību, mērķiem un pieeju visas augstākās vadības komandā. Šī pieeja komunicēta un pārrunāta arī ar uzraugošo iestādi, ja tas ir attiecināms;
- skaidras ziņas no augstākās vadības par risku vadības mērķiem, kas tiek nodotas visiem darbiniekiem, piemēram, kas tiek sagaidīts no risku vadības, no risku īpašniekiem, vai iestādes vadība ir gatava riskus mazināt un vadīt (vai uzskata, ka riski ir vājuma izpausme un tie nav pieļaujami un tamlīdzīgi);
- regulāra informācijas apmaiņa par riskiem un ar tiem saistītajiem lēmumiem starp augstākā līmeņa un vidējā līmeņa vadību;
- gatavība pārrunāt kļūdas, mērķu neizpildi, mācoties no kļūdām, notiek komunikācija un uzlabojumi iestādes darbībā, ja nepieciešams;
- pieaugot risku līmenim vai īstenojoties riskiem, netiek meklēti vainīgie, bet apzināti iespējamie risinājumi un uzlabojumi risku vadībā;
- pozitīvie piemēri un veiksmīgā pieredze risku vadībā tiek izcelta un novērtēta. Iestādes vadība rada drošu vidi, kas veicina atklātu un caurskatāmu risku informācijas pieejamību un diskusijas;
- iestādes vadība spēj izskaidrot un demonstrēt, kā un kur risku vadības rezultāti ņemti vērā iestādes stratēģijas un darbības plānu īstenošanā;
- iestādes vadība nodrošina regulāras iespējas un resursus darbiniekiem mācīties par risku vadības tēmām;
- iestādes vadītāji parasti izmanto iespēju komunicēt par iestādes panākumiem un pastāvīgi saistīt šos panākumus ar iestādes kultūru, tai skaitā darbinieku ieguldījumu šo panākumu sasniegšanā.

Darbinieki aktīvāk un produktīvāk sadarbojas un iesaistās iestādes darbībā un attīstībā, kad jūtas drošībā un kad var ietekmēt izmaiņas iestādē, nebaidoties no nekonstruktīvas kritikas vai nolieguma. Līdz ar to dominējošs jeb autoritatīvs vadības stils un nepacietība var radīt šķēršļus darbinieku iespējai un vēlmei izteikties publiski darba grupās/ komandā. Tādēļ ļoti būtiski veidot un fokusēties uz uzticības pieejas radīšanu iestādes kultūrā.

Viens no mūsdienu efektīvajiem risku līderības stiliem ir tā saucamā **iekļaujošā līderība**, kas veicina paļāvības, uzticamības un atklātības rašanos iestādē. Galvenās izmaiņas, kas iestādes

augstākajai vadībai ir jāveic, lai izveidotu elastīgu un pielāgotu kultūru savā darba vietā un komandām, ir kļūt iekļaujošākiem kā līderiem, izveidojot darba vidi, kurā visi darbinieki tiek novērtēti, ka iesaistās, piemēram, risku vadībā. Līderiem būtu daudz rūpīgāk jāieklausās darbinieku teiktajā, jāaicina un jāprot motivēt darbiniekus dalīties ar savām domām vai idejām, kā arī iesaistīties izaicinošās sarunās par nozīmīgiem riskiem un incidentiem, kas var kavēt viņu darbības un noteikto rezultātu un to rezultatīvo rādītāju sasniegšanu. Līderim risku vadības procesā katrā no posmiem būtu jāuzdod jautājums "Kā Jūsu domājiet?"

Piemērs: Lai kļūtu par iekļaujošo līderi, nepieciešams attīstīt, piemēram, šādas līdera īpašības:

- apņemšanās – līderim jāspēj ievērot vērtības un jābūt ētiskam (rīcība atbilst vārdiem, viedokļi nemainās diametrāli pretēji, ja tam nav pamatojuma). Līdera vērtībām ir jābūt vienādām ar iestādes vērtībām un jābūt pārliecinātam, ka tās ir jēgpilnas. Iekļaujoši līderi tiecas uz daudzpusību un integrēšanos, jo šie principi ir vienādi ar to personīgajām vērtībām un atbilst to iekšējai taisnīguma sajūtai. Līderim ir jāinvestē darbiniekos un komandā, veidojot kopējus mērķus un veicinot vienotu izpratni par tiem;
- drosme – spēja runāt par nepilnībām, tādējādi riskējot, ka darbiniekiem radīsies nevēlēšanās tās novērst papildu darbu dēļ vai arī novērot no malas, kā tiks risinātas apzinātās problēmas. Līderim jābūt vienlaikus gan cilvēcīgam, gan izlēmīgam. Līderim jāspēj izteikt savu viedokli, ja tas ir atšķirīgs, kā arī jāspēj runāt par savām stiprajām un vājajām pusēm, kā arī darbības ierobežojumiem;
- zinātkāre – līderim ir jābūt plašam redzeslokam un vēlmei saprast, kā citi indivīdi uztver un izprot procesus, kā arī jābūt vēlmei uzzināt savu darbinieku viedokli. Iekļaujošā līdera pamatprasmes ir spēja uzdot korektus jautājumus un aktīvi sadzirdēt darbinieku sniegtās atbildes par risku kultūras attīstību. Zinātkāre ļauj konstruktīvā veidā apmainīties ar idejām, kā arī labāk saprast komandu un klientus;
- kultūras inteliģence – līderim ir jābūt motivētam, zinošam un jāspēj adaptēties dažādās situācijās, vienlaikus esot elastīgam un saglabājot savu autentiskumu;
- sadarbība – līderim jāspēj būt orientētam uz darbu komandā un jāizmanto savas balsstiesības, lai pieņemtu izšķirošus lēmumus. Ja darbiniekiem tiks dota brīvība izteikt savu viedokli, un darbinieks sapratīs, ka viņa viedoklis tiek ņemts vērā, tas dos iespēju rast jaunus, efektīvus alternatīvus risinājumus;
- apzinība un bezaizspriedumu spriešanas spējas – līderim ir jāapzinās gan savi, gan iestādes kolektīvā piemītošie aizspriedumi un jāveic darbības, lai tos mazinātu. Piemēram, līderis nedrīkstētu nosodīt darbiniekus, ņemot vērā savus stereotipus, kā arī nedrīkstētu radīt situācijas, kad kādai struktūrvienībai vai darbiniekam tiek dotas priekšrocības salīdzinājumā ar citām. Tāpat nebūtu pieļaujama atšķirīga informācijas interpretācija, racionālu lēmumu pieņemšanas vietā izvēloties lēmumu, kas apmierina visas iesaistītās puses. Līderim ir jābūt apzinīgam, kā arī tam ir jāparedz attīstības perspektīvas. Aizspriedumainība var izraisīt situāciju, kad var tikt pieņemti netaisnīgi un neracionāli lēmumi. Lai nodrošinātu taisnīgu rīcību, līderim būtu jādomā gan par rezultātu (vai darbinieku snieguma vērtējums ir pamatots uz darbinieku spēju un snieguma vērtējumu), gan par procesu (vai procesi un to rezultāti

ir caurskatāmi un izsekojami un ir pamatoti ar precīzu un ticamu informāciju), gan arī komunikāciju (vai lēmumi ir saprotami tiem, uz kuriem tie attiecas).

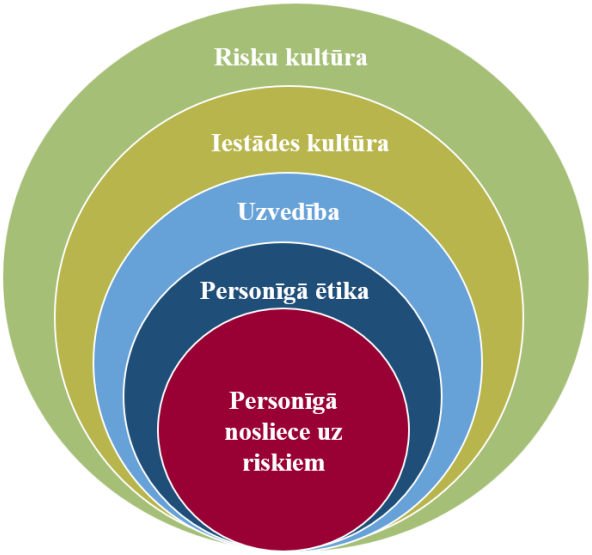
Veiksmīgai risku vadībai nepieciešama starpdisciplīnu sadarbības pieeja ar spēju eksperimentēt un izprast mainīgo iekšējo un ārējo vidi. Līdz šim izveidotajā hibrīdveida jeb attālinātajā (tiešsaistes) un klātienes kombinētajā darba vidē līderiem ir apzināti un ar nodomu jāiesaistās risku vadības procesā, lai izveidotu elastīgu tīklošanos, kas veicina sniegumu un atbalsta augstu iestādes darbinieku iesaistes līmeni. Līderiem un risku vadītajiem jāplāno, kā veidot gan iekšējās, gan ārējās tīklošanās iespējas par iestādes riskiem, kā arī, jānoskaidro risku vadības starptautiskā labā prakse. Līderiem risku vadības ieviešanā un uzturēšanā būtu jāuzdod darbiniekiem jautājums "Kā varu palīdzēt?".

Vismaz pēdējo divu gadu pieredze liecina, ka pasaule ir sarežģīta un neparedzama. Problēmas vairs nav tikai tehniskas, un nereti līderiem var nebūt atbildes reakcijas uz sarežģītām, jaunām problēmām. Lielākajai daļai līderu augstākās vadības līmenī neizdodas jaunu un inovatīvu risinājumu apgūšana. Līdz ar to var valdīt uzskats, ka "zināt jeb rast atbildi" ir pilnvaru deleģējuma jautājums. Līdz ar to līderim tas var nozīmēt radīt vidi nenoteiktībai un ļauties eksperimentiem, izmantojot iestādē izveidotās komandas jeb darba grupas. Līderiem risku vadības procesā nepieciešams uzdot jautājumu "Kas vēl pietrūkst?".

3.4. Indivīds un risku kultūra

Lielbritānijas Risku vadības institūts ir formulējis risku kultūras ietvaru (8. attēls), kas veido labāku izpratni par risku kultūras rašanos, ieviešanu un ietekmēšanu jebkurā iestādē.

8. attēls. Risku kultūras ietvars[17]



Risku kultūras ietvars ir jāaplūko, sākot no mazākā apļa un turpinot ar katru nākamo lielāko apli, vispirms saprotot indivīda "noslieces uz risku", kā arī "personisko ētiku", kas veido personīgo attieksmi un uzvedību, kas savukārt rada iestādes kultūru.

Šis ietvars paredz, ka risku kultūra apvieno:

[17] https://www.theirm.org/media/7230/risk-culture-resources-for-practitioners.pdf

- katra indivīda personīgo noslieci uz risku;
- personīgo ētiku;
- attieksmi un uzvedību;
- iestādes kultūru.

Līdz ar to risku kultūra ir vairāku iestādes vērtību mijiedarbību summa.

Katra indivīda personiskā nosliece uz risku ietekmē viņa ētisko nostāju, kā indivīds uzvedas un pieņem lēmumus. Katrs darbinieks (indivīds) iestādē ir ar savu personīgo un atšķirīgo uztveri par riskiem un to vadību. Grupu un tajā ietilpstošo indivīdu uzvedību veido indivīdu attieksme pret apkārtējo vidi.

Piemērs: Piemēram, šādas personības iezīmes liecina par noslieces uz riskiem raksturojumu - cik lielā mērā darbinieki ir spontāni un avantūristiski, neētiski vai organizēti, sistemātiski un ievēro atbilstības kultūru, vai arī cik lielā mērā ir piesardzīgi, pesimistiski, nepacietīgi vai arī optimistiski, izturīgi un pacietīgi un bezbailīgi.

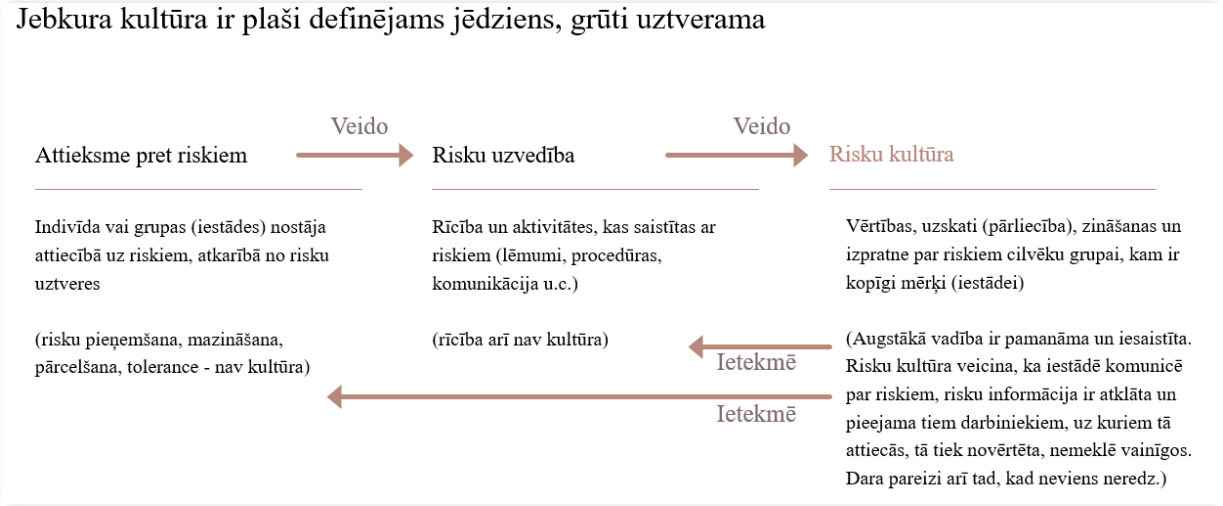
Personīgā ētika ir viens no risku kultūras pamata balstiem. Katram indivīdam ir savs morālo ētisko vērtību kopums, kam ir liela ietekme uz ikdienas lēmumiem, tādēļ iestādēs ir jāpievērš uzmanība darbinieku ētikas profilam, kuru var iedalīt, piemēram, šādi:

- atbilstības ētika (piemēram, atbilstība iekšējām kārtībām, noteikumiem, vadības norādījumiem);
- rūpīguma ētika (piemēram, empātija, rūpes, cieņa);
- saprāta ētika (piemēram, erudīcija, pieredze, piesardzība).

Iestādēs var darboties personas, kuru ētiskā nostāja vai nosliece uz risku var būt pretrunā ar augsta godīguma, ētikas standartiem/ normām, labas pārvaldības principiem, kā rezultātā var būt apgrūtinoši izveidot un ieviest efektīvu risku kultūru. Iestāžu ētikas principi paredzēti MK 21.11.2018. ieteikumos Nr.1 "Valsts pārvaldes vērtības un ētikas pamatprincipi", kas nosaka valsts pārvaldes vērtības un ētikas – uzvedības un rīcības – pamatprincipus, kurus ievēro MK padotībā esošās iestādes un tajās nodarbinātie – amatpersonas, ierēdņi un darbinieki.

Risku kultūra veidojas no darbinieku **attieksmes un uzvedības**, kad iestādē kopumā ir skaidri un vienoti uzskati un vērtības (pārliecība), attiecībā uz riskiem, un šie uzskati ir vērsti uz kopīgu, visiem skaidri izprotamu iestādes mērķu sasniegšanu (9. attēls). Gan uzvedību, gan attieksmi ietekmē grupā valdošā kultūra. Normas un kultūras tradīcijas, kas attiecas uz risku vadību, veidojas, daloties ar pieredzi.

9. attēls. Attieksmes, uzvedības un kultūras modelis[18]



Katrā iestādē tās vadītājiem un darbiniekiem ir sava zināma **attieksme** pret riskiem (kā riski tiek uztverti), kas ietekmē kopējo risku kultūru un pārvaldību. Attieksme ir indivīda izvēlētā nostāja konkrētajā situācijā, ko ietekmē uztvere. Tā veidojas no iepriekšējās pieredzes, formālajiem iekšējiem un ārējiem nosacījumiem, nozares, iestādes resursiem un kapacitātes, dažādu ieinteresēto pušu attieksmes un citiem apstākļiem. Piemēram, vienas iestādes ir gatavas uzņemties vairāk riskus, citas - vairāk ir gatavas veltīt resursus vai lielāko daļu (arī ne tik būtisko, piemēram, vidējā līmeņa risku) mazināšanai u.tml. Taču attieksme pret riskiem vēl nav kultūra, jo darbinieku attieksme vēl nerezultējas konkrētā rīcībā.

Risku uzvedība (reakcija) - konkrētas rīcības saistībā ar riskiem. Uzvedība izpaužas kā ārējās apkārtējiem novērojamas indivīda darbības, tostarp lēmumu pieņemšana, procesu īstenošana un komunikācija. Piemēram, kādi lēmumi tiek pieņemti risku mazināšanai, cik tie ir savlaicīgi, cik aktīvi darbinieki tajos iesaistās, cik plaši šie lēmumi un risku statuss tiek komunicēts iekšēji iestādē un tamlīdzīgi.

Risku uzvedība arī nav risku kultūra, jo negarantē, ka iestādes darbinieku rīcība atbildīs risku vadības labākajai praksei (piemēram, tiks pieņemts lēmums ieviest kādu risku mazināšanas pasākumu, tas netiks komunicēts nevienam ārpus struktūrvienības un pēc pasākuma ieviešanas riskam nemazinoties, netiks veiktas papildu darbības).

Svarīga ir atgriezeniskā saite no kultūras uz attieksmi un uzvedību. Kultūra nav statiska, jo kultūru veido uzvedība, ko, savukārt, veido attieksme, bet, savukārt, kultūra ietekmē pašreizējo un nākotnes attieksmi un uzvedību. Attieksme pret riskiem un uzvedība, kad riski tiek konstatēti, ir gan risku kultūras pamatnosacījumi, gan arī tās iznākums jeb rezultāts.

⚠ **Svarīgi**: Risku kultūra ir tas, ko un kā jebkurš iestādes darbinieks dara attiecībā uz riskiem neatkarīgi no tā, vai šis darbinieks tiek uzraudzīts, vai tā rīcība tiek vērtēta, vai ir noteikti formāli soļi rīcībai ar riskiem.

[18] https://www.theirm.org/media/7236/risk-culture-resources-for-practitioners.pdf

Par iestādes kultūru var uzskatīt kopīgu vērtību sistēmu (kas nosaka to, kas ir svarīgs) un normas, kas definē iestādes darbinieku attieksmi un uzvedību (kā justies un reaģēt). Risku kultūra ir indivīdu un grupu vērtības, uzskati, pārliecības, praktiskā pieredze un teorētiskās zināšanas risku vadībā, attieksme un izpratne par riskiem, kā arī uzvedības normas un tradīcijas iestādē, kas saistītas ar risku identificēšanu, izpratni, apspriešanu un reaģēšanu uz tiem.

Risku kultūra var rasties dabiski. Iestādes koncentrējas uz visu risku vadības elementu praktisko ieviešanu, kas ļautu pareizi vadīt riskus, kā arī piesaista piemērotus darbiniekus, kuriem ir profesionālā prakse un iemaņas risku vadībā. Veidu, kādā iestādē indivīdi uztver un novērtē riskus, kā arī to, kā tie reaģē uz riskiem un nenoteiktību, nosaka iestādes risku kultūra. Risku kultūra attiecas uz kopīgu izpratni par to, kas tiek uztverts kā risks, kā riski tiek novērtēti, kā reaģēt uz riskiem un kādi riski ir pieņemami.

Būtiski ir iestādēs ieviest beznosodījuma pieeju risku kultūrā, ja gadījumā tiek ziņots par riskiem vai incidentiem, kā arī sniegtas idejas risku mazināšanai, netiktu piemērotas soda sankcijas, tostarp netiktu izteikti pārmetumi vai aizrādījumi darbiniekiem, kuri informējuši par riskiem vai incidentiem. Tomēr vienlaikus jāņem vērā arī normatīvajos aktos paredzētās konsekvences, kas saistītas ar konkrēto incidentu.

Svarīgi. Ja darbinieki risku vadību izmantos savā ikdienas darbā, viņi sāks izjust mazāk problēmu un lielākas priekšrocības. Kad risku vadība darbosies darbinieku labā, darbinieki atzīs risku vadības nozīmi. Tādējādi darbinieku pārliecības par risku vadības vērtību pastiprināšanās izraisīs pareizo uzvedību un iestādes kultūras stiprināšanu. Līdz ar to arī risku kultūras pievienotā vērtība palielināsies.

Piemērs: Ceļu satiksme ir viens no klasiskajiem piemēriem, kas liecina, ka risku kultūra ietekmē indivīda uztveri un uzvedību. Plaši izplatīta risku kultūra pirms vismaz 20 gadiem bija vadīt automašīnu un pasažieriem braukt ar to, neizmantojot drošības jostas, jo par to netika piemērota soda nauda. Ņemot vērā, ka transportlīdzekļu daudzums un vienlaikus arī braukšanas ātrums strauji palielinājās, ceļu satiksmes negadījumu skaits pieauga. Ja šī risku kultūra, tostarp, uzvedība reaģēt uz riskiem, paliktu nemainīga, tad ceļu satiksmes negadījumu skaits turpinātu joprojām pieaugt. Taču iegūtā negatīvā pieredze veicināja domāšanas un risku kultūras izmaiņas, kas vienlaikus nodrošināja autovadītāju un pasažieru uzvedības maiņu, kā rezultātā piesprādzēto autovadītāju un pasažieru īpatsvars šobrīd ir tuvu 100%. Iepriekšminētās risku kultūras izmaiņas veicināja arī ieviestie naudas sodi par braukšanu bez drošības jostas.

Iepriekšminētais piemērs demonstrē, ka risku kultūra satiksmes drošības risku gadījumā ir stabila vidējā termiņā, bet mainīga ilgtermiņā. Tāpat var secināt, ka risku kultūra ir balstīta uz mācīšanos no gūtās pieredzes, jo braukšana bez drošības jostas izraisa nepieņemamus letālus iznākumus, un tāpēc no šī specifiskā riska ir jāizvairās. Cilvēku kā indivīdu vai kā sociālās grupas vai iestādes darbinieku uztveri, novērtēšanu un uzvedību ietekmē risku kultūra, indivīdiem neapzinoties tās ietekmi. Piemēram, regulāras un sistemātiskas ceļu satiksmes drošības kampaņas var izraisīt izmaiņas risku kultūrā, un samazināt riska pieņemšanu. Vienā risku kultūrā iespējams uzņemties dažādu līmeņu riskus, piemēram, vēlme lietot mobilo tālruni pie stūres var būt augsta,

turpretim – tajā pašā laikā – vēlme uzņemties citu risku, piemēram, braukšanu dzērumā vai nepiesprādzētā veidā, ir zema.

Piemērs: Ja iestāde ir noteikusi, ka tā nepieļauj (vai neatzīst) nekādas kļūdas vai mērķu neizpildi, tas liecina par ļoti stingru iekšējo kultūru visās jomās, stingri noteiktu procedūru un normatīvu izpildi un ievērošanu, un tas nozīmē, ka iestāde nav atvērta riskiem (t.i. tā maksimāli vēlas izvairīties no riskiem vai tos mazināt). Tam būtu jābūt atspoguļotam risku politikā vai risku apetītē, apzinoties, ka tas ierobežo iestādes iekšējās iniciatīvas, alternatīvos risinājumus vai jebkādas inovācijas, jo, lai pēc iespējas mazinātu riskus, ir jāievēro ierastas, stingri noteiktas procedūras.

Piemērs: Ja iestādes nozare un mērķi ir vērsti uz attīstību un inovācijām, jaunu nozares politikas aspektu vai pakalpojumu ieviešanu vai attīstību, tad iestādei jābūt gatavai un atvērtai zināmam risku apjomam un jāstrādā ar risku vadību. Ja iestāde atzīst riskus un atklāti iekšēji runā par pieļautajām kļūdām vai nesasniegtajiem mērķiem, tas veicina atvērtu risku kultūru, kas iedrošina mēģināt dažādus risinājumus un meklēt veidus, kā vadīt riskus.

3.5. Ieteikumi veiksmīgas risku kultūras attīstībai

Lai risku kultūra ikdienas rutīnā atbilstu mainīgajām iestādes vajadzībām un spētu nodrošināt efektīvu risku vadību, mazinot to risku līmeni, kas pārsniedz risku apetīti, risku kultūru nepieciešams attīstīt, tādējādi vienlaikus pakāpeniski paaugstinot risku vadības brieduma līmeni iestādē.

Piemērs: Lai attīstītu risku kultūru iestādē, nepieciešams: **definēt vērtības**. Iestādes vērtības un uzvedības normas var veicināt darbiniekus pieņemt konkrētajai situācijai atbilstošus lēmumus risku vadības ietvaros:

- pieaicināt risku vadības procesā piedalīties un iesaistīties iestādes augstāko vadību, lai veicinātu labāku izpratni par iestādes riskiem un paaugstinātu risku vadības nozīmīgumu iestādē;
- ieviest **saprotamu** un **samērīgu** risku vadību, kas nerada pretestību dēļ neoptimāla risku vadības procesa;
- iestādes vadībai **regulāri pārliecināties**, ka iestādes darbinieki un risku īpašnieki atbildīgi izturas pret riskiem (tas ir, atbilstoši iestādes risku apetītei, ja tāda noteikta, risku vadības politikai, reglamentējošajiem normatīvajiem aktiem). Iestādes vadība pārliecinās, ka risku īpašnieki apzinās, kādi ir to pienākumi risku vadības procesā;
- **pilnveidot darbinieku zināšanas par risku vadību**, iekļaujot praktiskus piemērus, tai skaitā par risku novērtēšanas metodēm un risku identificēšanu lēmumu pieņemšanas procesos un izmaiņu veikšanā. Jautājumus par risku vadību nepieciešams iekļaut arī jauno darbinieku apmācību programmās;
- iekļaut darbinieku kompetences attīstības pasākumus risku vadības jomā darbinieku individuālajos attīstību plānos un mācību plānos;

- **veikt aptaujas, lai noskaidrotu risku vadības sistēmas pašnovērtējumu**, tādējādi, novērtējot esošo iestādes risku vadības brieduma līmeni, apzinot vājās puses un potenciālās pilnveides iespējas;
- iekļaut darbinieku **amatu aprakstos pienākumus**, kas attiecas uz risku vadības jomu;
- **aktīvāk izmantot jau esošos iestādes iekšējos komunikācijas kanālus** informācijas apmaiņai par riskiem, to vadību, tai skaitā iestādes iekšējā tīklā (intranetā) publicēt ne tikai apstiprināto risku vadības politiku vai metodiku, bet arī citu noderīgu informāciju, piemēram, atsauces uz mācību materiāliem vai citiem noderīgiem informācijas avotiem risku vadības jomā;
- **darbinieku snieguma novērtēšanas metodoloģijā iekļaut rādītājus**, kas saistīti ar risku vadību (piemēram, risku mazinošo pasākumu ieviešanas izpildes īpatsvars, ziņoto nozīmīgo risku un incidentu skaits);
- lai vairāk iesaistītu un izglītotu darbiniekus, iespējams **izveidot iestādes iekšējā tīklā (intranetā) jautājumu un atbilžu sadaļu** par risku vadību, kurā tiktu sniegtas atbildes, tai skaitā uz visbiežāk uzdotajiem un neskaidrajiem jautājumiem;
- lai motivētu darbiniekus iesaistīties un nebaidīties sniegt informāciju par riskiem un incidentiem, **ieviest anonīmas ziņošanas kanālu vai rīkot aptaujas**, tostarp anonīmās, kurās darbiniekiem būtu iespēja sniegt šo informāciju;
- ziņojumos par iestādes riskiem iekļaut informāciju par risku līmeņu izmaiņām, lai spētu novērtēt risku vadības efektivitāti;
- risku vadībā iesaistīto darbinieku sadarbības ar kolēģiem kultūras stiprināšana, piemēram, **komandas saliedēšanas pasākumi** (piemēram, pasākumi, kuros tiek pilnveidota darbinieku uzvedība).

3.6. Risku kultūras novērtēšana

Sākotnējā risku vadības ieviešanas posmā, kā arī pilnveidojot risku vadību, ir svarīgi novērtēt esošās risku kultūras iespējamo ietekmi uz iestādes darbību un mērķu sasniegšanu.

Risku kultūras esamība un attīstība iestādē nozīmē, ka visi darbinieki saprot risku vadības pieeju iestādē, uzņemoties individuālu atbildību par risku vadību un veicinot pārējos sekot to piemēram.

Piemērs: Ja iestāde vēlas uzzināt struktūrvienību vadītāju vai visu darbinieku viedokli par risku kultūru, iespējams organizēt darbinieku aptauju, kuras laikā uzdot šādus jautājumus, tostarp pieļaujot atbildes iespējas (piemēram, "pilnībā piekrītu", "piekrītu", "nepiekrītu" un "pilnībā nepiekrītu"), kā arī dodot iespēju sniegt atbildes un komentārus par savu viedokli:

- vai mūsu iestādē pastāv efektīva sistēma, kas ļauj darbiniekiem ziņot vadībai par identificētajiem riskiem;
- kurš iestādē ir atbildīgs par risku kultūru – vai šis darbinieks ir pietiekami pieredzējis un zinošs par risku vadību un risku kultūras ieviešanu un uzturēšanu;
- vai iestādes pārvaldības sistēmas un kultūra atbalsta iestādes stratēģijas īstenošanu;
- vai darbinieku individuālās intereses, vērtības un ētiskās normas atbilst iestādes mērķiem un vērtībām;

- kādas vērtības ir/ nav iestādes kultūrā, lai veiksmīgi ieviestu risku kultūru;
- vai ir izveidota prakse konstatēt neatbilstības starp iestādes mērķiem un kultūru, kāds ir tipiskākais neatbilstību cēlonis;
- vai izstrādāta vienota valoda par risku vadības terminoloģiju, kas palielina informētības līmeni par riskiem visās iestādes darbībās un visos struktūras līmeņos;
- vai iestādes vadība savlaicīgi saņem informāciju par riskiem un apdraudējumiem, kas nepieciešama lēmumu pieņemšanai;
- vai iestādē tiek praktizēta laba pārvaldība un tiek ievērotas vērtības;
- vai darbinieki tiek pietiekami iesaistīti risku vadības procesā;
- iestādes vadība atbalsta un veicina darbiniekus atklāt un informēt par potenciālajiem riskiem;
- vai mūsu iestādē vairums darbinieki vienādi saprot, kas iestādē ir pieļaujamie riski;
- vai mēs zinām, pie kā vērsties ar jautājumiem par risku vadības metodiku un risku vadības koordināciju, mums ir zināms, kur meklēt un iegūt informāciju par riskiem;
- vai mums ir skaidrs risku vadības process un mūsu loma tajā;
- vai eksistē darbinieks/ vidējā līmeņa vadītājs "paraugs" un vai tas demonstrē uzvedību, kas pārliecina par risku vadības nozīmīgumu iestādē;
- vai tiek sniegti konsekventi un noderīgi ziņojumi par riskiem;
- vai darbinieki apspriež riskus, vai arī viņi baidās diskutēt par sarežģītiem jautājumiem.
- vai un cik ātri darbinieki atrisina problēmas;
- vai riski tiek ņemti vērā visos iestādes darbības veidos un līmeņos, novērtējot, vai tie tiek izmantoti, sākot no stratēģiskās plānošanas procesa un beidzot ar darbinieku ikdienas pienākumu veikšanu;
- vai darbinieki ir pietiekami apmācīti par risku vadību;
- vai ir nodrošināta praksē savlaicīga un izsekojama komunikācija;
- vai risku vadībā darbinieki uzņemas individuālu atbildību un vai ir kolektīvā atbildība;
- vai atalgojums un atzinība pastiprina pozitīvu risku kultūru;
- vai efektīva risku vadība ir iestādes darbības neatņemama sastāvdaļa;
- vai darbiniekiem ir skaidrs, par kuriem riskiem tie ir atbildīgi;
- vai darbiniekiem ir nepieciešamās prasmes, lai efektīvi vadītu riskus;
- vai iestādē ir neviennozīmīgi interpretējamas iekšējās normas, kas var radīt atšķirīgu pieeju;
- kādus rīkus iestādē izmanto, lai novērtētu risku vadības efektivitāti.

Piemērs: Ieviesto risku kultūru var vērtēt arī, ņemot vērā šādus aspektus:

- struktūrvienību vadītāju un darbinieku nostāja, attieksme par risku vadību, vienlaikus apzinot, cik lielā mērā iestādes darbinieki vēlētos riskēt, veicot savus ikdienas pienākumus, vai arī darbinieki negatīvi attiecas pret riskiem;
- informācijas aprite par ētikas un risku vadības jautājumiem, tai skaitā apzinot, vai darbinieki izprot noteiktās iestādes vērtības, vai darbinieki ir informēti, kam un kad iestādē ir jāziņo par riskiem;

- darbinieku motivācija strādāt atbilstoši iestādē noteiktajām prasībām;
- vai struktūrvienību vadītāji ir ņēmuši vērā riskus lēmumu pieņemšanas procesā;
- kāda ir ieviestās risku kultūras ietekme uz sadarbības partneriem un klientiem.

Svarīgi: Darbinieku sniegtais viedoklis un faktiskā rīcība vai uzvedība vislabāk raksturo esošo risku kultūru, salīdzinājumā ar risku vadības politiku un citiem iestādes iekšējiem dokumentiem.

Organizējot darbinieku aptauju, tajā var aptaujāt tikai risku vadības procesā iesaistāmos darbiniekus vai arī var aptaujāt visus vadītājus/visus darbiniekus. Aptaujājamo izvēle atkarīga no tā, kādus jautājumus plānots noskaidrot aptaujā.

Novērtējot risku kultūru, iestādes augstākā un vidējā līmeņa vadība saņems informāciju par darbinieku, tai skaitā to, kuri piedalās lēmumu pieņemšanā risku vadības izvērtējuma rezultātiem.

Ja tiek organizēts risku vadības pašnovērtējums, tai skaitā risku kultūras novērtējums, tad tas var būt daļa no kopējā risku vadības brieduma līmeņa pašnovērtējuma. Iestādē noteiktos mērījumus vai risku vadības brieduma modeļos[19] noteiktos kritērijus var izmantot kā pašnovērtējuma veikšanas kritērijus, lai novērtētu risku kultūras atbilstību un efektivitāti.

Svarīgi: Risku kultūru var vērtēt arī iestādes iekšējā audita struktūrvienība, sniedzot neatkarīgu novērtējumu par risku kultūru vai risku vadības efektivitāti kopumā, kā arī neatkarīgi ārējie novērtētāji – ārpakalpojuma sniedzēji, kuru sniegtais viedoklis par risku kultūras kritēriju novērtējumu būs neatkarīgs un objektīvi neitrāls.

KOPSAVILKUMS

Viens no svarīgākajiem efektīvas iestādes pārvaldības aspektiem ir risku kultūra. Viens no pamatuzdevumiem tās nostiprināšanai un attīstībai ir uz risku orientētas domāšanas ieviešana iestādē, kas veicinātu risku novērtēšanas precizitāti, attīstītu darbinieku kompetenci risku analīzē un lēmumu pieņemšanā. Risku kultūra ir svarīgs stūrakmens veiksmīgai, dzīvai un praktiskai risku vadībai iestādē.

Attīstīta risku kultūra iestādē nodrošina, ka riski tiks savlaicīgi novērtēti un tiks adekvāti reaģēts uz tiem (veikti atbilstoši risku vadības pasākumi), nepieļaujot to īstenošanos.

Par iestādes kultūru var uzskatīt kopīgu vērtību sistēmu (kas nosaka to, kas ir svarīgs) un normas, kas definē iestādes darbinieku attieksmi un uzvedību (kā justies un reaģēt). Risku kultūra ir indivīdu un grupu vērtības, uzskati, pārliecības, praktiskā pieredze un teorētiskās zināšanas risku

[19] Ekonomiskās sadarbības un attīstības organizācijas (OECD) Uzņēmumu risku vadības brieduma modelis (*Enterprise Risk Management Maturity Model*), 2021, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/enterprise-risk-management-maturity-model.pdf; Risku vadības brieduma modelis uzņēmumu risku vadībai (*RMM*), https://www.riskmaturitymodel.org/; Finanšu ministrijas izstrādātais risku vadības sistēmas brieduma līmeņa novērtēšanas modelis (skat. 1.pielikumu).

vadībā, attieksme un izpratne par riskiem, kā arī uzvedības normas un tradīcijas iestādē, kas saistītas ar risku identificēšanu, izpratni, apspriešanu un reaģēšanu uz tiem.

Risku kultūra ir vairāk nekā iestādes vērtību noteikšana, jo tā attiecās uz to transformēšanu praksē, īstenojot konkrētās rīcības.

Risku kultūras ietvars paredz, ka risku kultūra apvieno:

- katra indivīda personīgo noslieci uz risku;
- personīgo ētiku;
- attieksmi un uzvedību;
- iestādes kultūru.

Risku kultūras aspektu modelis identificē astoņus risku kultūras aspektus – galvenos risku kultūras "veselības" rādītājus, kas saskaņoti ar iestādes pamatdarbības modeli un kas sagrupēti četrās tēmās – "tonis" no augšas, pārvaldība, kompetence un lēmumu pieņemšana.

Iestādes vadībai ir jārāda piemērs, ja vadība vēlas, lai ikviens iestādes darbinieks tiem sekotu ar savu rīcību un ievērotu konsekvenci gan rīcībā, gan attieksmē. Iestādes līderiem jāspēj būt atvērtiem, lai saņemtu no darbiniekiem informāciju par problēmām un riskiem.

Augstākajai vadībai ir jānodrošina, ka tiek sniegta skaidra un nepārprotama informācija par to, kāda rīcība vai uzvedība ir sagaidāma no darbinieka risku vadības ietvaros. Lai vadības sniegtā informācija par risku kultūru tiktu uzklausīta, saprasta, un darbinieki to pielietotu praksē, darbiniekiem ir jāsaprot risku vadības būtība un nozīme, kā arī praktiskie risku piemēri un to īstenošanās sekas, kas apgrūtinās vai pat pārtrauks viņu ikdienas darbības.

Risku kultūras ieviešana ir ilglaicīgs un ne vienmēr vienkāršs process, kam jāsākas no iestādes līderu puses, apzinoties, ka risku vadības process ir kopīgs iestādes uzdevums un atbildība.

Risku kultūras esamība iestādē nozīmē, ka visi darbinieki saprot risku vadības pieeju iestādē, uzņemoties individuālu atbildību par risku vadību un veicinot pārējos sekot to piemēram.

Novērtējot risku kultūru, iestādes augstākā un vidējā līmeņa vadība saņems informāciju par darbinieku, tai skaitā to, kuri piedalās lēmumu pieņemšanā, risku vadības izvērtējuma rezultātiem.

Risku vadības pašnovērtējums, tai skaitā risku kultūras novērtējums, var būt daļa no kopējā risku vadības brieduma līmeņa pašnovērtējuma.

4. RISKU VADĪBAS PĀRVALDĪBA

Risku vadības pārvaldība nodrošina risku pārvaldības struktūru iestādē un veicina, ka, ieviešot pārmaiņas, tiek samazinātas risku negatīvās sekas un iestāde spēj operatīvi reaģēt uz izmaiņām iekšējā un ārējā vidē. Risku vadības pārvaldība koncentrējas uz labas korporatīvās pārvaldības principu piemērošanu risku vadībā, vienlaikus nodrošinot, ka iestādes vadītāji rīkojas, ievērojot risku apetīti un toleranci. Risku vadības pārvaldības ietvaros augstākajai vadībai ir jānodrošina, ka iestādes mērķu sasniegšanu atbalsta pārdomāts risku vadības ietvars (politika un tās ieviešanu skaidrojošas metodikas (iekšējie normatīvie akti)) un risku vadība, kas atbilst tās darbības būtībai un sarežģītībai.

4.1. Trīs līniju modelis efektīvai risku vadībai un kontrolei. Risku vadības lomas. Amatu pienākumu apvienošana

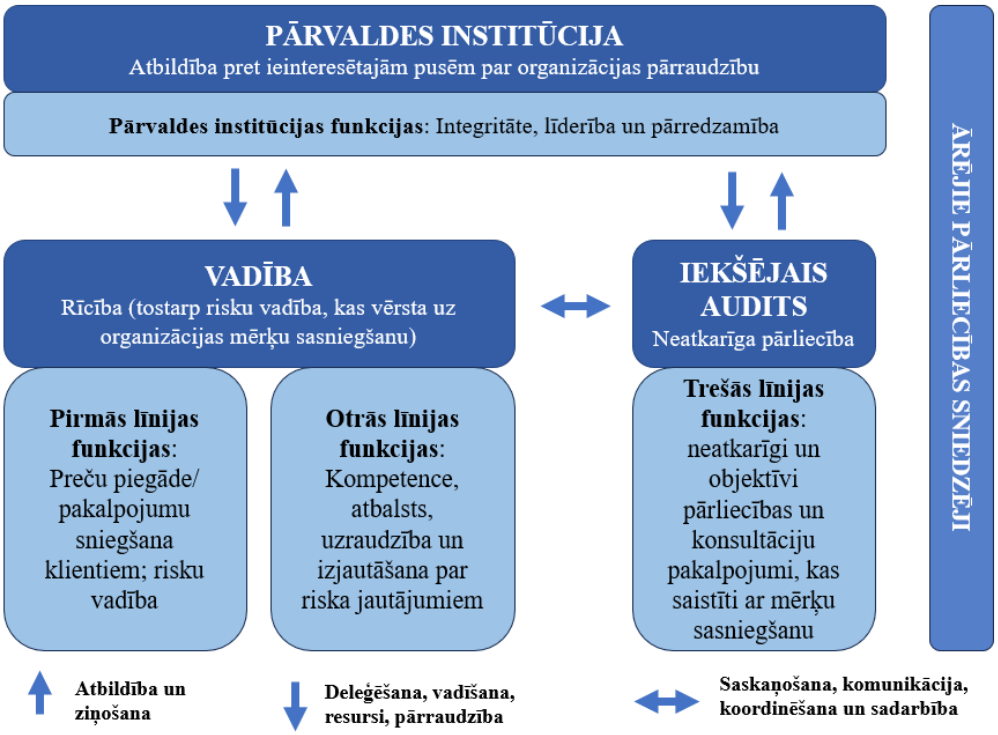
4.1.1. Trīs līniju modelis

Iestādē ir nepieciešama pārdomāta struktūra un vadlīnijas riska pārvaldības pienākumu un atbildību sadalei, īpaši ņemot vērā ārējās un iekšējās vides straujo mainību. Starptautiskais Iekšējo auditoru institūts ir izstrādājis "Trīs līniju modeli"[20], kas piedāvā sastrukturēt pārvaldības funkcijas un atbildības sadalījumu starp trīs līnijām – pārvaldes institūciju, vadību un iekšējo auditu.

Trīs līniju modelis (10. attēls) tika atjaunots ar mērķi palielināt iestādes vērtības radīšanu un tās aizsardzību, un tas skaidro, kādi iestādes amati ir iesaistīti risku vadībā un kādai būtu jābūt to koordinētajai rīcībai kopumā, lai veiksmīgi pārvaldītu riskus un uzturētu iekšējās kontroles sistēmu. Modeļa priekšnosacījums ir pārvaldības un kontroles pienākumu nodalīšana, kā arī skaidru pienākumu noteikšana visām lomām. Trīs līniju modelis paredz, ka risku vadībā ir iesaistīti visu līmeņu vadītāji, darbinieki un amati, kas īsteno dažādas iestādes funkcijas.

[20] Ar Iekšējo auditoru institūta izstrādāto "Trīs līniju modeli" latviešu valodā var iepazīties: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-latvian.pdf

10. attēls. Trīs līniju modelis[21]



Lai risku vadība trīs līniju modeļa ietvarā sekmīgi darbotos, iestādēm būtu jāievēro 6 principu pieeja, kuru iespējams pielāgot atbilstoši iestādes mērķiem un darbības videi:

- **Pārvaldība** – pārvaldīšanai nepieciešamas atbilstošas struktūras un procesi, kas ļauj pārvaldes institūcijai uzņemties atbildību pret ieinteresētajām pusēm, vadībai veikt apzinātu riska vadību un neatkarīgai iekšējā audita funkcijai sniegt pārliecību un konsultācijas;
- **Pārvaldes institūcijas funkcijas** – pārvaldes institūcija nodrošina efektīvai pārvaldībai atbilstošu struktūru un procesu ieviešanu, ka arī iestādes mērķu un darbību saskaņošanu ar ieinteresēto pušu prioritātēm;
- **Vadības funkcijas** – vadības atbildība par iestādes mērķu sasniegšanu, kā arī ietver gan pirmās, gan otrās līnijas funkcijas, arī atbalsta funkcijas, un otrās līnijas funkcijas var būt vērstas uz konkrētu risku kategoriju vadību mērķu sasniegšanā;
- **Iekšējā audita funkcija** – iekšējais audits sniedz neatkarīgu un objektīvu pārliecību, konsultācijas par risku vadības pārvaldības piemērotību un efektivitāti;
- **Trešās līnijas neatkarība** – iekšējā audita neatkarība no vadības funkcijas, ziņojot pārvaldes institūcijai, nodrošinot neierobežotu piekļuvi personālam, resursiem un informācijai, kas nepieciešama iekšējā audita darba izpildei, kā arī nodrošinot objektivitāti, lai nenotiktu iejaukšanās iekšējā audita funkcijas izpildē;
- **Vērtības radīšana un aizsardzība** – visas iepriekšminētās funkcijas nodrošina vērtību aizsardzību un palielināšanu, savstarpēji sadarbojoties un nodrošinot lēmumu pieņemšanai nepieciešamās informācijas ticamību un kvalitāti, lai pietiekami apzinātos saistītos riskus.

[21] https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-latvian.pdf

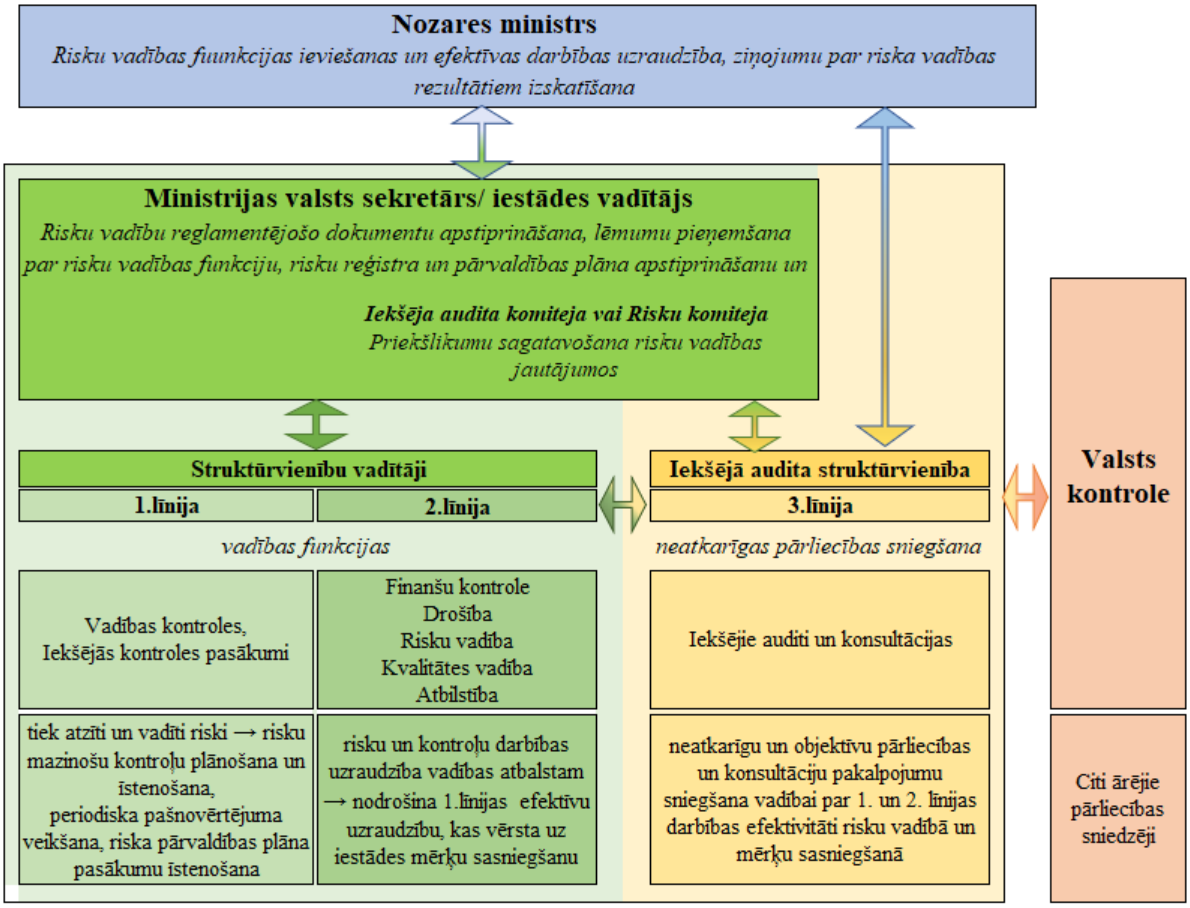
Jebkuras ārējās neatkarīgās puses veikts novērtējums vai uzraudzība (piemēram, ārējais audits vai kontrolējošās iestādes) tiek uzskatīts par nākamo līmeni un neformāli tiek dēvēts par "ceturto līniju".

Trīs līniju modelis arī detalizētāk apraksta nepieciešamo sadarbības modeli starp galvenajām funkcijām jeb trīs līnijām:

- starp pārvaldes institūciju un vadību:
  - pārvaldes institūcija nosaka iestādes darbības virzienu, definējot vīziju, misiju, vērtības un iestādes risku apetīti;
  - pārvaldes institūcija deleģē atbildību par iestādes mērķu sasniegšanu kopā ar nepieciešamajiem resursiem vadībai;
  - pārvaldes institūcija saņem vadības ziņojumus par plānotajiem, faktiskajiem un sagaidāmajiem rezultātiem, kā arī ziņojumus par risku vadības pieeju un rezultātiem.
- starp vadību (gan pirmās, gan otrās līnijas funkcijām) un iekšējo auditu:
  - iekšējā audita funkcijai nepieciešama neatkarība no vadības funkcijas, t.i., novēršot šķēršļus un subjektivitāti auditu plānošanā un izpildē, kā arī jebkādus ierobežojumus piekļuvē personālam, resursiem un informācijai, kas nepieciešama iekšējā audita funkcijas izpildei;
  - iekšējam auditam ir jābūt pakļautam pārvaldes institūcijai;
  - starp iekšējo auditu un vidējā līmeņa un augstāko vadību jānodrošina regulāra mijiedarbība, lai iekšējā audita darbs būtu mērķtiecīgs, efektīvs un atbilstu iestādes stratēģiskajām un operatīvajām vajadzībām;
  - iekšējam auditam sistemātiski jāuzkrāj zināšanas un izpratne par iestādes darbību, lai uzlabotu pārliecības gūšanas (auditu) un konsultāciju kvalitāti, kuras tas sniedz kā uzticams padomdevējs un stratēģiskais partneris augstākajai vadībai;
  - jānovērš nevajadzīgu darbību dublēšanās, pārklāšanās vai pārrāvumi starp līnijām, regulāri apmainoties ar informāciju.
- starp iekšējo auditu un pārvaldes institūciju:
  - iekšējais audits ir pakļauts pārvaldes institūcijai un ir tās sabiedrotais ("acis un ausis");
  - pārvaldes institūcija ir atbildīga par iekšējā audita pārraudzību, tas ir, nodrošinot iekšējā audita funkcijas izveidi, iekšējā audita vadītāja iecelšanu un atbrīvošanu no amata, audita plānu apstiprināšanu un resursu piešķiršanu, kā arī iekšējā audita vadītāja ziņojumu saņemšanu un izvērtēšanu.

Ņemot vērā Valsts pārvaldes iekārtas likumu, pielāgotais Trīs līniju modelis, kam ir rekomendējošs raksturs, konceptuāli ir attēlots 11. attēlā. Trīs līniju modelī iekļautās pārvaldes institūcijas funkcijas veic nozares ministrs, valsts sekretārs/ iestādes vadītājs un viņa vietnieki. Savukārt, vadības funkcijas izpilda administratīvais vadītājs (valsts sekretārs/ iestādes vadītājs, viņa vietnieki un struktūrvienību vadītāji). Tāpat vadības funkcijā ietilpst Iekšējā audita komiteja vai Risku vadības komiteja.

11. attēls. Valsts pārvaldei adaptēts Trīs līniju modelis



Nozares ministrs aicina vai iniciē ieviest risku vadību iestādē, kā arī saņem informāciju par riskiem.

Iestādes administratīvais vadītājs nodrošina risku vadības un iekšējās kontroles sistēmas ieviešanu un uzturēšanu un pārraudzību.

Ikdienas darba nodrošināšanai katrā iestādē pienākumi un atbildība, ņemot vērā struktūrvienību nolikumus vai citus iekšējos normatīvos aktus, ir sadalīti un deleģēti struktūrvienību vadītājiem, kuri nodrošina **pirmās līnijas** lomu, tostarp aizsardzību pret iestādes darbību ietekmējošajiem riskiem.

Pirmās līnijas lomu iestādēs veic tie struktūrvienību vadītāji, kuri īsteno pamatdarbības funkcijas, kā arī sniedz iekšējos vai ārējos pakalpojumus, ņemot vērā iestādes nolikumu. Līdz ar to šie vadītāji ir atbildīgi par riskiem savā tiešajā darbības jomā (veicamajos pienākumos, uzdevumos, kā arī procesos, ko tie īsteno vai pakalpojumos, ko tie sniedz). Tieši šo struktūrvienību vadītāju atbildība ir nodrošināt ikdienas operatīvos procesus, kontroles un risku vadību, tostarp uzraudzību, pēc iespējas pielietojot savas zināšanas un ekspertu lomu attiecīgajā jomā. Atbilstoši nosaukumam tieši pirmās līnijas uzdevums ir reaģēt uz ārējiem un iekšējiem apstākļiem un ieviest uzlabojumus vai izmaiņas, tiklīdz tie nepieciešami risku novēršanai vai mazināšanai. Pirmā līnija visbiežāk ir risku īpašnieki.

Atsevišķu riska kategoriju pārvaldībai **otrajā līnijā** var tikt rasti papildu personāla resursi (kā struktūrvienība vai amats), ja šo riska kategoriju pārvaldībai nepieciešamas īpašas zināšanas, metodikas vai rīki, vai arī lielā darba apjoma, kas nepieciešams risku vadībā dēļ, nav iespējams savienot pienākumu veikšanu ar esošo amatu (piemēram, informācijas/ IT drošības vadītājs,

darba drošības vadītājs, personas datu aizsardzības vadītājs, interešu konflikta, korupcijas un krāpšanas risku vadītājs u.tml.). Neatkarīgi no darba organizācijas un pienākumu sadalījuma, ir ļoti būtiski organizēt regulāru informācijas apmaiņu par iekšējās kontroles efektivitāti starp pirmās un otrās līnijas pārstāvjiem.

Otrā līnija veic pirmās līnijas pārraudzības un iestādes administratīvās/ atbalsta funkcijas. Otrā līnija sniedz atbalstu, lai ieviestu un attīstītu risku vadības funkciju, kā arī, lai nodrošinātu iestādes darbības atbilstību iekšējiem un ārējiem tiesību aktiem. Atbalsta funkcijas ir horizontālas visu iestādi aptverošas funkcijas, kas ir saistītas ar risku vadību, piemēram:

- risku vadības funkcija;
- finanšu vadības un grāmatvedības funkcija;
- personas datu aizsardzības funkcija;
- informācijas tehnoloģiju drošības funkcija;
- kvalitātes vadības funkcija;
- atbilstības funkcija;
- juridiskā funkcija un tamlīdzīgi.

Otrajā līnijā ir risku vadības funkcija, kuras ietvaros nepieciešams metodiski vadīt un koordinēt risku vadības posmus (piemēram, identificēšana, analizēšana, izvērtēšana, reaģēšana uz riskiem un uzraudzība), kā arī citas iestādes iepriekšminētās horizontālās visu iestādi aptverošās funkcijas ir saistītas ar risku vadību, tostarp risku apzināšanu un uzraudzību. Tieši otrā līnija var uzraudzīt ārējās vides apstākļus un iekšējās vides ietvaru, kas var ietekmēt visu iestādi un radīt tajā riskus. Otrajā līnijā ietilpstošo funkciju horizontālā un visu iestādi aptverošā būtība, ļauj šo funkciju ietvaros apzināt un ieviest piemērotākos risku mazināšanas pasākumus. Otrā līnija var uzraudzīt, kā pirmā līnija ievieš šādus visaptverošus risku mazināšanas pasākumus, kā arī iekšējās kontroles, un ziņot iestādes augstākajai vadībai par uzraudzības laikā gūtajiem secinājumiem.

Iekšējā audita likuma 6.panta pirmā daļa nosaka iestādes vadītāja pienākumus saistībā ar iekšējā audita funkciju jeb **trešo līniju**, tai skaitā, atbildību par iekšējā audita sistēmas darbību, iekšējā audita darba organizāciju un iekšējā audita ieteikumu ieviešanas uzraudzības kārtības noteikšanu iestādē, iekšējā audita struktūrvienības stratēģiskā plāna un gada plāna apstiprināšanu un citus iekšējā audita funkcijas pakļautības jautājumus.

Trešā līnija (iekšējā audita funkcija) sniedz neatkarīgu un objektīvu pārliecību (auditus) un konsultācijas par iestādes mērķu sasniegšanu, tostarp izvērtē, vai pirmā un otrā līnija darbojas atbilstoši tiesību aktiem un pietiekami aktīvi, lai vadītu riskus. Trešā līnija kā neatkarīga struktūrvienība no iestādes vadības un struktūrvienību vadītājiem ziņo iestādes augstākajai vadībai (t.i., augstākajam pārvaldības līmenim) par sava novērtējuma rezultātiem un priekšlikumiem risku vadības procesa pilnveidošanai.

Piemērs: Pārtikas veterinārā dienesta Pārtikas uzraudzības departaments, Veterinārās uzraudzības departaments, Robežkontroles departaments un to daļas pilda pirmās līnijas lomas. Informācijas analīzes un ātrās reaģēšanas daļa, Iekšējās kontroles galvenais speciālists un potenciālā risku vadītāja funkcija pildītu otrās līnijas lomu. Risku vadītājs sniegtu pietiekamu risku vadības metodoloģisko un koordinēšanas atbalstu. Savukārt iekšējā audita struktūrvienība ir trešā līnija, kas neatkarīgi novērtētu,

vai struktūrvienības, kuras atbildīgas par 1. un 2. līmeņa funkciju īstenošanu, laicīgi un pilnvērtīgi piedalās risku vadībā un risku vadības process ir efektīvs.

4.1.2. Risku vadības lomas un atbildība

Risku vadībā iestādē iesaistīti dažādu līmeņu darbinieki un vadītāji, un šajā nodaļā aprakstītas to atbildības attiecībā uz risku vadību. Šīs atbildības ir plašas, un aprakstīts to maksimālais apjoms, kas būtu piemērots iestādēm, kas sasniegušas vismaz trešo risku vadības brieduma līmeni. Taču atkarībā no iestādei pieejamā darbaspēka u.c. resursiem, kā arī risku vadības brieduma līmeņa, praksē iestādēs noteiktās atbildības un darbinieku faktiskie pienākumi var būt ne tik plaši un apjomīgi.

⚠ **Svarīgi**: Galvenā atbildība par risku vadības ieviešanu un uzturēšanu ir iestādes augstākajai vadībai. Risku vadītāja pienākums ir metodiski vadīt un koordinēt risku vadību. Savukārt, struktūrvienību vadītāju un dažādu citu līmeņu darbinieku atbildība ir pilnvērtīgi piedalīties dažādos risku vadības posmos un aktivitātēs, tostarp savlaicīgi ziņot par riskiem, kā arī sniegt informāciju par risku mazinošo pasākumu ieviešanas progresu/ izpildi.

Iestādes augstākās vadības un pārējo darbinieku pienākumiem saistībā ar risku vadību būtu jābūt noteiktiem to amatu aprakstos!

Risku vadības funkcijai jābūt neatkarīgai no iekšējā audita funkcijas!

Turpmāk tiks aprakstīta risku vadībā iesaistīto dalībnieku loma, atbildība un pienākumi, ņemot vērā starptautisko labo praksi (8.tabula).

8. tabula. Risku vadībā iesaistīto loma un atbildība

Iestādes vadības līmenis/loma	Atbildība risku vadībā
Iestādes augstākā vadība	• Nodrošināt IKS esamību, tai skaitā risku vadības funkcijas īstenošanu; • Izveidot un ieviest visaptverošu risku vadības sistēmu, nodrošinot, ka risku vadība ir integrēta visās iestādes funkcijās, procesos, sistēmās, struktūrvienībās un līmeņos, lai varētu sasniegt stratēģiskos un darbības mērķus; • Demonstrēt/izrādīt līderību un apņemšanos; • Noteikt iestādes kultūru, pamatvērtības, uzvedību, standartus un vēlamās kompetences; • Apstiprināt lomas, atbildību un pienākumus visos iestādes līmeņos. Noteikt visu iesaistīto pušu atbildību attiecībā uz risku vadību; • Apstiprināt un regulāri pārskatīt risku vadības sistēmas ietvaru, risku vadības politiku un risku vadības metodiku/vadlīnijas (iekšējos normatīvos aktus, kas reglamentē risku vadību);

Iestādes vadības līmenis/loma	Atbildība risku vadībā
	• Iepazīties ar risku vadības rezultātiem, stratēģiskajiem un būtiskajiem riskiem; uzraudzīt galveno/būtiskāko un jaunu risku vadību, izskatot regulārus (piemēram, reizi ceturksnī vai pusgadā) ziņojumus; • Regulāri izskatīt (piemēram, ne retāk kā reizi gadā) ziņojumus par situāciju risku vadības jomā, tostarp būtiskākajām risku vadības problēmām, notikušajiem incidentiem, risku vadības sistēmas nepieciešamajiem uzlabojumiem un pilnveidojumiem; • Pieņemt lēmumus stratēģisko un būtisko iestādes risku vadībai; • Apstiprināt risku vadības rezultātus – risku reģistrs (nozīmīgākie iestādes riski, riska līmenis, risku mazināšanas pasākumi (riskiem, kuru līmenis pārsniedz pieļaujamo līmeni), atbildīgie, ieviešanas termiņi), kas vienlaikus var būt arī risku mazināšanas pasākumu plāns. Iepriekšminēto plānu iespējams izstrādāt un apstiprināt arī atsevišķi no risku reģistra, pārnesot no tā nepieciešamo minimālo informāciju; • Noteikt risku apetīti un risku tolerances intervālus; • Uzraudzīt risku vadības funkcijas darbību un efektivitāti, atbilstību iestādes mērķiem; • Nodrošināt nepieciešamo resursu (finanšu, personāla, tehnoloģijas) piešķiršanu risku vadībai; • Nodrošināt, ka iestādes mērķu (stratēģisko, darbības) noteikšanas procesā pienācīgi un pietiekami tiek apsvērti riski un ņemta vērā iestādes riska apetīte; • Nodrošināt iestādes funkciju, procesu aprakstu izstrādi un aktualizēšanu, kā arī procesu vadības sasaisti ar risku vadību; • Nodrošināt risku vadības procesa nepārtrauktību; • Nodrošināt, ka informācija par riskiem un to vadīšanu tiek pienācīgi, savlaicīgi un pilnā apmērā paziņota, piemēram, iestādes augstākajai vadībai vai uzraugošajai iestādei (piemēram, padotības iestādes gadījumā – ministrijai).
Struktūrvienību (departamentu/nodaļu vadītāji)	• Ieviest un uzturēt IKS, tai skaitā, kontroles vidi un risku vadības elementus; • Nodrošināt iestādes pamatdarbības, vadības vai atbalsta procesu efektīvu īstenošanu stratēģisko mērķu sasniegšanai, nodrošināt procesu uzraudzību/ kontroli un pilnveidošanu; • Nodrošināt nepieciešamos darbinieku un laika resursus risku vadībai struktūrvienības ietvaros; • Identificēt, analizēt un izvērtēt riskus; • Piedalīties lēmumu pieņemšanā par risku mazināšanas pasākumiem, risku reģistru pārskatīšanā un apstiprināšanā u.tml.; • Uzraudzīt un nodrošināt risku vadību savā struktūrvienībā; • Sadarboties ar citām struktūrvienībām un vadības līmeņiem risku vadībai (piemēram, risku mazināšanas pasākumu ieviešanai); • Uzraudzīt risku mazināšanas pasākumu un risku statusus;

Iestādes vadības līmenis/loma	Atbildība risku vadībā
	• Ziņot par riskiem un to statusu augstākajai vadībai, vidējā līmeņa vadītājiem; • Piedalīties komunikācijā par būtiskajiem riskiem, tostarp stratēģiskajiem riskiem; • Proaktīvi izmantot risku vadības procesa rezultātus, operacionālajiem lēmumiem, plānošanai, piemēram, budžeta plānošanai; • Sagatavot un regulāri (piemēram, reizi gadā) pārskatīt, vai ir bijušas kādas izmaiņas, kas ietekmē funkcijas, procesus, un pieņemt lēmumu, vai ir jāveic procesu aprakstu/procedūru aktualizācija; • Analizēt iegūtos procesu snieguma rezultātus un to mērījumu tendences kontekstā ar risku analīzi.
Risku īpašnieki (var būt jebkura līmeņa darbinieks)	• Identificēt un analizēt riskus, piedalīties risku novērtēšanā; • Apzināt un definēt risku mazināšanas pasākumus; • Ieviest risku mazināšanas pasākumus un uzturēt kontroles risku vadībai; • Vadīt īstenojušos risku notikumus/incidentus; • Uzraudzīt risku tendences, ziņot par risku statusa izmaiņām, uzraudzīt risku indikatorus (ja tādi ir noteikti); • Sagatavot informāciju par riskiem, ziņot par riskiem saviem tiešajiem vadītājiem.
Risku vadītājs	• Izveidot un ieviest (uzturēt) iestādes risku vadības metodisko un procesu ietvaru, iekšējos normatīvos aktus (t.i., paredzot tajos risku vadības procesa posmus, to veikšanas regularitāti, iesaistītos dalībniekus, to atbildību un metodiku un tamlīdzīgi (tai skaitā, nepieciešamo dokumentu, piemēram, risku reģistra, incidentu reģistra, risku mazināšanas pasākumu plāna, ziņojuma augstākai vadībai formas/veidlapas)); • Veicināt konsekventu un precīzu risku vadības praksi, īstenojot efektīvu risku vadības plānošanu un attīstību; • Nodrošināt risku vadības procesa nepārtrauktību un norisi, atbilstoši iekšējos normatīvajos aktos iekļautajām prasībām un risku vadības politikā un metodikā noteiktajiem mērķiem; • Koordinēt un organizēt risku vadības procesus, komunicējot ar citiem šajā tabulā minētajām risku vadībā iesaistītajiem dalībniekiem (dažādu līmeņu vadītāji); • Uzturēt un aktualizēt vienotu/centralizētu iestādes risku reģistru; • Sniegt metodisko atbalstu un piedalīties risku identificēšanā un analīzē un izvērtēšanā, kā arī risku mazināšanas pasākumu noteikšanā; atbalstīt risku vadības praktisko ieviešanu iestādē, tostarp saistītās dokumentācijas pielietošanā; • Palīdzēt augstākajai vadībai veikt attiecīgos risku pārvaldības pārraudzības pienākumus;

Iestādes vadības līmenis/loma	Atbildība risku vadībā
	• Apkopot risku informāciju, ziņot par riskiem dažādās sanāksmēs un formātos, dažādiem iestādes vadības līmeņiem; • Uzraudzīt risku tendences un risku mazināšanas pasākumu ieviešanas progresu, proaktīvi apzināt ārējās un iekšējās vides apstākļus un tendences, kas var liecināt par riskiem, kā arī koordinēt risku pārvērtēšanu; • Organizēt apmācības risku vadības jomā un veicināt vienotas izpratnes rašanos par iestādes risku vadību; • Veicināt sadarbību ar risku īpašniekiem – sākumā – reizi pusgadā un vēlāk – ne retāk kā reizi gadā organizēt darba grupas vai tiešās intervijas ar risku koordinatoriem struktūrvienībās, ja šādi amati izveidoti, ar mērķi identificēt un novērtēt jaunus riskus, kā arī pārvērtēt jau identificētos un risku reģistrā iekļautos riskus; • Regulāri (piemēram, reizi ceturksnī vai pusgadā) pieprasīt informāciju no risku īpašniekiem par galveno/būtiskāko risku vadību, to mazināšanas pasākumu progresu, un notikušajiem incidentiem (riskiem, kuri īstenojušies vai arī incidentiem, par kuriem risku reģistrā nav iekļauta informācija), kā arī par jaunajiem identificētajiem riskiem; • Ņemot vērā iepriekšminēto informāciju, regulāri, piemēram, ne retāk kā reizi gadā, sagatavot augstākajai vadībai un vidēja līmeņa vadītājiem ziņojumu par situāciju risku vadībā, tostarp, būtiskākajām problēmām risku vadības procesā, iestādes riskiem, incidentiem un nepieciešamajiem pilnveidojumiem risku vadības procesā, tai skaitā pirmajā līnijā; • Koordinēt risku pārvērtēšanu, ja ir noticis incidents, notikušas izmaiņas ārējā vidē, kā arī, pamatojoties uz iekšējā audita vai ārējā audita rezultātiem; • Uzturēt un aktualizēt vienotu/centralizētu incidentu reģistru; • Sadarboties ar iestādes kvalitātes vadības/ atbilstības nodrošināšanas/ procesu vadības speciālistu/koordinatoru vai struktūrvienību vadītājiem, izstrādājot un aktualizējot iestādes funkciju, procesu aprakstus; • Pārbaudīt risku vadības pasākumu efektivitāti – uzraudzīt, lai risku mazinošie pasākumi/kontroles būtu atbilstoši un efektīvi, lai ziņošana/informācijas aprite būtu precīza un pilnīga un lai trūkumi risku vadībā tiktu novērsti savlaicīgi; • Sagatavot informāciju par iestādes risku vadību publiskošanai iestādes mājas lapā internetā (ja nepieciešams) vai atbilstoši kādas ārējās puses informācijas pieprasījumam.
Iekšējā audita funkcija	• Novērtēt iestādes iekšējās kontroles sistēmas darbību un tās efektivitāti kopumā, tai skaitā risku vadību; • Ņemt vērā risku vērtēšanas rezultātus audita plāna izveidē; • Informēt risku vadītāju par potenciālajiem identificētajiem riskiem;

Iestādes vadības līmenis/loma	Atbildība risku vadībā
	• Regulāri pārbaudīt un sniegt vadībai informāciju par risku vadības pārvaldības sistēmas organizāciju un darbību. Izvērtēt, vai riski ir pietiekami vadīti un vai risku novērtēšana un ziņošana par riskiem un kontrolēm ir atbilstoša un ticama, lietderīga un efektīva; • Sniegt ieteikumus vadībai, ja tiek identificēti jauni būtiski riski.
IT/drošības funkcija (ja ir)	• Nodrošināt risku incidentu informāciju risku vadītājam; • Piedalīties risku novērtēšanā un analīzē (IKT jomā); • Sniegt atbalstu risku vadības atbalstam nepieciešamās informācijas sistēmas ieviešanā un uzturēšanā.
Stratēģiskās/plānošanas funkcija (ja ir)	• Piedalīties stratēģisko risku identificēšanā, analīzē un novērtēšanā; • Noteikt iestādes stratēģiskos mērķus un darbības plānus to īstenošanai, kā arī citu līmeņu iestādes darbības plānus; • Ņemt vērā risku vadības rezultātus stratēģisko un operatīvo iestādes darba plānu izveidē (piemēram, paredzot resursus un scenārijus iestādes mērķu sasniegšanai, ņemot vērā būtiskos riskus, un to vadībai nepieciešamos mazināšanas pasākumus, kas varētu ietekmēt darbības plānu termiņus un budžetu).

Padoms: Iesaistot risku vadības procesā vairākus iestādes darbiniekus un vadības līmeņus, būs skaidrāk nosakāmi pienākumi un atbildība saistībā ar risku vadību, un līdz ar to būs veiksmīgāk iespējams iedzīvināt risku vadības kultūru, un darbinieki to neuztvers tikai kā viena darbinieka - risku vadītāja - pienākumu un ekspertīzes jomu.

Padoms: Risku vadītājam jābūt ar pietiekami hierarhiski augstu pakļautību iestādes organizatoriskajā struktūrā, lai būtu iespējams ziņot par risku vadības rezultātiem iestādes augstākajai vadībai, kā arī nodrošināt to, ka lēmumiem, kas saistīti ar risku vadību, ir pietiekama nozīme un ietekme iestādē.

4.1.3. Amatu pienākumu apvienošana

Dažāda veida iestādēs publiskajā sektorā, tostarp valsts pārvaldē, bieži vien risku vadību veic atsevišķs pilnas slodzes darbinieks un tas ir ieteicams, lai pilnvērtīgi ieviestu, uzturētu un attīstītu risku vadību. Taču mazās iestādēs var nebūt iespējas algot pilnas slodzes darbinieku, kas veiktu

tikai risku vadītāja amata pienākumus. Līdz ar to mazajās iestādēs[22] risku vadītāja pienākumus, iespējams, būs nepieciešams apvienot ar citiem pienākumiem, nelielā kopējā iestādes darbinieku skaita dēļ (var nebūt iespējams mazā iestādē algot pilnas slodzes darbinieku, kas veiktu tikai risku vadības funkciju). Šādos gadījumos iespējams apvienot risku vadītāja amata pienākumus ar citiem amata pienākumiem.

 **Svarīgi**: Lai pēc iespējas pilnvērtīgāk un veiksmīgāk ieviestu un attīstītu risku vadību iestādēs, ieteicams, lai risku vadības lomu veiktu pilnas slodzes darbinieks, kura amata pienākumos ietilpst tikai risku vadība.

 **Svarīgi**: Iestādes augstākajai vadībai un citiem darbiniekiem, kuri iesaistīti risku vadībā, kuriem amatu aprakstos iekļauti ar risku vadību saistītie pienākumi, tie nebūtu jāinterpretē kā amatu apvienošana. Šajā nodaļā aprakstītas situācijas, kas attiecas tieši uz risku vadītāja lomas apvienošanu ar citiem amatiem.

Papildu risinājumi, ko var izmantot iestādēs, kurās nav iespējas (darbinieku skaita, atalgojuma, finanšu resursu, iestādes vadības lēmumu attiecībā uz organizatorisko struktūru vai citu iemeslu dēļ) algot pilnas slodzes darbinieku, kas veiktu risku vadītāja pienākumus, ir šādi:

- ārpakalpojumu sniedzēju konsultācijas un pakalpojumi risku identificēšanai, novērtēšanai, risku mazināšanas pasākumu noteikšanai. Šādi pakalpojumi būtu jāizmanto ar zināmu regularitāti (vismaz reizi gadā), lai uzturētu risku vadību aktuālu. Iestādei iekšēji jānodrošina risku mazināšanas pasākumu ieviešana un to statusa uzraudzība.
- risku vadības "vēstnieku" principa ieviešana, tas ir, kad eksistē vairāki amati, kuru pienākumos ietilpst risku vadība savā kompetencē esošajā jomā (piemēram, par konkrētām iestādes funkcijām, darbības jomām vai struktūrvienībām). Šie "vēstnieki" regulāri ziņo iestādes vadībai par riskiem savā atbildības jomā. Priekšnosacījums šādai pieejai ir iepriekš centralizēti izstrādāta un apstiprināta risku vadības kārtība un/vai metodika. To var izdarīt, izmantojot iekšējos resursus un kapacitāti vai ārējo pakalpojumu sniedzēju, nodrošinot apmācības un vienotu izpratni visiem risku "vēstniekiem".

4.2. Risku pārvaldības reglamentējošie iekšējie normatīvie akti – izstrāde, ieviešana un īstenošanas uzraudzība

Turpmāk aprakstīti iekšējie normatīvie akti, kas būtu nepieciešami risku vadības funkcijas ieviešanai un to ieteicamais saturs, taču iestādes var atsevišķus no dokumentiem apvienot vai pielāgot to saturu atbilstoši savām vajadzībām un iestādes darbības specifikai.

[22] Atbilstoši MK 26.04.2022. noteikumiem Nr. 262 "Valsts un pašvaldību institūciju amatu katalogs, amatu klasifikācijas un amatu apraksta izstrādāšanas kārtība", mazas un ļoti mazas iestādes ir tādas, kurās ir attiecīgi 10-50 vai mazāk par 10 amata vietām.

Risku vadības politika – dokuments, kuru apstiprina iestādes administratīvais vadītājs un kas nosaka galvenās risku vadības vadlīnijas:

- vispārējā risku vadības koncepcija iestādē, tās mērķi un sasniedzamie rezultāti;
- risku vadības pamata principi un nosacījumi, kas jāievēro (var tikt veidoti, balstoties uz starptautiskajiem risku vadības standartiem, modeļiem, kā arī iestādes vajadzībām un kontekstu, nozares specifiku);
- risku vadības tvērums un risku veidi (risku pamata grupas, klasifikācija kategorijās);
- risku vadības lomas (īsumā) un atbildība, risku vadības funkcijas organizatoriskā shēma (padotība un vieta iestādes hierarhijā);
- risku vadības procesa posmu īss skaidrojums;
- risku pieļaujamais līmenis/ risku apetīte un tolerance (ja tādas ir noteiktas);
- risku vadības sasaiste un sadarbība ar citām pārvaldības un/vai atbalsta funkcijām un procesiem (iekšējās kontroles sistēmas ieviešana un uzturēšana, kvalitātes vadība, iekšējais audits u.tml.);
- risku vadības politikas pārskatīšanas un aktualizācijas principi;
- risku vadības funkcijas uzraudzības un novērtēšanas pieeja un regularitāte;
- būtiskākie risku informācijas apmaiņas un komunikācijas pasākumi iestādē.

Risku vadības procedūra/ kārtība/ instrukcija/ procesu shēma jeb metodika – ir iekšējais normatīvais akts, kuru apstiprina iestādes administratīvais vadītājs un kas nosaka, kā risku vadības politikā ietvertās vadlīnijas un principus ieviest praksē:

- galvenie iestādē izmantotie risku vadības termini;
- risku vadības procesa posmi, secīgi aprakstot to norisi, izmantojamos datus, rezultātus, iesaistītās puses, atbildības, pienākumus un to regularitāti, tai skaitā izmantotās metodes, tostarp risku matricas (risku līmeņi jeb zonas (piemēram, ļoti augsta līmeņa jeb "sarkanā", augsta līmeņa jeb "oranžā", vidēja līmeņa jeb "dzeltenā" un zema līmeņa jeb "zaļā")), kas katrā iestādē var atšķirties, veidlapas, risku vērtēšanas kritēriji un tamlīdzīgi (skat. 5. nodaļu "Risku vadības process", kurā pieejama detalizētāka aprakstošā informācija par katru no risku vadības procesa posmiem);
- risku informācijas dokumentācija, formāts, uzglabāšana, pieejamība (šī var nebūt atsevišķa sadaļa, bet gan integrēta informācija iepriekšminētajās metodikas sadaļās, kur tas ir visvairāk piemērots/ nepieciešams).

Nepieciešamības gadījumā procedūrā/kārtībā/instrukcijā jeb metodikā var norādīt atšķirības starp dažādām risku kategorijām vai līmeņiem (piemēram, stratēģiskie riski, projektu riski, operacionālie riski, tai skaitā informācijas un komunikācijas tehnoloģiju riski, korupcijas, interešu konflikta un krāpšanas riski un tamlīdzīgi). Šiem riskiem var atšķirties to vadībā iesaistītie dalībnieki, kā arī var atšķirties risku vadības metodika (piemēram, risku identificēšanas soļi un vērtēšanas kritēriji un skala). Piemēram, interešu konflikta un korupcijas risku vadībai, tai skaitā analīzei izmantojamas Korupcijas novēršanas un apkarošanas biroja sagatavotās un apstiprinātās vadlīnijas par iekšējās kontroles sistēmas pamatprasībām korupcijas un interešu konflikta riska novēršanai publiskas personas institūcijā[23].

[23] https://www.knab.gov.lv/lv/media/765/download?attachment

Risku reģistrs/ veidlapas – ir dokuments, kurā tiek apkopota informācija par iestādē identificētajiem riskiem un to raksturojumu. Risku vadības procedūrās/ kārtībās/ instrukcijās, kas skaidro risku vadības politikas ieviešanu, tiek paredzēta risku reģistra sagatavošanas un aktualizēšanas kārtība, kā arī var tikt paredzēta risku reģistrā iekļaujamā informācija (skat. 5.8. nodaļu).

Risku mazināšanas pasākumu plāns – ir iestādes administratīvā vadītāja apstiprināts dokuments, kurā apkopota informācija par tām papildu plānotajām darbībām, ko iestādes vadība un risku īpašnieki ir nolēmuši veikt, lai vēl vairāk samazinātu riska atlikušo līmeni (skat. 5.10. nodaļu).

Šo plānu iespējams integrēt iestādes darbības plānā, ievērojot, ka nepieciešams ieviest risku mazinošo pasākumu filtrēšanas iespējas, lai veicinātu risku mazinošo pasākumu izpildi, kā arī, lai iesniegtu ziņojumus augstākajai vadībai par riskiem, tostarp to mazinošo pasākumu ieviešanas progresu.

4.2.1. Risku vadības reglamentējošo dokumentu izstrāde

Risku vadības iekšējiem normatīvajiem aktiem jābūt izstrādātiem atbilstoši iestādes iekšējam normatīvajam aktam, kas reglamentē iestādes iekšējo normatīvo aktu sagatavošanu, saskaņošanu un apstiprināšanu.

Risku vadības politikas izstrādē jābūt iesaistītam gan risku vadītājam, gan iestādes augstākajai vadībai, kas apstiprina risku vadības politiku un tās ieviešanas metodiku. Risku vadītājs ir iesaistīts arī pārējo 4.2. nodaļā minēto dokumentu izstrādē un aktualizācijā, jo īpaši risku reģistra un risku mazināšanas pasākumu plāna veidlapu un satura izstrādē, kā arī to aizpildīšanā.

Pēc iestādes risku vadību reglamentējošo normatīvo aktu apstiprināšanas, ar tiem jāiepazīstina visi iestādes darbinieki, kuri iesaistīti risku vadībā. Lai veicinātu vienotas izpratnes rašanos par risku vadības prasībām, ņemot vērā iepriekšminētos iekšējos normatīvos aktus, iespējams sagatavot darbiniekiem mācību prezentācijas un testus.

> ⚠ **Padoms**: Veidojiet iekšējos normatīvos aktus, kas reglamentē risku vadību, izmantojot vienotu pieeju, tāpat kā, izstrādājot citus iekšējos normatīvos aktus jūsu iestādē. Svarīgi ir tos apstiprināt augstākās vadības līmenī un regulāri informēt par to saturu, izglītojot visus darbiniekus, kas iesaistīti risku vadībā.

4.2.2. Risku vadības reglamentējošo dokumentu ieviešana

Tā kā iekšējo normatīvo aktu prasības iestādēs ir saistošas visiem darbiniekiem (tostarp tiem, kas minēti un iesaistīti attiecīgo normatīvo aktu īstenošanā), tad risku vadība ieviešama praksē, ievērojot attiecīgo iekšējo normatīvo aktu prasības.

Risku vadības reglamentējošo iekšējo normatīvo aktu ieviešana un iedzīvināšana praksē ir visu to darbinieku atbildība, kuru amatu aprakstos ir minēta risku vadība. Primāri tā ir iestādes augstākā vadības un risku vadītāja atbildība. Vienlaikus arī visiem darbiniekiem, kas iesaistīti risku vadībā (piemēram, struktūrvienību vadītāji), iestādē jāievēro un ikdienā jāpiemēro risku vadības reglamentējošie dokumenti.

Risku vadības reglamentējošo iekšējo normatīvo aktu ieviešanu, it īpaši risku vadības attīstības sākuma posmā veicina skaidrojošais darbs, mācības, regulāra un atvērta komunikācija no vadības un risku vadītāja puses, tostarp par šo normatīvo aktu saturu un praktisko pielietošanu. Arī praktiski piemēri un demonstrēšana, kā izmantot, piemēram, risku vadības metodiku, noteikti veicinātu darbinieku izpratni par dokumentu saturu. Risku vadītāja līdzdalībai risku vadības procesā, tā posmos ir liela nozīme. Lai sākotnēji, ieviešot risku vadību, veidotu vienotu izpratni darbiniekiem par risku novērtēšanu, reaģēšanu uz riskiem, risku vadītājs var organizēt sanāksmes, kurās skaidro, kā definēt un formulēt, kā arī analizēt riskus, izmantojot apstiprinātos risku varbūtības un novērtēšanas kritērijus un skalas, un palīdz noteikt risku mazināšanas pasākumus, tādējādi veicinot, ka darbinieki kļūst patstāvīgāki un spēj autonomi pilnvērtīgi piedalīties risku vadībā.

4.2.3. Risku vadības reglamentējošo dokumentu uzraudzība

Iestādes risku vadības iekšējos reglamentējošos iekšējos normatīvajos aktos noteikto principu, soļu un atbildību ievērošanu un kvalitāti vai efektivitāti, atbilstību mērķiem un noteiktajām prasībām vērtē vienlaicīgi ar risku vadības funkcijas novērtēšanu, kad tāda tiek veikta.

> **Padoms**: Ja regulāri netiek ievēroti kādi no iekšējos normatīvajos aktos noteiktajiem principiem vai prasībām, risku vadītājam proaktīvi jāveic darbinieku informēšana, apmācības vai jāpārskata iekšējos normatīvajos aktos noteiktās prasības – iespējams, tās jāprecizē vai jāgroza. Risku vadītājam jābūt ieinteresētam, lai iekšējos normatīvajos aktos iekļautie principi un prasības būtu pēc iespējas objektīvi un skaidri saprotami, lai darbinieki varētu veikt savus amata pienākumus.

Iestādei attīstot risku vadību un sasniedzot arvien augstāku risku vadības brieduma līmeni, risku vadītājs var veikt iekšējo normatīvo aktu un risku vadības pašnovērtējumu un nepieciešamības gadījumā veikt reglamentējošo iekšējo normatīvo aktu aktualizēšanu (piemēram, ja ir mainījušies risku vadībā iesaistītie amati, vai ir izstrādāta specifiska metodika kādas konkrētas risku kategorijas vērtēšanai, vai ir precizēta risku vērtēšanas skala iestādes stratēģiskajiem riskiem, vai arī mainās risku apetīte).

Ar zināmu regularitāti ieteicams veikt arī risku vadības ārējo novērtējumu (atbilstoši risku vadības brieduma modelim, iestādes noteiktajiem risku vadības mērķiem, vai kādam no risku vadības modeļiem/ standartiem, ja tie ieviesti iestādē), kura ietvaros būtu jāveic risku vadības reglamentējošo iekšējo normatīvo aktu prasību ievērošanas uzraudzība un novērtēšana. Iekšējie vai ārējie auditori vai konsultanti var sniegt rekomendācijas risku vadību reglamentējošo iekšējo normatīvo aktu pilnveidošanai.

4.3. Risku apetīte, tolerance un iestādes vadības loma

Lai iestāde attīstītos, saskartos ar inovācijām un iekšējām vai ārējām pārmaiņām, tai jāuzņemas zināms risku apjoms.

Risku apetīte atklāj, kur iestāde atrodas spektrā no pilnīgi brīvas un atvērtas risku uzņemšanās līdz pilnīgai to kontrolei un pēc iespējas ierobežotai risku pieļaušanai. Risku apetīte ir iestādes apgalvojums un norāde par to, cik lielā mērā un kādus riskus tā ir gatava uzņemties, kurus riskus un kādā mērā nepieciešams vadīt un mazināt, kā arī kādi riski un cik lielā mērā ir pieņemami.

Lai noteiktu risku apetīti, svarīgākais priekšnosacījums ir skaidru iestādes mērķu esamība. Savukārt, risku tolerances noteikšanai nepieciešami mērāmi sasniedzamie un faktiskie darbības rādītāji, kas saistīti ar iestādes mērķiem.

Risku apetīte: iestādes (tās vadītāja) vēlme un gatavība uzņemties riskus. Tas ir risku apjoms, ko iestāde ir gatava uzņemties un vadīt, īstenojot savā kompetencē esošos procesus un ieviešot stratēģiju mērķu sasniegšanai, un līdz ar to katrai iestādei tā ir atšķirīga. Risku apetīte ir **kvalitatīvs apgalvojums** vai tēze par gatavību uzņemties riskus un par nepieļaujamiem risku apjomiem (t.i., risku apetītes noteikšanai nav obligāti nepieciešams kvantificēt risku rādītāju, ietekmes un varbūtības robežas). Risku apetīte ir apgalvojums, kas atspoguļo pieļaujamos riskus, jo pilnīga bezrisku vide nav iespējama, it īpaši, ja iestādei ir noteikti mērķi, kas paredz attīstību, uzlabojumus un pārmaiņas. Tāpat risku apetīte ir apgalvojums, kas atspoguļo risku apmēru, kas noteikti nebūtu pieļaujams (piemēram, jomas, kurās iestāde nav gatava pieļaut būtiskus riskus vai incidentus - darba vides drošība, klientu drošība un tamlīdzīgi).

Risku apetītes apgalvojumu var attiecināt uz un sasaistīt ar iestādes mērķiem vai jomām, aspektiem, ko riski var ietekmēt (piemēram, budžets, vide, personāla vadības jautājumi, reputācija u.tml.).

Piemērs: Risku apetītes apgalvojumi:

- Pieļaujam riskus, kas nelielā apmērā ietekmē un pagarina mūsu iestādes pakalpojumu sniegšanas termiņus.
- Pieļaujam riskus, kas negatīvi neietekmē iestādes reputāciju.
- Pieļaujam "zaļā" līmeņa riskus.
- Esam gatavi uzņemties riskus, kas īstermiņā apdraud un kavē informācijas sistēmu projektu ieviešanu, ja tas nepasliktina vai uzlabo turpmāku projektu vadības kvalitāti.
- Pieļaujam riskus, kas rada nelielu samazinājumu mūsu iestādes apkalpoto klientu skaitā gada laikā.
- Pieņemam un esam gatavi uzņemties riskus, kas būtiski nepalielinās darbinieku aprites rādītāju.

Risku apetīti ietekmē šādi iestādes faktori:

- iestādes darbības stratēģija un sasniedzamie mērķi (cik tie ir izaicinoši, piesardzīgi, reālistiski u.tml.);
- risku vadības politika un tajā noteiktie principi, risku vadības mērķi;
- nozare, kurā iestādes darbojas (piemēram, nozare, kurā pastāv augsti cilvēku drošības riski un līdz ar to stingras nozares prasības šajā jomā un tamlīdzīgi);
- vadītāju un darbinieku attieksme pret risku, tai skaitā, uzraugošās iestādes (piemēram, ministrijas un tās vadības) attieksme pret risku, ko savukārt veido iepriekšējā vadības pieredze un individuālā attieksme pret risku;
- kontrolējošās iestādes, to noteiktās prasības;
- tiesību akti (nacionālie un starptautiskie), kas attiecas uz iestādi, tajos iekļautās prasības;
- citas ieinteresētās puses un to vēlmes attiecībā uz iestādi.

Atkarībā no iestādes darbības jomas un specifikas, kā arī tās vadītāju iepriekšējās pieredzes un iestādes darbības rezultātiem, eksistēs jomas, kurās iestādei būs lielāka risku apetīte un turpretī

eksistēs arī tādas jomas, kurās tā nebūs gatava tolerēt riskus. Piemēram, ja iestāde pastāvīgi strādā ar inovācijām un vairākkārt ir realizējusi apjomīgus infrastruktūras projektus, tās vadība apzinās, ka šādi projekti var kavēties, līdz ar to, risku apetīte un tolerance atspoguļos, ka nobīdes no plānotajiem projektu īstenošanas termiņiem ir pieļaujamas noteiktā apmērā. Savukārt, ja iestāde darbojas stingri regulētā nozarē (piemēram, farmācija vai medicīna), tās risku apetīte un tolerance attiecībā uz sabiedrības drošības riskiem būs minimāla un nepieļaus nekādas vai ļoti minimālas novirzes no sasniedzamajiem drošības rādītājiem.

 **Svarīgi**: Iestādēs, neskatoties uz to, ka tās nav orientētas uz peļņas gūšanu un klasiskiem uzņēmējdarbības jeb biznesa attīstības posmiem, arī ir svarīga uz attīstību un izaugsmi vērstu mērķu un darbības rādītāju noteikšana, inovāciju veicināšana, kas neizbēgami rada nepieciešamību uzņemties zināmu risku apjomu. Līdz ar to arī publiskajā sektorā iestādēm un to vadītājiem ir jābūt noteiktai risku apetītei, t.i., risku apjomam, ko iestāde ir gatava uzņemties, lai sasniegtu mērķus un izaugsmi. Jāņem vērā, ka publiskā sektora iestādēs, tāpat kā privātajā sektorā, pilnīgi visus riskus izslēgt un novērst nebūs iespējams, jo tas prasītu nesamērīgus resursus.

Risku apetītei var noteikt pakāpes vai skalu, lai precīzāk atspoguļotu atšķirīgu risku apetīti dažādās jomās. Piemēram, iestādes risku apetīte darba drošības vai atbilstības jomā var būt minimāla, taču reputācijas vai komunikācijas jomā – vidēja vai atvērta.

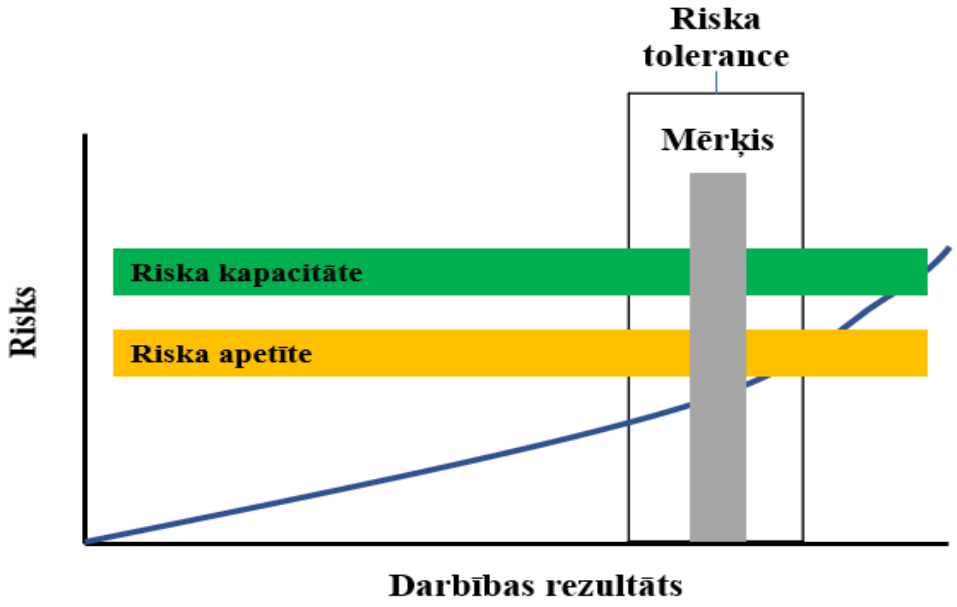
 **Piemērs**: Risku apetītes pakāpes vai skala:

- Noraidoša/ nepieņemama risku apetīte – riski šajā jomā netiek pieļauti un tolerēti;
- Minimāla – pieļaujami nebūtiski riski šajā jomā;
- Vidēja, piesardzīga – pieļaujami vidēji riski, līdzsvarā ar potenciālajiem ieguvumiem un iestādes mērķu sasniegšanu;
- Atvērta/ uzņēmīga risku apetīte – riski šajā jomā tiek pieņemti un apzināti pieļauti, lai stimulētu inovācijas vai veicinātu izmaiņas/ reformas.

Risku tolerance: risku uzņemšanās robežas. Vēlamais riska apjoms, izteikts kvantitatīvi kā intervāls, kura ietvaros paredzama riska vērtība; cik lielu riska apjomu iestāde ir gatava tolerēt un var pārvaldīt, lai sasniegtu mērķi (pieļaujamās novirzes). Nosakot risku toleranci, var lietot kvantitatīvus parametrus, risku indikatorus, iestādes sasniedzamos mērķus un novirzes no tiem, lai aprakstītu risku toleranci.

Risku kapacitāte: iestādes kopējā spēja uzņemties riskus (līdz maksimālai robežai) (12. attēls).

12. attēls. Riska kapacitāte



Piemērs: Risku tolerance var tikt noteikta kā risku indikatoru vai iestādes darbības rādītāju noviržu intervāls, kas ir pieļaujams, pārvaldot riskus:

- pieļaujamās novirzes darbinieku rotācijas rādītājam ir ne vairāk kā 5%;
- darba drošības jomā tolerējam tikai situāciju, kad nav neviena būtiska incidenta gada laikā;
- pieļaujam ne vairāk kā viena mēneša kavēšanos informācijas sistēmu datu migrācijas projektam;
- risku tolerance attiecībā uz mēneša laikā izsniegto jauno sertifikātu skaitu ir: katru mēnesi ne mazāk kā 10 jauni sertifikāti vai to samazinājums pret iepriekšējo periodu ne vairāk kā 20% apmērā;
- pieļaujam vienu nebūtisku incidentu gadā vides aizsardzības jomā.

Risku apetītes noteikšana ir iestādes vadības pienākums un, lai vienotos par kopīgu risku apetītes apgalvojumu, nepieciešama diskusija un izpratnes vienādošana iestādes augstākās vadības līmenī. Līdz ar to risku apetītes definēšana var būt lietderīga aktivitāte, lai iestādes vadītājs ar saviem tiešajiem padotajiem darbiniekiem apmainītos ar viedokļiem par pieļaujamajiem risku līmeņiem un iestādes iespēju pieņemt un vadītu riskus.

Pieaugot iestādes risku vadības brieduma līmenim, risku apetītes un tolerances apgalvojumus būtu jāizmanto iestādes lēmumu pieņemšanas procesā (piemēram, apstiprinot projektus, rīcības plānus, izstrādājot plānošanas dokumentus un tamlīdzīgi).

Risku apetīte un tolerance var mainīties atkarībā no iestādes iekšējās un ārējās vides, risku tendencēm, notikušajiem incidentiem, kontrolējošo institūciju uzstādījumiem un tamlīdzīgiem apstākļiem. Tādēļ ieteicams risku apetīti un toleranci pārskatīt vismaz reizi 1-2 gados.

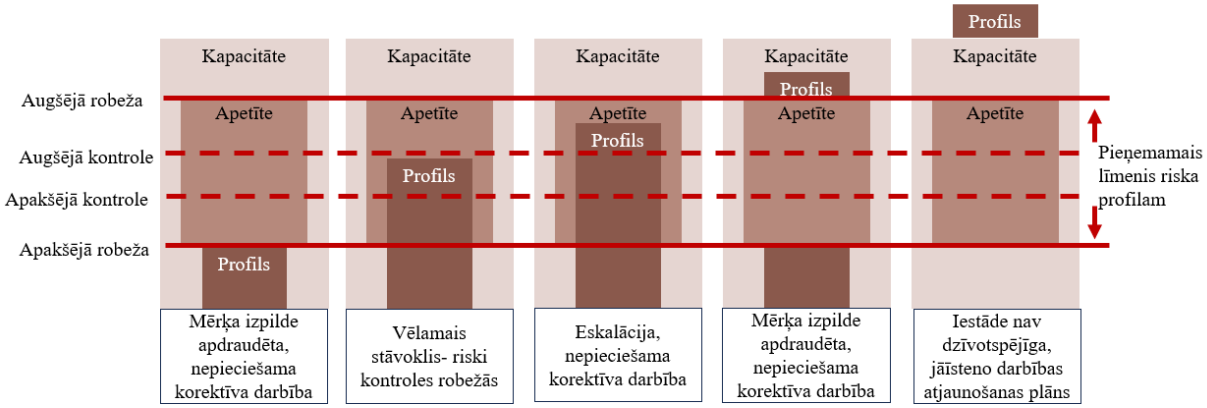
Risku apetītes un tolerances pielietošana praksē iespējama reaģēšanas uz riskiem pieejas noteikšanai un optimizēšanai, kā arī iekšējai komunikācijai.

Ja apzinātie un jau iepriekš novērtētie riski pieaug un pārsniedz risku apetīti/ toleranci (vai tuvākajā laikā iespējams to pārsniegs) tas nozīmē, ka jāpaaugstina risku novērtējums un jāpārskata reaģēšanas uz riskiem pieeja – iespējams, jāievieš papildu risku mazināšanas pasākumi. Tāpat, vērtējot riskus un secinot, ka risks nepārsniedz tolerances robežas un ir būtiski zemāks nekā iestādes risku apetīte, taču tā pārvaldībai tiek tērēti būtiski resursi (laiks, darbinieku noslodze, budžets), iespējams pārskatīt un optimizēt risku mazināšanas pasākumus (13. attēls).

Nosakot risku apetīti un tolerances intervālus, var tikt paaugstināta risku vadības izpratne iestādes augstākās vadības līmenī, kā arī risku apetītes un tolerances informācija var tikt izmantota komunikācijā ar iestādes darbiniekiem, kas veicina arī viņu izpratni par risku vadības pārvaldību. Risku apetīte un tolerance, ko nosaka un apstiprina iestādes augstākā vadība, ir kā signāls un norādes struktūrvienību vadītājiem par to, kāda līmeņa riski ir pieņemami un kurā brīdī, risku līmenim pieaugot, ir jāinformē iestādes augstākā vadība.

Pieņemtie lēmumi ir pārredzamāki un konsekventāki, ja ir skaidri noteikta un tiek izmantota risku vērtēšanas skala, apetīte un tolerance.

13. attēls. Iestādes risku profils un apetīte[24]



Ja iestādei ir noteikta risku apetīte, tolerance un kopējā risku kapacitāte, tad iespējams veikt analīzi par to, vai esošais iestādes risku profils (visi apzinātie riski kopumā) pārsniedz, iekļaujas vai nesasniedz risku apetīti un kapacitāti. Ja iestādes risku profils nesasniedz risku apetītes apakšējo robežu, tad iespējams noteiktie iestādes mērķi nav pietiekami izaicinoši vai arī ieviestās kontroles un risku mazināšanas pasākumi ir pārāk ierobežojoši, lai iestāde attīstītos un sasniegtu noteiktos mērķus. Tādējādi nepieciešama korektīva darbība, lai iestāde uzņemtos vairāk riskus atbilstoši risku apetītes līmenim. Optimālā situācijā risku profils iekļaujas risku apetītes augšējā un apakšējā robežā. Ja risku profils pārsniedz risku apetīti, nepieciešama korektīva rīcība – papildu risku mazināšanas pasākumu ieviešana, jo ir apdraudēta iestādes mērķu izpilde. Savukārt, ja risku profils pārsniedz jau kopējo risku kapacitāti, tad ne tikai iestādes mērķu izpilde, bet arī tās darbības turpināšana ir apdraudēta.

[24]Avots: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-0614.pdf

4.4. Risku vadības kompetenču attīstīšana

Pastāv dažādas pieejas, kā var attīstīt risku vadības kompetences. Turpmāk uzskaitītas dažas no tām:

- regulāras risku vadības mācības dažādu līmeņu iestādes darbiniekiem (vēlams kopīgi gan iestādes augstākajai vadībai, gan struktūrvienību vadītājiem, gan darbiniekiem, kas nav vadītāji, bet ir iesaistīti risku vadībā);
- pieredzes apmaiņa starp iestādes struktūrvienībām vai arī starp citām iestādēm, kas ieviesušas risku vadību, vai kuras darbojas tajā pašā nozarē;
- darba grupu organizēšana, iesaistot dažādu struktūrvienību pārstāvjus, lai vērtētu iestādes būtiskos riskus un kopīgi noteiktu to risku mazināšanas pasākumus;
- risku vadības analīzē iesaistīto darbinieku loka paplašināšana;
- risku ziņošanā iesaistīto darbinieku loka paplašināšana;
- risku informācijas un apkopojumu izmantošana arvien vairākiem iestādes iekšējiem procesiem (piemēram, regulārās atskaites par stratēģijas vai ikgadējā darba plāna izpildi, komunikācija ar uzraugošo vai kontrolējošo iestādi un tamlīdzīgi);
- atsevišķu būtisko risku padziļināta analīze, izmantojot jaunas risku analīzes metodes (piemēram, aptauja, cēloņu seku diagramma, strukturētā prāta vētra u.tml.).

4.5. Risku vadības sistēmas pārskatīšana un pilnveidošana

Pēc risku vadības ieviešanas iestādē, ja tā tiek aktīvi un praktiski izmantota, visdrīzāk risku vadības brieduma pakāpe dabiski pieaug un notiek risku vadības sistēmas pilnveidošana. Lai veicinātu risku vadības pilnveidošanu, pastāv dažādi veidi, kā to pārskatīt un novērtēt:

- risku vadītāja un iestādes vadības veikts risku vadības pašnovērtējums, izmantojot risku vadības brieduma modeli (vai kāda no risku vadības modeļa/ standarta prasībām, ja tas ieviests iestādē);
- ārējā pakalpojuma sniedzēja veikts risku vadības novērtējums (izmantojot risku vadības brieduma modeli, kādu no risku vadības modeļiem/ standartiem, vai pašas iestādes noteiktajiem risku vadības mērķiem un kārtību, tas ir, atbilstības novērtējums);
- iestādes iekšējā audita veikts risku vadības efektivitātes novērtējums (izmantojot risku vadības brieduma modeli un/ vai arī kādu no risku vadības modeļiem/ standartiem, vai iestādes noteiktajiem risku vadības mērķiem un kārtību).

Jebkurš no šiem novērtējumiem var sniegt konstatējumus un rekomendācijas risku vadības sistēmas pilnveidošanai, ko iestādes vadība nepieciešamības gadījumā var apstiprināt formāli, kā rīcības plānu ar termiņiem un atbildīgajiem par rekomendāciju ieviešanu. Risku vadības sistēmas pilnveidošana un attīstība lielā mērā atkarīga no iestādes augstākās vadības un risku vadītāja iniciatīvas un proaktīvas rīcības. Veidi, kā iestādes augstākā vadība un risku vadītājs var veicināt risku vadības pilnveidošanu (papildu iepriekš minēto novērtējumu veikšanai):

- organizēt regulāras mācības par risku vadību, kā arī saistītajām tēmām (piemēram, iekšējās kontroles sistēma) iestādes darbiniekiem;
- organizēt seminārus un darba grupas konkrētu risku izskatīšanai, vērtēšanai, vai neskaidro jautājumu par risku vadību pārrunāšanai;

- regulāri pārskatīt iestādes risku vadības iekšējos reglamentējošos iekšējos normatīvos aktus, aktualizēt tos nepieciešamības gadījumā un skaidri komunicēt veiktās izmaiņas un jaunumus iestādes darbiniekiem;
- regulāri ziņot par risku vadības kārtējā gada plāniem, kā arī risku analīzes rezultātiem, lai veicinātu komunikāciju un viedokļu apmaiņu, par iestādes būtisko risku vadību;
- veikt iekšējo aptauju par risku vadību, noskaidrojot praktiskus jautājumus (piemēram, vai darbinieki zina, kur atrast informāciju par risku analīzi iestādē, vai darbinieki pārzina risku vērtēšanas prasības iestādē, vai zina pie kā vērsties, ja konstatē, ka risku līmenis paaugstinās, vai darbinieki uzskata, ka iestādes būtiskie riski ir pietiekami pārvaldīti un tamlīdzīgi).

KOPSAVILKUMS

Risku vadības pārvaldība nodrošina struktūru, kuras ietvaros tiek īstenota risku vadība iestādē un veicina, ka, ieviešot pārmaiņas, tiek samazinātas risku negatīvās sekas un iestāde spēj operatīvi reaģēt uz izmaiņām iekšējā un ārējā vidē.

Trīs līniju modelis skaidro, kādi iestādes amati ir iesaistīti risku vadībā un kādai būtu jābūt to koordinētai rīcībai kopumā, lai veiksmīgi vadītu riskus, uzturētu iekšējās kontroles sistēmu un radītu vērtību:

- Pirmās līnijas lomu iestādēs veic tie struktūrvienību vadītāji un darbinieki, kas īsteno pamatdarbības funkcijas, kā arī sniedz iekšējos vai ārējos pakalpojumus, ņemot vērā iestādes nolikumu;
- Otrās līnijas lomu veic pirmās līnijas pārraudzības un iestādes administratīvās/ atbalsta funkcijas. Tā sniedz atbalstu, lai ieviestu un attīstītu risku vadības funkciju, kā arī, lai nodrošinātu iestādes darbības atbilstību iekšējiem un ārējiem normatīvajiem aktiem. Atbalsta funkcijas ir horizontālas visu iestādi aptverošas funkcijas, kas ir saistītas ar risku vadību, piemēram:
  - risku vadības funkcija;
  - finanšu vadības un grāmatvedības funkcija;
  - personas datu aizsardzības funkcija;
  - informācijas tehnoloģiju drošības funkcija;
  - kvalitātes vadības funkcija;
  - atbilstības funkcija;
  - juridiskā funkcija un tamlīdzīgi.
- Trešā līnija (iekšējā audita funkcija) sniedz neatkarīgu un objektīvu pārliecību un konsultācijas par iestādes mērķu sasniegšanu, tostarp izvērtē, vai pirmā un otrā līnija darbojas atbilstoši tiesību aktiem un pietiekami aktīvi, lai vadītu riskus.

Galvenā atbildība par risku vadības ieviešanu un uzturēšanu ir iestādes augstākajai vadībai. Risku vadītāja pienākums ir metodiski vadīt un koordinēt risku vadību. Savukārt struktūrvienību vadītāju un dažādu citu līmeņu darbinieku atbildība ir pilnvērtīgi piedalīties dažādos risku vadības posmos un aktivitātēs, tostarp savlaicīgi ziņot par riskiem, kā arī sniegt informāciju par risku mazinošo pasākumu ieviešanas progresu/ izpildi.

Lai pilnvērtīgi ieviestu, uzturētu un attīstītu risku vadību, vēlams lai to iestādē veic atsevišķs pilnas slodzes darbinieks, taču mazās iestādēs[25], ja nav pietiekamu finanšu resursu algot atsevišķu darbinieku, kas var nebūt samērīgi nelielā darbinieku skaita dēļ, šos pienākumus darbiniekiem iespējams apvienot ar citiem pienākumiem un funkcijām.

Risku vadības reglamentējošie iekšējie normatīvie akti:

- **Risku vadības politika** – iekšējais normatīvais akts, kuru apstiprina iestādes administratīvais vadītājs un kas nosaka galvenās riska vadības vadlīnijas un principus;
- **Risku vadības procedūra/kārtība/instrukcija** jeb metodika – ir iekšējais normatīvais akts, kuru apstiprina iestādes administratīvais vadītājs un, kas nosaka, kā riska vadības politikā ietvertos uzstādījumus ieviest praksē.

Risku vadības iekšējiem reglamentējošajiem normatīvajiem aktiem jābūt izstrādātiem atbilstoši iestādes iekšējam normatīvajam aktam, kas reglamentē iestādes iekšējo normatīvo aktu sagatavošanu, saskaņošanu un apstiprināšanu.

Risku vadības reglamentējošo iekšējo normatīvo aktu ieviešana un iedzīvināšana praksē ir visu to darbinieku atbildība, kuru amatu aprakstos ir minēta risku vadība. Primāri tā ir iestādes augstākā vadības un risku vadītāja atbildība, vienlaikus arī visiem darbiniekiem, kas iesaistīti risku vadībā (piemēram, struktūrvienību vadītāji) jāievēro un ikdienā jāpiemēro risku vadības reglamentējošie iestādes iekšējie normatīvie akti.

Attīstot risku vadību un sasniedzot arvien augstāku risku vadības brieduma līmeni, risku vadītājs var veikt iekšējo normatīvo aktu un risku vadības pašnovērtējumu un nepieciešamības gadījumā tos aktualizēt (piemēram, ja ir mainījušies risku vadībā iesaistītie amati, vai ir izstrādāta specifiska metodika kādas risku kategorijas vērtēšanai, vai ir precizēta risku vērtēšanas skala iestādes stratēģiskajiem riskiem, vai arī mainās risku apetīte).

Lai noteiktu risku apetīti, svarīgākais priekšnosacījums ir skaidru iestādes mērķu esamība. Savukārt, risku tolerances noteikšanai nepieciešami mērāmi sasniedzamie un faktiskie darbības rādītāji, kas saistīti ar iestādes mērķiem.

Risku apetīte ir kvalitatīvs apgalvojums vai tēze par gatavību uzņemties riskus un par nepieļaujamiem risku apjomiem (risku apetītes noteikšanai nav obligāti nepieciešams kvantificēt risku rādītāju, ietekmes un varbūtības robežas).

Risku tolerance - risku uzņemšanās robežas. Vēlamais riska apjoms, izteikts kvantitatīvi kā intervāls, kura ietvaros paredzama riska vērtība; cik lielu riska apjomu iestāde ir gatava tolerēt un var pārvaldīt, lai sasniegtu mērķi (pieļaujamās novirzes). Nosakot risku toleranci, var lietot kvantitatīvus parametrus, risku indikatorus, iestādes sasniedzamos mērķus un novirzes no tiem, lai aprakstītu risku toleranci. Risku kapacitāte - iestādes kopējā spēja uzņemties riskus (līdz maksimālai robežai).

Risku vadības sistēmas pilnveidošana un attīstība lielā mērā atkarīga no iestādes augstākās vadības un risku vadītāja iniciatīvas un proaktīvas rīcības.

---

[25] Atbilstoši MK 26.04.2022. noteikumiem Nr. 262 "Valsts un pašvaldību institūciju amatu katalogs, amatu klasifikācijas un amatu apraksta izstrādāšanas kārtība", mazas un ļoti mazas iestādes ir tādas, kurās ir attiecīgi 10-50 vai mazāk par 10 amata vietām.

5. RISKU VADĪBAS PROCESS

Iestādes proaktīva risku vadība ir viena no labas pārvaldības pamata komponentēm. Risku vadība palīdz identificēt un izprast riskus, tādējādi sniedzot atbalstu lēmumu pieņemšanā visos organizatoriskajos līmeņos, lai sasniegtu iestādes izvirzītos mērķus, ņemot vērā pieejamos resursus. Šajā Rokasgrāmatas sadaļā aprakstītais risku vadības process ir balstīts uz ISO 31000:2018 standartu[26], kas sniedz detalizētas vadlīnijas par risku vadības sistēmas plānošanu, ieviešanu un mērīšanu. ISO 31000:2018 standarta nodaļā par risku vadības procesu ir paredzēti šādi risku vadības pamata procesi jeb centrālie procesi – risku novērtēšana (kas iedalīta risku identificēšanā, analīzē un izvērtēšanā) un reaģēšana uz riskiem. Tāpat šī nodaļa paredz vides (iekšējās un ārējās vides) un kritēriju noteikšanu, komunikāciju un konsultācijas, uzraudzību un pārskatīšanu, kā arī dokumentēšanu un ziņošanu.

5.1. Risku vadības procesa posmu īss apraksts un shematisks attēlojums

Risku vadības ieviešanas posmi attēloti "ceļa kartēs", kas iekļautas Rokasgrāmatas 3. pielikumā, un tās attēlo risku vadības ieviešanu atkarībā no risku vadības brieduma līmeņa. Kopumā jebkurā iestādē neatkarīgi no tās esošā vai vēlamā risku vadības brieduma līmeņa ir šādi sākotnējie pasākumi risku vadības ieviešanai:

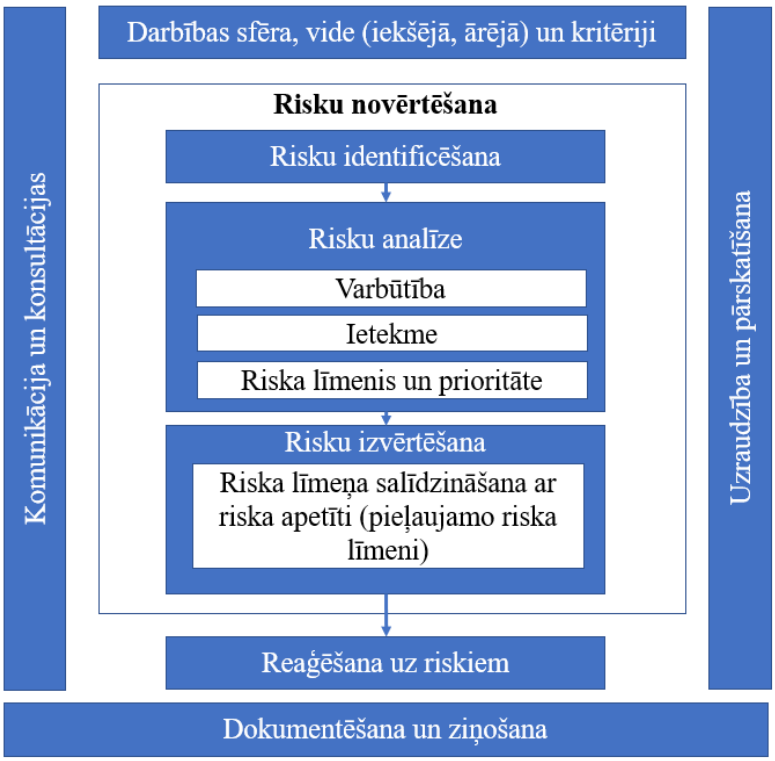
- risku vadības mērķu un pamatprincipu noteikšana (risku vadības politika);
- risku vadības kārtības un metodikas izstrāde. Risku vadības procesa posmiem, atbildības un pienākumu sadalījumam jābūt skaidri noteiktam iestādes iekšējos normatīvajos aktos, kas reglamentē risku vadību;
- risku vadībā iesaistīto darbinieku un citu nepieciešamo resursu nodrošināšana;
- darbinieku informēšana par risku vadības mērķiem, paredzamo izmantojamo metodiku;
- pakāpeniska risku vadības praktiskā īstenošana atbilstoši risku vadības procesa posmiem (kas aprakstīti turpmāk šajā nodaļā).

Visā risku vadības procesā ir jāņem vērā darbinieku uzvedības un risku kultūras dinamiskais un mainīgais raksturs.

Katrs no risku vadības procesiem (14. attēls) pievieno vērtību, lai būtu iespējams ierobežot risku īstenošanos un mazināt to negatīvo ietekmi. Risku vadības procesu iespējams attēlot, ņemot vērā ISO 31000:2018 standartu, ievērojot tajā paredzētos risku vadības procesus un to būtību.

[26] ISO 31000:2018 Risk Management – Guidelines

14. attēls. Risku vadības process



Risku vadības process sastāv no šādiem posmiem:

- **risku vadības darbības sfēras, vides un kritēriju noteikšana** nepieciešama, lai klasificētu riskus, piemēram, stratēģiskajā, darbības (operacionālajā) un projektu līmenī un apzinātu, kāda veida riski piemīt iestādei:
  - risku sfēru, risku vadības **vidi** (kontekstu) veido iestādes iekšējā un ārējā vide, kurā iestāde darbojas. Iekšējā vide attiecas uz iestādi, tās funkcijām un darbības jomām, kā arī iestādes darbinieku prasmēm, iekšējām ieinteresētajām pusēm, to vēlmēm un gaidām. Iekšējā vide ir saistīta ar iestādes kultūru, pieejamajiem resursiem un lēmumu pieņemšanu. Ārējā vide ietver, piemēram, sociālo, kultūras, politisko, normatīvā regulējuma, finanšu, tehnoloģisko, ekonomisko vidi un starptautiskos, nacionālos, reģionālos vai vietējos faktorus;
  - **kritēriju** (risku ietekmes un varbūtības novērtēšanas kritēriju) **definēšana** nepieciešama, lai noteiktu risku līmeni un būtiskumu, veicot risku analīzi. Kritērijiem jābūt vērstiem uz iestādes vērtībām, tostarp reputāciju, mērķiem, resursiem un citiem kritērijiem;
- **risku identificēšanas** rezultātā tiek apzināti risku notikumi, kas apdraud iestādes mērķu sasniegšanu. Praksē risku vadītājs veic priekšizpēti, lai apzinātu potenciālos riskus, un/vai risku īpašnieki novēro un piefiksē potenciālos riskus. Pēc tam risku vadītājs, sadarbojoties ar risku īpašniekiem/procesu īpašniekiem, formulē (identificē) riskus;
- **risku analīzes** rezultātā tiek noteikta identificēto risku varbūtība un ietekme (atbilstoši iestādes apstiprinātajai metodikai), veicot kvalitatīvu vai kvantitatīvu risku izvērtējumu un ņemot vērā to definētos novērtēšanas kritērijus. Tiek noteikts risku līmenis, kas ļauj turpmāk pieņemt lēmumu, vai un kā ir nepieciešams reaģēt uz risku. Risku analīze palīdz noteikt risku prioritāti un saaranžēt riskus, ņemot vērā to līmeni;
- **risku izvērtēšana** atbalsta lēmumu pieņemšanu un palīdz noteikt, vai ir nepieciešamas papildu darbības, lai reaģētu uz riskiem. Tiek salīdzināts riska atlikušais līmenis ar definēto riska apetīti (pieļaujamo riska līmeni);

- **reaģēšana uz riskiem** veicina risku ierobežošanu, ja atlikušais riska līmenis (skat. 5.7. nodaļu) nav pieņemams (pārsniedz riska apetīti), mainot risku sekas un/vai varbūtību, ievērojot, ka iespējams izmantot dažādas uz riskiem reaģēšanas stratēģijas un ieviešot jaunas vai papildinot esošās risku kontroles. Praksē tiek pieņemts lēmums (vienlaikus, ņemot vērā risku apetīti, ja tāda noteikta) rīcībai ar risku, tā vadībai, ņemot vērā jau esošās ieviestās kontroles, kā arī tiek noteikti iespējamie risku mazināšanas pasākumi, atbildīgie un termiņi šiem pasākumiem;
- **informācijas apmaiņa un komunikācija** starp iekšējām un ārējām ieinteresētajām pusēm **un konsultācijas** risku vadības procesā, ievērojot informācijas klasifikāciju, palīdz iestādē saglabāt piesardzīgumu un veicina darbinieku izpratni par iestādes riskiem un iespējām uz tiem reaģēt. Savukārt konsultācijas par risku vadības procesu palīdz pieņemt uz riskiem balstītus lēmumus. Praksē regulāri ir īstenojama komunikācija un iestādes vadības informēšana par risku analīzes rezultātiem;
- **uzraudzība un pārskatīšana** ietver informācijas par riskiem un to vadību apkopošanu un analīzi, tostarp ieviesto kontroļu pārskatīšanu, risku mazinošo pasākumu izpildes analīzi, kuras rezultāti būtu izmantojami iestādes snieguma vadībā. Praksē riski tiek uzraudzīti, mainoties to vērtējumam, aktualizējot risku reģistru (piemēram mainās riska tendences, ārējie vai iekšējie apstākļi, tiek ieviestas kontroles un attiecīgi mainās risku indikatoru vērtības). Īstenojoties riskam, tiek informēta vadība, pēc iespējas mazināt incidenta izraisītās negatīvās sekas, atkarībā no riska veida (ja tas var atkārtoties) tiek aktualizēts riska vērtējums un pārskatīti, pielāgoti riska mazināšanas pasākumi;
- **dokumentēšana un ziņošana** paredzēta, lai komunicētu par risku vadības rezultātiem iestādē, kā arī, lai nodrošinātu un atbalstītu stratēģisko un ikdienas (operacionālo) lēmumu pieņemšanu un pilnveidotu risku vadības procesu. Risku analīze tiek dokumentēta risku reģistrā. Par risku vadības rezultātiem tiek sagatavoti ziņojumi iestādes vadībai, kā arī tiek gatavoti un apstiprināti risku mazinošo pasākumu plāni.

Risku vadības process iestādē jāīsteno nepārtraukti un atkarībā no iestādes lieluma, darbības specifikas un risku vadības funkcijas kapacitātes. Risku vadības posmi var notikt secīgi visā iestādē, vai paralēli/ sinhroni, tas ir, kādā no procesiem vai struktūrvienībām tiek veikta risku identificēšana, taču citā struktūrvienībā vienlaikus tiek īstenota risku analīze vai uzraudzība. Būtiski nodrošināt vienmērīgu regularitāti, kādā riski tiek vadīti atkarībā no to līmeņa katras struktūrvienības vai procesa ietvaros (piemēram, vismaz reizi gadā vai pusotra gada laikā tiek veikta risku līmeņu pārvērtēšana būtiskākajos iestādes procesos). Risku vadības procesu var ieviest, izmantojot arī COSO ERM modeli.

Padoms: Kad iestādē ir ieviesta risku vadība un ir īstenots viss risku vadības cikls (visi risku vadības procesa posmi), būtu jāveic atkārtota risku vadības procesa uzsākšana - esošo iepriekš identificēto risku pārskatīšana, pārvērtēšana un papildu risku identificēšana (ja ir notikušas izmaiņas), kā arī ieviestā risku vadības procesa novērtēšana un pilnveidošana, ņemot vērā iegūto pieredzi, novērtējot aktuālos riskus, piemēram, jaunas risku identificēšanas metodes pielietošana vai risku analīzē iesaistīto darbinieku viedokļus. Risku vadības process nav vienreizējs process, bet gan ir ciklisks process, kas aizsargā iestādes vērtības, vienlaikus palielinot iestādes vērtību. Nepārtraukti nepieciešams uzraudzīt iekšējos un ārējos faktorus, tostarp apstākļus un notikumus, kas var ietekmēt risku, un, ja tādi radušies, tiek nodrošināta informācijas

apmaiņa un komunikācija, kā rezultātā būtiskā informācija par riskiem tiek sniegta iestādes augstākajai vadībai un tiek noteikta turpmāka riska vadības stratēģija.

Projektu risku vadības posmi ir līdzīgi, taču tiem ir sava specifika. Ja iestādē nav ieviesta risku vadība un nav risku vadītāja amata, tad projektu risku analīzi un vadību nodrošina projekta vadītājs. Ja iestādē ir ieviesta risku vadība, risku vadītājs var sniegt metodisku atbalstu projektu vadītājiem, koordinējot un vadot risku analīzes procesu, pārliecinoties, lai tiek īstenoti visi risku analīzes posmi – risku identificēšana, analīze, izvērtēšana, reaģēšana uz tiem, kā arī, lai tiktu izstrādāta projekta prasībām atbilstoša dokumentācija un nodrošināta komunikācija. Var arī projektu risku analīzi uzticēt projektu vadītajam.

Atbilstoši projekta pazīmēm, projekta risku vadību raksturo:

- riska pastāvēšanas laiks, kuru ierobežo projekta laiks. Risks var pastāvēt arī pēc projekta beigām, bet vairāk neietekmē projektu;
- risks var ietekmēt projekta termiņus, izmaksas un/vai kvalitāti un ietekmi ir iespējams aprēķināt atbilstoši projekta plānošanai/ projekta plānam;
- projekta laikā iespējama (vai visdrīzāk notiks) dinamiska risku vērtību maiņa un risku skaita samazināšanās vai palielināšanās;
- projekta ietvaros tiek noteikti mērķtiecīgi (precīzi mērķēti/orientēti) risku mazinošie pasākumi atbilstoši projekta plānošanai/ projekta plānam;
- projekta rezultāta/ produkta inovatīvais/ unikālais raksturs nosaka, ka projektam var būt unikāli riski, nav iespējama analogu, citu projektu, risku attiecināšana uz konkrēto projektu. Risku identificēšanai var būt nepieciešamas sarežģītas metodes.

5.2. Iestādes ārējās un iekšējās vides apzināšana un analīze

Pirms risku identificēšanas uzsākšanas un citiem risku vadības posmiem ir nepieciešams apzināt gan iestādes iekšējo, gan ārējo vidi ietekmējošos faktorus (9. tabula un 5. pielikums).

9. tabula. Iestādes iekšējo un ārējo vidi ietekmējošie faktori

Ārējās vides ietekmējošie faktori	Iekšējās vides ietekmējošie faktori
• Politiskie faktori (ārpolitika, eksporta/ importa politika, karadarbība, politiskās varas maiņa, politiskie lēmumi, valdības rīcības prioritātes u.c.); • Reglamentējošie faktori - darbību reglamentējošo Eiropas Savienības regulu, direktīvu, nacionālo normatīvo aktu prasību izmaiņas, iestādes un amatpersonu darbības ierobežojumi, kā arī politikas plānošanas dokumenti; • Ekonomiskie un finanšu faktori (fiskālā politika, monetārā politika, ārvalstu investīciju politika, inflācija, pirktspēja, krīzes, piegādes ķēžu pārtraukumi, resursu pieejamība u.c.); • Sociālie un kultūras aspekti – demogrāfiskā krīze, sabiedrības veselība, nodarbinātība,	• Iestādes vīzija, misija un vērtības; • Iestādes pārvaldības struktūra un kārtība, organizatoriskā struktūra (struktūrvienību padotība, skaits, savstarpējā atkarība), lomas un atbildības sadalījums; • Iestādes darbības mērķi; • Iestādei pieejamie finanšu resursi, to izmaiņas (piemēram, mērot īpatsvaru, kāda ir novirze salīdzinājumā ar iepriekšējo pārskata periodu); • Iestādes vajadzības; • Iestādes kultūra, tās izmaiņas, pilnveidojot, piemēram, atbilstības kultūru; • Iestādes iekšējie normatīvie akti, metodikas, vadlīnijas; • Funkcijas, procesi, tehnoloģijas;

Ārējās vides ietekmējošie faktori	Iekšējās vides ietekmējošie faktori
mērķa grupu izmaiņas, patērētāju vajadzības un tiesības, paražas, vērtības, klientu uzvedība un gaidas no iestādes rīcības, klientu skaita straujas izmaiņas u.c.); • Tehnoloģiskie faktori – jaunās tehnoloģijas, kiberdrošība, digitālā transformācija, mākslīgais intelekts u.c. faktori, kas maina un ietekmē procesu izpildi; • Vides faktori (ekstrēmi laikapstākļi, piesārņojums, neatjaunojamo resursu izsīkums un klimata izmaiņas); • Galvenie virzītājspēki un tendences, kas ietekmē iestādes mērķus, tai skaitā nozarēm specifiskās tendences; • Ārējo ieinteresēto pušu (sabiedrība, MK, NVO) uztvere, vērtības, vajadzības un gaidas; • Juridiskie faktori, piemēram, esošās līgumattiecības un saistības pret trešajām pusēm, sadarbības partneri; • Saziņas tīklu sarežģītība un atkarība no saziņas tīkliem.	• Augstākās vadības mainīgums un vadības stils; • Cilvēkresursi un intelektuālais īpašums (zināšanas, pieredze); • Iedibinātā prakse (dokumentētā un nedokumentētā); • Darbinieku ētika un savstarpējās attiecības (saskarsmes kultūra), darbinieku motivācija, laba komunikācija starp struktūrvienības vadītāju un darbiniekiem, kā arī starp struktūrvienībām, kas rada labvēlīgu darba vidi un mikroklimatu; • Dati, informācijas sistēmas un informācijas plūsmas; • Procesu vai pakalpojumu digitalizācija – automatizētu risinājumu ieviešana; • Attiecības ar iekšējām ieinteresētajām pusēm, ņemot vērā viņu uztveri un vērtības.

Viens no veidiem, kā noteikt, vai vidi raksturojošie faktori ir ārējie vai nē, ir jāuzdod jautājumu: "vai šis faktors attiecas arī uz citām iestādēm?" Piemēram, paaugstināta nodokļu likme attiecas uz visām iestādēm - ne tikai uz vienu konkrētu iestādi, tāpēc šis ir ārējais faktors. Savukārt, iestādes iekšējie normatīvie akti ir saistoši tikai iestādei un tādēļ tas ir iekšējs faktors.

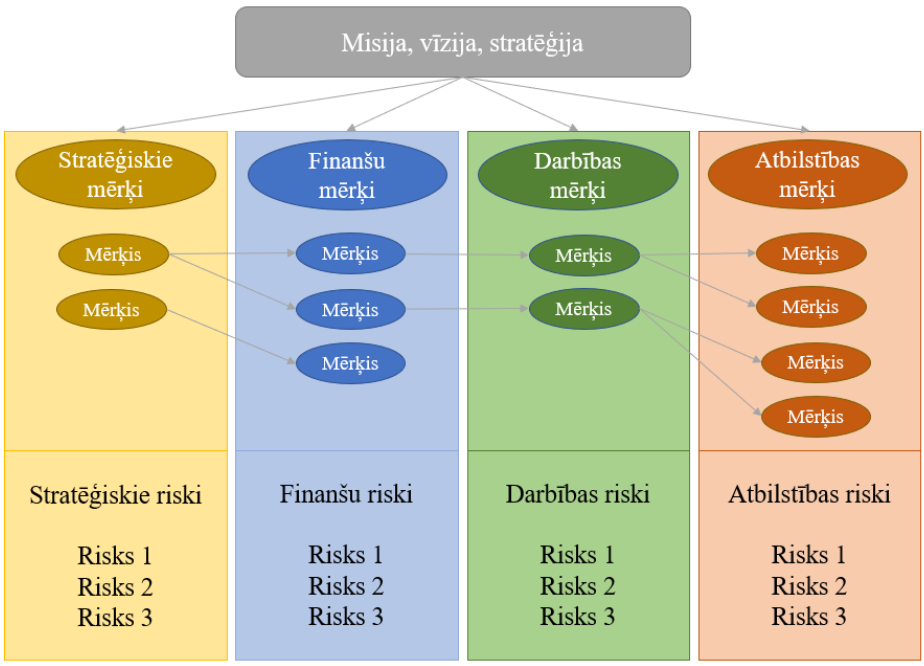
Risku vadības procesā, identificējot un vērtējot riskus ārējā un iekšējā vidē, jāņem vērā šādi risku identificēšanu apgrūtinošie ārējās un iekšējas vides faktori:

- ārējā un iekšējā vide var būt strauji mainīga;
- attīstības sistēmas plānošanas dokumentos var būt daudz pieņēmumu un neskaidru parametru, kas var radīt virkni scenāriju un apgrūtināt risku identificēšanu;
- risku indikatorus, kuriem ir tendence strauji palielināties, var būt sarežģīti pamanīt un noteikt;
- zināšanas var būt ierobežotas un informācija nepilnvērtīga, lai atbilstoši ārējās un iekšējās vides situācijai plānotu iestādes darbu un pieņemtu lēmumus;
- ieinteresēto pušu lēmumi un uzskati var nebūt objektīvi, ietekmējot lēmumus tālākos risku vadības posmos.

5.3. Risku grupas/klasifikācija – skaidrojumi un piemēri publiskā sektora kontekstā

Risku grupēšana ir dažāda veida risku sistematizēšana, pamatojoties uz dažām pazīmēm un kritērijiem, kas ļauj vienā grupā apvienot līdzīgus riskus. Risku grupas visbiežāk pakārtotas iestādes izvirzīto mērķu grupām, kas atklāj nozīmīgas attīstības vai risku tēmas iestādes darbībā, taču tās var tikt definētas arī vēl papildus un nesaistīti ar mērķa grupām (15. attēls un 6. un 7. pielikums).

15. attēls. Risku grupēšana atkarībā no izvirzīto mērķu grupām



Risku grupas var tikt izmantotas arī, lai efektīvāk tematiski organizētu risku identificēšanas posmu, jo katrā no riska grupām uzmanība tiek vērsta uz konkrētiem mērķiem un šim nolūkam var tikt pieaicināti attiecīgās risku grupas tēmas atbildīgie vadītāji, funkciju pārstāvji, procesu īpašnieki un eksperti. Tāpat risku grupas un klasifikācija var tikt izmantota arī citos risku vadības procesa posmos (komunikācijā, uzraudzībā).

Risku grupas ļauj iestādei saskatīt atšķirības vai tieši otrādi saikni starp dažādiem riskiem vienā risku grupā, kas ļauj diskutēt un pilnveidot risku formulējumus un aprakstus, iespējams optimizēt risku vadību, ja vairākus riskus var mazināt, izmantojot koordinētu iekšējo sadarbību.

Riskus var grupēt, ņemot vērā arī to, kā iestādes darbību ietekmē ārējā un iekšējā vide, tās mijiedarbība. Iestāde īsteno funkcijas, tām pakārtotos procesus, lai sasniegtu savus izvirzītos mērķus, ievērojot normatīvajos aktos noteiktās prasības, kā arī vienlaikus darbojoties atbilstoši ieinteresēto pušu, arī klientu interesēm. Iestādes neatkarīgi no to organizatoriskās struktūras un lieluma ietekmē iekšējās un ārējās vides faktori, kā rezultātā izvirzītie mērķi var netikt sasniegti. Līdz ar to riskus var iedalīt: ārējās riskos – izraisa notikumi ārējā vidē un iekšējās vides riskos – izraisa notikumi iekšējā vidē.

Ārējos riskus iestāde pilnībā nevar ietekmēt, jo risku rašanās iespējamības kontrole nav iestādes kompetencē (risku mazināšanai iespējams nepieciešama arī citu ieinteresēto pušu iesaiste un kompetence). Piemēram, par ārējiem riskiem var uzskatīt ekonomiskās un demogrāfiskās situācijas pasliktināšanos, dabas katastrofas (piemēram, plūdi, ugunsgrēki, bīstamas infekcijas slimības, epidēmijas un pandēmijas), kara draudi, ko iestāde nevar ietekmēt.

Savukārt iekšējie riski ir riski, kas rodas, ikdienā īstenojot normatīvajos aktos noteiktās iestādes funkcijas un tām pakārtotos procesus. Šos riskus iestāde var ietekmēt, ieviešot iekšējās kontroles, lai mazinātu risku rašanās varbūtību vai ietekmi. Iekšējos riskus, piemēram, procesu neatbilstību iekšējiem normatīvajiem aktiem, tostarp kļūdas var izraisīt iestādes darbinieki, informācijas sistēmu, interneta darbības pārtraukumi un kiberuzbrukums, kas vienlaikus ir ārējās vides faktors.

Ārējie riski var izraisīt iekšējo risku rašanos, piemēram, izmaiņas ārējos normatīvajos aktos, radīs iekšējo risku – iekšējo normatīvo aktu neatbilstību ārējiem normatīvajiem aktiem. Tāpat ieviešot izmaiņas procesos un ieviestajās sistēmās, rodas iekšējie riski, piemēram, aktualizētie jeb modificētie procesi un sistēmas var neatbilst iestādes mērķu sasniegšanai. Personāls var nevēlēties pieņemt jaunās izmaiņas procesos un sistēmās. Darbinieki var baidīties no darba zaudēšanas, ja procesi tiek modernizēti vai automatizēti un aizstāt cilvēku veikto darbu, piemēram, ieviešot informācijas sistēmas.

Tāpat riskus var iedalīt nefinanšu un finanšu riskos. Nefinanšu risku ietekme var būt pat nopietnāka par finanšu risku ietekmi, jo, piemēram, darba vai vides drošības riski, tiesvedības kas saistītas ar normatīvo aktu prasību neievērošanu, vai netiešu kaitējumu reputācijai, ko izraisa darbinieku nekorekta rīcība, var pārsniegt finanšu risku ietekmi (piemēram, cenu sadārdzinājuma vai likviditātes riska izraisītos zaudējumus).

Katra iestāde var izvēlēties veidu, kā grupēt tās darbību ietekmējošos riskus atkarībā no izvirzīto mērķu grupām, lai tai būtu ērtāk tos identificēt, analizēt un arī turpmāk uzraudzīt. Viens no variantiem ir grupēt riskus atbilstoši COSO Iekšējās kontroles - Integrētā ietvarā noteiktajām mērķu kategorijām, piemēram, stratēģiskie, finanšu, atbilstības, darbības (operacionālie) riski, kas iedalīti funkcionālās apakšgrupās, un atsevišķi izdalot ārējos un reputācijas riskus, kas valsts pārvaldes iestādēm ir būtiski un specifiski vadāmi (10. tabula 1. variants un 7. pielikums).

10. tabula. Risku grupas (1.variants)[27]

Risku grupa	Skaidrojums	Risku piemēri
Stratēģiskie riski	Notikuma vai apstākļu iestāšanās iespējamība, kas palielinās vai apdraudēs iestādes labklājību un pastāvēšanu ilgtermiņā.	• Nekvalitatīva, nepārdomāta, nepamatota iestādes darbības stratēģija; • Stratēģiskie mērķi var tikt pārspīlēti, var būt nesasniedzami vai neatbilstoši iestādes specifikai vai kultūrai; • Iestādes nespēja nodrošināt nepieciešamos resursus stratēģijas ieviešanai; • Iestādes nespēja savlaicīgi reaģēt uz ārējās vides izmaiņām; • Nepareizi noteikta informācijas un komunikācijas tehnoloģiju stratēģija, personālvadības un komunikācijas stratēģija; • Nekorekti, neatbilstoši mērķu sasniegšanai izvēlēti sadarbības partneri un citi riski.
Finanšu riski	Notikuma vai apstākļu iestāšanās iespējamība, kas ietekmē iestādes naudas plūsmu un finanšu darījumus.	• Neatbilstoša finansējuma plānošana; • Nodokļu izmaiņas; • Inflācijas risks; • Likviditātes risks; • Valūtas maiņas kursa svārstību risks; • Nelietderīgi izšķērdēti līdzekļi un citi riski.

[27] FM 19.05.2021. apstiprinātās vadlīnijas risku vadības iekšējam auditam un konsultācijai,

Risku grupa	Skaidrojums	Risku piemēri
Atbilstības riski	Notikuma vai apstākļu iestāšanās iespējamība, kas ietekmē iestādes spēju sasniegt mērķus nodrošinot atbilstību vērtību pievienojošiem iekšējiem normatīvajiem aktiem, vadlīnijām, līgumiem, lēmumiem vai ārējo uzraugošo iestāžu prasībām.	• Normatīvo aktu neievērošana; • Tiesību normu interpretācija nepareizi, neatbilstoši labākajai tiesību praksei; • Neētiska rīcība; • Personas datu aizsardzības pārkāpumi un citi riski.
Darbības (operacionālie) riski	Notikuma vai apstākļu iestāšanās iespējamība, kas saistīta ar nepilnvērtīgu vai iekšējos un ārējos normatīvajos aktos neatbilstošu funkciju, tām pakārtoto procesu norisi, nekorektām personāla darbībām vai ārējiem notikumiem, kā arī kas vienlaikus ietekmē iestādes spēju sasniegt mērķus, pārvēršot ieguldītos resursus sagaidāmajos rezultātos.	**Personāla riski** • Personāla kompetences trūkums konkrētā jomā; • Personāla brīvprātīgās rotācijas palielināšanās; • Cilvēciskā faktora kļūdas; • Atkarība no "atslēgas" cilvēkiem; • Nemotivēts darbinieks; • Personāla "izdegšana" un citi riski.
		Procesu riski • Neatbilstoši, nepilnīgi, neefektīvi iekšējie procesi; • Nekoordinētas darbības procesu ietvaros; • Uzskaites kļūdas; • Kļūdas procesu izpildē; • Iekārtu vai tehnikas bojājumi un citi riski.
		Projektu riski • Finansējuma nepietiekamība vai pārtēriņš; • Piegāžu, pakalpojumu izpildes kavēšanās; • Nekvalitatīvu materiālu piegādes; • Projekta plānošanas kļūdas un citi riski.
		Informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) riski • IS darbības traucējumi (pieejamība); • Datu kvalitātes (integritāte) nepietiekamība; • Informācijas drošības (konfidencialitāte) apdraudējumi; • Nepietiekams informācijas sistēmu atbalsts un citi riski.
		Juridiskie riski • Līgumsaistību neizpilde; • Kļūdas un trūkumi iekšējo normatīvo aktu un citu dokumentu sagatavošanas juridiskajā tehnikā;

Risku grupa	Skaidrojums	Risku piemēri
		• Nepietiekama juridiskā analīze un atbalsts, izstrādājot un ieviešot jaunus, un pilnveidojot esošos dokumentus un citi riski.
		Korupcijas un krāpšanas riski • Interešu konflikts; • Kukuļošana; • Tīša finanšu informācijas un pārskatu sagrozīšana; • Materiālo un nemateriālo aktīvu nelikumīga piesavināšanās; • Negodprātīga rīcība, tostarp, izmantojot dienesta stāvokli un citi riski.
		Darba vides drošības riski • Darba vides drošības pārkāpumi; • Nepietiekama individuālo aizsarglīdzekļu izmantošana; • Neatbilstoša darba vide, tostarp temperatūra un citi riski.
Ārējie riski	Ārējās vides notikumu vai apstākļu iestāšanās iespējamība, ko iestāde nespēj kontrolēt un tai ir jāpielāgojas, tādējādi būtiski ietekmējot iestādes spēju sasniegt mērķus.	• Valsts/ pasaules ekonomiskās krīzes; • Pandēmija un epidēmijas, bīstamas infekcijas slimības; • Izmaiņas normatīvajos aktos, kas apgrūtina iestādes mērķu īstenošanu; • Politiskā ietekme, kas negatīvi ietekmē iestādes darbību, darbinieku morāli, sabiedrības attieksmi u.tml.; • Jaunas tehnoloģijas, kuru ieviešanai iestāde nav gatava; • Ārējie noziegumi, kas var radīt iestādei zaudējumus; • Piegādātāju/ ārpakalpojumu sniedzēju negodprātīga rīcība u.c.
Reputācijas riski	Notikuma vai apstākļu iestāšanās iespējamība, kas ietekmē iestādes reputāciju un labo tēlu, tādējādi apgrūtinot iespējas sasniegt mērķus.	• Zema sniegto pakalpojumu kvalitāte klientiem; • Neētiska vai nelegāla iestādes vadības un darbinieku rīcība; • Savlaicīga nodokļu nemaksāšana; • Grāmatvedības uzskaites neatbilstība normatīvo aktu prasībām; • Vāja korporatīvā pārvaldība; • Iestādes darbības neatbilstība saistošajiem normatīvajiem aktiem un standartiem; • Nav sasniegti paredzētie politikas un darbības rezultāti un rezultatīvie rādītāji.

Iestādes ārējās un iekšējās vides izpētes procesā vai jau pēc risku identificēšanas risku grupas atkarībā no risku būtiskuma un daudzuma konkrētā tēmā jeb jomā, var tikt sarindotas vai sastrukturētas tālākam loģiskākam darbam ar noteiktas tematikas riskiem. Rokasgrāmatā turpmāk tiek piedāvāts vēl viens variants, kā grupēt riskus. (10. tabula 2. variants) (skat. arī 7. pielikumu). Katra iestāde var grupēt un klasificēt riskus, ņemot vērā tās darbības jomas un izvirzītos mērķus.

10. tabula. Risku grupas (2.variants)

Risku grupa	Risku piemēri
Stratēģiskie riski	• Iestādes nozares politikas vai pamatnostādņu neieviešana (piemēram, neskaidra vai starp nozarēm / nozares ietvaros nepietiekami koordinēts nozares politikas, pamatnostādņu ieviešanas process); • Attīstības prioritāšu straujas izmaiņas - negaidītas, sasteigtas, regulāras pārmaiņas, kas neļauj īstenot iestādes noteiktos vidēja termiņā mērķus; • Politiskās ietekmes rezultātā var tikt pieņemti steidzīgi, nepārdomāti, subjektīvi, pretrunīgi un nekoordinēti lēmumi, kā rezultātā tiek nelietderīgi tērēti iestādes resursi trūkumu novēršanai un skaidrojošā darba veikšanai.
Makrolīmeņa (ārējie) riski	• Makroekonomiskā nestabilitāte; • Ģeopolitiskā nestabilitāte; • Starptautiskās piegādes ķēdes pārtraukumu riski; • Politiskie lēmumi ar negatīvu ietekmi uz iestādes darbību.
Finanšu riski	• Finanšu rādītāju svārstības/ neizpildes, kas pārsniedz pieļaujamo novirzi; • Valsts budžeta līdzekļi netiek iztērēti lietderīgi - izmantotie budžeta līdzekļi nav sasaistīti ar noteiktu nozares politikas mērķu sasniegšanu, izvēlētie izpildes rādītāji neatspoguļo mērķus vai to sasnieguma pakāpi; • Budžeta konsolidācijas pasākumi tiek izvēlēti un ieviesti, neizvērtējot un nepārskatot iestādes veicamās funkcijas un tai izvirzītās prasības, kā rezultātā iestāde var nespēt izpildīt tai uzticētās funkcijas pilnā apjomā un sagaidītajā kvalitātē. Konsolidācijas pasākumi var tikt veikti novēloti un nedod gaidāmo izmaksu ietaupījumu.

Darbības (operacionālie) riski	• Cilvēciskās kļūdas;
	• Datu apstrādes kļūdas informācijas sistēmās;
	• Materiālo resursu bojājumi, to zaudēšana;
	• Interešu konflikta, korupcijas un krāpšanas riski;
	• Klientu apkalpošanas un pakalpojuma sniegšanas riski:
	  o klientu apkalpošanas atbalsta sistēmu piemērotības un darbības riski;
	  o darbinieku kompetences un attieksmes (saskarsmes kultūras) riski;
	  o pakalpojumu sarežģītības riski;
	  o klientu plūsmu iestādes riski;
	• IKT riski:
	  o IS attīstība un izveide, uzturēšana;
	  o IKT darbības nepārtrauktība;
	  o kiberdrošības risks;
	  o informācijas drošības riski;
	  o fizisko personu datu drošības riski;

Risku grupa	Risku piemēri
	• Atbilstības (iekšējiem un ārējiem normatīvajiem aktiem, normām, labajai praksei) riski, tostarp sankciju riski, iestādes administratīvie pārkāpumi; • Juridiskie riski: o saistību vai līguma nosacījumu neievērošana; o juridiskā atbalsta nesniegšana; • Personāla vadības riski (piesaiste, motivācija, kapacitāte, prasmes); • Darbības nepārtrauktības riski (infrastruktūras, tostarp, telpu, IKT, sakaru, komunālo pakalpojumu pieejamības apdraudējumi/ pārtraukumi, ārkārtas situācijas u.tml.); • Komunikācijas un informācijas apmaiņas riski: o nepietiekama iekšējā komunikācija, informācijas apmaiņa un darbinieku informētība; o nepietiekama ārējā komunikācija, vienota izpratne, regularitāte un kvalitāte.
Projektu riski	• Kavēti termiņi; • Nekvalitatīvi materiāli, pakalpojumi no trešajām pusēm; • Juridiski, politiski vai tehniski ierobežojumi projekta īstenošanai; • Projekta resursu nepietiekamības riski (darbaspēks, finanses - izmaksu sadārdzinājums).
Ilgtspējas riski	• Vides riski: o fiziskie riski: ▪ hroniskie riski (pakāpeniskas klimata pārmaiņas, piemēram, temperatūras paaugstināšanās, dabas resursu iztrūkums); ▪ akūtie riski (piemēram, plūdi, sausums, vētras); o pārejas riski - politika un regulējums (izmaiņas tiesību aktos, kas reglamentē ilgtspējas aspektus un iestāde tiem var neatbilst), tehnoloģiju attīstība (tiek izmantotas tehnoloģijas, kas nav pietiekami energoefektīvas) un tirgus (klientu paradumu maiņa, ņemot vērā zaļo kursu); • Sociālie riski: o darba tiesisko attiecību regulējuma neievērošana; o darba vides riski; • Pārvaldības riski: o interešu konfliktu, korupcijas un krāpšanas riski; o personas datu aizsardzības riski.

Risku grupēšana var arī praktiski palīdzēt, lai apkopotu, sastrukturētu un atspoguļotu analītisku informāciju par riskiem un to līmeņiem, ņemot vērā to grupēšanas pazīmi, kas ir svarīgi risku īpašniekiem un vadītājiem gan uzraugot, gan salīdzinot riskus. Ja identificēto risku skaits ir liels, riska grupas ļauj tematiski sadalīt darba apjomu un arī informāciju par riskiem, lai reaģētu uz šiem riskiem un ziņotu par katru riska grupu atsevišķi.

5.4. Risku identificēšana – avoti, metodes, risku indikatori

Risku identificēšanas mērķis ir strukturēti un objektīvi apzināt un apkopot iestādes riskus, identificējot iekšējās un ārējās vides faktorus, vienlaikus apzinoties vidi, kādā iestāde darbojas.

Risku identificēšanas ietvaros definē riskus, kas varētu traucēt iestādes darbībai un ietekmēt tās stratēģisko un darbības mērķu sasniegšanu. Vienam riskam var būt vairāki cēloņi un sekas, viens risks var attiekties uz vairākiem iestādes mērķiem, kā arī vienu mērķi var apdraudēt vairāki riski.

Risku identificēšanas mērķi var raksturot kā analīzi, kas atbild uz jautājumu "Kas slikts var notikt?". Tātad risku īpašniekiem risku vadītāja uzraudzībā būtu jāspēj objektīvi un atklāti norādīt uz iespējamām negatīvajām situācijām, to iznākumiem un sekām. Pilnvērtīgs riska apraksts ietver ne tikai nevēlamo/ negatīvo scenāriju, kas var notikt (un apdraudēt kāda mērķa sasniegšanu), bet arī riska cēloņus un sekas.

Risks ir nezināms negatīvs notikums nākotnē, kas var iestāties (tātad tam ir zināma kvantitatīvi vai kvalitatīvi novērtējama varbūtība). Ir svarīgi vēlreiz uzsvērt to, ka risks ir vēl neīstenojies notikums, tātad viena no riska pazīmēm vienmēr būs tā iestāšanās varbūtība. Turpmāk Rokasgrāmatā iekļautas nodaļas par risku novērtējumu (ietekmi un varbūtību).

Risku identificēšanas posmā ir veicamas šādas darbības:

- Iestādes aktuālo mērķu apzināšana un izpratne (kas jāsasniedz?);
- Mērķu sasniegšanu ietekmējošo faktoru apzināšana (kas var novirzīt no mērķa, neļaus to sasniegt?);
- Riska informācijas apkopošana, "tīrīšana", strukturēšana (kas ko ietekmē?);
- Riska formulēšana – riska "esences" definēšana, nosaukums, apraksts, līdzsvarošana un mērogošana ar citiem riskiem (kas var neizdoties?);
- Riska cēloņu analīze (kāpēc var neizdoties?);
- Riska seku analīze (kas notiks, ja risks patiešām īstenosies?).

Svarīgi: Risku identificēšanas pirmais un svarīgākais uzdevums ir precīzi definēt riskus. Riska definīcijai un/vai aprakstam jāsatur šādi elementi: iespējamā notikuma apraksts, rašanās cēloņi, potenciālās negatīvās sekas.

Esošu problēmu, negatīvu vai nelabvēlīgu apstākļu, faktu uzskaite un apraksts vēl nav riski.

Tāpat arī kādas tēmas vispārīgs virsraksts vai procesa nosaukums (piemēram, "autopārvadājumi" vai "iepirkumu process") nav riski, jo procesu un jomu nosaukumi neraksturo, kas var notikt un apdraudēt to mērķus!

Piemērs:

Nepilnvērtīgi definēti riski:

1. "Trūkst darbinieku, nav iespējams piesaistīt personālu"
2. "Var netikt izpildīts attīstības plānošanas dokumentā noteiktais rīcības plāns"
3. "Nav izstrādāts iestādes darbības plāns".

Priekšlikums definēt risku aprakstus, atklājot detalizācijas pakāpi un konkrētību:

1. "Riska notikuma apraksts "Vakance xy amatā netiks ilgstoši (vairāk kā seši mēneši) aizpildīta (dēļ nekonkurētspējīgā atalgojuma), kas var izraisīt xy procesa ievērojamu (līdz 3 mēnešiem) īstenošanas kavēšanos un kvalitātes pasliktināšanos, kā arī var radīt ārējo klientu neapmierinātību"".

2. “Riska notikuma apraksts: “Var nebūt iespējams veikt būvdarbus savlaicīgi un plānotajā apjomā (tirgū pieejamie būvmateriāli, kas tiek izmantoti celtniecībā, ir ierobežotā apjomā), kā rezultātā var netikt sasniegti iestādes mērķi, kas saistīti ar konkrētās infrastruktūras izveidi vai pilnveidi””.
3. “Riska notikuma apraksts: “Iestāde var nesasniegt darbības stratēģijā noteiktos mērķus. Cēloņi: nav izstrādāts iestādes darbības plāns, mērķi nav kaskadēti pasākumu līmenī, nav noteikta atbildība un pienākumi stratēģisko mērķu sasniegšanai. Sekas: Klientu neapmierinātība un reputācijas pasliktināšanās””.

5.4.1. Risku identificēšanas avoti

Risku identificēšanas avoti (11. tabula) ir atbalsta rīks risku identificēšanas procesā, ko izmanto neatkarīgi no paredzamās izmantojamās risku identificēšanas metodes, tā kā tajos var būt informācija par jau iepriekš identificētiem riskiem, risku pazīmēm, iestādes mērķu neizpildes indikatoriem un tamlīdzīgi.

Risku identificēšanas avoti var kalpot par sākuma punktu risku identificēšanai, kā arī var būt labs informatīvs atbalsts risku vadītājam, risku īpašniekiem un iestādes vadībai.

11. tabula. Risku identificēšanas avoti

Avots	Skaidrojums risku identificēšanas iespējām
Attīstības plānošanas dokumenti, tostarp Latvijas ilgtspējīgas attīstības stratēģija, Nacionālais attīstības plāns un politikas plānošanas dokumenti (pamatnostādnes, plāns un konceptuāls ziņojums)	• Attiecīgajam plānošanas periodam noteiktās prioritātes; • No prioritātēm izrietošie iestādes mērķi; • Sasniedzamie rezultāti jeb pārmaiņas, kuras raksturos noteiktā mērķa sasniegšanas pakāpi, un to snieguma rādītāji; • Galvenie sasniedzamie rādītāji, tai skaitā tādi par kuriem jāsniedz informācija starptautiskā līmenī.
Iestādes vidēja termiņa stratēģija	• Iestādes prioritātes; • No prioritātēm izrietošie iestādes stratēģiskie mērķi; • Iestādes attīstības virzieni; • Sasniedzamie rezultāti jeb pārmaiņas, kuras raksturos noteiktā mērķa sasniegšanas pakāpi, un to snieguma rādītāji; • Galvenie snieguma rādītāji, kuri demonstrēs iestādes darbības progresu un raksturos svarīgākos institūcijas sasniedzamos rezultātus.
Iestādes darbības plāni	• Jaunas darbības jomas, funkcijas; • Darbības mērķi, uzdevumi; • Sasniedzamie rezultāti; • Izmaiņas iestādes darbībā; • Iespējami trūkstoša kompetence, resursi jauno funkciju veikšanai.
Iepriekš veiktie iekšējie un ārējie auditi	• Iepriekš atklāti kontroles trūkumi, novērtēts atlikušais risks; • Iepriekš atklāti draudi, šķēršļi un iestādes mērķus ietekmējošie faktori;

Iekšējie normatīvie dokumenti, to izmaiņas	• Iekšējās kontroles trūkumi un to atbilstība ārējiem normatīvajiem aktiem; • Izmaiņas iekšējā kontrolē vai to nepilnības/ trūkumi.
Sanāksmju protokoli	• Informācija par problēmām un plānotajām izmaiņām iestādes darbībā; • Informācija par ieviešamajiem uzlabojumiem, inovācijām.
Ārējie pētījumi	• Nepieciešamas izmaiņas iestādes darbības virzienos, pieejās, uzstādījumos; • Ārējās vides izmaiņas.
Mediji, informācija sociālajos tīklos, arī negatīvā	• Reputācijas apdraudējums; • Ārējas vides izmaiņas.
Citu iestāžu un uzņēmumu piemēri, risku situācijas	• Nozarē vai līdzvērtīgā iestādē notikuši vai gaidāmi riska notikumi.
Incidentu, pārkāpumu, neatbilstību reģistrs, kļūdu paziņojumu statistika	• Iespējami trūkumi procesos, pakalpojumos, iestādes vērtībās un iekšējā kultūrā.
Sūdzības, atsauksmju apkopojumi	• Iespējami trūkumi procesos, pakalpojumos, iestādes vērtībās un iekšējā kultūrā.
Incidentu reģistri	• Īstenojušies riski.
Aptauju rezultāti	• Pilnveidojamās jomas procesos/ pakalpojumos un darbībās; • Izmaiņas ārējā un iekšējā vidē.
Procesu shēmas	• Potenciāli trūkumi procesos, to neefektīva darbība; • Lieka birokrātija un administratīvais slogs.

Viens no visbiežāk izmantojamajiem risku identificēšanas avotiem ir Incidentu reģistrs (8. pielikums), ja tāds ir izveidots, jo tajā pieejama informācija par riskiem, kas īstenojušies, un jaunajiem riskiem, kas saistīti ar šiem incidentiem, kā arī vērojama tendence, vai incidenti atkārtojas, un vienlaikus iegūstama informācija par veiktajiem pasākumiem to rašanās cēloņu novēršanai.

Padoms: Sākot ieviest risku vadību, uzsāciet risku identificēšanu iestādē pakāpeniski. Nosakiet secīgi, kuriem procesiem, funkcijām, vai struktūrvienībām to veiksiet iestādei vēlamajā kopējā risku cikla periodā. Piemēram, sākotnēji risku identificēšanu un analīzi var veikt atsevišķiem prioritārajiem iestādes darbības

virzieniem, vai tajās struktūrvienībās, kurās tuvākajā laikā tiek plānoti svarīgi un vērienīgi projekti.

Pakāpeniski uzturot jau esošu risku vadības funkciju, nosakiet regularitāti, kādā risku identificēšana (un pārējie risku vadības posmi) jāveic visos risku vadības līmeņos (t.i. visās struktūrvienībās, procesos un/vai funkcijās).

5.4.2. Risku identificēšanas metodes

Risku informācijas apkopošana bieži sagādā grūtības, jo riski ir jāspēj formulēt tā, lai tie ir salīdzināmi savā starpā (iestādes ietvaros, piemēram, dažādu struktūrvienību riski). Formulējumam pēc iespējas objektīvi un korekti jāatspoguļo būtiskākie riski un vadītāju skatījums par iespējamajiem negatīvajiem scenārijiem, kas var ietekmēt iestādes darbību un mērķu sasniegšanu.

Risku identificēšanā un formulēšanā var tikt izmantotas dažādas metodes (12. tabula), kas var būt vērstas uz pagātnes notikumu, šodienas situācijas un nākotnes iespēju analīzi.

12. tabula. Risku identificēšanas metodes

Pagātnes notikumu analīzes metodes	Tagadnes situāciju analīzes metodes	Nākotnes iespēju analīzes metodes
• Incidentu un problēmu reģistru datu analīze; • Disciplinārlietu un citu pārkāpumu analīze; • Pagātnes kļūdu analīze – programmu, projektu, sadarbības pieredzes mācības; • Ārējo un iekšējo auditu un citu pārbaudītāju ziņojumu analīze; • Darbības uzraudzības pārskatu analīze; • Pārbaudes (kvalitātes) lapu izmantošana; • Aptauja.	• Pieņēmumu un ierobežojošo faktoru analīze; • SVID analīze; • Iestādes procesu analīze; • Aptauja.	• "Prāta vētras"; • Ekspertu un fokusa grupu diskusijas; • Aptaujas; • Riska grupu modelēšana; • Scenāriju analīze.

5.4.3. Risku indikatori

Lielākā daļa valsts pārvaldes iestāžu plāno un uzrauga galveno snieguma rādītāju izpildi, ņemot vērā MK 18.06.2008. noteikumus Nr. 344 "Par Rezultātu un rezultatīvo rādītāju sistēmas pamatnostādnēm 2008.-2013. gadam". Taču, lai iestādes augstākajai vadībai būtu iespējams detalizētāk un savlaicīgi uzraudzīt iespējamās riska līmeņa izmaiņas vai arī apzināt jaunus saistītos riskus, nepieciešams noteikt risku indikatorus (KRI – *Key Risk Indicator*) (13. tabula).

Riska indikators ir mērījums, kas norāda uz riska potenciālo klātbūtni, līmeni un tendenci, tas var norādīt, vai risks ir tikko iestājies vai tā līmenis paaugstināsies, kāds ir tā līmenis, izmaiņu tendence.

Riska indikatorus izmanto, lai mērītu iespēju, vai un cik lielā mērā iestādes darbība tiks pakļauta riskam, tas var būt kā agrās brīdināšanas signāls, ka iestādes darbību un izvirzīto mērķu sasniegšanu drīzumā ietekmēs konkrēts risks. Risku indikatori kalpo arī kā palaidējmehānisms riska mazinošo pasākumu ieviešanai, lai samazinātu zaudējumus vai novērstu incidentus, kā arī ir kā skaidrs eskalācijas mehānisms informācijas par riskiem ziņošanai iestādes vadībai.

Efektīva riska indikatoru noteikšanas mērķis ir identificēt mērāmus rādītājus, kas raksturo potenciālu risku iestādes mērķu sasniegšanai. Tāpēc efektīvu risku indikatoru izstrāde sākas ar vienotu izpratni par iestādes mērķiem un to rezultatīvajiem rādītājiem, mērķu sasniegšanu ietekmējošiem potenciāliem riska notikumiem, to cēloņiem, un risku apetīti jeb slieksni, kuru pārsniedzot var būt nepieciešami risku mazināšanas pasākumi.

Iestādes darbībā var būt novērojami daudzi riska indikatori, taču būtiski ir izvēlēties svarīgākos riska indikatorus un to detalizācijas pakāpi atkarībā no plānoto mērķu būtības un tā, kādi lēmumi tiks pieņemti, pamatojoties uz riska indikatoru mērījumiem (13. tabula).

Riska indikatorus nosaka būtiskākajiem iestādes riskiem un izvēlas tos, kuri visspēcīgāk raksturo riska cēloni, nodrošinot, ka izvēlētie indikatori tiek skaidri izprasti, dokumentēti un faktiski arī mērīt (t.i., par tiem pieejami aktuāli dati).

Riska indikatori var būt vērsti uz pagātni (piemēram, krāpšanā iesaistīto darbinieku skaits) vai uz nākotni (piemēram, darbinieku skaits, kuri neizmanto atvaļinājumu). Vērtīgāki ir uz nākotni vērstie indikatori, jo tie palīdz iestādes vadībai paredzēt, vai mērķi tiks vai netiks sasniegti.

Riska indikatoru noteikšanas procesā var piesaistīt attiecīgās mērķu vai funkciju jomas pārstāvjus no iestādes, jo šīs personas kā eksperti vislabāk varētu zināt, kādi ir riska pamatcēloņi, kā risks izpaužas un kādi ir iespējamie mērāmie notikumi starp cēloni un risku. Tomēr jāpatur prātā, ka var rasties šo darbinieku neobjektīvs skatījums uz jaunu svarīgu indikatoru ieviešanu, jo izmaiņas esošajā rādītāju sistēmā prasīs papildu resursu datu ieguvei, analīzei un saskaņošanai pirms jauno indikatoru apstiprināšanas.

Informācijai par risku indikatoriem (to aktuālo līmeni) jābūt pieejamai gan risku īpašniekam, gan atbildīgajiem par riska kontrolēm, gan risku vadītājam. Jābūt skaidri noteiktai atbildībai, datu īpašniekam, kura pienākums ir regulāri nodrošināt aktuālu informāciju par risku indikatoru vērtību, ko risku īpašnieks un risku vadītājs varētu izmantot turpmāku lēmumu pieņemšanā.

13. tabula. Risku indikatoru piemēri

Personāls	Procesi
• Ierosināto disciplinārlietu īpatsvars/ skaits; • Atlaisto darbinieku skaits; • Darba tiesisko attiecību izbeigušo pieredzējušu darbinieku skaits; • Personāla aptauju rezultāti par darbinieku viedokli; • Vidējais darba stāža ilgums iestādē; • Virsstundu apjomi; • Darbinieku īpatsvars, kas saņēmuši nepietiekami augstu novērtējumu; • Vidējais nepieciešamais laiks vakanču aizpildīšanai.	• Saņemto sūdzību skaits; • Krāpšanas gadījumu skaits; • Kļūdainu dokumentu īpatsvars; • Normatīvo aktu pārkāpumus skaits; • Piegādātāja darbības novērtējums; • Klientu apmierinātības novērtējums; • Klientu gaidīšanas laiks rindā; • Neatbildēto klientu zvanu skaits/ īpatsvars; • Darba izpildes rādītāji (darba plāna izpildes rādītāji).

IT sistēmas	Ārējā vide
• IT sistēmas un cita aprīkojuma darbības traucējumu skaits; • IT sistēmu un cita aprīkojuma darbības traucējumu vidējais ilgums; • Pieteikumu skaits IT atbalsta saņemšanai; • Informācijas drošības incidentu skaits; • IT sistēmas atjauninājumu / publicēto versiju skaits.	• Fiziskās drošības incidentu skaits; • Sekmīgo kiberuzbrukumu skaits; • Netestēto darbības atjaunošanas plānu īpatsvars; • Inflācijas līmenis; • Darbaspēka vidējās algas līmenis tirgū katrai profesijai; • Klientu palielinājums % salīdzinājumā ar iepriekšējo periodu; • Piegāžu vidējās kavējuma dienas.

Piemērs: Riskam, ka darbinieki var neievērot iestādes atbilstības kultūru, var tikt izmantots riska indikators - ierosināto disciplinārlietu īpatsvars/ skaits (piemēram, palielinājums par 10% salīdzinājumā ar iepriekšējo gadu vai 5 disciplinārlietas gadā) un atlaisto darbinieku skaits (piemēram, 5 darbinieki gadā), kas saistīts ar darbinieka atbilstības pārkāpumiem.

Savukārt riskam, ka var rasties informācijas sistēmu darbības traucējumi, kas apgrūtina tajā pieejamo datu analīzi un eksportēšanu uz citu saistītu informācijas sistēmu, iespējams izmantot riska indikatoru - IT sistēmu un cita aprīkojuma darbības traucējumu vidējais ilgums (piemēram, ne vairāk kā 2 stundas, ņemot vērā tās prioritāti iestādē).

Svarīgi: Ja gadījumā, veicot mērījumus ikdienā, ņemot vērā iestādes vajadzības, tiek konstatēts, ka kāds no riska indikatoriem tuvojas pieļaujamajam slieksnim (noteikta vērtība, risku tolerances robeža, ja tāda ir noteikta) vai to pārsniedz (riska līmenis pārsniedz iestādē pieļaujamo jeb riska apetīti), tad riska līmenis palielinās un ir nepieciešams savlaicīgi uz to reaģēt, ieviešot papildu riska mazinošos pasākumus.

5.5. Risku analīze un izvērtēšana – kritēriji, metodes, prioritizēšana, būtiskāko risku noteikšana

Riska analīzi izmanto, lai izprastu identificēto risku veidu, avotus un cēloņus un rezultātā noteiktu riska līmeni. Šis process nodrošina, ka iestāde var iegūt informāciju par to, cik nozīmīgs ir katrs risks tās mērķu un snieguma rādītāju sasniegšanā. Veicot risku analīzi, tiek noteikti būtiskākie riski, kā arī citas risku grupas, kuras var vadīt atbilstoši iestādes risku vadības politikai un izvēlētajai pieejai. Tas palīdz arī pēc iespējas atbilstoši novirzīt dažādus resursus (laika, finanšu, darbinieku) risku mazināšanai. Risku analīzes detalizācijas un sarežģītības pakāpe katrā atsevišķā gadījumā var atšķirties atkarībā no analīzes nolūka, informācijas pieejamības un uzticamības, kā arī no pieejamajiem resursiem, risku vadības brieduma pakāpes.

Pēc risku identificēšanas nepieciešams veikt to izvērtēšanu. Bez risku izvērtēšanas nav iespējams tos prioritizēt un nodrošināt lēmumu pieņemšanu attiecībā uz risku mazināšanas pasākumiem un vērtēt esošo kontroļu darbību. Risku izvērtējums paredz risku mērīšanu un prioritāšu noteikšanu,

lai risku līmeņus vadītu, ņemot vērā iestādes noteiktās mērķu robežas jeb riska pieļaujamo līmeni(riska apetīti).

Tā kā iestādes iekšējā un ārējā vide mainās, risku novērtējumu nepieciešams regulāri aktualizēt. Mainoties apstākļiem un risku novērtējumam, iespējams, ka jāpielāgo risku mazināšanas pasākumi un iekšējās kontroles, lai riskus būtu iespējams saprātīgi vadīt.

5.5.1. Risku novērtēšanas kritēriji

Lai noskaidrotu riska līmeni, kā arī savstarpēji salīdzinātu un prioritizētu riskus, iestādē jānosaka vienoti risku vērtēšanas kritēriji un skala. Risku vērtēšanas kritēriji būtu jāiekļauj iestādes risku vadības metodikā. Ja risku vērtēšanas kritēriji būs pieejami un izskaidroti visiem risku vadībā iesaistītajiem, risku analīzes rezultāti būs objektīvāki, precīzāki un praktiskāk izmantojami.

Divi parametri, kas veido risku novērtējumu un izmantojami risku analīzē, ir risku iestāšanās **varbūtība** un **ietekme**. Šo parametru novērtēšanai iestādē jāizvēlas un jānosaka konkrēta novērtēšanas skala (piemēram, no 1 līdz 5), lai iegūtu skaitlisku vērtību, kā arī jāsniedz katra iespējamā piešķirtā novērtējuma skaidrojums. Vērtēšanas kritēriju skalas aprakstam jābūt skaidram, lai novērtējums būtu pēc iespējas viennozīmīgs ar ierobežotām iespējām to dažādi un subjektīvi interpretēt.

Katrai iestādei ir atšķirīgas funkcijas, darbības sarežģītība, lielums un nozare, tādēļ risku novērtējuma skalas būtu atbilstoši jāpielāgo iestādes darbības specifikai.

Tradicionāli iestādes izmanto piecu punktu skalu, kas ir precīzāka novērtējumu variācijām risku zonās salīdzinājumā ar trīs punktu skalu. Savukārt, piemēram, septiņu un vairāk punktu skala varētu radīt administratīvo slogu, lai to gan izstrādātu, gan precīzi izprastu, kāda ir atšķirība starp dažādiem piešķirtajiem novērtējumiem.

Lai noteiktu risku novērtēšanas kritērijus, jāapsver šādi aspekti:

- kāda veida nenoteiktības var ietekmēt rezultātus un mērķus (gan materiālos, gan nemateriālos);
- kā tiks konstatētas un izmērītas sekas (kā pozitīvās, tā negatīvās);
- ar laiku saistīti faktori;
- konsekvence mērījumu izmantošanā;
- kā tiks noteikts riska līmenis;
- kā tiks ņemts vērā vairāku risku apvienojums;
- iestādes kapacitāte skalas sarežģītības noteikšanai.

Risku izvērtēšanas uzdevums ir pamatot risku vadības lēmumus (t.i., iespējamās rīcības ar riskiem, skat. 5.7. nodaļu).

Risku izvērtēšanas rezultāti jāreģistrē, jākomunicē un pēc tam jāapstiprina rīcība reaģēšanai uz riskiem atbilstošajos iestādes līmeņos (skat. 5.8. un 5.10. nodaļu).

Risku izvērtēšanas rezultātā var tikt pieņemts lēmums par reaģēšanu uz riskiem (skat. 5.7. nodaļu).

Risku vērtēšanas skalas detalizācijas pakāpei un niansēm jāatbilst datiem, kas iestādē pieejami, nav lietderīgi risku vērtēšanas skalā iekļaut tādus kritērijus, par kuriem dati iestādē nav vai ir ļoti reti pieejami.

Bez **varbūtības** nav iespējama risku novērtēšana, jo risks ir prognozēts, vēl neīstenojies notikums (esošs notikums ar 100% varbūtību ir incidents, nevis risks). Savukārt, bez potenciālās **ietekmes** novērtējuma nav iespējama risku prioritizēšana un risku mazināšanas pasākumu noteikšana (jo kritiskāka iespējamā riska ietekme, jo lielāka vērība un attiecīgi lielāka uzmanība un resursi būtu jāvelta riska mazināšanai).

Varbūtības novērtēšanai var izmantot skalu, kas saistīta ar notikuma atkārtošanās biežumu vai arī īpatsvaru no kopējā notikumu apjoma (14.-16.tabula, 9. pielikums).

14. tabula. Risku varbūtības skalas piemērs (1.variants)

Punktu skaitliskā vērtība	Skaitliskās vērtības nozīme	Skaidrojums (I) (riska notikuma norises biežums laika periodā)	Skaidrojums (II) (riska notikuma īpatsvars no kopējo notikumu apjoma)
5	Ļoti bieži	Vismaz vienu reizi gada laikā vai biežāk	90% un vairāk iespējamība
4	Bieži	Vismaz vienu reizi 2- 5 gadu laikā	50 -90% iespējamība
3	Iespējams	Vismaz vienu reizi 5 – 10 gadu laikā	30 – 50% iespējamība
2	Maz ticams	Vismaz vienu reizi 10 – 15 gadu laikā	10 – 30% iespējamība
1	Gandrīz neiespējams	Retāk kā vienu reizi 15 gados	Mazāk nekā 10% iespējamība

Arī projektu vadībā izmantotās varbūtības skalas ir līdzīgas un tās raksturo riska rašanās varbūtības īpatsvaru (15. – 16. tabula).

15. tabula. Risku (projektu risku) varbūtības skalas piemērs (2.variants)

Punktu skaitliskā vērtība	Skaitliskās vērtības nozīme	Varbūtība	Skaidrojums
5	Ļoti liela	>70%	Risks īstenosies
4	Liela	51-70%	Risks drīzāk īstenosies, nekā neīstenosies
3	Vidēja	31-50%	Risks var īstenotie, var neīstenoties (50/50)
2	Maza	11-30%	Risks drīzāk neīstenosies, kā īstenosies
1	Ļoti maza	<10%	Risks neīstenosies

16. tabula. Risku (projektu risku) varbūtības skalas piemērs (3.variants)

Punktu skaitliskā vērtība	Skaitliskās vērtības nozīme	Varbūtība	Skaidrojums
3	Ļoti liela	>50%	Risks drīzāk īstenosies, kā neīstenosies
2	Vidēja	31-50%	Risks var īstenotie, var neīstenoties (50/50)
1	Ļoti maza	<30%	Risks drīzāk neīstenosies, kā īstenosies

Lai novērtētu risku **ietekmi**, var tikt izmatoti, piemēram, šādi kritēriji – ietekme uz iestādes stratēģiskajiem mērķiem un darbību, ietekme uz reputāciju un finansēm, ietekme uz atbilstību tiesību aktiem, veselību, drošību, apkārtējo vidi, darbiniekiem un ieinteresētajām pusēm (17.-19. tabula, 10. pielikums).

Tiek izvēlēta kombinācija no iepriekšminētajiem kritērijiem, izvēloties, piemēram, vidējo vai arī maksimālo ietekmes vērtību (ietekme uz stratēģiskajiem mērķiem, reputāciju un finansēm) (ja tiek izmantots vairāk par vienu ietekmes novērtēšanas kritēriju). Rokasgrāmatas piemēros tiek izmantota ietekmes maksimālās vērtības pieeja, kas salīdzinājumā ar vidējo ietekmes vērtību, ir piesardzīgāka pieeja, jo atlikušā riska līmenis tiek novērtēts augstāk. Ne visiem riskiem iespējams novērtēt visus iepriekšminētos ietekmes veidus. To iespējams pamatot un paskaidrot. Piemēram, ne vienmēr un visiem riskiem būs ietekme uz finansēm vai arī to nebūs iespējams aprēķināt, kas nozīmē, ka šo ietekmes veidu nav nepieciešams novērtēt. Līdz ar to iespējams novērtēt ietekmi uz stratēģiskajiem mērķiem un reputāciju.

Savukārt riskam, ka var rasties informācijas sistēmu darbības traucējumi, kas apgrūtina tajā pieejamo datu analīzi un eksportēšanu uz citu saistītu informācijas sistēmu, iespējams izmantot riska indikatoru - IT sistēmu un cita aprīkojuma darbības traucējumu vidējais ilgums (piemēram, ne vairāk kā 2 stundas, ņemot vērā tās prioritāti iestādē).

Piemērs: Riskam, ka iekšējais normatīvais akts par pārskatu sagatavošanu neatbilst ārējiem normatīvajiem aktiem, nav iespējams noteikt precīzu finanšu ietekmi, tāpēc šajā gadījumā to iespējams nevērtēt, novērtējot citus ietekmes veidus..

17. tabula. Risku ietekmes skalas piemērs (ietekme uz finansēm, reputāciju un mērķiem)

Punktu skaitliskā vērtība	Skaitliskās vērtības nozīme	Skaidrojums
5	Katastrofāla	Var rasties ļoti būtiski finansiālie zaudējumi valsts budžetā (piemēram, vairāk nekā 500 000 EUR)
		Negatīva publicitāte nacionālajos un starptautiskajos plašsaziņas līdzekļos ar plašu rezonansi un ilgstošu ietekmi uz reputāciju
		Stratēģiskie mērķi tiek būtiski ietekmēti, kavēsies lielākā daļa vai visu mērķu īstenošana vairāk nekā 3 – 5 gadus
4	Būtiska	Var rasties būtiski finansiālie zaudējumi valsts budžetā (100 000 – 500 000 EUR vai vairāk)
		Negatīva publicitāte nacionālajos un vairākos starptautiskajos plašsaziņas līdzekļos ar būtisku ietekmi uz reputāciju
		Stratēģisko mērķu sasniegšana tiek ietekmēta, kavēsies dažu mērķa īstenošana par 1 – 3 gadiem
3	Vidēja	Var rasties ievērojami finansiālie zaudējumi valsts budžetā (piemēram, 10 000 – 100 000 EUR)
		Negatīva publicitāte nacionālajos un dažos starptautiskajos plašsaziņas līdzekļos ar mērenu ietekmi uz reputāciju
		Stratēģiskie mērķi tiek ietekmēti, kavēsies dažu mērķa īstenošana līdz vienam gadam
2	Zema	Var rasties nebūtiski finansiālie zaudējumi valsts budžetā (piemēram, 1 000 EUR līdz 10 000 EUR)
		Negatīva publicitāte nacionālajos plašsaziņas līdzekļos ar īslaicīgu ietekmi uz reputāciju

Punktu skaitliskā vērtība	Skaitliskās vērtības nozīme	Skaidrojums
		Stratēģiskie mērķi tiek ietekmēti nebūtiski, var kavēties viena mērķa īstenošana līdz pusgadam
1	Ļoti zema	Var rasties nebūtiski finansiālie zaudējumi valsts budžetā (piemēram, līdz 1 000 EUR)
		Dažas nepamatotas relīzes/ raksti plašsaziņas līdzekļos ar īslaicīgu ietekmi, kam nav ietekmes uz reputāciju
		Netiek ietekmēti stratēģiskie mērķi

Projektu risku vadībā izmantojamā ietekmes novērtējuma skala var tikt pielāgota projekta risku izraisītajai ietekmei uz projekta ieviešanas termiņu, sadārdzinājumu, rezultātu sasniegšanu (18. un 19. tabula), taču arī projektu riskiem var vērtēt vides, reputācijas, drošības u.c. kritēriju ietekmi, atkarībā no projekta satura un konteksta.

18. tabula. Projekta risku ietekmes skalas piemērs (1. variants)

Punktu skaitliskā vērtība	Skaitliskās vērtības nozīme	Ietekme uz projektu		
		Termiņš	*Finansiāla ietekme (**izmaksu pieaugums**)*	*Rezultāts*
5	Ļoti liela	>6 mēneši vai >20%	>30 tk. EUR	Projekta sākotnējie mērķi netiks sasniegti. Nepieciešams pārskatīt projekta aktualitāti/ mērķus
4	Liela	3-6 mēneši/ 10-20%	20 tk. EUR – 30 tk. EUR	Projekta sākotnējie mērķi, visdrīzāk, netiks sasniegti. Nepieciešams pārskatīt projekta aktualitāti/ mērķus
3	Vidēja	1-3 mēneši/ 5-10%	10 tk. EUR – 20 tk. EUR	Projekta sākotnējie mērķi, visdrīzāk, tiks sasniegti
2	Maza	2-4 nedēļas/ 5-10%	4 tk. EUR – 10 tk. EUR	Projekta sākotnējie mērķi tiks sasniegti ar nelielu novirzi
1	Ļoti maza	1 nedēļa/ <1%	<4 tk. EUR	Projekta sākotnējie mērķi tiks sasniegti pilnā apmērā

19. tabula. Projekta risku ietekmes skalas piemērs (2. variants)

Punktu skaitliskā vērtība	Skaitliskās vērtības nozīme	Ietekme uz projektu		
		Termiņš	*Finansiāla ietekme (**izmaksu pieaugums**)*	*Rezultāts*
5	Ļoti liela	>3 mēneši	>30 tk. EUR	Projekta sākotnējie mērķi, visdrīzāk, netiek sasniegti. Nepieciešams pārskatīt projekta aktualitāti/ mērķus
3	Vidēja	1-3 mēneši	10 tk. EUR – 20 tk. EUR	Projekta sākotnējie mērķi, visdrīzāk, tiks sasniegti
1	Ļoti maza	<1 mēnesis	<4 tk. EUR	Projekta sākotnējie mērķi tiks sasniegti pilnā apmērā

Visiem tabulās iekļautajiem skaidrojumiem ir indikatīvs jeb provizorisks raksturs, jo kritēriju vērtības jāpiemēro iestādes darbības nozares specifikai.

Praksē varbūtības un ietekmes novērtēšanai izmanto iestādes vai citu organizāciju iepriekšējo pieredzi, vēsturiskos datus, ekspertu prognozes un balstās uz risku īpašnieku pieredzi attiecīgajā jomā, kā arī iestādes spēju ietekmēt risku tendences, cēloņus un sekas.

Atsevišķos gadījumos kā papildu risku novērtēšanas kritērijs var tikt izmantota risku **atklāšanas iespēja**, tas ir, vai riska pazīmes vai iestāšanos varētu atklāt un viegli laicīgi pamanīt bez īpašām aktivitātēm, vai riska atklāšanai nepieciešami specifiski risinājumi, vai to varētu atklāt tikai ārpus iestādes (tādējādi informācija par risku līdz iestādei var atnākt novēloti un nepilnīgi)[28]. Šo kritēriju visbiežāk izmanto IKT drošības riskiem.

Piemērs: Iestādē pastāv risks par to, ka vienai no būtiskākajām IS faktiski ir tikai viens izstrādātājs un uzturētājs, šīs sistēmas nodošana citam uzturētājam, ja vienīgais pakalpojuma sniedzējs aiziet no Latvijas tirgus, būtu neiespējama vai ļoti apgrūtinoša. Tiek secināts, ka riska varbūtība ir 3, bet ietekme 5. Tika pieņemts lēmums veikt pārrunas ar esošo pakalpojuma sniedzēju, lai noskaidrotu, kādas garantijas un risinājumus tas varētu piedāvāt, lai sistēmas uzturēšanu atvieglotu, gadījumā, ja tas aizietu no tirgus. Papildu tam tika panākta vienošanās par papildu IS uzturēšanas instrukciju un dokumentācijas izstrādi. Pēc instrukciju saņemšanas riska ietekme tika samazināta uz 3.

Parasti riska līmeņa un vērtības noteikšanai izmanto kombināciju no varbūtības un ietekmes, t.i., piešķirtā varbūtības un ietekmes novērtējuma reizinājumu (skat. 5.6. un 5.8. nodaļu).

Lai novērtētu risku scenārijus atbilstoši to kategorijām (skat. 6. nodaļu) iestādes struktūrvienību, kuras varētu ietekmēt konkrētais risks, griezumā iespējams izmantot 18. pielikumā iekļauto veidlapu, kurā kolonnas "Varbūtības vērtējums (A)" un "Ietekmes vērtējums B" aizpilda, ņemot vērā katras struktūrvienības vadītāja individuālo piešķirto novērtējumu. Lai iegūtu vienotu kopējo novērtējumu, tiek aprēķināts vidējā varbūtības un ietekmes vērtība, kuras reizinot tiek iegūts vidējais riska līmenis. Šādā veidā iespējams konsolidēt konkrēta riska scenārija novērtējumu vienā struktūrvienībā, kurā ir izveidotas apakšstruktūrvienības.

5.5.2. Risku novērtēšanas metodes

Risku novērtēšanā var izmantot kvantitatīvas un kvalitatīvas metodes vai abu šo pieeju apvienojumu. Piemēram, varbūtībai izmantot kvalitatīvo vērtēšanas skalu, taču ietekmei izmantot aptuvenu aprēķinu par sagaidāmajām papildu izmaksām, kas iestādei varētu rasties, riskam iestājoties.

Kvalitatīvais risku novērtējums fokusējas uz risku rašanās iespējamību un to, kā tas ietekmēs iestādi (piemēram, finansiāli, juridiski, reputāciju u.c.). Kvalitatīvā risku novērtēšanas metode ir piemērota valsts iestādēm, kā arī privātajam sektoram, gadījumos, kad riski ir ļoti nenoteikti un

[28] Kvalitatīva risku novērtēšanas metode, kas ietver atklāšanas iespēju: DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis | EC-Council (eccouncil.org)

grūti prognozējami, kā arī nozarēs, kurām nav raksturīga un nepieciešama detalizēta katras darbības uzskaite (piemēram, kā tas ir automatizētā ražošanā vai komercbanku nozarē u.tml.).

Kvantitatīvā pieeja risku varbūtības vērtēšanā paredz matemātisku vai skaitlisku varbūtības vērtības piešķiršanu attiecīgajam riska scenārijam, vai vairākiem tā apakšscenārijiem. Kvantitatīvā pieeja risku ietekmes vērtēšanā paredz skaidrus skaitliskus aprēķinus risku ietekmes noteikšanai atbilstoši iepriekš definētai ietekmes skalai un ņemot vērā pagātnē īstenojušos risku izraisītās sekas, tostarp faktiskos zaudējumus.

Iestādei, kura pirmo reizi vērtēs riskus, analīze, visticamāk, būs intuitīva un vienkāršāka. Turpretī iestādei, kas katru gadu vērtē un analizē riskus, būs uzkrājusies pieredze, vēsturiskie dati, kas var tikt izmantoti precīzākā vērtēšanā.

Svarīgi: Risku novērtēšanas kritērijiem un skalai jābūt izveidotai (vadības apstiprinātai) pirms tiek uzsākta pilnvērtīga risku identificēšana. Par to jābūt vienādai izpratnei visos līmeņos - gan augstākajai iestādes vadībai, gan arī pārējiem riska novērtēšanas procesā iesaistītajiem.

Iestādei jānosaka tāda risku novērtēšanas skala, kas atspoguļo tai atbilstošas risku materialitātes pakāpes, piemēram, visā iestādē kopumā par būtiskiem riskiem tiek uzskatīti tādi, kuru novērtējums ir xy un par nebūtiskiem vai ļoti zemiem, tādi, kuru novērtējums ir yx, kur xy>yx.

Ja dažām mazāka izmēra struktūrvienībām, vērtējot riskus, šī skala šķiet nepiemērota, tā nav jāpielāgo un jāmaina, jo mērķis ir apzināt iestādes risku kopumu.

Katrai struktūrvienībai un tās vadītājiem jāpārvalda savā pārziņā esošie riski jebkurā gadījumā, un tas ļauj tiem strādāt ar riskiem, pat, ja tie iestādes kopējā līmenī nav novērtēti kā ļoti būtiski.

Iestādes augstākās vadības interesēs ir saņemt risku sarakstu ar novērtējumu un riska līmeni, kam ir skaitliskā vērtība, lai spētu pieņemt lēmumu par riskiem, kuriem nepieciešama tūlītēja vai prioritāra rīcība to mazināšanai, kā arī vienoties par riskiem, kuri var tikt uzskatīti par pieņemamiem (t.i., to mazināšanai nav jāveic papildu pasākumi, vai arī tos var risināt vēlāk).

Analizējot riskus, var rasties situācijas, kad nesakrīt viedokļi, ir subjektīvie uzskati, risku uztvere un spriedumi. Tāpat to var ietekmēt arī izmantotās informācijas kvalitāte, izdarītie pieņēmumi un izņēmumi, ar izvēlētajām metodēm saistītie ierobežojumi un veids, kā šīs metodes tiek lietotas. Visus šos aspektus jāņem vērā risku novērtēšanā, nepieciešamības gadījumā jādokumentē un jāinformē par tiem lēmumu pieņēmējus. Risku novērtējuma dokumentācija, it īpaši aktualizējot novērtējumu (tam mainoties), palīdzēs nodrošināt pieņemto lēmumu izsekojamību.

Piemērs: Administratīvais departaments identificējis iepirkuma veikšanas risku, ka savlaicīgi netiek veikts jaunu biroja mēbeļu iepirkums. Taču tā kā iestāde saskaras ar daudz citiem nozīmīgākiem riskiem, tad šis risks varētu būt nenozīmīgs, ja salīdzina to ar, piemēram, risku, ka pamatdarbības nodrošināšanai nepieciešamās informācijas sistēmas funkcionalitāte ir novecojusi (Informācijas tehnoloģiju departamenta identificēts informācijas sistēmu uzturēšanas risks), un līdz ar to svarīgāk

ir nodrošināt ātrāku tās pilnveidošanu/ atjaunošanu, lai struktūrvienībām būtu iespējams īstenot funkcijas un uzdevumus, nevis atjaunot biroja mēbeles.

Neskatoties uz atšķirīgiem risku līmeņiem, abu struktūrvienību vadītājiem jāreaģē uz attiecīgajiem riskiem un jāievieš pasākumi risku mazināšanai.

5.5.3. Stresa testēšana

Stresa testēšanu var izmantot kā risku novērtēšanas metodi vai kā risku kvantificēšanas metodi (skat. 5.6. nodaļu).

Stresa testēšana (vai arī stresa testi) ir process, kura laikā tiek novērtēta iestādes spēja turpināt darbu un uzturēt svarīgus pakalpojumus arī ārkārtas situācijās, piemēram, dabas katastrofu gadījumos, finanšu krīzēs, politiskās krīzēs utt. Šāda veida testēšana ir svarīga, lai nodrošinātu iestādes spēju turpināt darbu un nodrošināt pakalpojumus arī neplānotās situācijās, kas varētu negatīvi ietekmēt darbības turpināšanu.

Iestādes stresa testēšanas mērķis ir novērtēt iestādes spēju pārvaldīt un koordinēt situācijas, kas varētu ietekmēt iestādes vai plašāk valsts darbību un drošību. Stresa testēšanas procesā tiek novērtēts, kā iestāde spēj risināt iespējamos riskus stresa situācijās, kā arī kādas būtu sekas, ja tie netiktu pienācīgi risināti. Stresa testi var ietvert situāciju simulācijas, izmantojot gan reālu, gan virtuālu vidi, lai novērtētu darbinieku spējas un iestādes infrastruktūru. Stresa testēšana var ietvert dažādus elementus, piemēram, organizatoriskos, komunikācijas un interneta sakarus, tehniskos un cilvēkresursus. Šādi testi palīdz novērst iespējamos riskus un nodrošināt, ka iestāde ir sagatavota efektīvai reaģēšanai uz ārkārtas situācijām.

Piemērs (stresa testi):

- Iestādē nav pieejami interneta sakari vismaz trīs dienas, kāda būs ietekme uz informācijas sistēmu darbību, attālināto darbu un pamatdarbības funkcijām pēc vienas, divām un trīs dienām? Būtu jānosaka procesi un funkcijas, kas varēs turpināties un, kam ir pieejami alternatīvi risinājumi, kā arī funkcijas, kuras nevarēs īstenot. Pēc tam jānovērtē, kāda būs ietekme uz funkcijām, kas neturpināsies – neapkalpotie klienti, apturēta dokumentu un finanšu plūsma, ietekme uz iestādes budžetu, ietekme uz drošību, ja netiek sniegti sabiedrībai nepieciešami pakalpojumi un tamlīdzīgi. Būtu jānosaka, cik ilgs pārtraukums radīs kritiskas sekas, piemēram, ja izziņas, ko sniedz iestāde, netiek izsniegtas vairāk nekā nedēļu, tiek būtiski kavēti arī citu iestāžu procesi.
- Bīstamu infekcijas slimību, pandēmijas un epidēmijas dēļ iestādē nav pieejams personāls pamatdarbības funkcijās – darbinieku īpatsvara trūkums 10%, 20%, 35% no funkciju īstenošanā iesaistītajiem darbiniekiem, vai un kādas būs izmaiņas darba organizācijā, kā tas ietekmēs ikdienas darbu, procesu īstenošanu? Kāda būs ietekme uz sasniedzamajiem mērķiem un iestādes finansējumu, ārējiem klientiem sniegtajiem pakalpojumiem?

Stresa testu rezultātus var izmantot darbības nepārtrauktības risinājumu darbības novērtēšanai. Piemēram – pārbaudīt sakaru pakalpojumu sniedzēja iespējas nodrošināt

alternatīvu sakaru kanālu (tehnisko risinājumu) un, ja identificētas nepilnības, veikt grozījumus līguma nosacījumos, tai skaitā nosakot papildu atbildību ārkārtas situācijā.

Iestādei ir svarīgi regulāri veikt stresa testēšanu, lai nodrošinātu pārliecību, ka tā spēj tikt galā ar dažādiem izaicinājumiem un saglabāt nepārtrauktu iestādes darbību. Stresa testēšana palīdz identificēt vājās vietas un plānot papildus pasākumus iestādes darbības pilnveidei. Svarīgi atzīmēt, ka stresa testēšana ir ilgtermiņa process, kas jāveic regulāri, lai novērtētu iestādes spējas un uzlabotu tās, kad tas ir nepieciešams.

Lai praksē varētu veikt stresa testēšanu, iestādēm būtu jāizveido speciālas izglītības un apmācības programmas, lai darbinieki būtu sagatavoti reaģēt šādās situācijās. Šāda apmācība var ietvert krīzes pārvaldību, vadību, sadarbību un komunikāciju, darbības nepārtrauktības plānu izstrādi. Tāpat šos plānus nepieciešams faktiski testēt, lai pārliecinātos par to faktiskajām īstenošanas iespējām un, ka darbinieki zinās, kā būtu jārīkojas ekstrēmos apstākļos.

5.5.4. Būtiskāko risku noteikšana

Būtiskākie jeb prioritārie riski ir tie, kam ir augstākā iestāšanās varbūtība un ietekme. Iestādei jānosaka, kuri riski (risku līmeņi) tiek uzskatīti par būtiskajiem, atkarībā no risku apetītes, risku vadības pieejas, kapacitātes, kā arī mērķiem, tas ir, kāda rīcība un papildu darbības paredzētas būtiskāko risku vadībai.

Risku analīzes rezultātā iegūto būtisko risku saraksts ir izmantojams iestādes stratēģijas un ikgadējo darba plānu sagatavošanas posmā, sasaistot risku ietekmi uz iestādes stratēģiskajiem mērķiem un sasniedzamajiem darbības rādītājiem, kā arī, plānojot resursus, kas nepieciešami risku mazināšanai (piemēram, ja nepieciešami konkrēti finanšu resursi budžetā, vai IS projekti, kas jāieplāno kopējā IKT projektu kalendārā).

Lai precīzi definētu riskus, kas iestādē uzskatāmi par būtiskiem, jāizmanto iepriekš aprakstītie risku novērtēšanas kritēriji, piemēram, nosakot, ka riski ar konkrētu varbūtības, ietekmes un atlikušā līmeņa novērtējumu uzskatāmi par būtiskiem (piecu līmeņu skalā par būtiskiem riskiem uzskata tos, kuriem piešķirts varbūtības un ietekmes vērtējums - 4 un 5).

Papildu pazīmes, kas var liecināt, ka riski uzskatāmi par būtiskiem:

- riski attiecas uz visu iestādi vai vairākiem tās procesiem vai struktūrvienībām;
- risku vadībai (mazināšanai) nepieciešami ievērojami laika, finanšu, cilvēkresursi (tai skaitā vairāku struktūrvienību iesaiste, kā arī iespējams ārējo pušu iesaiste un atbalsts), materiālie resursi;
- riski tieši ietekmē vai apdraud iestādes stratēģiskos / augstākā līmeņa mērķus.

Risku vadības hierarhijā, prioritizējot riskus, var nodalīt atsevišķas risku dimensijas (20. tabula).

20. tabula. Risku dimensijas

Dimensijas nosaukums	Dimensijas apraksts
Stratēģiskie riski	Stratēģiskie riski ir kompleksi riski, kas ietekmē visu iestādi kopumā, apdraud tās stratēģisko mērķu izpildi un darbību. Bieži vien tie ir saistīti ar ārējiem faktoriem. To pārvaldībai ir nepieciešami būtiski resursi, sarežģīti lēmumi un citu pušu iesaiste. Šiem riskiem noteikti jābūt iestādes augstākās vadības un citu līmeņu vadītāju redzeslokā.
Operacionālie riski	Operacionālie riski ir dažādu veidu, jomu un tēmu riski iestādes struktūrvienību, funkciju, darbības virzienu vai procesu līmenī (t.i. tie nav tik apjomīgi, ka ietekmētu pilnīgi visu iestādi kopumā kā stratēģiskie riski). Operacionālo risku portfeļus veido jomās, kuras iestādei būtiskas un jāspēj demonstrēt laba pārvaldība. Arī par būtiskajiem operacionālajiem riskiem ar zināmu regularitāti jāinformē iestādes augstākā vadība, taču pārsvarā uz šiem riskiem jāreaģē vidējā un augstākā līmeņa vadītājiem.
Ikdienas riski	Ikdienas operacionālos riskus vada struktūrvienību vadītāji, izmantojot pieredzi savas kompetences jomā, un kuri uzrauga gan ārējo vidi, gan iekšējo vidi, un spēj identificēt potenciālos riskus, ņemot vērā pieredzēto dinamiku un operatīvi pievērsties to ierobežošanai. Ikdienas riskus pārsvarā nav nepieciešams atsevišķi apzināt, aprakstīt un reģistrēt risku reģistrā, jo bieži vien tie tiek mazināti ātri, operatīvi ikdienas darbībās dažādu līmeņu darbiniekiem, veicot savus tiešos darba pienākumus.

Padoms: Komunikācijai par būtiskajiem riskiem jābūt regulārai, formāli noteiktai iestādes iekšējos procesos un tajā jāiesaista iestādes dažādu līmeņa vadītāji.

Piemērs: Būtisko risku statusa analīze veicama reizi ceturksnī, izvērtējot risku tendences un risku mazināšanas pasākumu ieviešanas statusu regulārajās vadības sanāksmēs. Ziņošana par būtiskajiem riskiem jānodrošina attiecīgajiem risku īpašniekiem sadarbībā ar risku vadītāja metodisko atbalstu vai risku vadītājam, ņemot vērā risku īpašnieku sniegto informāciju.

Padoms: Riski, kas nav novērtēti kā būtiski, būtu risināmi iestādes operatīvajā līmenī. Komunikācija par tiem var notikt ne tik regulāri, kā par būtiskajiem riskiem un ne vienmēr vai vispār neiesaistot augstāko vadību. Taču ja, šo risku risināšanai nepieciešami samērīgi resursi un tie novērš zināmus apgrūtinājumus kādā konkrētā struktūrvienībā vai procesā, to pārvaldību nevajadzētu atlikt vai ignorēt.

Ja risku analīzes rezultātā secināts, ka tam ir zems līmenis, tas nozīmē, ka papildu rīcība nav nepieciešama (risks ir pieņemams), arī tas ir vērā ņemams risku vadības rezultāts.

5.6. Risku kvantificēšana – riska iestāšanās notikuma novērtēšana naudas izteiksmē (metodika, aprēķini, praktiski piemēri)

Risku kvantificēšana jeb riska kvantitatīvā analīze tiek veikta ar mērķi skaitliski analizēt katra riska varbūtību un ietekmi uz mērķu sasniegšanu. Riska kvantitatīvajā analīzē varbūtība tiek izmantota, lai nodalītu dažādus riska scenārijus vai kā ietekmes pastiprinātāja koeficientu.

Riska ietekmi var kvantificēt dažādās precizitātes pakāpēs atkarībā no pieejamajam datiem un to kvalitātes, piemēram:

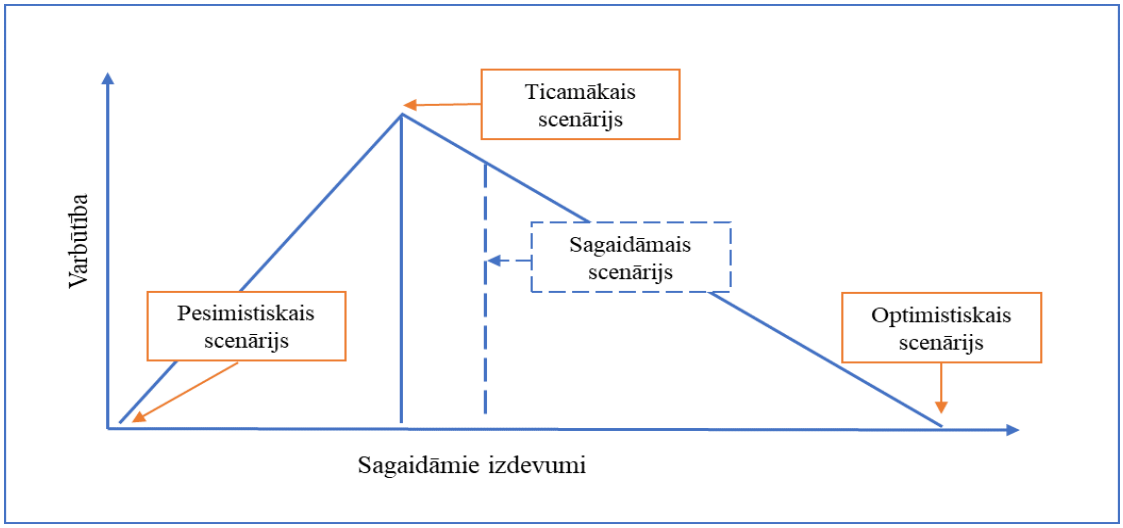
- **Finansiālā izteiksmē** kā potenciālo zaudējumu apjomu, ja iestādei ir pieejami vēsturiskie dati un ir iespēja precīzāk aprēķināt un modelēt, cik izmaksātu riska iestāšanās un cik bieži tas varētu notikt noteiktā laika periodā (piemēram, gada laikā);
- **Apjoma izteiksmē** kā potenciālo ietekmēto vai zaudēto vienību skaitu, līmeni, proporciju vai citu rādītāju, ja nav iespējams finansiāli novērtēt vidējo riska iestāšanās ietekmi vai arī riska iestāšanās scenāriji ir tik ļoti dažādi, ka vidējais zaudējumu skaits nebūtu korekts mērs;
- **Subjektīva aplēse** par potenciālo ietekmi, pamatojot pieņēmumus aplēsēm, piemēram, kā proporcija vai koeficients no citu zināmu rādītāju dinamikas, vēsturiskā dinamika, vidējie rādītāji valstī vai nozarē u.c.

Visbiežāk iestādes vadība un ieinteresētās puses vēlēsies apzināt riska potenciālo ietekmi naudas izteiksmē, turklāt, lielākajai daļai risku ietekme agri vai vēlu būs redzama vai izsakāma finansiāli. Finansiālā ietekme no riska iestāšanās var rasties ieņēmumu vai izdevumu daļā un visbiežāk to mēra budžeta pārskata periodā – viena kalendārā gada ietvaros, bet var mērīt arī ilgākā periodā.

Viena no iespējām kvantificēt riskus monetāri publiskajā sektorā ir izmantot finanšu modeļus un rēķināt potenciālos finanšu zaudējumus, kuri var rasties no dažādiem riskiem. Pasaulē tiek izmantotas daudzas risku kvantitatīvās analīzes metodes, no kurām visbiežāk lietotās ir šādas:

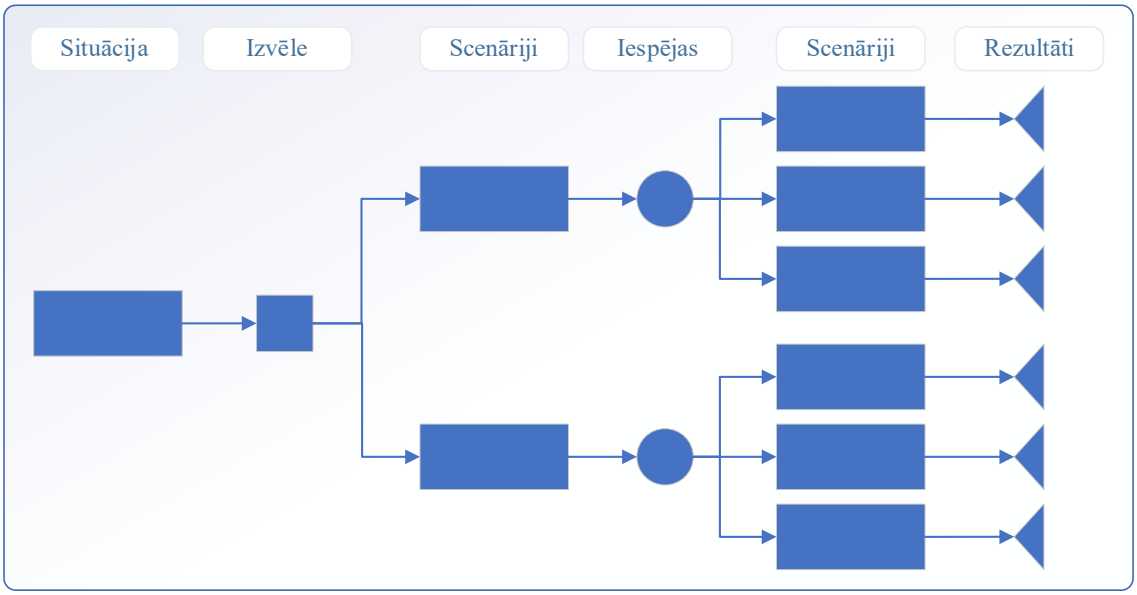
- **Trīs punktu novērtēšana** (*Three-points estimation* – angļu val.) (16. attēls) – tiek veidoti un salīdzināti trīs attīstības scenāriji: optimistiskais (viss notiek kā plānots, bez sarežģījumiem), ticamākais (rodas dažādi šķēršļi, bet sekmīgi tiek pārvarēti) un pesimistiskais (ja nekas nenotiek pēc plāna), mainoties dažādiem pieņēmumiem. Matemātiski izrēķinot aritmētisko vidējo no visiem trīs scenārijiem, var noteikt sagaidāmo scenāriju, kas varētu raksturot riska ietekmi. Iestādes varētu izmantot šādu scenāriju analīzi, lai novērtētu iespējamo risku ietekmi uz tām pieejamo finansējumu.

16. attēls. Sagaidāmo izdevumu scenāriji



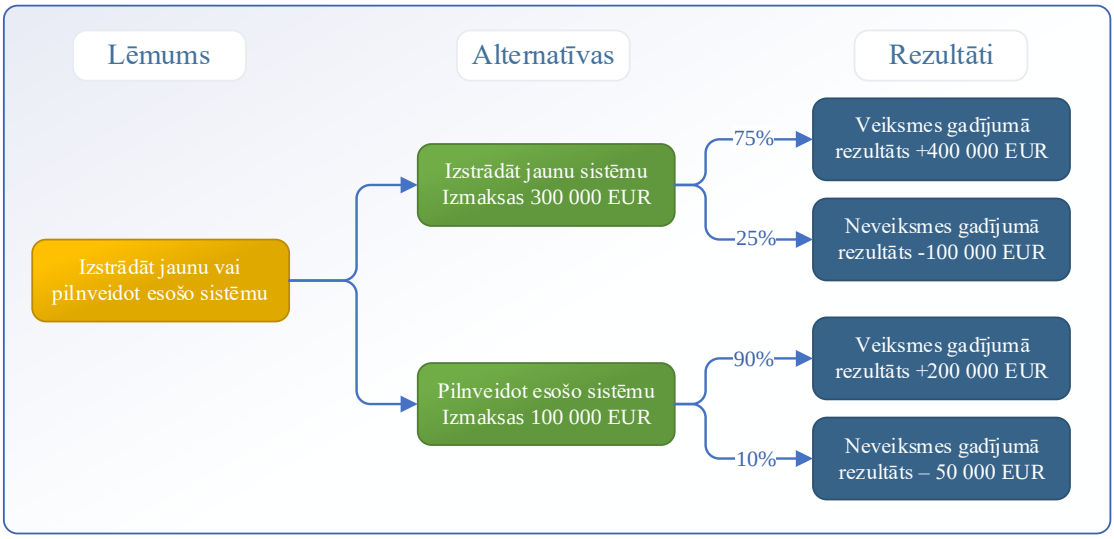
- **Lēmumu pieņemšanas analīze** – tiek veidota diagramma (17. attēls), kas vizuāli parāda dažādu alternatīvo izvēles scenāriju radītās iespējas, tālākas rīcības scenārijus, rezultātus jeb sekas. Šī metode palīdz kompleksu un sarežģītu problēmu risināšanā un dod iespēju apskatīt dažādus rīcības scenārijus, tai skaitā, scenāriju, kurā nekas netiek darīts, kas tiek salīdzināts ar dažādiem aktīvas rīcības scenārijiem.

17. attēls. Lēmumu pieņemšanas analīze



- **Sagaidāmā monetārā vērtība** – statistiska metode, kuru izmanto vadība pirms lēmumu pieņemšanas, lai apzinātu lēmuma iespējamos rezultātus un sekas un aprēķinātu nepieciešamību taupīt resursus (18. attēls). Šī metode paredz izstrādāt alternatīvos scenārijus, kas izriet no pieņemtā lēmuma un ar varbūtības palīdzību nosaka, cik sekmīgs varētu būt katrs no izvēlētajiem rīcības scenārijiem un plānotais ieguvums no katra scenārija realizācijas. Šāda scenāriju vērtēšana palīdz vadībai padziļināti salīdzināt dažādus alternatīvos rīcības scenārijus, ņemot vērā arī atdevi naudas izteiksmē.

18. attēls. Sagaidāmās monetārās vērtības analīze

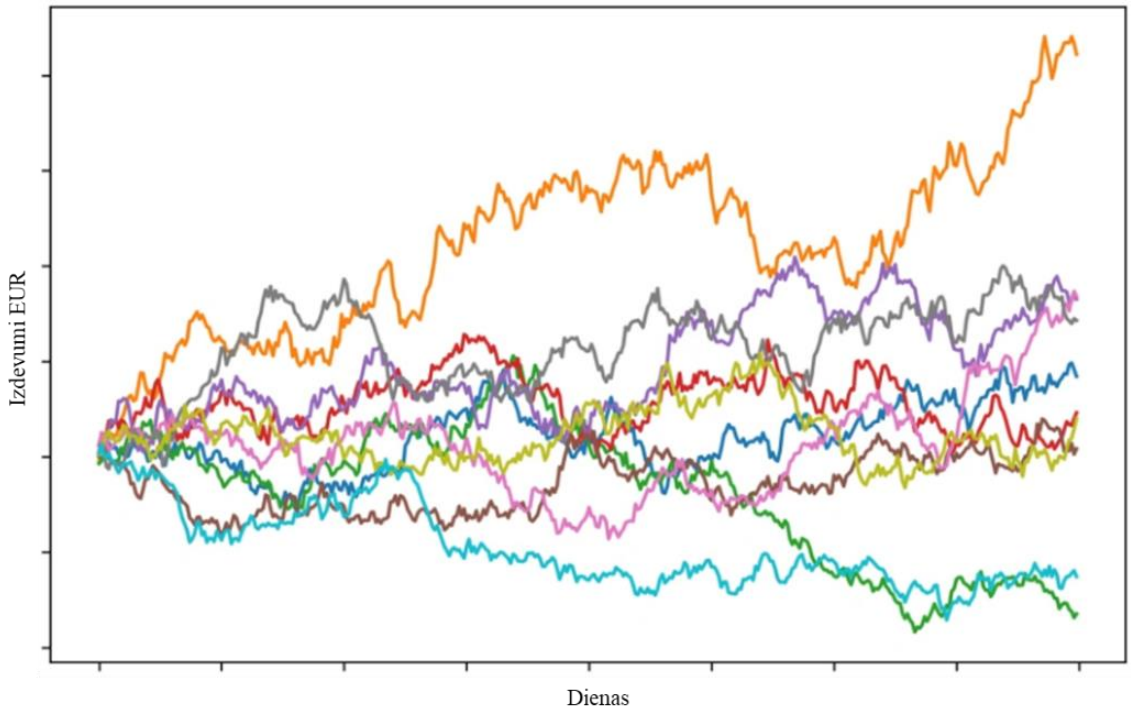


- **Monte Karlo analīze** – statistiska metode, kuru izmanto sarežģītāku matemātisku modeļu veidošanā, ģenerējot nejaušus mainīgos (19. attēls).

Šīs metodes atslēga ir izprast terminu "simulācija". Simulācijas veikšana sastāv no reālu raksturlielumu un to uzvedības atkārtošanas vai dublēšanas. Tādējādi Monte Karlo simulācijas galvenais mērķis ir mēģināt atdarināt reālo mainīgo uzvedību, lai pēc iespējas analizētu vai paredzētu, kā tie attīstīsies.

Šī metode tiek izmantota datorprogrammās, lai simulētu dažādus scenārijus un novērtētu to ietekmi uz iestādes finanšu līdzekļiem. Šādā veidā iestādes varētu novērtēt, kādas būtu risku sekas, ja, piemēram, iestātos ekonomiskā krīze, valsts neveiktu nepieciešamos reformu pasākumus vai ja būtu kāds cits faktors, kas ietekmētu iestāžu finanses.

19. attēls. Monte-Karlo metode



- **Finanšu modeļi –** tiek veidoti matemātiski modeļi, kas ļauj pētīt scenārijus atkarībā no riska iestāšanās, identificēt, kāda finansiāla ietekme radīsies uz iestādes darbību un budžeta izpildi. Iestādes varētu izmantot finanšu modeļus, lai novērtētu iespējamos zaudējumus no konkrētiem riskiem, piemēram, finanšu krīzēm, investīciju neatmaksāšanos vai dabas katastrofām. Šī metode ļauj novērtēt finanšu riskus un to ietekmi uz iestāžu budžetu.
- **Jutīguma analīze** – metode, kas pēta sakarības starp atkarīgajiem un neatkarīgajiem mainīgajiem un ļauj noteikt riskus, kuriem ir vislielākā ietekme. Lai veiktu jutīguma analīzi, koncentrējoties uz finanšu aspektiem, tiek aprēķinātas naudas plūsmas un ieguldījuma nākotnes vērtība jeb NPV (*Net Present Value* – angļu val.). Mainot vienu no mainīgajiem faktoriem, piemēram, riska ietekmē pieaugušās resursu izmaksas, izpildes laikus vai jebko citu, skatās, kas notiek ar jauno NPV vērtību un izrēķina procentuālo variāciju starp dažādajiem scenārijiem. No iegūtajiem rezultātiem par variācijām var secināt, kurš riska scenārijs visbūtiskāk ietekmē nākotnes ieguldījuma vērtību.
- **Iespējamo kļūdu un seku analīze** (*Failure Mode and Effects Analysis – FMEA* – angļu val.) – sistemātiska metode kļūdu atklāšanā un analizēšanā, lai organizētu preventīvu un korektīvu pasākumu plānošanu. Šīs metodes ietvarā tiek apskatīti visas iespējamās komponentes, sastāvdaļas un procesi, kas var potenciāli nedarboties un radīt kļūdu, kā rezultātā rodas novirze un ietekme uz sistēmas darbības rezultātu. Tādējādi tiek noteikti riski jeb kļūdas un to radītās sekas, kuras ir iespējams kvantificēt.

- **Ekspertu viedoklis** – metode, kuras ietvaros ar ekspertu palīdzību tiek veikta risku kvantificēta analīze gadījumos, kad nav pieejami nepieciešamie dati.

Iestādē pieejamie dati, to kvalitāte un detalizācijas pakāpe ietekmē to, kādas risku kvantificēšanas metodes var izmantot. Ja iestādei ir vēlme un vajadzība precīzi aprēķināt risku potenciālo ietekmi, ir nepieciešams savlaicīgi apzināt nepieciešamo datu kopumu.

Daži piemēri finansiālās risku ietekmes mērīšanai apkopoti 21. tabulā.

21. tabula. Risku finansiālās ietekmes piemēri

Ieņēmumu/pieejamā finansējuma zudums	Palielināti izdevumi/papildu izmaksas
• Laicīgi neapgūti un zaudēti budžeta līdzekļi; • Ierobežojumi budžeta līdzekļu pārvirzīšanā, neiztērētās daļas zaudēšana; • "Atņemti" jeb nepiešķirti budžeta līdzekļi pārkāpumu dēļ; • Nesaņemtas maksas par iestāžu maksas pakalpojumiem; • Krāpnieku radītie ieņēmumu zudumi.	• Sadārdzināts otrreizējais iepirkums; • Ēku, telpu, aprīkojuma atjaunošanas izmaksas; • Jauna aprīkojuma, iekārtu iegāde pilnīgas bojāejas gadījumā vai esošā aprīkojuma pielāgošana; • Ražotāja sniegtā atbalsta izmaksas, kas mazina risku sekas; • Patērētais darba laiks seku novēršanai izteikts finansiālā izteiksmē, ņemot vērā vidējās algas likmi; • Soda naudu apmērs; • IT sistēmu izmaiņu ieviešanas izdevumi; • Krāpšanas gadījuma zaudējumi.

Kopumā risku kvantificēšana publiskajā sektorā būtu svarīgs process, lai izprastu un novērstu iespējamās finanšu resursu zaudējumu sekas.

5.7. Reaģēšana uz riskiem, stratēģijas rīcībai ar riskiem, reaģēšanas uz riskiem pasākumu noteikšana, atlikušā riska novērtēšana, risku mazināšanas pasākumu efektivitātes novērtēšana

Risku vadības stratēģijai kopumā jābūt saistītai ar iestādes darbības plānu un pēc iespējas integrētai ar to. Visizplatītākās stratēģijas rīcībai ar riskiem ir:

- nodošana, pārcelšana/ risku sadalīšana;
- pieņemšana;
- izvairīšanās, atteikšanās no darbības, kas rada risku (piemēram, no sniegtā pakalpojuma, produkta izmantošanas, veiktā procesa vai tml.);
- riska mazināšana.

Tās plašāk aprakstītas un izskaidrotas nākamajā Rokasgrāmatas nodaļā.

Rīcības, reaģējot uz riskiem, ir tieši atkarīgas no risku novērtējuma un resursiem, kas tiek patērēti risku mazināšanai. Ieguldītajiem resursiem un īstenotajām rīcībām jābūt samērīgām salīdzinājumā ar ieguvumu no riska mazināšanas (skat. 5.7.4. nodaļu).

5.7.1. Reaģēšana uz riskiem, stratēģijas rīcībai ar riskiem

Stratēģija rīcībai ar riskiem ir atkarīga no iestādes kopējās risku apetītes, tolerances un vispārējās risku vadības politikas.

Lai adekvāti reaģētu uz riskiem, nepieciešams izprast, kādas darbības nepieciešams īstenot, ja risks pārsniedz pieļaujamo līmeni/ risku apetīti.

Iespējamās risku vadības stratēģijas var būt:

1. **Riska nodošana** – pārveidojot procesu, lai samazinātu riska varbūtību/ ietekmi, piemēram, sadalot to vairākos procesos un vienlaikus pārdalot resursus vai arī riska nodošana citiem sadarbības partneriem, nododot kādu procesa daļu vai arī apdrošinot risku. *Riska nodošana* vai dalīšanās ar risku visbiežāk ir iespējama, izmantojot sadarbību ar trešajām pusēm, piemēram, apdrošināšanas formā, t.i. apdrošinot riska scenāriju un sekas, lai riska iestāšanās gadījumā būtu pieejams atbalsts riska seku novēršanai. Otrs veids, kā dalīties ar risku, ir izvērtēt sadarbības un līguma nosacījumus ar ārējiem partneriem un ieinteresētajām pusēm. Lai vadītu riskus, šādā veidā jāveic pārrunas ar partneriem par līguma nosacījumiem, iespējams pārskatot līguma prasības, sagaidāmo rīcību no partneriem, precizējot kvalitātes u.c. nosacījumus;
2. **Riska pieņemšana** – riska līmeņa akceptēšana, neieviešot risku mazinošos pasākumus, nepilnveidojot iekšējās kontroles. Šo stratēģiju izmanto tikai tad, ja nav iespējams noteikt papildu jaunus risku kontroles pasākumus vai arī, ja kontroles pasākumu ieviešana nav ekonomiski izdevīga, kā arī, ja varbūtība riskam salīdzinājumā ar ieguldāmajām investīcijām ir tik liela, ka nav ekonomiski un lietderīgi tērēt šos līdzekļus. Riska līmenis var būt *pieņemams* gadījumā, ja iestādei nav objektīvu iespēju to mazināt ar samērīgiem līdzekļiem, ir ieviestas esošās kontroles, kas ir pietiekami efektīvas riska vadībai (t.i. kontroles tiek īstenotas un novērš riska iestāšanās varbūtību vai mazina tā ietekmi un riska līmenis atbilst iestādes riska apetītei). Risku statusa un izmaiņu uzraudzība ir svarīga un jāveic visu veidu riskiem, taču pieņemamajiem riskiem, tā, iespējams, ir vienīgā no papildu veicamajām aktivitātēm. Riska pieņemšana var tikt izmantota arī, ja riska kontrole atrodas ārpus iestādes kompetences. Alternatīva šai darbībai ir kāda pilnveidošanas pasākuma apturēšana vai pārtraukšana, ja riska varbūtība ir liela un iestāde nespēj to ietekmēt nekādā veidā.

Piemērs: Iestādes **risks**, ka struktūrvienībā var nebūt pietiekama darbinieku, kuri būtu atbildīgi par attīstības plānošanas sistēmas dokumentu sagatavošanu, kompetence. Šis ir vidēji zems risks un tam ir noteikts **mazinošais pasākums** – nosūtīt struktūrvienības darbinieku vienu reizi divu gadu laikā uz Valsts administrācijas skolas mācību kursu par attīstības plānošanas sistēmu un tās dokumentēšanu (mācību kurss tiek regulāri pilnveidots, ņemot vērā izmaiņas normatīvajos aktos, kas reglamentē šīs sistēmas ieviešanu un uzturēšanu, kā arī kursu dalībnieku sniegto informāciju par problēmām, sagatavojot šos dokumentus). Līdz ar to šī riska mazinošais pasākums jeb esošā kontrole jāturpina īstenot, jo mācību programma tiek aktualizēta. Taču nepieciešams vērtēt riska tendences, jo pastāv iespēja, ka riska varbūtība var pieaugt, ja, piemēram, šī apmācītā darbinieka vietā atnāk jauns darbinieks.

3. **Izvairīšanās** no riska ir iespējama, atsakoties no procesa vai aktivitātes, kurā risks var rasties, nepieļaujot riskam īstenoties. Šo stratēģiju iespējams izmantot, ja tā nav pretrunā ar tiesību aktos noteiktajām prasībām. Taču bieži vien šāda iespēja praksē nepastāv, jo iestāde nevar atteikties no pakalpojumiem, ko tā sniedz, no kādiem ārējiem apstākļiem vai nosacījumiem, kas jāievēro vai tiešā veidā ietekmē iestādes darbību vai arī riski skar iestādes pamata

procesus un funkcijas. Tādā gadījumā ar risku ir jāsadzīvo un jāpieņem pēc iespējas izsvērti un uz informāciju un datiem balstīti lēmumi;

4. **Risku mazināšana**:
   - riska līmeņa samazināšana, ieviešot pasākumus riska ietekmes/ varbūtības mazināšanai līdz pieļaujamajam riska līmenim (riska apetītei);
   - riska rašanās cēloņu novēršana, izvēloties citu procesa/ pakalpojuma pārveides īstenošanas plānu, kurā šis risks vairs nevar rasties;
   - riska ietekmes mazināšana, veicot papildu darbības, kas iepriekš plānā netika paredzētas, bet, kuras savlaicīgi veicot, gadījumā, ja risks iestātos, tā ietekme būtu ļoti minimāla vai tās nebūtu vispār;
   - riska ietekmes novēršana, jau iepriekš pieņemot, ka risks noteikti iestāsies, un jau iepriekš īstenojot visas tās darbības, un, veicot preventīvās kontroles, lai novērstu potenciālos draudus.

Risku mazināšana ir dažādu risku mazināšanas pasākumu ieviešana (skat. piemērus turpmāk šajā nodaļā). Visiem risku mazināšanas pasākumiem jānosaka termiņi un atbildīgie, līdz ar to nedrīkst pieļaut situāciju, ka par risku mazināšanu atbildīgie nav informēti par uzdotajiem uzdevumiem, pieņemtajiem lēmumiem un sagaidāmajiem termiņiem uzdevumu izpildei.

Riska mazināšana ir izplatītākā stratēģija rīcībai ar riskiem un tā nozīmē kontroļu ieviešanu, iekšējās kontroles sistēmas uzturēšanu, risku mazināšanas pasākumu īstenošanu. Šo pasākumu mērķis nav pilnībā novērst riskus, taču samazināt un kontrolēt tos, līdz pieņemamam līmenim (vai atbilstoši iestādes risku apetītei, ja tāda noteikta). Tādējādi arī pēc risku mazināšanas pasākumu ieviešanas riski vēl var pastāvēt, taču ar zemāku riska līmeņa novērtējumu un/vai kļūt jau pieņemami.

Apsverot un apstiprinot jebkuru no risku vadības stratēģijām, ir jāizvērtē nepieciešamie resursi un ieguldījumi pret potenciālajiem ieguvumiem, risku mazinot vai novēršot. Ir vērtējami ne tikai finansiālie un materiālie aspekti, bet arī iestādes ieinteresēto pušu un partneru prasības un intereses, kā arī nosacījumi un saistības, kas iestādei jāievēro (skat. 5.7.1. nodaļu).

Svarīgi! Jebkuru no pieņemtajiem riska vadīšanas paņēmieniem (gan pieņemamiem riskiem, gan tādiem, kam nepieciešams risku mazināšanas pasākumu plāns) ir jāapstiprina atbilstošā līmenī. Būtiskajiem un stratēģiskajiem iestādes riskiem - šo pieeju apstiprina iestādes augstākā vadība.

Padoms! Riskiem ar augstu ietekmi un zemu iestāšanās varbūtību, piemēram, darbības nepārtrauktības risku gadījumā var būt noderīga stresa testēšanas pieeja, jo šādiem scenārijiem ir grūti paredzama varbūtība, taču ir svarīgi izstrādāt un apzināt risku mazināšanas pasākumus (esošos un ieviešamos), lai incidenta gadījumā spētu pēc iespējas risināt situāciju un tai pēc iespējas sagatavotos (Stresa testēšana aprakstīta 5.5.3. nodaļā).

Izplatītākie risku mazināšanas pasākumu veidi ir šādi:

- Atbildības noteikšana un nodalīšana;

- Datu analīze un kontroles;
- Mācības un konsultācijas;
- Tehniskās kontroles, infrastruktūras risinājumi;
- Izlases veida pārbaudes;
- Automatizētās informācijas sistēmas (turpmāk – IS) kontroles, IS risinājumu ieviešana;
- Stratēģiskie lēmumi, rīcības plāni;
- Analīzes, izpētes, incidentu izmeklēšanas, aptaujas;
- Metodiku un normatīvu izstrāde;
- Iekšējās diskusijas, lēmumu pieņemšana;
- Auditi un juridiskie izvērtējumi.

5.7.2. Reaģēšanas uz riskiem pasākumu noteikšana

Reaģēšanas uz riskiem pasākumu noteikšanā piedalās:

- risku īpašnieks;
- risku mazināšanas pasākumu ieviesēji (t.i., darbinieki, kuri uztur esošās kontroles, kā arī potenciālie jauno kontroļu ieviesēji);
- risku vadītājs;
- iestādes vadība (padomes/valdes locekļi, struktūrvienību vadītāji) atkarībā no risku līmeņa (stratēģiskajiem un būtiskajiem riskiem).

Risku mazināšanas pasākumiem un ieviešamajām kontrolēm jābūt pēc iespējas precīzāk definētām, konkrētām, reāli izdarāmām, kura ieviešanai ir piekritušas iesaistītās puses (t.i. riska īpašnieks un citi iesaistītie darbinieki) un šo pasākumu ieviešanai ir pieejami atbilstoši resursi.

Apzinot risku apstrādes darbības, jānosaka šādi aspekti:

- risku mazināšanas pasākuma ieviešanas termiņi;
- atbildīgie par risku mazināšanas pasākumiem;
- nepieciešamie resursi papildu ieviešamajiem risku mazināšanas pasākumiem (finanšu, laika, darbinieku, tehniskie u.tml.);
- kurus riska indikatorus vai darbības rādītājus risku mazināšanas pasākums ietekmēs (lai piefiksētu to, vai pasākums darbojas kā iecerēts).

Lai noteiktu risku mazināšanas pasākumus, iespējams nepieciešama padziļināta izpēte, ko var īstenot, veidojot darba grupas, kas var veikt papildu analīzi, jo var būt situācijas, ka sākotnēji identificējami tikai pirmie vai vispārīgie soļi risku vadībai, un tos nepieciešams sadalīt pa posmiem un precizēt. Piemēram, ieviešamā kontrole ir jaunas informācijas sistēmas funkcionalitātes izveide, un tās soļi būtu:

- Funkcionalitātes mērķa noteikšana darba grupā;
- Prasību izstrāde;
- Iepirkuma organizēšana;
- IS izstrādātāja izvēle;
- IS izstrāde;
- IS testēšana;
- IS ieviešana produkcijas vidē;
- Procedūru pielāgošana.

5.7.3. Atlikušā riska novērtēšana

Lai noteiktu atlikušā riska līmeni, vispirms var noteikt sākotnējā riska līmeni, iedomājoties situāciju, kāda būs riska varbūtība un sekas, ja vispār nav ieviestas un apstiprinātas iekšējās kontroles (22. tabula).

Pēc tam jāidentificē ieviestās iekšējās kontroles, kas mazina riska līmeni, un, balstoties uz profesionālo spriedumu, nepieciešams novērtēt riska atlikušo līmeni, vai un cik lielā mērā tiek samazināts riska līmenis, ja tiek efektīvi īstenotas šīs kontroles.

Bieži vien praksē iestādes uzreiz vērtē atlikušo risku, jo sākotnējais risks ir vairāk teorētisks, jo iestādes riskiem ir noteiktas un tiek īstenotas esošās iekšējās kontroles, attiecīgi šie riski tiek mazināti līdz atlikušā riska līmenim.

Analizējot jaunus riskus, kas radušies iekšējo vai ārējo apstākļu izmaiņu rezultātā, un nosakot to atlikušo riska līmeni, iespējams ņemt vērā iekšējās kontroles, kas samazina to sākotnējo līmeni. Taču, ja riska līmeni mazinošas iekšējās kontroles nav ieviestas, tad tiek noteikts riska sākotnējais līmenis, paredzot jaunas riska mazināšanas kontroles (risku mazinošos pasākumus). Pēc to ieviešanas, veicot risku līmeņa pārskatīšanu, tiks noteikts atlikušais riska līmenis (11. pielikums).

22. tabula. Riska sākotnējais un atlikušais līmenis

NPK	Risks, riska notikuma apraksts	Riska klasifikators	Varbūtība	Ietekme	Riska vērtība	Sākotnējais riska līmenis	Esošie riska kontroles pasākumi	Varbūtība	Ietekme	Riska vērtība	Atlikušā riska līmenis	Riska vadības stratēģija
1	2	3	4	5	6	7	8	9	10	11	12	13
1	Var savlaicīgi netikt veikts jaunu biroja mēbeļu iepirkums	Operacionālais riski	5	2	10	Ļoti augsts	Apstiprināta iepirkumu veikšanas procedūra, kas paredz iepirkumu veikšanas kārtību, tostarp iepirkumu dokumentācijas sagatavošanas termiņus	3	2	6	Vidējs	Riska mazināšana
2	IT sistēmu funkcionalitāte ir novecojuši un nav iespējama datu pārnese starp informācijas sistēmām, kā arī nav iespējams ģenerēt pārskatus	Operacionālais risks	5	5	25	Ļoti augsts	Apstiprināta IKT uzturēšanas kārtība, kas paredz informācijas sistēmu administrēšanas procedūru. (Nenodrošina riska līmeņa samazināšanu, jo šī kārtība nenosaka informācijas sistēmu izmaiņu pieprasījumu sagatavošanas un virzības kārtību) Apstiprināta kārtība, kādā tiek nodrošinātas IKT sistēmu drošības prasības (Nenodrošina riska līmeņa samazināšanu, jo šī kārtība attiecās tikai uz IKT drošības prasībām, nevis jaunas funkcionalitātes ieviešanu IS)	4	4	16	Ļoti augsts	Riska mazināšana

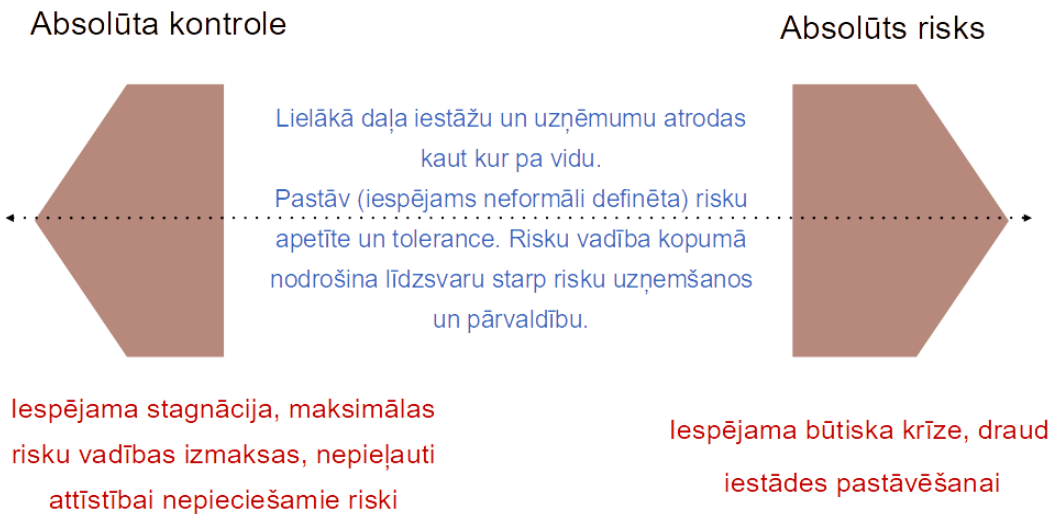
22. tabulā redzams, ka pirmā riska esošās kontroles samazina riska līmeni. 22. tabulā minēto informāciju par sākotnējo riska līmeni (7. kolonna) un atlikušo riska līmeni (12. kolonna) iespējams iekļaut risku reģistrā. 2. riska gadījumā esošās kontroles nesamazina riska līmeni. Ja esošās kontroles nesamazina riska līmeni, tās nepieciešams pilnveidot vai noteikt jaunus risku mazinošos pasākumus. Izstrādāts iekšējais normatīvais akts negarantē, ka esošās kontroles ir pilnvērtīgas. Izanalizējot normatīvā akta prasības, var konstatēt, vai tās ir vērstas uz riska cēloņa minimizēšanu. Atlikušā riska līmeni nepieciešams mazināt, ja tas pārsniedz pieļaujamo riska līmeni (riska apetīti, riska toleranci). Ja gadījumā kontroles nav vērstas uz cēloņu novēršanu, tas nozīmē, ka atlikušā riska līmeni iespējams samazināt, nosakot šo kontroļu pilnveidošanu, kas iepriekšminētā piemēra gadījumā nozīmē papildināt iekšējos normatīvos aktus ar jaunām prasībām.

5.7.4. Risku mazināšanas pasākumu efektivitātes analīze

Pieņemot lēmumus par risku mazināšanas pasākumu ieviešanu, jāpatur prātā līdzsvars starp resursiem, kas nepieciešami risku mazināšanas pasākumiem un kopumā kontroļu uzturēšanai iestādē, un potenciālajiem zaudējumiem, ko var radīt riski. Tas attiecas gan uz resursu patēriņu, gan uz iestādes risku kultūru un attieksmi pret riskiem kopumā.

Pārmērīga kontroļu ieviešana un uzturēšana prasa daudz resursus, kas var tikt izmantoti nelietderīgi un apdraudēt iestādes attīstību, kuras ietvaros nepieciešama risku uzņemšanās, jo arī publiskā sektora iestādēs nepieciešami inovatīvi risinājumi, procesu un pakalpojumu attīstība un modernizācija (20. attēls). Savukārt pilnīga riska kontroļu neesamība un risku nepietiekama vadība var būtiski apdraudēt iestādes aktīvus, resursus un pastāvēšanu kopumā, ja tā nevarēs pildīt savus pamata uzdevumus un funkcijas.

20. attēls. Absolūtā kontrole un absolūtais risks



Ieviesto risku mazinošo pasākumu efektivitāte ir jēdziens, ko lieto, lai raksturotu, cik lielā mērā kontrole samazina vai iedarbojas uz konkrēta riska izpausmi. Jo efektīvāka ir kontrole, jo lielāka ir pārliecība, ka risks tiek pietiekami vadīts. Kontrole ir efektīva, ja tā ir:

- būtiska, jo iedarbojas uz iestādes mērķu sasniegšanu apdraudošo risku;
- piemērota, jo iedarbojas uz konkrēto risku;
- pilnvērtīga, jo pilnībā vai gandrīz pilnīgi samazina risku;
- iedarbīga, jo novērš riska negatīvās sekas un/vai palielina pozitīvās sekas mērķu sasniegšanā: samazinot riska iestāšanās varbūtību un/vai samazinot riska iestāšanās ietekmes apmēru;
- uzticama, jo darbojas kā paredzēts;
- savlaicīga, jo iedarbojas pareizā brīdī un pietiekami ātri;
- lietderīga, jo ieguvums no kontroles ir lielāks nekā kontroles izmaksas.

Kontroles efektivitātes novērtēšana (21. attēls) ietver regulāru ieviestās kontroles pārskatīšanu, lai pārliecinātos, ka tā ir pareizi izveidota un efektīvi samazina vai pietiekami vada risku. Tas ietver sevī konkrētam riskam izveidotās esošās kontroles rezultātā atlikušā riska izvērtēšanu pret noteikto riska apetīti, lai noteiktu, vai esošā kontrole ir pietiekama. Ja atlikušais risks pārsniedz pieļaujamo riska līmeni (apetīti), tad esošā kontrole tiek pilnveidota un atkārtoti novērtēts tā rezultātā samazinātais atlikušā riska līmenis pret pieļaujamo riska apetīti.

21. attēls. Kontroles efektivitātes novērtēšana

Kontroles efektivitāti un nepieciešamās izmaiņas var skatīt un vērtēt no dažādiem aspektiem, piemēram:

- Kontroles uzbūve, kurā biežākie trūkumi var būt šādi:
  - Kontrole attiecīgajam riskam neeksistē;

- Kontrole tikai daļēji mazina attiecīgo risku;
- Kontrolei nav noteikti kritēriji (kas ir pieņemams un kas - nē);
- Pilnvaru trūkums kontroles izpildītājiem;
- Pienākumu nepietiekams nodalījums;
- Kontroles pierādījumu trūkums.

- Kontroles izpildījums, kurā biežākie trūkumi var būt šādi:
  - Kontrole darbojas citādāk nekā paredzēts;
  - Netiek veikta visā pārskata periodā;
  - Netiek veikta savlaicīgi un regulāri;
  - Netiek piemērota visiem paredzētajiem darījumiem/ darbībām;
  - Balstās uz šaubīgu informāciju;
  - Netiek veiktas korektīvās darbības.
- Kontroles rentabilitāte, kur visbiežāk kontroles ieguvumi neatsver:
  - Kontroles izmaksas (atbildīgo darbinieku par kontroles/ pārbaužu veikšanu darbs, aprīkojums, mērinstrumenti u.c. uz kontroles izpildi attiecināmās izmaksas) salīdzinājumā ar mazinātā vai novērstā riska sekām;
  - Atklāto kļūdu novēršanas izmaksas (atkārtotas darbības, remonti, seku novēršana u.c. labošanas darbu izmaksas);
  - Soda vai atlīdzības izmaksas, kas jāmaksā neatbilstību vai pārkāpumu gadījumos.

Būtisko risku gadījumā ir svarīgi kontroļu efektivitāti novērtēt regulāri, lai gūtu pārliecību par kontroles spēju samazināt risku un veikt to ekonomiski visizdevīgākajā veidā.

Kontroļu efektivitātes novērtēšana vairāk piemērota būs iestādēm, kurās ir stabila iekšējās kontroles vide, augstāks riska vadības briedums un var tikt veltīti resursi kontroļu rezultāta regulārai mērīšanai un kontroļu efektivitātes novērtēšanai.

Kontroles pietiekamības novērtēšanas process ietver šādus posmus:

1. Izprast kontroles mērķi – uz kuru risku kontrolei būtu jāiedarbojas, kā šī kontrole darbojas (preventīva, korektīva vai atklājoša) un kāds ir paredzamais kontroles rezultāts;
2. Iegūt datus par kontroles rezultātu, apkopojot kvantitatīvus un/vai kvalitatīvs datus par to, vai kontrolei ir izdevies sasniegt paredzēto rezultātu, piemēram, pašnovērtējums, atsauksmes, sūdzības, pētījumu rezultāti, kvalitātes kontrole, zaudējumu gadījumi, apdrošināšanas pieteikumi, lietotāju testu rezultāti u.c. dati;
3. Novērtēt kontroles efektivitāti, nosakot kontroles efektivitātes līmeni, piemērojot dažādas novērtēšanas skalas, piemēram, izmantojot šādu skalu:
   - Efektīva – kontrole novērš riska avotu/pamatcēloni, kontrole ir pietiekami dokumentēta, sistemātiski izpildīta, vadība tai lielā mērā uzticas;
   - Daļēji efektīva – kontrole ir izveidota, bet ir daļēji dokumentēta un ziņota, ne visos gadījumos ir izpildīta un reti novērtēta, kontroles trūkumi ir nebūtiski vai vidēji būtiski un parāda kontroles uzlabošanas iespējas, bet ne būtiskus kontroles sistēmas trūkumus;
   - Neefektīva – kontrole nav dokumentēta vai ziņota, nav pilnvērtīgi ieviesta praksē, kontrole nedarbojas atbilstoši tās paredzētajai uzbūvei un neiedarbojas uz paredzēto risku un tā cēloni.
4. Noteikt pasākumus kontroles pilnveidošanai – atkarībā no atklātajiem kontroles trūkumiem jānosaka, vai kontroli ir iespējams pilnveidot vai arī ir nepieciešami jauni vai papildu pasākumi riska ierobežošanai.

Piemērs:

Riska apraksts	Nav ievēroti nepieciešamie ugunsdrošības pasākumi un ir noticis lokāls ugunsgrēks, kā rezultātā iestāde nevar iedzīvotājiem sniegt savus pakalpojumus klātienē.
Kontroles novērtējums	**Daļēji efektīva** Apmācību apmeklētības pieraksti parāda, ka 10% no visiem darbiniekiem nav apmeklējuši obligāto ugunsdrošības instruktāžu. Paplašinot vai mainot nomātos īpašumus, netiek pārbaudīts, vai būs spēkā apdrošināšanas polise, lai segtu ugunsgrēku radītos zaudējumus.
Kontroles	**Preventīvā kontrole:** Obligātā ugunsdrošības instruktāža visiem darbiniekiem, lai tie ir informēti par uguns izcelsmes avotiem un nepieciešamo rīcību ugunsgrēka gadījumā. **Atklājoša kontrole:** Dūmu detektoru brīdinošais signāls par ugunsgrēku. **Korektīvā kontrole:** Īpašuma apdrošināšanas polise, kas sedz ugunsgrēka nodarītos zaudējumus.
Riska mazināšanas pasākumi	• Izveidot procesu, kādā apzināt tos darbiniekus, kuri nav izgājuši obligāto ugunsdrošības instruktāžu. • Papildināt līgumu slēgšanas procesu ar pārbaudi, lai pārliecinātos par apdrošināšanas polises esamību nomātajos īpašumos.

5.8. Risku reģistrs – izveidošana, formāts un uzturēšana, aktualizēšana

Risku reģistrs ir "risku informācijas krātuve" jeb datubāze. Risku reģistrs ir pamata informācijas avots komunikācijai par riskiem dažādos vadības līmeņos, sanāksmēs, dažādām auditorijām, kā arī tas tiek izmantots risku uzraudzībai un aktualizācijai.

Kad iestādei ir vienota izpratne un metodes, kā veikt risku identificēšanu un novērtēšanu, tad informāciju par riskiem, ņemot vērā iestādes vajadzības, reģistrē risku reģistrā. Visi riski un ar tiem saistītā informācija tiek apkopota risku reģistrā. Risku reģistra piemēri pieejami 12. pielikumā.

Risku reģistrā ievada vismaz šādu informāciju:

1. riska nosaukums - parasti tiek definēts īsi, saprotami un konkrēti;
2. riska notikuma apraksts ir izvērsts riska scenārija apraksts, kā rezultātā tiek radīti zaudējumi (kvantitatīvi vai kvalitatīvi), aprakstā var iekļaut izklāstu par to, kuri iestādes darbības mērķi tiek apdraudēti;
3. cēloņus (var uzdot šādus jautājumus – kas, kāpēc, pie kādiem apstākļiem notiktu);
4. sekas – kādas būtu vissliktākās sekas, kuras notiktu, iestājoties riskam (var vairākkārt uzdot jautājumu – un kas tālāk/ ko tas ietekmēs?);
5. būtiskākās esošās kontroles;
6. riska varbūtība un ietekme, to vērtības atbilstoši iestādē apstiprinātajai risku vadības, tai skaitā novērtēšanas metodikai;
7. riska līmenis – visbiežāk varbūtības un ietekmes reizinājums;
8. risku vadības stratēģija, ņemot vērā riska līmeni;

9. risku mazinošie pasākumi, atbildīgie, ieviešanas termiņi;
10. riska līmeņa izmaiņas pēc risku mazinošo pasākumu ieviešanas.

Iestādes risku vadītājam būtu jāuztur aktuāls risku reģistrs, šajā procesā var iesaistīties arī attiecīgo risku īpašnieki. Ja risku reģistrs ir digitalizēts un tā aktuālā versija pieejama visiem procesā iesaistītajiem zināmā vietā, tad riska reģistrā esošās informācijas aktualizāciju var veikt vienlaikus vairākas personas, tādā gadījumā nodrošinot, ka veiktās izmaiņas tiek fiksētas.

Risku reģistram jābūt saistītam ar risku mazināšanas pasākumu plānu un tajā atkarībā no risku mazināšanas pasākumu statusa un progresa jāveic risku novērtējuma aktualizācija. Var veidot atsevišķus dokumentus – Risku reģistru un Risku mazinošo pasākumu plānu, kuru sagatavo, izmantojot vienkāršoto risku reģistru (12. pielikums), bet neiekļaujot varbūtības un ietekmes novērtējumus, norādot tikai riska līmeni (skat. 5.10. nodaļu).

Risku reģistru var apstiprināt vai citā veidā formalizēt iestādes augstākā vadība, lai tajā iekļautā informācija tiktu skaidri un formāli piefiksēta, kā arī pieņemtie lēmumi, balstoties uz riskiem vai pasākumi to mazināšanai, būtu izsekojami. Praksē parasti var apstiprināt vienkāršotus risku reģistrus, kas ir vienlaikus risku mazinošo pasākumu plāni. Savukārt detalizētākos risku reģistros visu iekļauto informāciju var neapstiprināt, lai izvairītos no dublējošām apstiprināšanas darbībām, jo tajos var tikt uzskaitītas, piemēram, apstiprinātas iekšējās kontroles, kuras jau ir noteiktas iekšējos normatīvajos dokumentos.

Ziņojumos un citos risku vadības analītiskajos apkopojumos un augtākā līmeņa vadības sanāksmēs iespējams izmantot vienkāršotu un saīsinātu risku reģistra formātu.

Piemērs: Izveidots risku reģistrs un dažiem riskiem apstiprināti risku mazināšanas pasākumi.

- Ik ceturkšņa būtisko risku statusa ziņojumā augstākajai vadībai tiek ziņots par risku Nr. 1, kura mazināšanai bija jāievieš divi pasākumi. Abi pasākumi ir ieviesti plānotajā termiņā un riska īpašnieks koordinējot ar risku vadītāju, pazemina riska iestāšanās varbūtību (un attiecīgi riska kopējo novērtējumu), pirms tam pārliecinoties, ka pasākumi ir ieviesti atbilstoši plānam. Papildu tam, riska īpašnieks sniedz komentāru, ka pie atkārtotas riska vērtēšanas jāatgriežas pēc sešiem mēnešiem, lai pārliecinātos par riska tendenci un novērtējumu. Šī informācija tiek atspoguļota risku reģistrā;
- Savukārt riskam Nr. 2 viens pasākums ir jāatliek uz vēlāku laiku, jo tā īstenošanai nepieciešama padziļināta izpēte, kam nepieciešams ilgāks laika periods. Tikmēr risks turpina kļūt arvien aktuālāks. Vadība lemj pārcelt riska mazināšanas pasākuma termiņu par četriem mēnešiem vēlāk atbilstoši risku vadītāja un risku īpašnieka rekomendācijai. Vadība aicina paaugstināt riska novērtējumu un piedāvā piesaistīt papildu ārējo pakalpojumu, lai atbalstītu un veicinātu izpētes īstenošanu. Paaugstinātais riska novērtējums (ietekme) un jaunais riska mazināšanas pasākuma termiņš tiek atspoguļots risku reģistrā.

5.9. Incidentu reģistrs

Ja iestādē tiek uzturēts incidentu reģistrs (par jebkādu procesu vai funkciju, piemēram, IT drošības incidenti, darba aizsardzības incidenti, ārējo klientu sūdzības u.tml.), to var sasaistīt ar risku reģistru šādā veidā:

- Incidentu reģistrs var tikt izmantots kā avots un pamatojums risku identificēšanai (skat. 5.4. un 5.9. nodaļu);
- Incidentu reģistrs var tikt izmantots kā risku indikatoru datu avots (piemēram, ja pieaug vai īstenojas incidenti, tas var liecināt par riska varbūtības un ietekmes palielināšanos);
- Incidentu reģistrs var tikt izmantots kā avots risku kvantificēšanai.

Atkarībā no iestādē izmantotā risku reģistra un incidentu reģistra formāta un tā, vai tie tiek uzturēti dokumentu veidā (piemēram, MS Excel formātā) vai informācijas sistēmās, šos reģistrus var un ir ieteicams sasaistīt. Risku reģistru var papildināt ar kolonnu par incidentu rādītājiem attiecīgajā risku jomā.

5.10. Risku mazināšanas plāna izstrāde

Risku mazināšanas pasākumu plāns ir dokuments, kurā apkopoti ieviešamie risku mazināšanas pasākumi un tā saturā var iekļaut, piemēram:

1. Atsauci uz attiecīgajiem riskiem (piemēram, to identifikators, saite uz atrašanās vietu, īss apraksts vai nosaukums);
2. Riska mazināšanas pasākumus: īss nosaukums un plašāks apraksts, secīgi pasākuma soļi, ja nepieciešams sadalot pasākumu vairākās aktivitātēs;
3. Riska mazināšanas pasākuma un tā soļu/ aktivitāšu veikšanas termiņi un atbildīgie;
4. Ja nepieciešams papildu informācija par riska mazināšanas pasākumu (piemēram, nepieciešamie resursi, pasākuma izvēles pamatojums, riska mazināšanas pasākuma statuss - uzsākts, izpildē, atlikts u.tml.).

Risku mazināšanas pasākumus nepieciešams apstiprināt vai citā veidā formalizēt atbilstošā iestādes vadības līmenī, lai tiem būtu skaidri paredzēti un pieejami laika, darbinieku un materiālie, kā arī jebkādi citi nepieciešamie resursi. Iestādes augstākajai vadībai jāapstiprina risku mazināšanas pasākumu plāns vismaz būtiskākajiem riskiem.

Visbiežāk iestādes izvēlas integrēt risku mazināšanas pasākumus risku reģistros (skat. 5.8. nodaļu), taču var arī sagatavot un apstiprināt atsevišķus risku mazinošo pasākumu plānus vai risku mazinošos pasākumus integrēt iestādes darbības plānā, kas pakārtots iestādes stratēģiskajiem mērķiem.

Risku mazinošo pasākumu plānu sagatavo atbildīgais darbinieks par risku vadību sadarbībā ar risku īpašniekiem, to saskaņo struktūrvienību vadītāji, kuru kompetencē ir ieviest risku mazinošos pasākumus, kā arī apstiprina iestādes administratīvais vadītājs. Tāpat atbildīgais darbinieks par risku vadību var piedalīties iestādes darbības plāna sagatavošanā, sniedzot šī plāna sagatavošanai nepieciešamo papildu informāciju par risku mazinošajiem pasākumiem.

Pēc risku mazināšanas pasākumu plāna (13. pielikums) izstrādes jāveic formāla, regulāra un caurspīdīga risku mazināšanas pasākumu izpildes statusa kontrole un uzraudzība, kā arī regulāra informācijas apmaiņa par pasākumu ieviešanas statusu.

5.11. Risku kartes izveide un uzturēšana, aktualizēšana

Risku karte ir kopējais iestādes visu risku novērtējuma vizuāls attēlojums (14. un 15. pielikums). Tas vienā grafikā pārskatāmi parāda risku skaitu dažādos novērtējuma līmeņos uz varbūtības un ietekmes asīm. Papildu tam, atkarībā no iestādē apstiprinātās risku vadības politikas, tas vizuāli atspoguļo paredzamo risku vadības valdības stratēģiju atkarībā no risku pakāpes. Risku karte sniedz priekšstatu par iestādes kopējo risku līmeni un profilu.

Lai attēlotu risku prioritāti atbilstoši to novērtējumam, tiek izmantota risku matrica un tajā attēlotās risku līmeņu jeb zonu krāsas, piemēram, "sarkanā" zona – ļoti augsta līmeņa risks, "oranžā" zona – augsta līmeņa risks, "dzeltenā" zona – vidēja līmeņa risks un "zaļā" zona – zema līmeņa risks jeb pieļaujamais riska līmenis (16. pielikums). Matricā uz asīm attēlotas risku ietekmes un varbūtības vērtības. Katrā iestādē risku matricas zonas var atšķirties.

Risku kartē var arī vizuāli attēlot risku grupas, piemēram, iekšējie/ ārējie riski; stratēģiskie, darbības (operacionālie) (personāla, juridiskie, tehniskie riski) un finanšu riski.

Piemērs: Sagatavotajā piemērā (14. pielikums) ir attēloti seši riski (zili apunkti, kuriem blakus ir risku identifikācijas numuri):

Risks Nr. SR 1, SR 2 un FR1 atrodas sarkanajā zonā, un tas ir ļoti augsts (katastrofāls), kas nozīmē, ka risks gandrīz noteikti iestāsies ar būtiskām un katastrofālām sekām.

Risks Nr. OR 1 un OR 2 atrodas oranžajā zonā, tas ir ar iespējamību, ka notiks tuvākajā laikā, taču, ja iestāsies, tad negatīvās sekas būs vidējas.

Savukārt, risks Nr. OR 3 atrodas zaļajā zonā, tas ir ar zemu iespēju, ka varētu notikt, tomēr sekas būtu minimālas.

5.12. Risku uzraudzība un izmaiņu eskalēšana

Risku uzraudzība ir svarīga visos risku vadības procesa posmos un visu veidu un līmeņu riskiem. Risku uzraudzība praksē nozīmē regulāru risku pārskatīšanu, nosakot, vai iepriekš piešķirtais novērtējums atbilst faktiskajai situācijai, vai un kā ir mainījušās riska kontroles un kā tās darbojas, kā arī, kāds ir risku mazināšanas pasākumu ieviešanas progress un tā ietekme uz risku.

Uzraudzības un pārvērtēšanas uzdevums ir nodrošināt un uzlabot risku vadības procesu plānošanas, īstenošanas un rezultātu kvalitāti un efektivitāti. Procesam jāietver rezultātu pastāvīgu pārraudzību un periodisku pārskatīšanu, skaidri nosakot atbildību.

Uzraudzība un pārvērtēšana ietver plānošanu, informācijas iegūšanu un analīzi, rezultātu reģistrēšanu un atgriezeniskās saiknes nodrošināšanu.

Uzraudzības un pārvērtēšanas rezultātus var izmantot ziņojumu sagatavošanai un iestādes snieguma novērtēšanai.

Risku vadītāja pienākums ir koordinēt un iniciēt risku uzraudzību un būtisku izmaiņu eskalēšanu iestādes vadībai. Risku īpašnieku pienākums ir sniegt informāciju, uzraudzīt riskus un eskalēt izmaiņas. Iestādes vadības atbildība ir vērst uzmanību uz risku vadības nozīmīgumu, ja nepieciešams padziļināti analizēt riskus, kā arī saņemot informāciju par eskalāciju no risku īpašniekiem - pieņemt nepieciešamos lēmumus un nodrošināt risku vadību.

Risku uzraudzības ziņošanu var apvienot vai sasaistīt ar jau esošajiem iestādes regulārajiem procesiem, kuros tiek ziņots par iestādes darbības rezultātiem un darba plānu izpildi, kā arī veikta uzraudzība. Tas nozīmē, ka atbilstoši plānotajiem pasākumiem un termiņiem atbildīgie par risku mazināšanas pasākumiem sniedz atskaites darba grupai un vadībai.

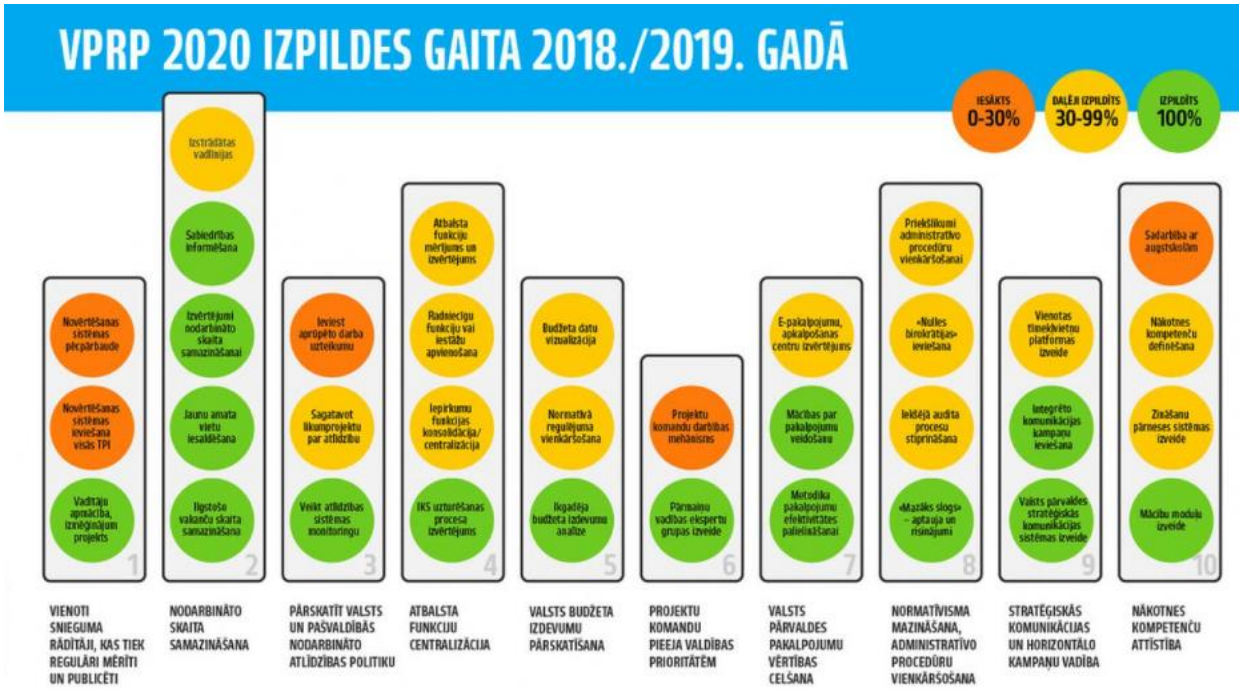
Risku uzraudzības procesu var palīdzēt īstenot iekšējā audita struktūrvienība, veicot periodiskas pārbaudes, tostarp izlases veidā pārliecinoties par risku mazinošo pasākumu ieviešanas statusu.

Lai uzskatāmi parādītu risku mazināšanas pasākumu uzraudzību, var izmantot veidlapu "Riska profils" (17. pielikums). Riska profils nodrošina detalizētu dokumentāciju un riska atribūtus ar informāciju par riska mazināšanai plānotajām darbībām. Profils satur informāciju par risku, to veicinošiem faktoriem, riska rādītājiem, kontroles dokumentāciju un rīcības plānu.

Lai uzraudzītu risku mazinošo pasākumu izpildi, labs uzskates materiāls, ko var izmantot, ir "Luksofora princips". Regulāri sniedzot atskaites, ir redzams, kādā izpildes posmā pasākuma ieviešana notiek, cik tas ir kritiski.

Piemēram, MK 2019. gadā savā tīmekļvietnē ievietoja pārskatu par reformu plāna izpildi, izmantojot "luksofora principu" (22. attēls) "Reformu plāns – valsts pārvaldes attīstības impulss."

22. attēls. VRP 2020 izpildes gaita 2018./2019. gadā [29]



[29] https://www.mk.gov.lv/lv/jaunums/reformu-plans-lauj-nostiprinat-parmainas-valsts-parvalde-ka-pastavigu-attistibas-procesu

5.13. Risku informācija, komunikācija un ziņošana – riska informācijas komunicēšana, informācijas plūsmas un ziņojumi vadībai par riskiem, kultūru un izpildi – saturs, regularitāte

Risku informācijas komunikācija ir viens no svarīgākajiem priekšnosacījumiem praktiskas, elastīgas un efektīvas risku vadības ieviešanai.

Risku informācijai ir jābūt **pieejamai un izsekojamai** iestādes augstākās vadības lēmumu pieņemšanas procesā. Risku informācijai ir jābūt **pietiekamai un aktuālai**, lai augstākā vadība varētu pieņemt uz pamatota izvērtējuma balstītus pilnvērtīgus lēmumus.

Arī iestādes augstākajai un citu līmeņu vadībai, darbiniekiem, kas strādā ar riskiem, jāspēj definēt, kādu risku informāciju tie vēlās saņemt, kāda informācija par riskiem ir nepieciešama operatīvajai ikdienas vadībai, lēmumu pieņemšanai. Tas var atšķirties atkarībā no vadības līmeņa un darbinieka lomas, arī lomas Trīs līniju modelī, taču ir iespējamas un ieteicamas dažāda veida risku informācijas komunikācijas aktivitātes. Katrai no tām būtu jānosaka regularitāte, atbildīgais par informācijas sagatavošanu un satura formāts. Risku komunikācijai ir vienots mērķis - pēc iespējas uzlabot un optimizēt risku vadību iestādē, līdz ar to jāseko līdzi tam, lai informācijas apmaiņa nedublētos, taču tajā arī nedrīkst būt pārrāvumu.

Lai risku komunikācija būtu pēc iespējas lietderīgāka, ir nepieciešams **iesaistīt dažādu funkciju, līmeņu un struktūrvienību pārstāvjus**, pēc iespējas nodrošinot to, ka tiek uzrunāti un informēti visi, kurus skar attiecīgie riski un, kuri var piedalīties risku mazināšanas pasākumos, t.i., risku komunikācijai pēc iespējas jābūt **starpdisciplinārai**. Papildu nosacījums veiksmīgai risku komunikācijai un tās pielietošanai risku vadībā ir **informācijas plūsmas nepārtrauktība un regularitāte**.

> ⚠ **Padoms:** Risku informācijas apriti un komunikāciju iekļaut esošajos komunikācijas un ziņošanas kanālos, tādējādi šī informācija tiks integrēta saturiski un netiks uztverta kā papildu administratīvais slogs.

Risku informācijai jābūt iekļautai, izmantotai un atspoguļotai lēmumu pieņemšanā šādos iestādes procesos:

- iestādes stratēģijas izstrāde un stratēģisko mērķu noteikšana, stratēģijas apstiprināšana;
- iestādes stratēģijas izpildes ziņošana;
- ikgadējo vai vidēja termiņa darbības plānu izstrāde;
- iestādes ikgadējo vai vidēja termiņa darbības plānu izpildes ziņošana;
- regulārās operatīvās iestādes vadības un struktūrvienību vadītāju sanāksmes;
- regulārā lēmumu pieņemšana par investīcijām, budžeta sadalījumu un izlietojumu, projektu apstiprināšana un uzraudzība u.tml. dažādos iestādes vadības līmeņos, bet vismaz augstākajā un vidējā vadības līmenī;
- struktūrvienību operatīvā darba plānošanas un uzraudzības sanāksmes, uzdevumu un mērķu izpildes uzraudzības un statusa pārrunas;
- specifiski pasākumi un sanāksmes paredzēti tieši ziņošanai par riskiem, piemēram, gada atskaite par risku vadību, regulāra (piemēram, reizi ceturksnī) būtisko risku statusa un mazināšanas pasākumu ziņošana vai neplānotu, krīzes situāciju risku ziņošana.

Papildu risku ziņošanai ir ieteicama regulāra risku īpašnieku diskusiju grupu organizācija, lai pārrunātu risku attīstību un risku mazināšanas pasākumu statusu. Regulāras sanāksmes nodrošina to, ka informācija ir aktuāla un tiek iedzīvināta risku vadības kultūra dažādos līmeņos, kā arī iestādes vadībai var tikt nodrošināta būtiskākā informācija par riskiem.

Kā satura pamatu risku komunikācijai būtu jāizmanto risku reģistrs (pilnā vai vienkāršotā, pielāgotā formā un risku mazināšanas pasākumu plāns, ja tas veidots atsevišķi), jo tas vienkopus atspoguļo informāciju par riskiem, to novērtējumu, mazināšanas pasākumiem un izmaiņu tendencēm.

Svarīgi: Risku komunikācijai jābūt ar mērķi nodrošināt visus iesaistītos ar vienlīdzīgu informācijas apjomu un vienādot izpratni par risku vadību, dalīties risku vadības pieredzē, nepieciešamības gadījumā saskaņot rīcības un pieņemt informētus lēmumus, nevis tikai formāli atskaitīties kādam, jo šāds pienākums ir uzdots.

Padoms: Iestādei būtu jāparedz gan skaidri noteikti un regulēti informēšanas un risku komunikācijas pasākumi ar noteiktu regularitāti un atbildīgajiem, kā arī jāparedz iespēja veikt neplānotu risku informācijas komunikāciju nepieciešamības gadījumā (piemēram, lai reaģētu uz iestājušos risku, vai iepriekš neidentificēta riska apdraudējuma pieaugumu). Komunikācijas saturam, regularitātei un iesaistītajiem jābūt noteiktiem iestādes risku vadības kārtībā, procedūrā vai citā iekšējā normatīvajā aktā.

Komunikācijai par riskiem var izšķirt šādus līmeņus:

1. Līmenis: komunikācija funkcijas vai struktūrvienības ietvaros par riska profila izmaiņām (ikdienas sanāksme, saruna);
2. Līmenis: komunikācija ar citiem speciālistiem, parasti darba grupas, starpfunkcionālās sanāksmes;
3. Līmenis: eskalācija funkcijas vadītājam, kad nepieciešams lēmumu uzraudzīt, izstrādāt priekšlikumus riska ierobežošanai;
4. Līmenis: eskalācija augstākajai vadībai, kad riskam ir potenciāls atkārtoties, pieaugt, pārsniegt riska apetīti;
5. Līmenis: eskalācija uzraudzības iestādēm, kad iestādei var nebūt iespēju pilnībā pastāvīgi tikt galā ar risku un sasniegt iepriekš noteiktos mērķus.

5.13.1. Būtisko risku izmaiņu komunikācija

Funkciju vai struktūrvienību vadītāju pienākums ir eskalēt risku informāciju augstākajai vadībai, vismaz par būtiskajiem riskiem, ja pieaug to novērtējums vai rodas šķēršļi risku mazināšanas pasākumu ieviešanai. Risku īpašnieki vai struktūrvienību vadītāji var ziņot par riskiem regulārajās vadības sanāksmēs vai atskaitēs, kā arī var ziņot Trīs līniju modeļa otrajai līnijai (kontroles specializētajām funkcijām, piemēram, informācijas drošības vadītājam).

Risku vadītājs, komunicējot ar struktūrvienību vadītājiem vai iestādes vadību, sniedz informāciju par risku izmaiņām, statusu un risku mazināšanas pasākumu statusu, kā arī priekšlikumiem turpmākajai risku vadībai.

Risku informāciju funkciju/ procesu vadītājiem var sniegt dalīti, ņemot vērā funkcionālo piederību vai pilnā apjomā kā atgriezenisko saiti pieredzes apmaiņai un izpratnes veicināšanai iestādes iekšienē. Ir svarīgi, lai riska informācijai piekļūtu arī otrās līnijas funkcijas (10.attēls) pārstāvji. Savukārt specializētu informāciju par riskiem sagatavo arī ārējām pusēm pēc pieprasījuma vai ikgadējos pārskatos.

Iespējami šādi šķēršļi efektīvai komunikācijai par riskiem:

- vadības un struktūrvienību vadītāju nepieejamība riska informācijas apmaiņai;
- nav ērtu un ātru komunikācijas formu un kanālu;
- lēmumu pieņēmējiem nav pilnvērtīga un savlaicīga informācija;
- kavēšanās pieņemt lēmumus riska vadīšanai /mazināšanai;
- drosmes trūkums lēmumu pieņemšanā;
- vēršanās pret ziņnesi;
- koncentrēšanās uz lielajām neatbilstībām, nepamanot mazus signālus potenciālam riskam;
- operacionālie jautājumi norit ātrāk nekā riska ziņošana augstākajai vadībai.

Lai apietu šos šķēršļus, ieteicams ņemt vērā šajā nodaļā minētos padomus par risku komunikācijas regularitāti, atbildīgajiem un formalizāciju, kā arī būtiski uzturēt un attīstīt labvēlīgu risku vadības kultūru. Risku komunikācijai noteikti būs līdzīgas iezīmes kā iestādes vispārējai komunikācijas kultūrai.

5.13.2. Risku komunikācija un eskalācija valsts līmenī

Par riskiem, kas ir būtiski un skar ne tikai vienu iestādi, bet vairākas, kas ir prioritāri valstiskā līmenī un saistīti, piemēram, ar Nacionālajā attīstības plānā vai citos valsts līmeņa plānošanas dokumentos noteiktajiem mērķiem, būtu nepieciešama plašāka komunikācija.

Šī Rokasgrāmata nevar noteikt un risināt valstiska līmeņa komunikācijas un risku vadības jautājumus, taču valsts iestādēm būtu ieteicams apzināt tos riskus, kuri pastāv valsts līmenī, kurus valsts iestādes var vadīt un mazināt tos, sadarbojoties starp resoriem. Tas iedrošinātu iestāžu pārstāvjus eskalēt savu iestāžu un nozaru riskus, kas ietekmē augstāka līmeņa mērķus. Tādā veidā komunikācija par riskiem, kas attiecas uz valsts līmeņa attīstības sistēmas plānošanas dokumentiem, kļūtu strukturētāka, vienlaikus būtu pieejama aktuālāka informācija par valsts līmeņa riskiem, kā arī būtu iespējams laicīgāk plānot rīcības šo risku vadībai.

Kopīgo starpnozaru risku komunikācija ļautu arī izveidot valsts līmeņa risku reģistru, kas būtu ļoti noderīgs gadījumos, kad risku mazināšanā jāsadarbojas dažādām iestādēm no dažādiem resoriem, jo var rasties situācijas, kad kādas iestādes identificēto risku var risināt tikai cita iestāde.

Tas uzlabotu Latvijas kā valsts reputāciju un tēlu kopumā, jo starptautiskajā līmenī, atskaitoties par sasniedzamajiem politiku mērķiem un rādītājiem, mēs būtu gatavāki runāt un laicīgāk identificētu riskus, ko varētu efektīvāk pārvaldīt. Šāda pieeja var pozitīvi ietekmēt valsts iestāžu reputāciju arī nacionālajā līmenī, demonstrējot sabiedrībai, ka iestādēs lēmumi tiek pieņemti riskos balstītā domāšanā, ka valsts iestādēs ir apzināti būtiskākie riski un ka tie tiek vadīti.

5.14. Risku vadības integritāte ar citām iestādes informācijas sistēmām un datu bāzēm

Iestādēs izmantoto informācijas sistēmu funkcionalitāti iespējams izmantot risku vadības procesa digitalizēšanai un optimizēšanai, ieskaitot risku identificēšanu, analīzi, risku reģistra uzturēšanu, risku mazinošo pasākumu plānošanu, kā arī pārskatu/ ziņojumu par risku vadību sagatavošanai (automātiski ģenerēti pārskati, tostarp iestādes augstākās vadības informēšanai ikdienā) (23. attēls). Vairāku informācijas sistēmu funkcionalitātes pārzināšana un to savstarpējā integrēšana var atvieglot risku vadības procesa norisi (23. tabula).

23. attēls. Automātiski ģenerēta pārskata par riskiem piemērs

23. tabula. Programmu, informācijas sistēmu funkcionalitātes pielietošana risku vadības procesā

Lietojumprogrammas, informācijas sistēmu lietojumi	Iespējamais pielietojuma veids risku vadīšanā, ja iestādē nav risku vadības informācijas sistēma	Iespējamais mijiedarbības veids risku vadīšanā, ja iestādē ir risku vadības informācijas sistēma
***Microsoft Excel, Libre Calc*, izklājlapu programmatūras programma**	Risku reģistra uzturēšana. Datu analīze risku identificēšanai. Ziņojumu/pārskatu par risku vadību sagatavošanai. Datu vizualizācija risku kartes uzturēšanai.	Datu analīze risku identificēšanai un datu analīzes rezultātu pārnešana uz risku vadības informācijas sistēmu. Datu vizualizācija risku kartes uzturēšanai, ja risku vadības informācijas sistēmā nav atbilstošu vizualizācijas rīku.
***Microsoft Project, Project Libre*, projektu vadības programmatūra**	Projektu risku reģistra uzturēšana. Datu analīzei projektu risku identificēšanai un analīzei.	Datu analīze projektu risku identificēšanai un datu analīzes rezultātu pārnešana uz risku vadības informācijas sistēmu.
Lietvedības un dokumentu vadības sistēmas	Risku vadības dokumentācijas aprites nodrošināšana. Risku reģistra uzturēšana.	Risku vadības dokumentācijas aprites nodrošināšanai, risku vadības dokumentu apmaiņa ar lietvedības un dokumentu vadības sistēmu.
***PowerBI, Microstrategy*, biznesa inteliģences risinājumi**	Datu analīze risku identificēšanai un analīzei, ziņojumu/pārskatu par risku vadību sagatavošanai. Datu vizualizācija risku kartes uzturēšanai. Risku mazinošo pasākumu plānošanai.	Datu analīze risku identificēšanai un analīzei un datu analīzes rezultātu pārnešana uz risku vadības informācijas sistēmu. Datu vizualizācija risku kartes uzturēšanai, ja risku vadības informācijas sistēmā nav atbilstošu vizualizācijas rīku.
Uzdevumu pārvaldības sistēmas	Risku mazinošo pasākumu plānošana. Risku mazinošo pasākumu izpildes organizēšanai un kontrole.	Risku mazinošo pasākumu izpildes organizēšana un kontrole, ja risku vadības informācijas sistēmā nav atbilstoša rīka vai iestādē ir viena/vienota uzdevumu pārvaldības sistēma.
Lēmumu pieņemšanas atbalsta sistēmas	Risku reģistra un risku kartes datu izmantošana lēmumu pieņemšanā.	Informācijas par lēmumiem izmantošana risku identificēšanā, analīzē un risku mazinošo pasākumu plānošanā.
Iestādes darbības/funkciju nodrošināšanas sistēmas, uzņēmumu informācijas sistēmas	Datu analīze risku identificēšanai un novērtēšanai. Risku mazinošo pasākumu plānošanai. Risku mazinošo pasākumu izpildes organizēšanai un kontrolei.	Datu analīze risku identificēšanai un analīzei un datu analīzes rezultātu pārnešana uz risku vadības informācijas sistēmu. Risku mazinošo pasākumu izpildes organizēšana un kontrole, ja risku vadības informācijas sistēmā nav atbilstoša rīka vai iestādē ir viena/vienota informācijas sistēma.

Lietojumprogrammas, informācijas sistēmu lietojumi	Iespējamais pielietojuma veids risku vadīšanā, ja iestādē nav risku vadības informācijas sistēma	Iespējamais mijiedarbības veids risku vadīšanā, ja iestādē ir risku vadības informācijas sistēma
Sociālie tīkli, attālināta darba organizēšanas rīki	Risku identificēšanas un analīzes organizēšana. Risku mazinošo pasākumu plānošana. Risku mazinošo pasākumu izpildes organizēšana un kontrole.	Risku identificēšanas un analīzes organizēšana un datu analīzes rezultātu pārnešana uz risku vadības informācijas sistēmu.

Informācijas sistēmu piemēri, ko var izmantot tieši risku vadībai:

- JIRA specifiski izveidots risku vadības modulis;
- Confluence;
- IBM Notes speciālā bāze.

Priekšrocības, ko sniedz IS izmantošana risku vadībā:

- aktuālas risku vadības informācijas pieejamība vienkopus;
- informācijas un veikto izmaiņu izsekojamība;
- interaktivitāte - iespēja plašākam darbinieku lokam pastāvīgi piekļūt informācijai un nepieciešamības gadījumā to aktualizēt, izmantot operatīvajām ikdienas darba vajadzībām, kā arī automatizēt atgādinājumus par risku mazināšanas pasākumu termiņiem;
- iespēja pievienot papildu failus kā pielikumus vai attēlus risku aprakstiem;
- vizualizācijas, grafiku un atskaišu veidošanas iespējas, kas var būt automatizētas (atkarībā no sistēmas funkcionalitātes);
- sasaiste ar citām iestādes pārvaldības funkcijām, piemēram, iekšējo auditu, operatīvajiem uzdevumiem, kas tiek pārvaldīti informācijas sistēmās (piemēram, riski, kas saistīti ar kādu no iekšējā audita konstatējumiem vai risku mazināšanas pasākumi, kas saistīti ar kādu no struktūrvienības vadītāja gada darba plānā noteiktajiem pasākumiem, kārtējā perioda uzdevumiem u.tml.). Tāpat iespējama sasaiste ar incidentu reģistriem, ja tie tiek reģistrēti IS.

Padoms: Neuzsāciet risku vadības ieviešanu savā iestādē ar risku vadības IS iegādi vai izveidi. Risku vadības IS vai citu IS pielāgošana risku vadības vajadzībām nav paredzēta un ieteicama sākotnējos risku vadības brieduma līmeņos, pirms šī funkcija un process ir praktiski notestēta, izveidota tā metodiskā un procesa soļu bāze un ir gūtas pirmās atziņas par nepieciešamajiem uzlabojumiem. Turklāt bieži vien advancētas un risku vadībai specifiski veidotas IS mēdz būt sarežģītākas, standartizētas un nav konfigurējamas (adaptējamas iestādes vajadzībām) un vairāk piemērotas finanšu sektora vai automatizētās ražošanas organizācijām.

KOPSAVILKUMS

Jebkurā iestādē, neatkarīgi no tās esošā vai vēlamā risku vadības brieduma līmeņa, ir šādi sākotnējie pasākumi risku vadības ieviešanai:

- risku vadības mērķu un pamatprincipu noteikšana (risku vadības politika);

- risku vadības kārtības un metodikas izstrāde;
- risku vadībā iesaistīto darbinieku un citu nepieciešamo resursu nodrošināšana;
- darbinieku informēšana par risku vadības mērķiem, paredzamo izmantojamo metodiku;
- pakāpeniska risku vadības praktiskā īstenošana atbilstoši risku vadības procesa posmiem (kas aprakstīti turpmāk šajā nodaļā).

Risku vadības procesa posmiem, atbildības un pienākumu sadalījumam jābūt skaidri noteiktam iestādes iekšējos normatīvajos aktos, kas reglamentē risku vadību.

Risku vadības process atbilstoši ISO 31000:2018 standartam sastāv no šādiem posmiem:

- **risku vadības darbības sfēras, vides un kritēriju noteikšana** nepieciešama, lai klasificētu riskus, piemēram, stratēģiskajā, darbības (operacionālajā) un projektu līmenī un apzinātu, kāda veida riski piemīt iestādei. **Kritēriju** (risku ietekmes un varbūtības novērtēšanas kritēriji) **definēšana** nepieciešama, lai noteiktu risku līmeni un būtiskumu, veicot risku analīzi;
- **risku identificēšanas** rezultātā tiek apzināti riski, kas apdraud iestādes mērķu sasniegšanu. Risku vadītājs veic priekšizpēti, lai apzinātu potenciālos riskus, un/vai risku īpašnieki novēro un piefiksē potenciālos riskus. Pēc tam, sadarbojoties ar risku īpašniekiem/procesu īpašniekiem, formulē (identificē) riskus;
- **risku analīzes** rezultātā tiek noteikta identificēto risku varbūtība un ietekme (atbilstoši iestādes apstiprinātajai metodikai), veicot kvalitatīvu vai kvantitatīvu risku izvērtējumu;
- **risku izvērtēšana** atbalsta lēmumu pieņemšanu un palīdz noteikt, vai ir nepieciešamas papildu darbības, lai reaģētu uz riskiem;
- **reaģēšana uz riskiem** nozīmē risku ierobežošanu, ja atlikušais riska līmenis nav pieņemams (pārsniedz riska apetīti), iespēju robežās mainot risku sekas un varbūtību, ieviešot jaunas vai papildinot esošās risku kontroles;
- **informācijas apmaiņa un komunikācija** starp iekšējām un ārējām ieinteresētajām pusēm palīdz iestādē saglabāt piesardzību un veicina darbinieku izpratni par iestādes riskiem, konsultācijas par risku vadības procesu palīdz pieņemt uz riskiem balstītus lēmumus;
- **uzraudzība un pārskatīšana** paredz risku reģistru aktualizāciju, mainoties to vērtējumam, pielāgojot risku mazināšanas pasākumus;
- **dokumentēšana un ziņošana** paredzēta, lai komunicētu par risku vadības rezultātiem iestādē, kā arī, lai nodrošinātu un atbalstītu stratēģisko un ikdienas (operacionālo) lēmumu pieņemšanu.

Risku identificēšanas mērķis ir strukturēti un objektīvi apzināt un apkopot iestādes riskus, identificējot iekšējās un ārējās vides faktorus.

Risku identificēšanas avoti var kalpot par sākuma punktu risku identificēšanai, kā arī var būt labs informatīvs atbalsts risku vadītājam, risku īpašniekiem un iestādes vadībai.

Risku identificēšanā un formulēšanā var tikt izmantotas dažādas metodes, kas var būt vērstas uz pagātnes notikumu, šodienas situācijas un nākotnes iespēju analīzi.

Riska indikators ir mērījums, kas norāda uz riska potenciālo klātbūtni, līmeni un tendenci, tas var norādīt, vai risks ir tikko iestājies vai tā līmenis paaugstināsies, kāds ir tā līmenis, izmaiņu tendence. Risku indikatori kalpo arī kā palaidējmehānisms riska mazinošo pasākumu ieviešanai.

Riska analīzi izmanto, lai izprastu identificēto risku veidu, avotus un cēloņus un rezultātā noteiktu riska līmeni. Veicot risku analīzi, tiek noteikti būtiskākie riski, kā arī citas risku grupas,

kuras var pārvaldīt atbilstoši iestādes risku vadības politikai un izvēlētajai pieejai. Tas palīdz arī pēc iespējas atbilstoši novirzīt dažādus resursus (laika, finanšu, darbinieku) risku mazināšanai.

Bez risku novērtēšanas nav iespējams tos prioritizēt un vadīt lēmumu pieņemšanu attiecībā uz risku mazināšanas pasākumiem un vērtēt esošo kontroļu darbību.

Divi parametri, kas veido risku novērtējumu un izmantojami risku analīzē, ir risku iestāšanās varbūtība un ietekme. Šo parametru novērtēšanai iestādē jāizvēlas un jānosaka konkrēta novērtēšanas skala. Vērtēšanas kritēriju skalas aprakstam jābūt skaidram, lai novērtējums būtu pēc iespējas viennozīmīgs ar ierobežotām iespējām to dažādi un subjektīvi interpretēt.

Risku izvērtēšanas uzdevums ir pamatot risku vadības lēmumus.

Bez varbūtības nav iespējama risku novērtēšana, jo risks ir nezināms, vēl neiestājies notikums. Savukārt, bez potenciālās ietekmes novērtējuma nav iespējama risku prioritizēšana un risku mazināšanas pasākumu noteikšana (jo kritiskāka iespējamā riska ietekme, jo lielāka vērība un attiecīgi lielāka uzmanība un resursi būtu jāvelta riska mazināšanai).

Parasti riska līmeņa noteikšanai izmanto kombināciju no varbūtības un ietekmes, t.i., piešķirtā novērtējuma reizinājuma.

Risku novērtēšanā var izmantot kvantitatīvas un kvalitatīvas metodes vai abu šo pieeju apvienojumu.

Kvalitatīvā risku novērtēšanas metode ir piemērota valsts iestādēm, kā arī privātajam sektoram, gadījumos, kad riski ir ļoti nenoteikti un grūti prognozējami, kā arī nozarēs, kurām nav raksturīga un nepieciešama detalizēta katras darbības uzskaite.

Kvantitatīvā pieeja risku ietekmes vērtēšanā paredz skaidrus skaitliskus aprēķinus risku ietekmes noteikšanai atbilstoši iepriekš definētai ietekmes skalai un ņemot vērā pagātnē īstenojušos risku izraisītās sekas, tostarp faktiskos zaudējumus.

Stresa testēšanu var izmantot kā risku novērtēšanas metodi vai kā risku kvantificēšanas metodi. Stresa testēšana (vai arī stresa testi) ir process, kura laikā tiek novērtēta iestādes spēja turpināt darbu un uzturēt svarīgus pakalpojumus arī ārkārtas situācijās.

Būtiskākie jeb prioritārie riski ir tie, kam ir augstākā iestāšanās varbūtība un ietekme. Iestādei jānosaka, kuri riski tiek uzskatīti par būtiskajiem, atkarībā no risku apetītes, risku vadības pieejas, kapacitātes, kā arī mērķiem, t.i., kāda rīcība un papildu darbības paredzētas būtiskāko risku vadībai.

Stratēģiskie riski ir kompleksi riski, kas ietekmē visu iestādi kopumā, apdraud tās stratēģisko mērķu izpildi un darbību. To pārvaldībai ir nepieciešami būtiski resursi, sarežģīti lēmumi un citu pušu iesaiste.

Operacionālie riski ir dažādu veidu, jomu un tēmu riski iestādes struktūrvienību, funkciju, darbības virzienu vai procesu līmenī (t.i., tie nav tik apjomīgi, ka ietekmētu pilnīgi visu iestādi).

Ikdienas riskus pārsvarā nav nepieciešams atsevišķi apzināt, aprakstīt un reģistrēt risku reģistrā, jo bieži vien tie tiek mazināti ātri, operatīvi ikdienas darbībās dažādu līmeņu darbiniekiem, veicot savus tiešos darba pienākumus.

Risku vadības stratēģijai kopumā jābūt saistītai ar iestādes darbības plānu un pēc iespējas integrētai ar to. Visizplatītākās stratēģijas rīcībai ar riskiem ir:

- nodošana, pārcelšana/risku sadalīšana - pārveidojot procesu, lai samazinātu riska varbūtību/ ietekmi, vai arī riska nodošana citiem sadarbības partneriem, nododot kādu procesa daļu vai arī apdrošinot risku;
- pieņemšana – riska līmeņa akceptēšana, neieviešot risku mazinošos pasākumus, nepilnveidojot iekšējās kontroles. Šo stratēģiju izmanto tikai tad, ja nav iespējams noteikt papildu jaunus risku kontroles pasākumus vai arī, ja kontroles pasākumu ieviešana nav ekonomiski izdevīga;
- izvairīšanās, atteikšanās no darbības, kas rada risku (piemēram, no sniegtā pakalpojuma, produkta izmantošanas, veiktā procesa vai tml.). Šo stratēģiju iespējams izmantot, ja tā nav pretrunā ar tiesību aktos noteiktajām prasībām;
- riska mazināšana – ieviešot pasākumus riska ietekmes/ varbūtības mazināšanai līdz pieļaujamajam riska līmenim.

Risku mazināšanas pasākumiem un ieviešamajām kontrolēm jābūt pēc iespējas precīzāk definētām, konkrētām, reāli izdarāmām, kura ieviešanai ir piekritušas iesaistītās puses (t.i. riska īpašnieks un citi iesaistītie darbinieki) un šo pasākumu ieviešanai ir pieejami atbilstoši resursi.

Pieņemot lēmumus par risku mazināšanas pasākumu ieviešanu jāpatur prātā līdzsvars starp resursiem, kas nepieciešami risku mazināšanas pasākumiem un kopumā kontroļu uzturēšanai iestādē, un potenciālajiem zaudējumiem, ko var radīt riski.

Ieviesto risku mazinošo pasākumu efektivitāte ir jēdziens, ko lieto, lai raksturotu, cik lielā mērā kontrole samazina vai iedarbojas uz konkrēta riska izpausmi. Jo efektīvāka ir kontrole, jo lielāka ir pārliecība, ka risks tiek pietiekami vadīts.

Risku reģistrs ir "risku informācijas krātuve" jeb datubāze. Risku reģistrs ir pamata informācijas avots komunikācijai par riskiem dažādos vadības līmeņos, sanāksmēs, dažādām auditorijām, kā arī tas tiek izmantots risku uzraudzībai un aktualizācijai.

Visi riski un ar tiem saistītā informācija tiek apkopota risku reģistrā.

Iestādes risku vadītājam būtu jāuztur aktuāls risku reģistrs, šajā procesā var iesaistīties arī attiecīgo risku īpašnieki.

Ja iestādē tiek uzturēts incidentu reģistrs, to var sasaistīt ar risku reģistru.

Risku reģistram jābūt saistītam ar risku mazināšanas pasākumu plānu un tajā, ņemot vērā risku mazināšanas pasākumu statusa un progresu, jāveic risku novērtējuma aktualizācija.

Risku reģistru var apstiprināt vai citā veidā formalizēt iestādes augstākā vadība, lai tajā iekļautā informācija tiktu skaidri un formāli piefiksēta, kā arī pieņemtie lēmumi, balstoties uz riskiem, vai pasākumi to mazināšanas pārvaldībai būtu izsekojami.

Risku mazināšanas pasākumu plāns ir dokuments, kurā apkopoti ieviešamie risku mazināšanas pasākumi.

Risku mazināšanas pasākumus nepieciešams apstiprināt vai citā veidā formalizēt un piefiksēt atbilstošā iestādes vadības līmenī, lai tiem būtu skaidri paredzēti un pieejami laika, darbinieku un materiālie, kā arī jebkādi citi nepieciešamie resursi.

Visbiežāk iestādes izvēlas integrēt risku mazināšanas pasākumus risku reģistros.

Pēc risku mazināšanas pasākumu plāna izstrādes jāveic formāla, regulāra un caurspīdīga risku mazināšanas pasākumu izpildes statusa kontrole un uzraudzība, kā arī regulāra informācijas apmaiņa par pasākumu ieviešanas statusu.

Risku karte ir kopējais iestādes visu risku novērtējuma vizuāls attēlojums. Tas vienā grafikā pārskatāmi parāda risku skaitu dažādos novērtējuma līmeņos uz varbūtības un ietekmes asīm. Risku kartē var arī vizuāli attēlot risku grupas, piemēram iekšējie/ ārējie riski; personāla, juridiskie, tehniskie riski.

Risku uzraudzība nozīmē regulāru risku pārskatīšanu, nosakot, vai iepriekš piešķirtais novērtējums atbilst faktiskajai situācijai, vai un kā ir mainījušās riska kontroles un kā tās darbojas, kā arī, kāds ir risku mazināšanas pasākumu ieviešanas progress un tā ietekme uz risku.

Risku vadītāja pienākums ir koordinēt un iniciēt risku uzraudzību un būtisku izmaiņu eskalēšanu iestādes vadībai. Risku īpašnieku pienākums ir sniegt informāciju, uzraudzīt riskus un eskalēt izmaiņas. Iestādes vadības atbildība ir vērst uzmanību, ja nepieciešams riskus padziļināti analizēt, kā arī saņemot informāciju par eskalāciju no risku īpašniekiem - pieņemt nepieciešamos lēmumus, virzīt procesus risku vadībai.

Risku informācijas komunikācija ir viens no svarīgākajiem priekšnosacījumiem praktiskas, elastīgas un efektīvas risku vadības ieviešanai.

Risku informācijai ir jābūt pietiekamai un aktuālai, lai augstākā vadība varētu pieņemt uz pamatota izvērtējuma balstītus pilnvērtīgus lēmumus.

Lai risku komunikācija būtu pēc iespējas lietderīgāka, ir nepieciešams iesaistīt dažādu funkciju, līmeņu un struktūrvienību pārstāvjus. Papildu nosacījums veiksmīgai risku komunikācijai un tās pielietošanai risku vadībā ir informācijas plūsmas nepārtrauktība un regularitāte.

Kā satura pamatu risku komunikācijai būtu jāizmanto risku reģistrs un risku mazināšanas pasākumu plāns, ja tas veidots atsevišķi.

Iestādei būtu jāparedz gan skaidri noteikti un regulēti informēšanas un risku komunikācijas pasākumi, ar noteiktu regularitāti un atbildīgajiem, kā arī jāparedz iespēja veikt neplānotu risku informācijas komunikāciju nepieciešamības gadījumā.

Par riskiem, kas ir būtiski un skar ne tikai vienu iestādi, bet vairākas, kas ir būtiski valstiskā līmenī un saistīti, piemēram, ar Nacionālajā attīstības plānā vai citos valsts līmeņa plānošanas dokumentos noteiktajiem mērķiem, būtu nepieciešama plašāka komunikācija.

Iestādēs izmantoto informācijas sistēmu funkcionalitāti iespējams izmantot risku vadības procesa digitalizēšanai un optimizēšanai, ieskaitot risku identificēšanu, analīzi, risku reģistra uzturēšanu, risku mazinošo pasākumu plānošanu, kā arī pārskatu/ ziņojumu par risku vadību sagatavošanai.

6. PUBLISKAJAM SEKTORAM RAKSTURĪGĀKIE/ TIPISKĀKIE RISKI

Šajā nodaļā apkopota un strukturēti atspoguļota informācija par publiskajā sektorā identificētajiem piemītošajiem riskiem, to uzskaitījums un sadalījums (grupēti) atbilstoši jomām, balstoties uz valsts pārvaldē veikto projektu un auditu/konsultāciju ietvaros gūtiem informāciju avotiem:

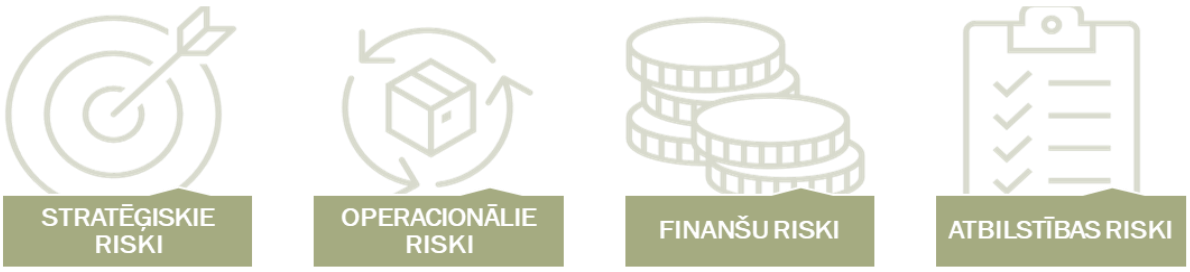
1. Iekšējo auditoru institūts sadarbībā ar Finanšu ministriju īstenoja kopīgu projektu - valsts pārvaldes iestāžu darbībā pastāvošo risku apzināšanas projektu "Riski valsts pārvaldes iestādēs"[30];
2. Atbilstoši 2021. gada 25. janvāra MK rīkojumam Nr. 47 "Par kopējām valsts pārvaldē auditējamām prioritātēm 2021. gadam", kopējā risku sarakstā integrēta risku informācija, kas iegūta auditā/konsultācijās par valsts pārvaldes iestāžu funkcijās/procesos vadītajiem riskiem"[31].

Ņemot vērā mainīgo ārējo un iekšējo vidi, apkopotā informācija par riskiem ir tikai informatīva satura materiāls (paraugs).

Risku informācijas apkopošanai un grupēšanai tika noteiktas galvenās 4 riska grupas un 17 riska apakšgrupas, kas ļauj grupēt 43 riskus pēc to rašanās cēloņiem (24. attēls).

Svarīgi: Risku grupēšanai izmanto risku grupas un risku apakšgrupas. Minētās risku grupas un apakšgrupas ir pietiekami vispārīgi formulētas, lai būtu piemērojamas praktiski visās iestādēs, taču tās var tikt apvienotas, mainītas vai papildinātas atkarībā no iestādes lieluma, darbības specifikas un sarežģītības.

24. attēls. Risku grupas

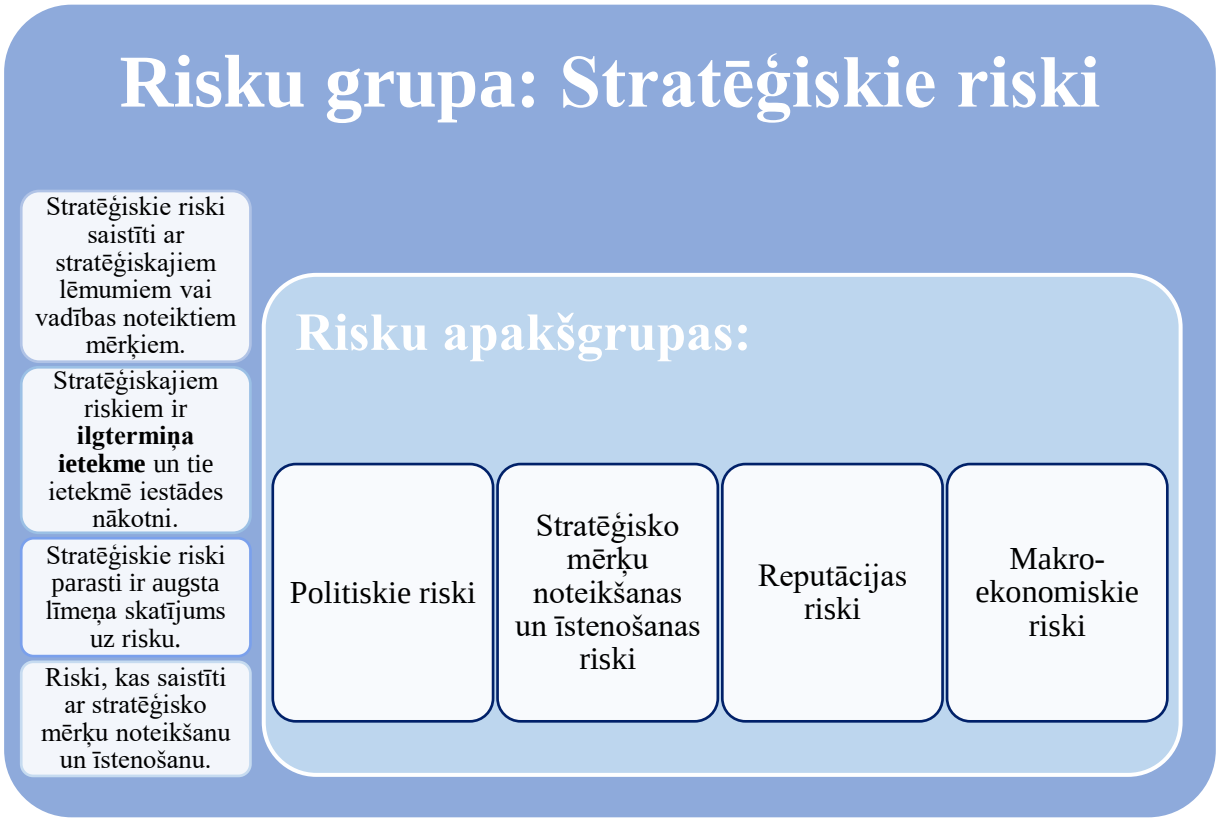


[30] Skatīt: vadlīnijas „Risku modelis valsts pārvaldei" https://iai.lv/lv/kopejais-projekts-ar-valsts-parvaldes-iestadem)
[31] Informācija no 106 dažādām valsts pārvaldes iestādēm, kuras sniedza informāciju par būtiskajiem riskiem un to izpausmes formām.

Risku sadalījums risku grupās:

- **Stratēģiskie riski**
  Stratēģisko risku grupa un apakšgrupas apraksts (25. attēls, 24. tabula, 7. pielikums):

25. attēls. Stratēģiskie riski



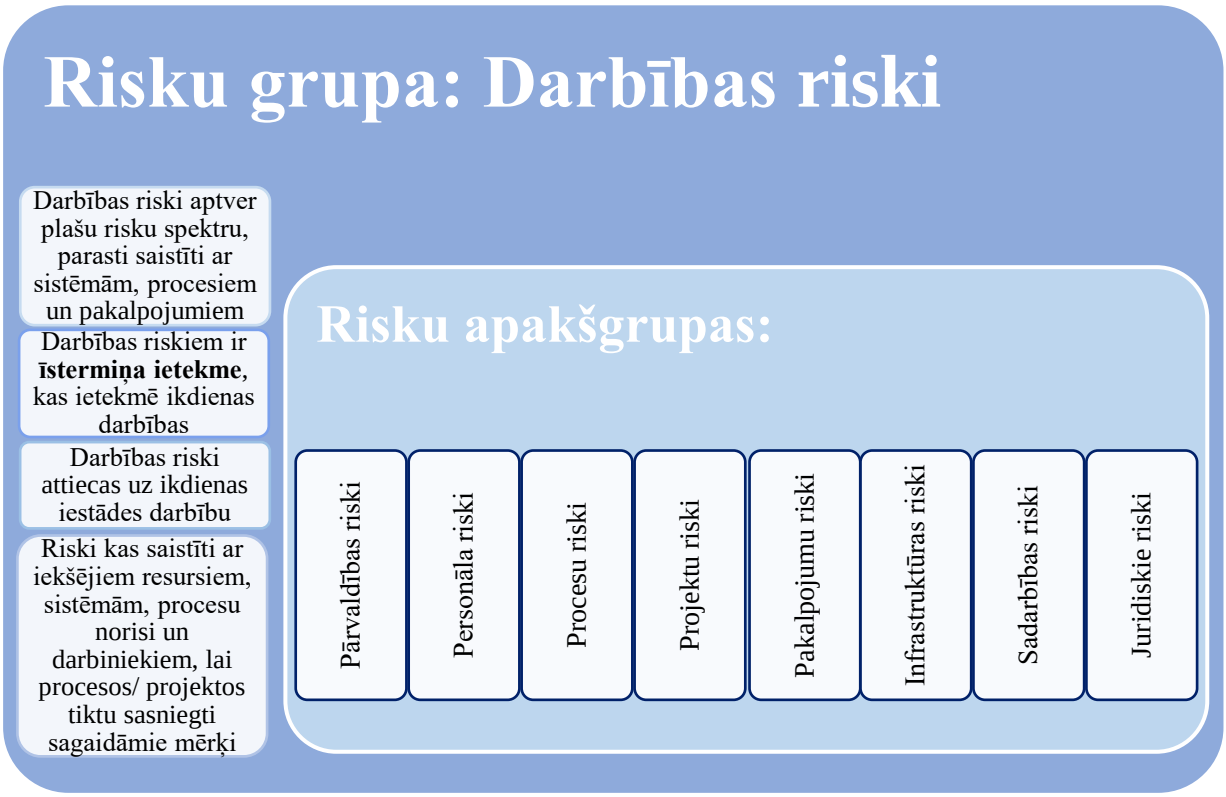
24. tabula. Stratēģisko risku apakšgrupas

Nr.p.k.	Risku apakšgrupa	Risku apraksts	**Piemērs:** Ieteikumi un kontroļu piemēri risku mazināšanai
1.	**Politiskie riski**	Politiskās vides mainība, politiski lēmumi, būtiskas izmaiņas nozares attīstības prioritātēs, bieža izmaiņu veikšana, neplānoti uzdevumi neļauj sasniegt noteiktos stratēģiskos mērķus vai pilnībā nodrošināt iestādes funkciju izpildi, apgrūtināta ilgtermiņa plānošana un plānu izpilde. Piemēram: • Politisko lēmumu ietekmes risks; • Attīstības prioritāšu svārstību/ izmaiņu risks.	Izstrādāti un aktualizēti politikas plānošanas dokumenti, izvirzīti mērķi, noteikti sasniedzamie rezultāti un termiņi. Stratēģiskās plānošanas procesa attīstības virzienu un mērķu noteikšana pēc potenciālo risku apzināšanas. Sociālo partneru iesaiste. Savlaicīga reaģēšana uz ārējās vides izmaiņām, atbilstoši aktualizējot politikas plānošanas dokumentus.
2.	**Stratēģisko mērķu noteikšanas un īstenošanas riski**	Pamatojuma trūkums prioritātēm, Īstermiņa redzējums. Politikas dokumentu kvalitāte - sasaiste ar	Veikta priekšizpēte. Skaidri, definēti un mērāmi un uz izaugsmi/ attīstību vērsti uzdevumi/darbības

Nr.p. k.	Risku apakšgrupa	Risku apraksts	**Piemērs:** Ieteikumi un kontroļu piemēri risku mazināšanai
		rādītājiem, pēctecība, savietojamība dažādām politikām. Stratēģiskā plānošana neveicina mērķu sasniegšanu. Piemēram: • Stratēģijas īstenošanas risks; • Stratēģiskās plānošanas dokumentu kvalitātes risks.	mērķu sasniegšanai, uzdevumu kaskadēšana pasākumos. Stratēģijas ieviešanai nodrošināti nepieciešamie resursi. Stratēģijas mērķu kvalitātes pārbaude (SMART, *Balanced ScoreCard*, citas metodes). Regulāra stratēģisko mērķu un darbību izpildes uzraudzība un novērtēšana, atskaitīšanās kontrolējošām iestādēm.
3	**Reputācijas riski**	Reputācijas risks var rasties gan iestādes darbības, gan bezdarbības rezultātā. Reputācijas risks ir saistīts ar negatīvo potenciālo sabiedrības viedokli par iestādi. Negatīva retorika, publiskais tēls, iedzīvotāju uzticēšanās. Piemēram: • Plašsaziņas līdzekļu neprognozējamas rīcības risks; • Sabiedrības nekorektas informētības risks.	Izstrādāta un apstiprināta aktuāla Komunikācijas stratēģija, savlaicīga komunikācija ar plašsaziņas līdzekļiem. Plašsaziņas līdzekļu un sociālo tīklu monitorings. Proaktīva atgriezeniskās saites iegūšana no klientiem un sabiedrības. Izstrādāti un apstiprināti klientu apkalpošanu reglamentējošie iekšējie normatīvie akti. Izstrādāts un apstiprināts aktuāls Krīžu komunikācijas plāns. Caurskatāma, izsekojama iestādes darbība. Regulāri un sistemātiski tiek organizēti informatīvie un komunikācijas pasākumi/kampaņas sabiedrībai, interešu grupām, ieinteresētajām pusēm.
4	**Makro-ekonomiskie riski**	Makroekonomiskās izmaiņas ietekmē ilgtermiņu attīstību un mērķu sasniegšanu. Piemēram: • Demogrāfiskās situācijas izmaiņu risks; • Globālās ekonomiskās ietekmes risks.	Stratēģiskās plānošanas analīze un makroekonomisko faktoru izmaiņu (dinamikas), tendenču un ietekmes analīze. Scenāriju izstrāde iestādes darbībai, ņemot vērā dažāda līmeņa makroekonomikas izmaiņas.

- **Darbības riski**
  Darbības risku grupa un apakšgrupas apraksts (26. attēls, 25. tabula un 7. pielikums):

26. attēls. Darbības riski



25. tabula. Darbības risku apakšgrupas

Nr.p.k.	Risku apakšgrupa	Risku apraksts	**Piemērs:** Ieteikumi un kontroļu piemēri risku mazināšanai
1.	**Pārvaldības riski**	Risks, ka iestādes struktūra neveicina iestādes mērķu sasniegšanu. Plānošana un uzraudzība haotiska, nav noteikts vienots process, kā rezultātā var neadekvāti tikt salikti uzsvari uz svarīgāko nozares politiku īstenošanas uzraudzību. Piemēram: • Organizatoriskās struktūras risks; • Darba plānošanas un uzraudzības risks.	Darbības plānā uzdevumi kaskadēdi atbilstoši iestādes mērķiem. Noteikts un apstiprināts vienots plānošanas un uzraudzības process. Skaidri noteikti uzdevumi un atbildības iestādes struktūrvienībām un amatiem, regulāra uzdevumu plānošana un izpildes uzraudzība.
2.	**Personāla riski**	Riski, kas attiecas uz personālu, tā nepietiekamām zināšanām vai prasmēm, kompetences trūkumu, personāla mainību, cilvēkresursu nepietiekamību. Atkarība no "atslēgas" cilvēkiem. Pēctecības neesamība. Attālināta darba organizēšana. Piemēram: • Darbinieku pietiekamības risks;	Personāla attīstības plānošana, tai skaitā vakanču, izaugsmes un apmācību plānošana. Ieviesta un uzturēta personāla motivācijas sistēma. Personāla aizvietošanas un pēctecības plāns. Cilvēkresursu stratēģija. Ikgadēja esošo un vēlamo kompetenču esamības izvērtēšana iestādē. Ikgadēja darbinieku novērtēšana.

Nr.p.k.	Risku apakšgrupa	Risku apraksts	**Piemērs:** Ieteikumi un kontroļu piemēri risku mazināšanai
		• Darbinieku zināšanu risks; • Darbinieku motivācijas risks.	
3.	**Procesu riski**	Riski, saistīti ar neatbilstošu, nepilnīgu, neefektīvu iekšējo procesu, nekoordinētām darbībām, kļūdām. Piemēram: • Birokrātijas/ administratīvā sloga risks; • Procesa darbību dublēšanas risks.	Procesi tiek optimizēti, izmantojot digitālos risinājumus. Noteikts process, tā soļi un procesa norises kontroles. Atbildīgo noteikšana un atbildības nodalīšana. Datu analīze un kontroles. Mācības un konsultācijas. Tehniskās kontroles un infrastruktūras risinājumi. Automatizētās sistēmu kontroles, IT risinājumu ieviešana. Stratēģiskie lēmumi, rīcības plāni. Metodiku, normatīvo aktu izstrāde. Izvērtējums par procesu atbilstību.
4.	**Projektu riski**	Riski, kā rezultātā tiek būtiski traucēta vai kavēta projekta īstenošana, neprecīza/neloģiska aktivitāšu plānošana, nepilnīga/neatbilstoša organizatoriskā struktūra, neprecīzi/neskaidri definēti uzdevumi, cilvēkresursu nepietiekamība iestādē vai to neefektīvs sadalījums, lai veiktu projektā paredzētās aktivitātes noteiktajā apjomā un laika periodā. Riski, kas saistīti ar projekta finanšu instrumentiem, finansējuma nepietiekamība vai pārtēriņš, nepareizi saplānota finanšu plūsma un inflācija, kuras dēļ uzsākot projekta īstenošanu plānotās izmaksas var būtiski atšķirties no reālajām. Riski, no piegāžu, pakalpojumu izpildes kavēšanās. Piemēram: • Projekta vadības risks; • Saistību izpildes risks.	Priekšizpēte, saplānoti un rezervēti resursi projektu īstenošanai. Laika grafiku kontrole. Starpposmu nodevumi un to kontrole.
5.	**Pakalpojumu riski**	Risks, ka iestāde nespēj savlaicīgi, pilnā apjomā un efektīvi apkalpot iestādes klientus.	Iestādē, ieviests e-pakalpojumu sniegšanas veids, kas nodrošina pakalpojumu izpildi elektroniskā veidā. Ar e-pakalpojumu palīdzību iestādei paaugstināta pakalpojumu

Nr.p.k.	Risku apakšgrupa	Risku apraksts	**Piemērs:** Ieteikumi un kontroļu piemēri risku mazināšanai
		Piemēram: • Klientu apkalpošanas kvalitātes risks; • Informācijas pieejamības risks.	pieejamība, pilnveidota iedzīvotāju apkalpošanas kvalitāte. Proaktīva atgriezeniskā saite no apkalpotajiem klientiem, sūdzību izskatīšana. Klientu apkalpošanas kvalitātes mērījumi, aptaujas.
6.	**Infrastruktūras riski**	Risks, ka iestādei nav pietiekamas tehniskās iespējas, kā arī zināšanas par infrastruktūras tehnoloģisko darbību, uzturēšanu un atjaunošanu. Piemēram: • Fiziskās drošības risks; • Darbības nepārtrauktības risks; • Īpašumu pārvaldības risks.	Darbības nepārtrauktības plāns. Skaidras noteiktas rīcības, lai nodrošinātu iestādes darbības funkcionālu nepārtrauktību. Fiziskās piekļuves kontrole. Infrastruktūras darbības uzraudzība, kritiskās infrastruktūras dublēšana.
7.	**Sadarbības riski**	Risks, kas saistīts ar valsts interešu pietiekamu un kvalitatīvu dalību starptautiskajās un vietējās organizācijās. Saistošo prasību izpratnes un piemērošanas risks. Piemēram: • Dalības starptautiskajās organizācijās risks; • Iestāžu sadarbības un informācijas apmaiņas risks; • Atkarības no ārpakalpojuma sniedzēja risks; • Deleģēšanas risks.	Tiek nodrošinātas uzņemtās starptautiskās saistības un vienošanās. Iekšēji koordinēta, iespējams, pat centralizēta sadarbība ar ārējām ieinteresētajām pusēm. Alternatīvo pakalpojumu sniedzēju izpēte. Pārdomāti deleģējuma līgumi un uzraudzības sistēma.
8.	**Juridiskie riski**	Riski, kas attiecas uz normatīvo aktu prasību neievērošanu, līgumsaistību neievērošanu un citiem juridiskiem aspektiem. Nepietiekoša juridiskā analīze un atbalsts, izstrādājot un ieviešot jaunus, un pilnveidojot esošos dokumentus u.c. Riski, kas saistīti ar normatīvo aktu neesamību, izmaiņām, piemērošanas sarežģītību, pārsūdzību pārvaldību un tiesvedības procesa efektivitāti. Piemēram: • Tiesību aktu izmaiņu riski; • Tiesiskuma nodrošināšanas riski.	Pārskatītas novecojušās normas, normatīvie akti kļūst pārskatāmi, novērstas pretrunas normatīvajos aktos. Normatīvo aktu izmaiņu monitorings.

- **Finanšu riski**
  Finanšu risku grupa un apakšgrupas apraksts (27. attēls, 26. tabula, 7. pielikums):

27. attēls. Finanšu riski

26. tabula. Finanšu risku apakšgrupa

Nr.p.k.	Risku apakšgrupa	Risku apraksts	**Piemērs**: Ieteikumi un kontroļu piemēri risku mazināšanai
1.	**Budžeta plānošanas un finanšu pārvaldības riski**	Risks, ka budžeta līdzekļi nav sasaistīti ar nozares politikas mērķu sasniegšanu, plānotie izpildes rādītāji neatspoguļo mērķu sasniegšanu. Neatbilstoša finansējuma plānošana. Plānošanas procesā netiek ņemtas vērā iespējamie nodokļu un/vai inflācijas izmaiņas. Liels uzsvars tiek likts uz budžeta izdevumu samazināšanu un pārāk mazs uzsvars uz budžeta ieņēmumu gūšanu. Piemēram: • Budžeta izdevumu risks; • Finansējuma avotu pieejamības risks; • Finanšu resursu pārvaldības risks.	Finansējuma plānošana izriet no atbilstošas nozares politikas mērķu sasniegšanas. Izstrādāti plāni budžeta sasaistei ar politikas plānošanas mērķiem. Budžeta plānošana balstās uz ilgtermiņa prognozēm un izmaiņām. Noteiktas budžeta izpildes rādītāju ievērošanas kontroles.
2.	**Budžeta izpildes riski**	Risks saistīts ar budžeta plāna faktisko izpildi. Kavēti maksājumi ar soda procentiem. Risks, ka finanšu	Noteikta un veikta regulāra finanšu līdzekļu uzskaite, digitalizācija un kontrole. Finanšu līdzekļu izpilde atbilstoši mērķim.

Nr.p.k.	Risku apakšgrupa	Risku apraksts	**Piemērs**: Ieteikumi un kontroļu piemēri risku mazināšanai
		līdzekļi tiks izmantoti nelikumīgi un neatbilstoši sabiedrības interesēm, iespējama līdzekļu izšķērdēšana un nelietderīga izmantošana. Piemēram: • Budžeta izpildes disciplīnas risks; • Budžeta struktūras un uzskaites sarežģītības risks; • Finanšu pārskatu risks.	Regulārs uzraudzības pārskats par budžeta līdzekļu izlietojumu.

- **Atbilstības riski**

  Atbilstības risku grupa un apakšgrupas apraksts (28. attēls, 27. tabula un 7. pielikums):

28. attēls. Atbilstības riski

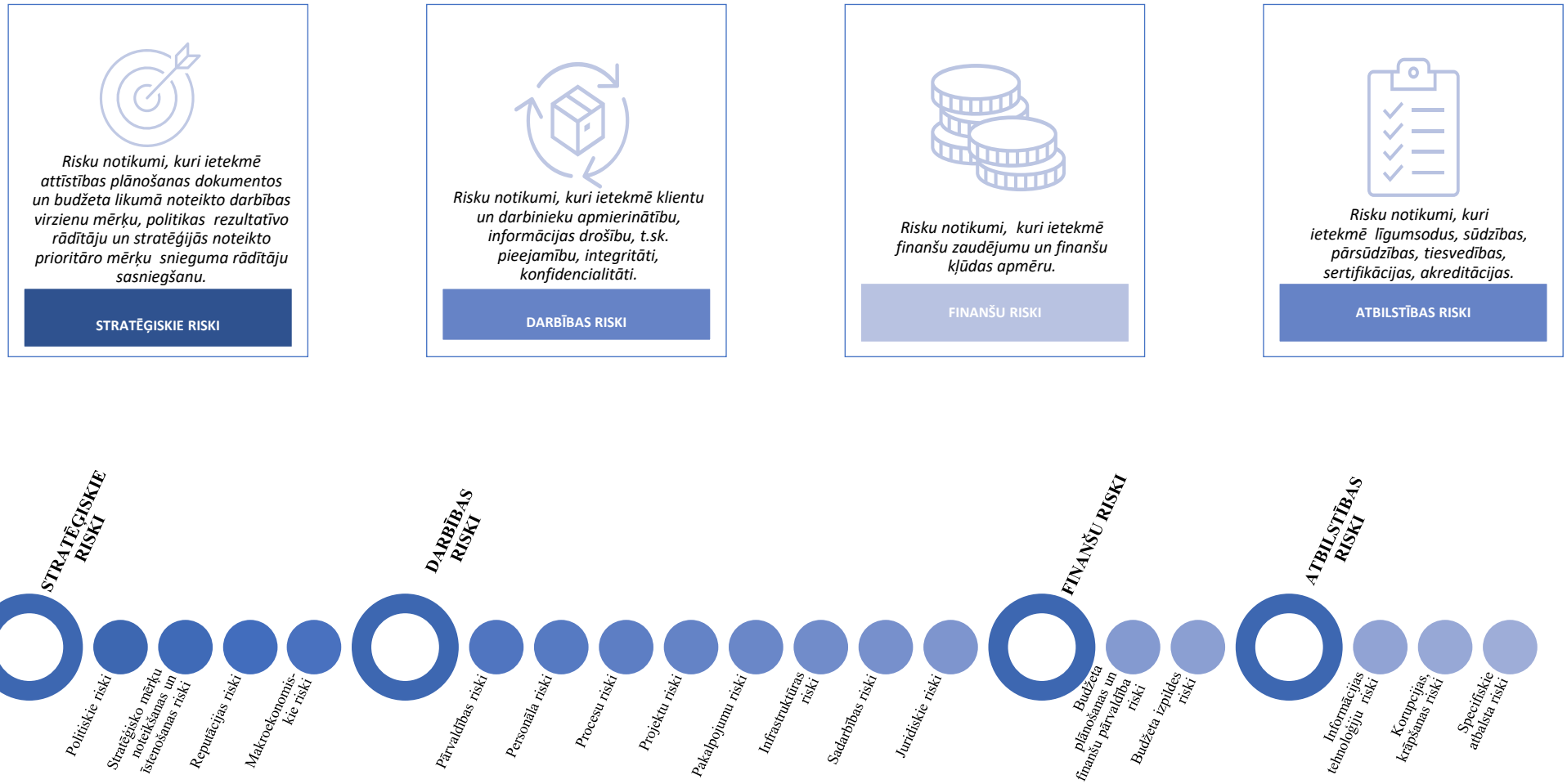
27. tabula. Atbilstības risku apakšgrupas

Nr.p.k.	Risku apakšgrupas	Risku apraksts	**Piemērs**: Ieteikumi un kontroļu piemēri risku mazināšanai
1.	**Informācijas tehnoloģiju riski**	Risks, ka informācijas drošība apdraudēta, informācijas sistēmām tiek radīti darbības traucējumi.	Informācijas tehnoloģiju (IT) pārvaldības plāni, nodrošināta to atjaunošana un darbības nepārtrauktība. Loģiskās piekļuves kontroles.

Nr.p.k.	Risku apakšgrupas	Risku apraksts	**Piemērs**: Ieteikumi un kontroļu piemēri risku mazināšanai
		Piemēram: • Nesankcionētas piekļuves risks; • Jaunu tehnoloģiju risks; • Datu kvalitātes risks.	IT sistēmu atjaunošanas plāni un rezerves kopijas. Jauno tehnoloģiju testēšana nodalītā vidē.
2.	**Korupcijas un krāpšanas riski**	Risks, ka valsts amatpersonai ir personiskas intereses, kas var ietekmēt godīgu un objektīvu valsts amatpersonas oficiālo pienākumu veikšanu. Neētiska un negodprātīga rīcība. Piemēram: • Interešu konflikta risks; • Korupcijas/ krāpšanas risks.	Strukturētu, praktisku un mērķtiecīgu korupcijas/ krāpšanas risku vadība. Rīcības plāns, kurā izklāstītas darbības korupcijas/ krāpšanas novēršanā un tās mērķu sasniegšanai, virzība un uzraudzība. Pilnvērtīgas un skaidras procedūras, ko piemēro, lai reaģētu gadījumos, kad radušās aizdomas par krāpšanu. Skaidra kārtība ziņošanai par nelikumīgām darbībām, kas nodrošina ziņotāja aizsardzību. Apmācību stratēģija korupcijas un krāpšanas apkarošanas jomā.
3.	**Specifiskie atbalsta riski**	Riski, kas saistīti ar drošību pārkāpumiem un normatīvo aktu specifisko prasību neievērošanu, kā arī neatbilstošu rīcību. Tiesību normu interpretācija. Piemēram: • Personas datu aizsardzības risks; • Darba vides risks; • Iepirkumu risks; • Sankciju risks.	Izveidota iekšējās kontroles sistēma, kas veicina sankciju regulējuma ievērošanu Kontrolējošo iestāžu un tiesas lēmumu (precedenti) analīze Apmācība, semināri, praktiski procesi un rokasgrāmatas vienotu prasību ievērošanai. Neatbilstošu situāciju uzskaite, analīze un pilnveidojumu noteikšana.

KOPSAVILKUMS

29. attēls. Tipiskie riski



7. IEKŠĒJĀ AUDITA LOMA

Iekšējais audits ir neatkarīga, objektīva pārliecības radīšana un konsultēšana, lai palielinātu iestādes vērtību un pilnveidotu tās darbības. Iekšējais audits ir viens no iekšējās kontroles sistēmas nozīmīgiem elementiem, kas palīdz iestādei sasniegt tās mērķus, ieviešot sistemātisku, disciplinētu pieeju, lai novērtētu un pilnveidotu risku vadības, kontroles un pārvaldības procesu efektivitāti[32]. Iekšējais audits novērtē iestādes iekšējās kontroles sistēmas darbību un tās efektivitāti kopumā, tai skaitā arī risku vadību un sniegt iestādes augstākai vadībai pārliecību, vai iestādē risku vadības sistēma, tostarp risku vadības process ir efektīvs, tai skaitā atbilstošs, sistemātisks, konsekvents, izsekojams, kā arī, vai risku vadības process sniedz atbalstu vadības lēmumu pieņemšanai un ir vērsts uz iestādes mērķu sasniegšanu.

Iekšējais audits sadarbojas ar atbildīgo darbinieku par risku vadību, citām struktūrvienībām un augstāko vadību un informē atbildīgo par risku vadību un augstāko vadību par audita ietvaros identificētajiem riskiem.

Iekšējais audits ir trešā līnija[33], kas neatkarīgi no pirmās un otrās līnijas, sniedz objektīvu vērtējumu par risku vadības sistēmas darbības atbilstību un efektivitāti, tai skaitā, gūstot pārliecību par pirmās un otrās aizsardzības līnijas darbības efektivitāti.

Riska vadības procesa novērtējumā iekšējam auditam jāņem vērā organizācijas darbības vide, riska apetīte un riska kultūras specifika, kā arī riska vadības ietvars.

➔ Piemērs: Iekšējais audits, veicot iekšējo auditu vai sniedzot konsultācijas, veicina risku vadības procesa pilnveidošanu un attīstību, piemēram:

- palīdz labāk izprast iestādes mērķus un novērtēt, vai tie atbilst iestādes misijai un veicina tās īstenošanu, kā arī cik lielā mērā tie ir integrēti iestādes rīcības plānos;
- novērtē, vai identificēti un novērtēti būtiskākie riski;
- palīdz koncentrēties uz sistēmiskiem un būtiskiem riskiem, kas var negatīvi ietekmēt vairākas iestādes funkcijas un uzdevumus, un novērtēt, vai nodrošināta efektīva risku pārvaldība;
- novērtē, vai iestādes stratēģija ir saskaņota ar iestādes vīziju un misiju un vai tā ir piemērota mūsdienu prasībām;
- novērtē, vai iestādei ir efektīvi un savlaicīgi risinājumi, lai nodrošinātu informācijas par riskiem pieejamību iestādes darbiniekiem, kuri iesaistīti attiecīgā riska vadībā;
- novērtē, vai iestādē nodrošināta efektīva risku mazinošo pasākumu ieviešana, tai skaitā, vai risku mazināšanas pasākumi atbilst iestādes risku apetītei;
- novērtē, vai iestādē nodrošināta atbilstošas informācijas par riskiem identificēšana un savlaicīga ziņošana.

[32] Iekšējā audita profesionālās prakses starptautiskie standarti https://iai.lv/lv/standarti-un-noradijumi
[33] Informācija par Trīs līniju aizsardzības modelis - rokasgrāmatas 3.1. nodaļā Risku vadības pārvaldība
IAI Trīs līniju modelis https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-latvian.pdf

Saskaņā ar Iekšējā audita profesionālās prakses starptautiskajiem standartiem[34] iekšējam auditam ir jāvērtē risku vadības efektivitāte un jāsekmē risku vadības procesu uzlabošana.

Risku valdības process tiek uzskatīts par efektīvu, ja iekšējais audits konstatē, ka:

- iestādes mērķi atbilst organizācijas misijai un veicina tās īstenošanu;
- ir identificēti un novērtēti būtiski riska veidi;
- ir izvēlēti piemēroti riska novēršanas pasākumi, kas atbilst organizācijas riska apetītei;
- visā organizācijā notiek atbilstošas informācijas par riskiem identificēšana un savlaicīga ziņošana, atvieglojot pienākumu izpildi personālam un vadībai.

Iekšējais audits, veicot auditu vai sniedzot konsultācijas, var ņemt vērā pieejamo informāciju par riskiem.

Piemērs: Iekšējais audits, veicot iekšējo auditu vai sniedzot konsultācijas, pārliecinās vai iestādē ir:

- noteikta misija, mērķi, izstrādāti stratēģiskie un operacionālie darbības plāni;
- izveidots un praksē izmantots risku vadības sistēmas ietvars, tai risku novērtēšanas metodika;
- noteikts risku vadības uzraudzības process, lai reaģētu uz riskiem un iespējām, kā arī, vai ir pieejami risku uzraudzības rezultāti;
- risku vadības process izveidots, ņemot vērā iestādes lielumu, darbības specifiku, dzīves ciklu, briedumu, ieinteresēto personu struktūru un tiesisko vidi;
- noteikts lomu, pienākumu un atbildības sadalījums risku vadībā;
- nodrošināta informācijas apmaiņa un diskusijas par reaģēšanas uz riskiem stratēģiju un tās piemērotību;
- informācija par vēsturiski pieredzētajiem riskiem (incidentiem);
- apzinātas izmaiņas iekšējā un ārējā vidē, kas var radīt jaunus riskus vai ietekmēt jau esošos riskus (izmaiņu vadībā tiek izmantota risku vadība);
- apzināti potenciālie riska darījumi un iespējas; tostarp jauni notikumi, nākotnes nozares izmaiņu tendences, jauni riski un iespējamie traucējumi vai pārtraukumi iestādes darbībā;
- apzināti visas tiesību aktu un citas prasības, kas attiecas uz iestādi un jurisdikcijām, kurās tā darbojas, kā arī noskaidrotas ieinteresēto pušu cerības/gaidas.

Piemērs: Iekšējā audita vai konsultācijas ietvarā iekšējie auditori iegūst informāciju par iestādes riskiem un to vadības stratēģiju no piemēram, šādiem informācijas avotiem:

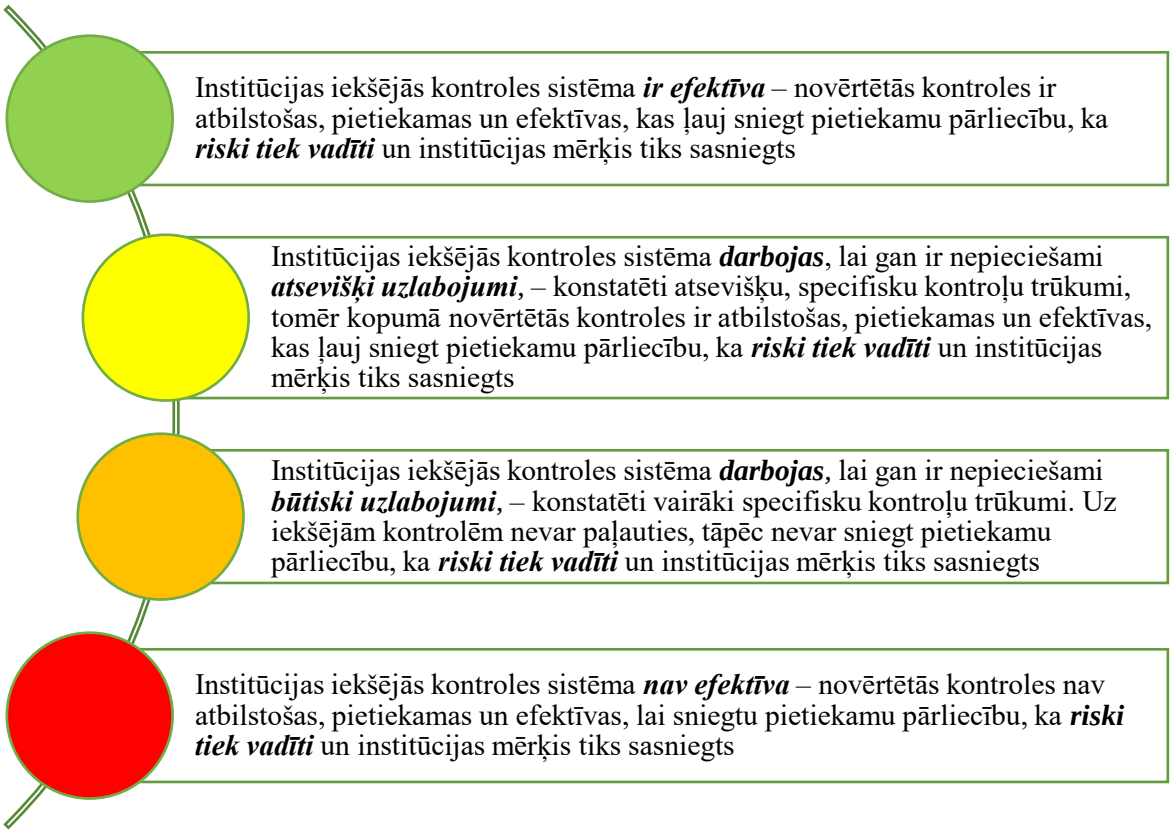
- dokumenti, kas attiecās uz risku vadības procesu (iestādes nolikumi, politikas, instrukcijas, kārtības, vadlīnijas un citi dokumenti);
- informācija par iestādē noteikto riska apetīti;

[34] Iekšējā audita profesionālās prakses starptautiskie standarti, 2120 "Risku vadība" https://iai.lv/lv/standarti-un-noradijumi

- iestādes darbības stratēģija un rīcības plāni;
- vadības/kontroles ziņojumi vai citas vadības atskaites, kas satur informāciju par darba izpildi;
- augstākās vadības, audita komitejas un citu attiecīgo komiteju, piemēram, risku vadības komitejas sanāksmju protokoli;
- nozīmīgu investīciju projektu dokumentācija;
- ārējo auditu ziņojumi;
- iestādes vadības, struktūrvienību, funkciju, procesu risku novērtējumi;
- informācija par identificētajiem riskiem (risku saraksts vai reģistrs);
- risku vadības procesa dokumentācija, kas apliecina risku identificēšu, novērtēšanu, reaģēšanu uz riskiem, tostarp mazināšanu un uzraudzību;
- risku vadības uzraudzības pasākumu rezultāti.

Lai pilnveidotu iekšējās kontroles sistēmas darbību ministrijā un iestādē[35], iekšējais audits sniedz iekšējās kontroles sistēmas darbības novērtējumu, sniedzot viedokli par iekšējās kontroles sistēmu, tai skaitā par risku vadību[36] (30. attēls).

30. attēls. Novērtējums par iekšējo kontroles sistēmu



[35] Iekšējā audita likums https://likumi.lv/ta/id/253680-iekseja-audita-likums

[36] MK 2013.gada 9.jūlijā noteikumi Nr.385 "Iekšējā audita veikšanas un novērtēšanas kārtība" https://likumi.lv/ta/id/258270-iekseja-audita-veiksanas-un-novertesanas-kartiba

Iekšējais audits var sniegt **konsultāciju pakalpojumus,** kas sniedz pievienoto vērtību un uzlabo iestādes pārvaldību, risku vadību un kontroles procesus. Iekšējo auditoru pieredze risku izvērtēšanā un izpratne par saikni starp riskiem un pārvaldību nozīmē, ka iekšējā audita struktūrvienība ir profesionāla un kompetenta, lai konsultētu augstāko vadību un veicinātu risku vadības sistēmas ieviešanu, jo īpaši tās sākumposmā.

Konsultācijas apjoms risku vadībā būs atkarīgs no iekšējā audita struktūrvienībai pieejamiem resursiem un no iestādes vajadzībām. Konsultācijas mērķis, piemēram, var būt:

- sniegt profesionālu atbalstu iestādei risku vadības sistēmas ietvara izveidei un sagatavojot "ceļa karti" tā elementu ieviešanai iestādē;
- sniegt profesionālu atbalstu iestādei risku vadības sistēmas attīstībai;
- veicināt izpratni iestādē par risku vadības mērķi un lomu iestādes pārvaldībā un mērķu sasniegšanā;
- apmācīt vadītājus un darbiniekus par risku vadības procesu, tā elementu savstarpējo saistību;
- sniegt atbalstu vadītājiem un darbiniekiem jautājumos par risku identificēšanu, analīzi, risku mazināšanas pasākumiem un iekšējām kontrolēm;
- novērtēt iestādes risku vadības sistēmas briedumu;
- dalīties ar informācijas avotiem par riskiem un to vadību;
- apzināt galvenās un būtiskākās risku vadības sistēmas problēmas vai trūkumus, to cēloņus un sniegt ieteikumus konstatēto problēmu vai trūkumu novēršanai un to seku mazināšanai.

Piemērs: Konsultatīvo pakalpojumu ietvaros iekšējais audits, piemēram, var:

- vadībai piedāvāt rīkus un metodes, ko izmanto iekšējais audits, lai identificētu un analizētu riskus un kontroles;
- organizēt seminārus, izglītot iestādes darbiniekus par riskiem un kontrolēm, kā arī veicināt kopēju valodu, izpratni un kultūru;
- sniegt padomus augstākajai vadībai par nepieciešamajiem soļiem, lai izveidotu un ieviestu risku vadības sistēmas ietvaru;
- veicināt ikgadēju risku novērtēšanu iestādē;
- sniegt atbalstu struktūrvienību vadītājiem jautājumos par risku mazināšanas pasākumiem;
- veikt salīdzinošo novērtēšanu, lai noteiktu iespējas pielāgoties vai optimizēt risku vadības praksi;
- sniegt priekšlikumus par risku vadības sistēmas attīstību.

Svarīgi: Ja iekšējais audits tiek aicināts palīdzēt vai piedalīties risku vadības procesu izstrādē, jāņem vērā iekšējā auditora neatkarības jautājums, jāizvērtē uz iekšējiem auditoriem attiecināmu Iekšējā audita profesionālās prakses starptautisko standartu (turpmāk - Standarts) prasību ietekme[37], piemēram, Standarts 1100

[37] Iekšējā audita profesionālās prakses starptautiskie standarti https://iai.lv/lv/standarti-un-noradijumi
1100 "Neatkarība un objektivitāte", 1112 "Iekšējā audita vadītāja funkcijas ārpus iekšējā audita", 1130 "Ietekme uz neatkarību vai objektivitāti" , Standarts 1130 A2

"Neatkarība un objektivitāte", īpašu uzmanību pievēršot Standartam 1130 "Ietekme uz neatkarību vai objektivitāti", kā arī Standarts 1112 "Iekšējā audita vadītāja funkcijas ārpus iekšējā audita" paredz, ja iekšējā audita vadītājs pilda vai no viņa tiek sagaidīts, ka viņš/viņa pildīs funkcijas un/vai pienākumus ārpus iekšējā audita jomas, ir jāizveido drošības sistēma, kas ierobežo neatkarības un objektivitātes mazināšanos. Ja iekšējā audita vadītājs ir atbildīgs par risku vadību vai ar to saistītām funkcijām, tad iekšējā audita darba uzdevums attiecībā uz šīm funkcijām ir jāpārrauga pusei, kas nav iekšējā audita struktūrvienībā.

Iekšējais audits palīdz izveidot vai uzlabot risku vadības procesu, taču iekšējiem auditoriem ir jāatturas no risku faktiskās vadības, proti, iekšējiem auditoriem nevajadzētu:

- veidot, uzturēt un attīstīt risku vadības sistēmu vai ietvaru;
- izstrādāt risku vadības politiku/stratēģiju, tostarp noteikt riska apetīti un toleranci;
- piemērot risku vadības procesus;
- pieņemt lēmumus par reaģēšanas uz risku stratēģiju;
- iestādes vietā ieviest risku mazināšanas vai novēršanas pasākumus;
- sniegt konsolidētus pārskatus par riskiem;
- uzņemties atbildību pār risku vadību.

Piemērs: Lai nodrošinātu iekšējā audita neatkarību un objektivitāti, gadījumos, ja iestādē iekšējam auditam noteikta atbildība par risku vadības procesu, tad šādos gadījumos, kā viens no iespējamiem risinājumiem var būt, piemēram, izveidot atsevišķas grupas iekšējā audita struktūrvienībā, kur viena komanda strādā pie risku vadības procesiem, bet otra novērtē šo procesu efektivitāti.

Svarīgi: Kad risku vadība kļūst vairāk integrēta iestādes darbībās un/ vai visos procesos, iekšējā audita loma risku vadības stiprināšanā var samazināties. Kā arī, ja iestādē tiek izveidota risku vadības funkcija, iekšējais audits lielāku pievienoto vērtību var dot, veicot iekšējos auditus nekā sniedzot konsultācijas.

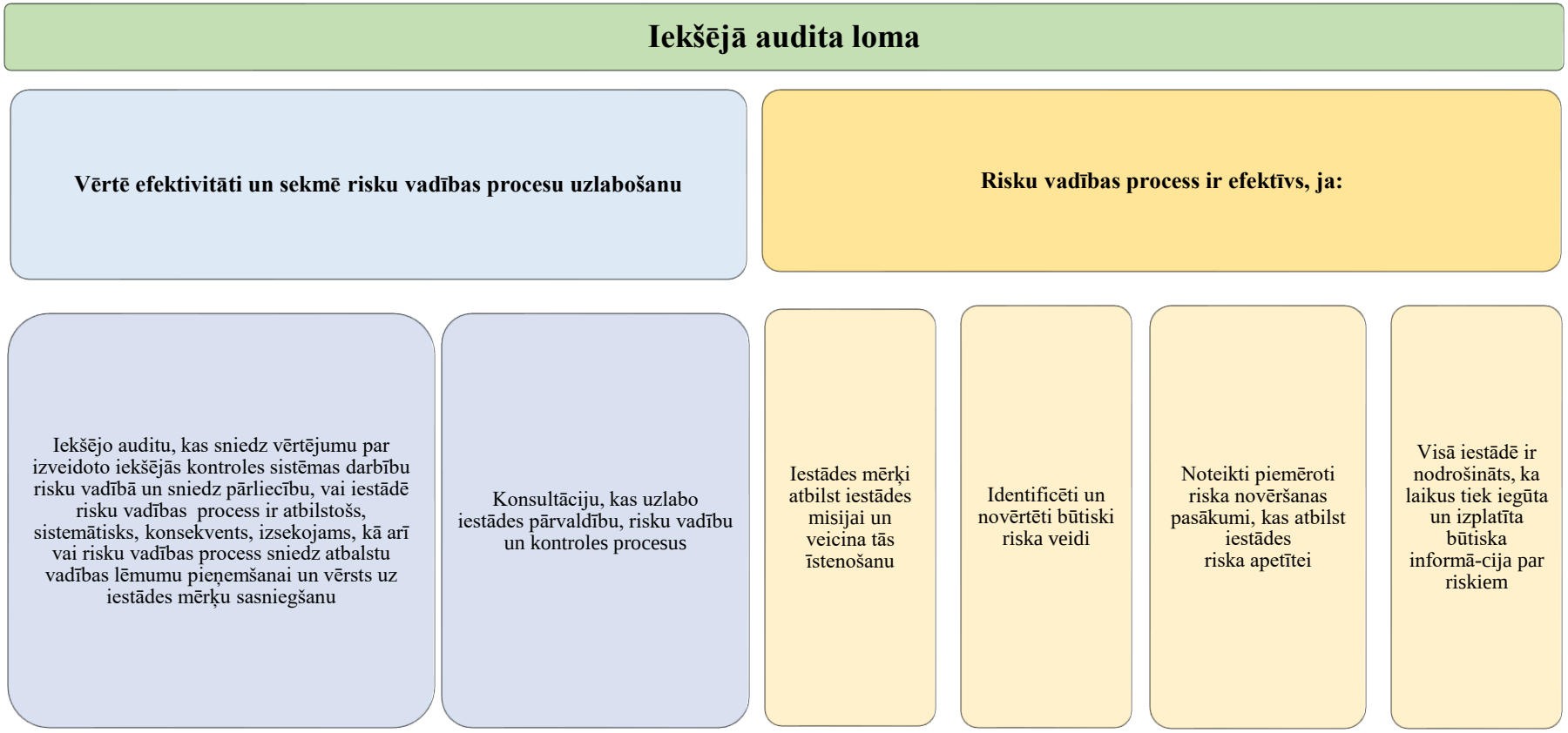
Iekšējais audits ziņo iestādes augstākai vadībai par iekšējā audita vai konsultācijas rezultātiem, kā arī sniedz ieteikumus pilnveidojumiem pirmajā un otrajā līnijā (saskaņā ar Trīs līniju modeli).

https://www.theiia.org/globalassets/site/standards/mandatory-guidance/ippf/2017/ippf-standards-2017-latvian.pdf.

KOPSAVILKUMS

Iekšējais audits veicina risku vadības procesa pilnveidošanu un attīstību, veic iekšējo auditu vai sniedz konsultāciju par risku vadības piemērotību un risku vadības procesa efektivitāti (31. attēls).

31. attēls. Iekšējā audita loma



Pielikumi

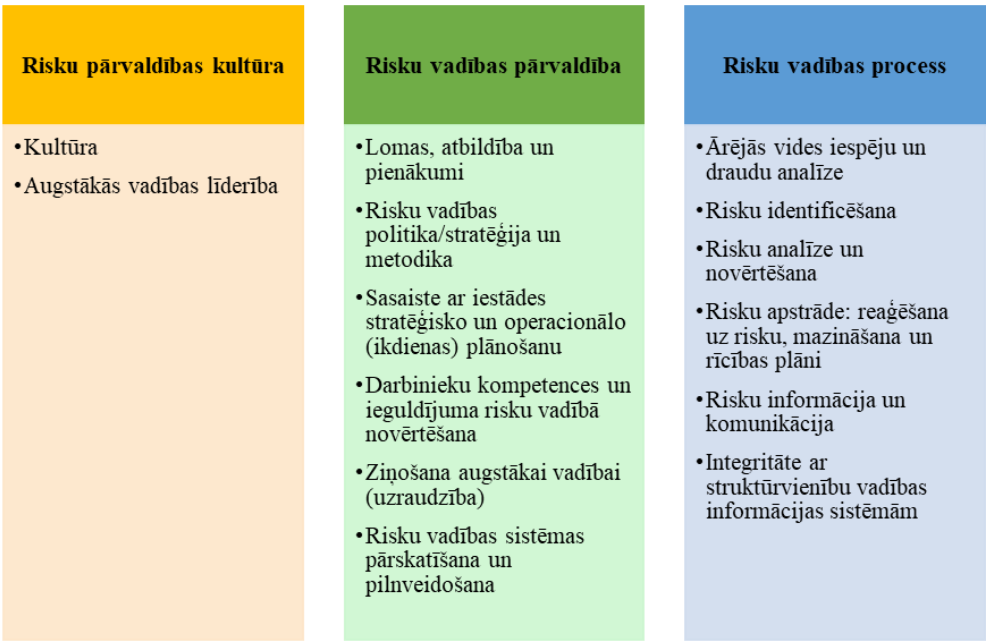
1. pielikums

1. Iestādes risku vadības sistēmas brieduma līmeņa novērtējums[38]

Vērtējot iestādes risku vadības sistēmas esošo brieduma līmeni, augstāku vērtējumu/līmeni katrā apakšjomā var piešķirt, ja iestādē ir pilnībā izpildītas zemākā/iepriekšējā līmeņa visas prasības. Vienlaikus ir jāskatās, kādas prasības ir izpildītas un kādas nē – to būtiskums kopējā risku vadības sistēmā.

Jāņem vērā, ka tiekšanās uz augstāku vai vēlamo brieduma līmeni ir jābūt iestādes augstākās vadības līmeņa lēmumam un uzstādījumam, attiecīgi augstākai vadībai sniedzot atbalstu, nepieciešamos resursus, nodrošinot kompetences celšanu.

Detalizēta novērtējuma veikšanai risku vadības sistēma ir sadalīta **3 blokos ar kopumā 14 apakšjomām**, un katrai apakšjomai tiek noteikts brieduma līmenis: esošais līmenis un vēlamais līmenis, kuru iestāde vēlētos sasniegt nākotnē. Kopumā risku vadības sistēmas briedumu iestādē vērtē piecos līmeņos (no 1. – viszemākais līdz 5. – visaugstākais).



[38] Finanšu ministrijas izstrādātais risku vadības sistēmas brieduma modelis

Risku vadības sistēmas brieduma līmeņu kopējais raksturojums:

1 Sākotnējs	2 Pamata	3 Definēts, ieviests	4 Integrēts, vadīts	5 Optimizēts, progresīvs
Iestādē tiek īstenota problēmu vadība – tiek identificēti, analizēti incidenti, problēmas, notiek informācijas apmaiņa un pieņemti lēmumi to novēršanai. Iestādes darbības plānošanā tiek ņemti vērā tikai jau notikuši incidenti, problēmas. Ikdienas pienākumu, uzdevumu īstenošana funkciju/procesu ietvaros netiek saistīta ar risku vadību – nav augstākās vadības ieinteresētība, līdz ar to nav noteikti pienākumi un atbildība, nav izstrādāti risku vadības dokumenti, nav definēta risku kultūra, nav piešķirti resursi un veicināta darbinieku izglītošana risku jautājumos.	Augstākā vadība saprot un vienojas par visaptverošas risku vadības nepieciešamību, piešķirot ierobežotus resursus risku vadības ieviešanai. Riski tiek identificēti, novērtēti un mazināti tikai atsevišķās, ļoti svarīgās iestādes darbības jomās – turklāt neregulāri un ar atšķirīgu pieeju. Iestādē galvenokārt tiek ievērotas minimālās ārējo tiesību aktu prasības risku vadības jomā. Risku vadības politika/stratēģija un metodika ir izstrādes procesā. Pienākumi un atbildība risku vadībā ir noteikta ierobežotam personālam, kuru kompetencē ietilpst risku mazināšanas jautājumi. Komunikācija par riskiem notiek ārkārtas gadījumos. Izglītošanās risku vadības jautājumos notiek darba procesā, apmācības ir reti. Atsevišķos gadījumos risku informācija tiek ņemta vērā pie darbības rezultātu izvērtēšanas un lēmumu pieņemšanas.	Augstākā vadība ievieš risku vadību, nosakot vēlamo risku kultūru, skaidru lomu, atbildības un pienākumu sadalījumu, nodrošinot nepieciešamos resursus. Risku vadība notiek iestādes stratēģiskās plānošanas, budžeta plānošanas, IKT un pamatdarbības procesos saskaņā ar skaidri reglamentētiem risku vadības principiem un pēc detalizētas metodoloģijas. Risku vadības process ir vienoti organizēts/koordinēts, dokumentāli izsekojams un uzraudzīts. Risku vadība ir stratēģiskās plānošanas sastāvdaļa. Ir regulārs ārējās vides monitorings. Komunikācija par riskiem notiek vertikāli un horizontāli. Būtisku lēmumu pieņemšanā tiek izmantota analītiskā riska informācija. Tiek pilnveidotas darbinieku kompetences risku vadības apmācībās. Risku vadības sistēmas darbības	Augstākā vadība ir proaktīva, motivē, vada un uztur visaptverošu risku vadību. Risku vadība ir nepārtraukts, konsekvents process – integrēts visās funkcijās/procesos un visos līmeņos. Prioritāte ir darbinieku pilnveidošanās risku vadībā. Risku vadības politika/stratēģija ir sasaistīta ar iestādes darbības stratēģiju. Riska apetītes formulējumi ietver gan kvantitatīvos, gan kvalitatīvos rādītājus. Riska informācija ir strukturēta vienkopus ar darba plāniem un darbības rezultatīvajiem rādītājiem. Lēmumu pieņemšana balstās uz analītisko riska informāciju, ārējās vides izpētes rezultātiem un ņemot vērā apstiprināto riska apetīti un tolerances līmeņus. Risku vadības dokumentācija, procesa/prakses un spēju efektivitāte tiek sistemātiski novērtēti pēc noteiktiem kritērijiem. Augstākā vadība	Visaptveroša risku vadība veicina iestādes procesu pilnveidošanos, optimizēšanu, sekmē iestādes darbības efektivitāti un stratēģisko mērķu sasniegšanu. Augstākā vadība ir līderis un sniedz konsultācijas citām iestādēm. Risku vadība ir integrēta iestādes pamatvērtībās, darbinieku ikdienas uzvedībā un katrs darbinieks atbilstoši savai kompetencei ir "risku vadītājs". Aktuālākā starptautiskā risku vadības pieeja tiek pārņemta iestādes risku vadības praksē, to adaptējot atbilstoši iestādes specifikai un vajadzībām. Regulāri tiek celta darbinieku kompetence. Aktīvi tiek izmantoti progresīvi, inovatīvi rīki/ tehnoloģijas, tostarp automatizējot risku vadības procesu. Riska informācijas ziņošanai ir tālredzīgs skatījums, un proaktīvi atbalsta augstāko vadību lēmumu pieņemšanā. Risku vadības sistēmas izpilde tiek

1 Sākotnējs	2 Pamata	3 Definēts, ieviests	4 Integrēts, vadīts	5 Optimizēts, progresīvs
		vērtēšanai vēl nav sistemātiskuma raksturs.	uzņemas atbildību un uzrauga nepieciešamo pilnveidojumu ieviešanu.	pastāvīgi mērīta, un augstākā vadība atbalsta pilnveidojumus, inovācijas risku vadībā, piešķirot resursus.

1. RISKU PĀRVALDĪBAS KULTŪRA

Visaptveroša risku vadība ir kultūra, iespējas/spējas un prakse, ko iestāde integrē iestādes stratēģijas izstrādes procesā un izmanto, īstenojot šo stratēģiju, ar mērķi vadīt riskus, radot, saglabājot un realizējot vērtību.

Risku pārvaldības kultūra ir attieksme, izturēšanās un izpratne par risku (gan pozitīva, gan negatīva), kas ietekmē iestādes augstākās vadības un personāla lēmumus un atspoguļo iestādes misiju, redzējumu un pamatvērtības. Kopējās kultūras veidošanā būtiska loma ir augstākajai vadībai, kurai jādemonstrē līderība, jāpierāda un jāformulē sava pastāvīga apņemšanās vadīt riskus.

1.1. Kultūra				
1 Sākotnējs	**2 Pamata**	**3 Definēts, ieviests**	**4 Integrēts, vadīts**	**5 Optimizēts, progresīvs**
• Iestādē darbība vērsta uz incidentu[39] un problēmu[40] (iestājies risks), to seku novēršanu. Veiktās aktivitātes pamatā ir	• Vajadzība pēc efektīvas risku vadības tiek veicināta augstākās vadības līmenī - augstākā vadība saprot un vienojas	• Risku vadība tiek veikta visos iestādes vadības līmeņos un galvenokārt iestādes stratēģiskās plānošanas, budžeta	• Risku vadība ir nepārtraukts, konsekvents process, kas ir vērsts uz pilnveidi.	• Risku vadība ir integrēta visās iestādes funkcijās/procesos, veicinot īstenoto procesu pilnveidošanu,

[39] Incidents - vienreizējs gadījums, notikums.
[40] Problēma - viena vai vairāku incidentu cēlonis. Problēmu vadība, lai preventīvi novērstu incidentus, noskaidrotu incidentu rašanās cēloņus un mazinātu incidentu, ko nevar novērst, ietekmi.

1.1. Kultūra				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
reaktīvas darbības (darbs ar sekām), kas iestādē liecina par problēmu vadību (esošo problēmu risināšana). • Nav risku vadības (problēmu nepieļaušana jeb nākotnes problēmu risināšana). Nav skaidras lomas, atbildība un pienākumi par risku vadīšanu. Risku vadība drīzāk tiek uzskatīta par šķērsli/ apgrūtinājumu. • Riskus vērtē iekšējā audita struktūrvienība, veicot pārliecības sniegšanas un konsultatīvos pakalpojumus.	par risku vadības nepieciešamību un pievienoto vērtību. • Iestādē tiek ievērotas minimālās ārējo tiesību aktu[41] prasības risku novēršanas jomā. Riski tiek identificēti atsevišķās iestādes darbības jomās, piemēram, pretkorupcijas, IKT, ES fondu/ĀFI projektu vadības jomās. • Galvenā uzmanība tiek pievērsta galvenajiem paredzamajiem riskiem un augsta līmeņa projektiem ar reputācijas ietekmi, nevis vispārējai iestādes kultūrai. • Augsta līmeņa riski tiek vispārīgi novērtēti	plānošanas, IKT un pamatdarbības procesos. Tā ir izveidota, lai iestāde proaktīvi rīkotos attiecībā uz potenciāli pastāvošiem riskiem (paredzētu riskus un izstrādātu plānus risku mazināšanai). • Riskiem ir noteikti vadītāji/turētāji. • Pastāv risku vadības procedūras, kas ir daļa no ikdienas darba. Ir definētas risku novērtēšanas metodes un ziņošanas līnijas. • Vienota izpratne par labas risku vadības nozīmi rada konsekventu valodas lietošanu un ar risku saistītu jēdzienu izpratni.	• Tiek regulāri veicināta visu darbinieku zināšanu, prasmju pilnveidošana, kā arī tiek motivēta to iesaistīšanās risku vadībā (atbilstoši kompetencei). Tiek atbalstīts radošums un inovatīva pieeja risku vadībā. • Vēlamā riska kultūra ir formulēta atbilstoši iestādes stratēģiskajiem mērķiem, vadības noteiktajai riska apetītei un tolerancei. • Iestādes pašreizējā riska kultūra regulāri tiek novērtēta attiecībā pret vēlamo riska kultūru. Tiek īstenotas iniciatīvas, lai palielinātu riska kultūru.	optimizēšanu, sekmējot iestādes darbības efektivitāti. Risku vadība ir integrēta visu lēmumu pieņemšanas procesā, kā arī stratēģisko un darbības mērķu noteikšanas procesā. • Risku vadība ir pilnībā integrēta iestādes profesionālajās pamatvērtībās un atspoguļojas ikdienas uzvedībā un uz inovācijām vērstā organizatoriskajā kultūrā. To atbalsta daudzpusīga pieeja nepārtrauktai apmācībai un attīstībai. • Ir uzvedības un lēmumu uzraudzība, lai

[41] Piemēram, MK 08.05.2012. noteikumi Nr. 326 "Noteikumi par iekšējās kontroles sistēmu tiešās pārvaldes iestādēs", MK 28.07.2015. noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām", MK 17.10.2017. noteikumi Nr. 630 "Noteikumi par iekšējās kontroles sistēmas pamatprasībām korupcijas un interešu konflikta riska novēršanai publiskas personas institūcijā", MK 07.10.2014. noteikumi Nr. 611 "Prasības Eiropas Savienības struktūrfondu un Kohēzijas fonda 2014.-2020.gada plānošanas perioda vadības un kontroles sistēmas izveidošanai".

1.1. Kultūra				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Augstākā vadība nav definējusi vēlamo riska kultūru.	augstākās vadības līmenī, bet risku vadība netiek veicināta visā iestādē kā proaktīvs instruments. • Risku vadība praksē var būt ļoti atšķirīga un bieži dokumentēta daļēji. • Nav skaidra sasaiste starp iestādes vērtībām un darbinieku uzvedību/rīcību un ar risku pamatotu lēmumu pieņemšanu. • Atsevišķi darbinieki un augstākā vadība lieto un saprot kopīgu riska valodu, bet šie termini nav konsekventi saprotami visā iestādē.	• Vēlamā iestādes riska kultūra ir formulēta un paziņota darbiniekiem, taču tā nav integrēta plašākā iestādes pārvaldībā – visās funkcijās/ procesos. • Pastāv skaidra sasaiste starp iestādes vērtībām un darbinieku uzvedību/rīcību un ar risku pamatotu lēmumu pieņemšanu. Vadītāji veicina un atbalsta ar risku pamatotu lēmumu pieņemšanu. • Ir pieejami pamatapmācības kursi. Tomēr lielākā daļa pieredzes tiek iegūta darbā. Daļa darbinieku norāda uz nepieciešamību paaugstināt kompetenci risku vadības jomā.		nodrošinātu atbilstību pamatvērtībām un riska apetītei, tostarp izmantojot automatizētus un iebūvētus progresīvus tehnoloģiju rīkus un paņēmienus/metodes. Tas arī ļauj iestādei veikt pamatotas, dinamiskas izmaiņas riska apetītē un procesos, lai reaģētu uz vides pārmaiņām.

1.1. Kultūra				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):				
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:				
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:				
Ir/nav nepieciešamība paaugstināt brieduma līmeni:				
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):				
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:				

1.2. Augstākās vadības līderība				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Visas aktivitātes un darbības ir problēmu risināšanas jomā, tās iniciē iestādes augstākā	• Aktivitātes, iniciatīvas risku jomā pamatā iniciē iestādes augstākā vadība, kas nodrošina ārējā normatīvajā regulējumā[42]	• Iestādes augstākās vadības darbs ikdienā saistīts ar risku vadību (piemēram, uz risku	• Augstākā vadība akcentē risku vadības nozīmīgumu un ir proaktīva, virzot, vadot un uzturot risku vadības	• Augstākā vadība apliecina pastāvīgu apņemšanos veikt risku vadību – tā nodrošina integrētu pieeju ikdienas darbības risku un

[42] Piemēram, MK 08.05.2012. noteikumi Nr. 326 "Noteikumi par iekšējās kontroles sistēmu tiešās pārvaldes iestādēs", MK 28.07.2015. noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām", MK 17.10.2017. noteikumi Nr. 630 "Noteikumi par iekšējās kontroles

1.2. Augstākās vadības līderība				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
vadība, un šīs iniciatīvas saistītas ar incidentu, problēmu novēršanu, to seku likvidēšanu, nosakot reaktīvus pasākumus problēmu novēršanā. • Iestādē nav apstiprināta risku vadības stratēģija/ politika un nepastāv integrācija ar citiem iestādes procesiem. • Risku vadībai nav piešķirti īpaši resursi.	noteikto pamatprasību ievērošanu iestādē. Vadības iniciatīvas ir neregulāras. Tā pārsvarā dod uzdevumus risku jomā ārēju iemeslu dēļ, piemēram, kad atbilstoši ārējam regulējumam jāveic kādas jomas risku analīze u.tml. • Pastāv piesardzīga attieksme aplūkot risku vadību kā visaptverošu procesu. • Augstākā vadība ir piešķīrusi ierobežotus resursus risku vadības ieviešanai.	analīzi balstītu lēmumu pieņemšana). • Vadība nodrošina iestādes stratēģisko risku identifikāciju un izvērtēšanu stratēģiskās plānošanas procesā. • Vadība pārrauga risku vadības procesu un identificētu trūkumu gadījumā pieņem lēmumus risku vadības pilnveidošanai. • Vadība nodrošina nepieciešamos resursus, lai varētu efektīvi īstenot, uzraudzīt un pārskatīt riskus.	iekļaušanu un integrēšanu visās iestādes funkcijās/ procesos – nosakot risku vadības principus, kritērijus un kārtību, kā arī nodrošinot no augšas uz leju apņemšanos labi vadīt riskus, lai atbalstītu un veicinātu inovāciju un iespēju izmantošanu iestādē. • Iestādes vadība aktīvi iesaistās risku vadības pilnveidošanas aktivitātēs. Vadība ir atvērta iniciatīvām attiecībā uz risku vadības jomu.	stratēģisko risku vadībā, pielietojot sistemātisku pieeju un piešķirot pietiekamus resursus. • Augstākā vadība rosina inovatīvu ideju, risinājumu ieviešanu risku vadībā, tostarp izmantojot jaunus rīkus, programmatūru, apmācības utt. • Augstākā vadība ir līderis un tiek uzskatīta par paraugu. Vadība sniedz konsultācijas citām iestādēm.
Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):				
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:				

sistēmas pamatprasībām korupcijas un interešu konflikta riska novēršanai publiskas personas institūcijā", MK 07.10.2014. noteikumi Nr. 611 "Prasības Eiropas Savienības struktūrfondu un Kohēzijas fonda 2014.-2020.gada plānošanas perioda vadības un kontroles sistēmas izveidošanai".

1.2. Augstākās vadības līderība				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:				
Ir/nav nepieciešamība paaugstināt brieduma līmeni:				
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 - 5):				
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:				

2. RISKU VADĪBAS PĀRVALDĪBA

Risku vadības pārvaldība ietver lomu, atbildības un pienākumu sadalījumu, risku vadības politikas/stratēģijas, metodoloģijas, tostarp riska apetītes un tolerances noteikšanu, risku vadības kompetenču attīstīšanu, kā arī risku vadības sistēmas darbības novērtēšanu un pilnveidošanu. Efektīva risku vadība caurvij visu iestādes pārvaldību – tā ir klātesošā iestādes misijas un vīzijas definēšanā, darbības stratēģijas un operacionālo plānu izstrādē, iestādei deleģēto funkciju īstenošanā (ikdienas darbībās, procesos), kā arī augstākās vadības pārraudzības pasākumos un lēmumos.

2.1. Lomas, atbildība un pienākumi				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Incidentu, problēmu novēršana praksē saistās tikai ar iestādes augstākā un vidējā vadības līmeņa kompetenci. • Iestādes vadība iesaista struktūrvienību vadītājus un darbiniekus incidentu,	• Risku vadības struktūra ir neskaidra, un kopumā nepastāv visaptveroša koordinācija. • Iestādes augstākā vadība risku jautājumiem pievēršas nepieciešamības gadījumos (piemēram,	• Iestādes augstākā vadība apzinās savu lomu un atbildību risku vadībā. Iestādē noteikta struktūrvienību vadītāju loma risku vadībā un atbildība par risku novēršanu un risku	• Risku vadības struktūra ir integrēta kopējā iestādes pārvaldības struktūrā. • Augstākā vadība apstiprina riska apetīti un riska toleranci un pārrauga pastāvīgu risku	• Iestādē ir izveidota laba/atbilstoša risku vadības struktūra, tostarp, deleģētas atbildības, viennozīmīgi skaidri un saprotami definēti pienākumi un uzdevumi. Tos regulāri izvērtē

2.1. Lomas, atbildība un pienākumi				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
problēmu novēršanā atkarībā no to kompetences, t.sk. jomas (procesa), kurā noticis incidents/ radusies problēma. • Iestādē noteikti atsevišķi darbinieki vai struktūrvienība, kam nepieciešamības gadījumā konkrētos iestādes procesos ir pienākums iesaistīties incidentu/ problēmu novēršanā. • Lomas, atbildība un pienākumi iestādes risku vadībā nav dokumentēti. • Iekšējā audita struktūrvienība identificē riskus un novērtē kontroļu darbību risku mazināšanai.	iestādei saņemot ministrijas, citas institūcijas vēstuli, kas paredz iestādes konkrētu rīcību risku jomā). • Lomas, atbildība un pienākumi nav pietiekami dokumentēti, saprotami vai konsekventi piemēroti/īstenoti visā iestādē. • Iestādes vadība noteikusi dažus darbiniekus, kas iestādē atbild par risku novēršanas jautājumiem atsevišķās/dažās iestādes darbības jomās/funkcijās un nepieciešamības gadījumā koordinē minētajās jomās/funkcijās īstenojamās aktivitātes. Šo darbinieku pienākumi risku mazināšanas jomā ir noteikti, tomēr tie ir vispārīgi. Citi konkrēto jomu darbinieki neizprot savu lomu risku	vadības procesa uzraudzību. • Visiem iestādes procesiem noteikti atbildīgie par risku vadības jautājumiem. Šo darbinieku loma, atbildība un pienākumi attiecībā uz risku vadību ir skaidri noteikti, kā arī darbinieki tos izprot un ievēro. • Risku vadības lomas un pienākumi tiek konsekventi atspoguļoti iestādes iekšējos normatīvajos aktos, amatu aprakstos, darba plānos, uzdevumos, līgumos, un politiku dokumentos. • Ir izveidota neatkarīga risku vadības speciālista amata vieta ar skaidri noteiktu atbildību un pienākumiem. Risku vadības speciālists ir atbildīgs par palīdzības sniegšanu citām	vadības sistēmas uzlabošanu. • Iestādes visu līmeņu vadītāji labi izprot risku vadības jautājumus, kā arī savu atbildību tajā. Vadītāji ir vērsti uz attīstību, un viņiem ir vadoša loma risku vadības nepārtrauktības nodrošināšanā un tās attīstīšanā (t.sk. inovāciju ieviešanā). • Risku vadībā iesaistīto darbinieku lomas (procesu vadītāji/turētāji, risku turētāji u.c.) ir skaidri nodalītas, to atbildība un pienākumi ir noteikti precīzi un viennozīmīgi saprotami. Pienākumi ir iekļauti individuālajos darbības mērķos. • Risku vadības speciālists vai risku vadības struktūrvienība koordinē	vadība, tostarp veicot periodiskas neatkarīgas pārbaudes, lai noteiktu/gūtu pārliecību, vai pienākumus un atbildību piemēro/īsteno pareizi un vai ir vajadzīgas izmaiņas, ņemot vērā mainīgos apstākļus. • Iestādes augstākā vadība tiek uzskatīta par inovatoriem risku vadības jomā. Vadība dalās pieredzē, sniedz atbalstu citām institūcijām minētās jomas jautājumos. • Katrs iestādes darbinieks atbilstoši savai kompetencei ir "risku vadītājs", kuram risku vadība caurvijas ar ikdienas pienākumu izpildi un ietverta uzvedībā (piemēram, ziņojot par risku jomu atbildīgajām personām

2.1. Lomas, atbildība un pienākumi				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
	mazināšanā, jo tā nav noteikta. • Augstākā vadība apsver iespēju veidot atsevišķu, neatkarīgu risku vadības speciālista amata vietu vai noteikt speciālistu, kuram jākoordinē risku vadības jautājumi amata pienākumu apvienošanas kārtībā.	struktūrvienībām, vienlaikus nodrošinot konsekventu un strukturētu pieeju. • Tomēr robežas starp otro un trešo aizsardzības līniju nav skaidri nodefinētas, pastāv pienākumu dublēšanās.	risku vadības aktivitātes un periodiski uzlabo risku vadības procedūras, informācijas apmaiņas procesus, kā arī regulāri ziņo augstākai vadībai par risku vadības sistēmas darbību. • Robežas starp otro un trešo aizsardzības līniju ir skaidri noteiktas un pastāv sistēmiska sadarbība starp iekšējo auditu un risku vadības speciālistu/struktūrvienību.	par riskiem vai izsakot priekšlikumus risku mazināšanai u.tml.). • Risku vadības lomas un pienākumi ir vērsti uz labās prakses integrēšanu, optimizēšanu iestādē. • Aktīvākie iestādes darbinieki – risku vadītāji tiek motivēti, kā arī atzinīgi uzslavēti. • Ir profesionāls, kompetents risku vadības speciālists (vai speciāla struktūrvienība), kas iestādē tiek uzskatīts par galveno risku vadības konsultantu un koordinatoru. • Augstākā vadība regulāri saņem pārliecības novērtējumus par risku vadības sistēmas darbības atbilstību un efektivitāti. Iekšējā audita ieteikumi veicina vienotu riska vadības praksi resorā.

2.1. Lomas, atbildība un pienākumi				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
				• Pastāv efektīva sadarbība un komunikācija starp visām trim aizsardzības līnijām.

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

2.2. Risku vadības politika/stratēģija un metodika				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Iestādē ir iedibināta hierarhiska lēmumu pieņemšanas un uzraudzības kārtība (process), kas līdzās citiem procesiem attiecas arī uz	• Risku vadības politika/stratēģija ir izstrādes procesā. • Augstākai vadībai ir izpratne par riska apetīti, bet tā vēl nav sasaistīta ar	• Risku vadības politika/stratēģija ir izstrādāta, apstiprināta un efektīvi nokomunicēta visā iestādē.	• Risku vadības politikā/stratēģijā, kas izstrādāta balstoties uz starptautisko praksi (modeļi, standarti), ir iekļauts redzējums par	• Politikā/stratēģijā risku vadība tiek uzskatīta/uzsvērta par neatņemamu iestādes kopējās pārvaldības sistēmas daļu,

2.2. Risku vadības politika/stratēģija un metodika				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
incidentu un problēmu novēršanu. • Iestādes augstākā vadība apzinās nepieciešamību izstrādāt risku vadības politiku/stratēģiju. • Augstākā vadība nav definējusi riska apetīti. • Nav noteikta vienota risku vadībā izmantojamā terminoloģija. • Metodika, kas nosaka risku vadības procesu iestādē, nav noteikta un dokumentēta.	iestādes darbības stratēģiju un nav noteikta. • Risku novēršanā iekšējais regulējums – vienkāršota metodika (t.sk. lomas, atbildība) ir noteikta atsevišķās iestādes darbības jomās (piemēram, IKT jomā u.c.), un ar to iepazinušies tie darbinieki, kas iesaistīti risku mazināšanas aktivitātēs. • Risku vadībā izmantojamā terminoloģija ir atrunāta daļēji un praksē tiek atšķirīgi pielietota (nav viennozīmīga izpratne).	• Risku vadības politikā/stratēģijā ir noteikts risku vadības politikas/stratēģijas mērķis, galvenie principi, lomu, atbildības un pienākumu sadalījums, risku, kuras iestāde vada, dalījums kategorijās un galvenās ziņošanas un uzraudzības prasības. Politika/stratēģija atspoguļo risku vadības procesu (vispārīgi galvenās līnijās). • Augstākās vadības riska apetītes paziņojums ir kvalitatīvs un skaidri ietverts risku vadības politikā/stratēģijā. Iestādes vēlme uzņemties risku pienācīgi paziņota, lai veicinātu stratēģisko un darbības plānošanu un informētu par diskusijām, kas saistītas ar risku.	risku vadības turpmāku attīstību. • Risku vadības politikā/stratēģijā ir atsauce uz riska apetīti un attiecīgajiem riska tolerances līmeņiem, kā arī izklāstīts veids, kā tiks mērīti un paziņoti risku vadības sistēmas darbības rezultāti. Politika/stratēģija ir sasaistīta ar iestādes darbības stratēģiju. • Riska apetītes formulējumi katrai riska kategorijai ietver gan kvantitatīvos, gan kvalitatīvos rādītājus/kritērijus. • Riska apetīti un ar to saistītos tolerances līmeņus augstākā vadība ņem vērā stratēģiskās plānošanas un lēmumu pieņemšanas procesos.	atspoguļojot saikni starp riskiem un iestādes stratēģisko mērķu sasniegšanu. • Risku vadības politika/stratēģija ir izstrādāta balstoties uz starptautisko labāko praksi un adaptēta atbilstoši iestādes specifikai un vajadzībām. Dokuments ir publiski pieejams sabiedrībai. • Risku vadības politika/stratēģija ietver informāciju visiem darbiniekiem un ieinteresētajām personām par resursiem un procesiem, kas paredzēti risku vadībai. • Risku vadības politikā/stratēģijā ir skaidri noteikts, kā tiks mērīti risku vadības sistēmas darbības

2.2. Risku vadības politika/stratēģija un metodika				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
		• Kopumā riska valoda (terminoloģija) ir skaidri noteikta, un to piemēro visā iestādē. • Ir izstrādāta atsevišķa (detalizēta) risku vadības metodika (kārtība, vadlīnijas u.tml.), kas aptver visus iestādes procesus un veido regulāru risku identificēšanas, analīzes, novērtēšanas, kā arī risku novēršanas/mazināšanas pasākumu noteikšanas un to izpildes mērīšanas ietvaru. Ar risku vadības iekšējo regulējumu ir iepazinušies darbinieki, kuri ir tieši iesaistīti risku vadībā. • Visaptverošā metodikas ievērošanā/pielietošanā ir vērojamas nepilnības.	Riska apetīte un tolerances līmeņi periodiski tiek pārskatīti. • Risku vadības politika/stratēģija tiek pārskatīta (uzraudzīta tās ieviešana) un atjaunināta, lai atspoguļotu izmaiņas iestādes darbības vidē. • Kopumā riska valoda (terminoloģija) ir skaidri noteikta un lielākā daļa darbinieku to viennozīmīgi izprot un pareizi pielieto. • Metodika (kārtība, vadlīnijas u.tml.) risku identificēšanai, analīze novērtēšanai, prioritizēšanai, mazināšanai, komunicēšanai un ziņošanai tiek konsekventi ievērota/pielietota viscaur	rezultāti un kā tiks pieņemti un paziņoti lēmumi par risku vadību. • Risku apetītes noteikšanā tiek izmantoti IT rīki. Informācijas sistēmās noteikti indikatori, kas norāda, kad nepieciešama rīcība attiecībā uz risku. Ir noteikta standartizēta par risku vadību atbildīgo nodarbināto rīcība (atbildība) konkrētu indikatoru rādījumu gadījumiem. • Risku vadības politika/stratēģija, tostarp riska apetīte un tolerances līmeņi sistēmiski tiek aktualizēti. • Darbinieki izprot risku vadības politiku/stratēģiju. • Risku vadības metodika (kārtība, vadlīnijas u.tml.) ir detalizēta, kvalitatīva,

2.2. Risku vadības politika/stratēģija un metodika				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
			iestādē – visos līmeņos, funkcijās/ procesos. • Metodika tiek atbilstoši aktualizēta, balstoties uz vērtējumiem par tās pielietošanu iestādē. • Metodika ir viegli pieejama darbiniekiem iestādes iekšējā tīmeklī.	papildināta ar visu procesu atspoguļojumu plūsmu shēmās, viennozīmīgi skaidri izprotama un ērti lietojama iestādes darbiniekiem.
Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):				
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:				
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:				
Ir/nav nepieciešamība paaugstināt brieduma līmeni:				
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):				
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:				

2.3. Sasaiste ar iestādes stratēģisko un operacionālo (ikdienas) plānošanu				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Iestādes darbības plānošanā tiek analizēta un izmantota informācija saistībā ar jau notikušiem incidentiem, problēmām, bet netiek vērtēti riski.	• Risku izvērtēšana, analīze tiek veikta atsevišķās iestādes jomās (procesos), piemēram, IKT riski, korupcijas riski u.tml. Analīzes rezultātā tiek sagatavoti risku novēršanas plāni. Risku analīze iestādes darba plānošanā tiek izmantota ierobežoti - iestādes stratēģijas izstrādāšanā izmantoti ārējās ietekmes iespēju un draudu un iekšējās vides aspektu analīzes materiāli, savukārt iestādes gada darba plānā tiek iekļauti atsevišķi, ar risku jomu saistīti uzdevumi, lai izpildītu ārējā tiesību akta prasību vai noteiktu pasākumus kāda riska vai problēmas novēršanai.	• Izstrādājot iestādes darbības stratēģiju, tiek ņemta vērā iespējamā ietekme, ko var radīt lielas izmaiņas iekšējā un ārējā vidē (piemēram, izmaiņas valdības politikā). Korekcijas tiek veiktas pēc vajadzības atbilstoši iestādes vadības vispārējai riska apetītei. • Risku vadība ir iestādes stratēģiskās un ikdienas darba plānošanas integrēta sastāvdaļa (piemēram, risku izvērtēšana iestādes stratēģijas un darba plānu izstrādes procesā, kā arī pirms nozīmīgiem lēmumiem). • Stratēģiskie un operacionālie riski ir izdalīti atsevišķi risku reģistrā. Risku mazināšanai izstrādāti risku novēršanas plāni vai	• Iestādes darbības stratēģija tiek izstrādāta un izdiskutēta, veicot visaptverošu "horizonta skenēšanu" un scenārija izplānošanu, šajā procesā iesaistot plašu iekšējo un ārējo ieinteresēto personu loku. Detalizētie iestādes darbības stratēģijas sasniegšanas mērķi tiek attiecīgi pielāgoti atbilstoši iestādes augstākās vadības riska apetītei un riska tolerancei konkrētās jomās. • Iestādes darba plānošanas ietvaros tiek analizēta informācija par iestādes riskiem, tādējādi darba plānos ietvertie pasākumi aptver iestādei īstenojamās aktivitātes tās funkciju izpildē un pasākumus risku ietekmes un to iespējamības mazināšanai.	• Iestādes darbības plānošanas procesa ietvaros risku izvērtēšanā tiek izmantoti progresīvi, inovatīvi rīki/ tehnoloģijas, automatizējot konkrētas darbības informācijas par riskiem apstrādē. • Stratēģiskās plānošanas procesā tiek piesaistīts plašs iekšējo un ārējo ieinteresēto personu loks, lai prognozētu dažādus scenārijus un to ietekmi uz iestādes darbības stratēģijas īstenošanu. Tas tiek darīts nepārtraukti, ļaujot reāllaikā pielāgot stratēģiju, mērķus un/vai darbības rezultatīvos rādītājus, tostarp mainoties iestādes augstākās vadības riska apetītei un riska tolerancei.

2.3. Sasaiste ar iestādes stratēģisko un operacionālo (ikdienas) plānošanu				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
		risku mazināšanas pasākumi tiek iekļauti iestādes darba plānā. Minēto plānu izpilde tiek uzraudzīta.		

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

2.4. Darbinieku kompetences un ieguldījuma risku vadībā novērtēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Prasības iestādes darbinieku kompetencēm (papildu tām, kas nepieciešamas tiešo amata pienākumu pildīšanai)	• Nepieciešamās kompetences un prasmes risku mazināšanas jomā ir apzinātas tikai tiem darbiniekiem, kas iestādē atbild par risku	• Darbinieki regulāri apmeklē mācības risku vadības jomā. Mācības īpaši tiek plānotas jomās, kurās konstatēts prasmju trūkums. Darbinieki, kuri	• Iestādes darbinieki (t.sk. jaunie darbinieki) tiek apmācīti risku jautājumos atbilstoši darba specifikai. Riska vadības mācības ir	• Darbinieku, kuru pienākumos ietilpst risku vadība, kompetence ir atzīta ārpus iestādes. • Iestādē izveidots un darbojas risku vadības

2.4. Darbinieku kompetences un ieguldījuma risku vadībā novērtēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
attiecībā uz risku novēršanas procesa specifiku nav noteiktas vai tās ir minimālas (piemēram, amata aprakstā tiem darbiniekiem, kuru pienākumos noteikta risku novēršana (piemēram, IKT jomā)). • Iestādē nav darbinieku kvalitatīvai risku analīzei, kas būtu izmantojama vadības lēmumu pieņemšanā. Iestādē ir atsevišķi speciālisti incidentu novēršanai, problēmu risināšanai tajās jomās, kur nepieciešamas speciālas zināšanas (piemēram, IKT joma).	novēršanas jautājumiem. Kopumā ir vispārīga izpratne par risku jomas pamatlietām. • Nodrošinātas atsevišķas apmācības tiem darbiniekiem, kuru kompetencē ietilpst risku mazināšanas jautājumi. Darbinieku zināšanas tiek paaugstinātas arī pašmācības ceļā un darba procesā. • Darbinieku iesaistīšanās risku apzināšanā/ mazināšanā notiek, galvenokārt, izpildot vadības norādes, rezolūcijas. Risku analīzi un novērtēšanu veic tikai atsevišķās jomās nepieciešamības gadījumā. Iestādes vadība retos gadījumos lēmumu pieņemšanai izmanto darbinieku, kuru kompetencē ietilpst risku	apmeklējuši apmācības, dalās iegūtajās zināšanās ar kolēģiem. • Darbiniekiem visos līmeņos ir zināšanas, izpratne un prasmes risku vadības jautājumos. • Darbinieki, kuru pienākumos ietilpst risku vadība, konsultē iestādes vadību specifiskos risku vadības jautājumos, kā arī sniedz analīzi (piemēram, pirms būtisku lēmumu pieņemšanas). Par risku vadības jomu atbildīgie nepieciešamības gadījumos konsultē risku jomā jebkuru iestādes darbinieku. • Ikgadējā darba novērtēšanā tiek vērtētas darbinieku, kuriem tieši deleģēti uzdevumi risku vadībā, īstenotās darbības šajā jomā.	darbinieku apmācību integrēta sastāvdaļa. • Pastāv konsekventa pieeja risku vadības prasmju noteikšanai un attīstīšanai. Risku vadības apmācību vajadzības ir iekļautas individuālajos darbības uzlabošanas plānos. • Ir ieviests mehānisms, lai darbinieki būtu informēti par risku vadības attīstību, piemēram, iestādes iekšējā avīze un citi regulāri iekšējie sakari. • Darbiniekiem, ir padziļinātas zināšanas, prasmes un augsts izpratnes līmenis, lai efektīvi vadītu riskus. • Darbinieki, kuru pienākumos ietilpst risku vadība, ir galvenie risku vadības izmaiņu iniciatori un virzītāji iestādē. Viņi pārzina iestādes procesus un spēj piemērot	centrs (struktūrvienība), kura darbinieki ir eksperti risku vadības jomā un kuri konsultē iestādes vadību, darbiniekus risku vadības jautājumos. • Iestādes eksperti risku vadību kompleksi analizē potenciālo visu līmeņu risku, iestādes procesu attīstības, kā arī risku vadības rīku progresa kontekstā. Analītiskā darba rezultātā eksperti iestādē sniedz padomus, nāk ar iniciatīvām jautājumos, kas saistīti ar iestādes risku vadības attīstību. • Tiek demonstrēta teicama zināšanu apmaiņas kultūra. • Tiek nodrošinātas regulāras profesionālas risku vadības mācības, ietverot aktualitātes, kā arī

2.4. Darbinieku kompetences un ieguldījuma risku vadībā novērtēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
	mazināšanas jautājumi, atbalstu. • Ikgadējā darba novērtēšanā netiek vērtēts darbinieku, kuri iestādē atbild par risku novēršanas jautājumiem, ieguldījums šajā jomā.		progresīvus instrumentus, rīkus risku vadības īstenošanā. • Darbinieku ikgadējā darba novērtēšanā tiek novērtētas aktivitātes risku mazināšanā. Tiek atzinīgi vērtētas darbinieku iniciatīvas risku vadībā.	labās prakses apmaiņa starptautiskā līmenī. • Periodiski tiek mērītas darbinieku kompetences risku vadības jomā. • Pastāv iespēja rotēt starp pamatdarbības un risku vadības funkcijām.

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 - 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 - 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

2.5. Ziņošana augstākai vadībai (uzraudzība)				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Iestādē ir iedibināta prakse ziņot par notikušiem incidentiem, problēmām. • Iestādes darbības rezultātu mērīšanas, novērtēšanas ietvaros netiek veikta procesu (pakalpojumu) darbību ietekmējošo faktoru analīze. Atsevišķos gadījumos tiek analizēti konkrētā procesa izpildes rādītāji, lai noteiktu, vai tajā novērsti problēmu izraisījušie faktori. • Iestādei būtisku lēmumu (piemēram, par izmaiņām struktūrā) pieņemšana tiek veikta atbilstoši vadības zināšanām, izpratnei, pieredzei konkrētajā jomā, tomēr pirms šādu lēmumu pieņemšanas netiek veikts potenciālo lēmumu izpildi	• Ziņošana par riskiem notiek pēc augstākās vadības pieprasījuma vai gadījumos, kad struktūrvienības vadība vēlas aktualizēt jautājumu (nekonsekventa prakse iestādē). Informācija galvenokārt ir par riskiem tikai atsevišķās iestādes darbības jomās/procesos (piemēram, IKT jomā), lielajos projektos. • Risku ietekmes uz procesu darbību analīze iestādes/ struktūrvienību darbības rezultātu novērtēšanas (mērīšanas) kontekstā tiek veikta vien atsevišķiem iestādes procesiem. • Uz risku izvērtēšanu balstītu būtisku lēmumu pieņemšana notiek retos gadījumos atsevišķās jomās (piemēram, IKT jomā).	• Ziņošana augstākai vadībai ir reglamentēta. • Visas struktūrvienības regulāri sagatavo un paziņo riska informāciju. Risku vadības speciālists/ struktūrvienība koordinē procesus. • Detalizētāki darbības rezultatīvie rādītāji ir ieviesti visiem procesiem iestādē. Riska informācijas ziņošanas formāts ļauj struktūrvienībām izprast attiecības starp risku un darba sniegumu. Struktūrvienību vadītāji analizē rezultatīvo rādītāju izpildi un tendences noteicošos/ ietekmējošos faktorus (riskus). Analīzes rezultāti tiek izmantoti turpmākajā darbības plānošanā un, ja nepieciešams, kontroļu pilnveidošanā.	• Risku vadības pārskati/ziņojumi ir iekļauti iestādes kopējā pārvaldības sistēmā. • Informācija par riskiem, to ietekmi un mazināšanas pasākumiem, iestādes darba plāniem un darbības rezultatīvajiem rādītājiem ir strukturēta vienkopus datu bāzē. Šī sasaiste kalpo arī kā darba plānu izpildes uzraudzības sastāvdaļa. Tiek veikta iestādes darbības stratēģijas, darba plānu, rezultatīvo rādītāju izpildes analīze, ņemot vērā risku mazināšanas pasākumu rezultātus un to ietekmi. • Dati regulārajiem pārskatiem/ziņojumiem augstākai vadībai, kā arī īpašos gadījumos pēc lēmumu pieņēmēju un risku vadītāju/turētāju	• Iestādes/ struktūrvienību darbības rezultātu novērtēšanā (mērīšanā) tiek izmantotas progresīvas, inovatīvas tehnoloģijas (rīki), nodrošinot mērījumu rezultātus no dažādiem aspektiem, atbilstoši dažādiem kritērijiem. • Pārskata/ziņojuma par riskiem sagatavošana standartizētā formā notiek automatizēti. Arvien vairāk pārskatu/ziņošanas formātu var pielāgot konkrētu lietotāju prasībām. • Regulāri tiek izvērtēta saziņas kanālu efektivitāte un funkcionalitāte, nodrošinot, ka pārskati/ziņojumi ir visaptveroši, savlaicīgi un precīzi. • Lēmumu pieņemšanas process atbilst iestādes

2.5. Ziņošana augstākai vadībai (uzraudzība)				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
ietekmējošo risku izvērtējums. Nav kritēriju esošās prakses analīzes/ novēršanas vērtēšanai.		• Lai gan pārskati ir konsekventi, datu savlaicīgums, precizitāte un kvalitāte dažādās struktūrvienībās atšķiras. • Pieņemot būtiskus lēmumus, iestādē tiek izvērtēti (analizēti) ar lēmuma pieņemšanu saistītie/ ietekmējošie riski.	pieprasījuma, tiek iegūti no kopējas datu noliktavas. • Lēmumu pieņemšanas process ir sasaistīts ar risku vadību (lēmumu pieņemšana balstās uz riska apetīti, ārējās vides analīzes rezultātiem, finanšu jomas risku izvērtējumu u.c.). • Augstākā vadība, cieši sadarbojoties ar pārskatu lietotājiem, regulāri novērtē, kāda informācija ir nepieciešama (gan lēmumu pieņēmējiem, gan administrācijas darbiniekiem kopumā), cik bieži ziņojumi ir nepieciešami, un vajadzības gadījumā veicot izmaiņas risku vadības politikā/stratēģijā, metodikā. Ir īpašas metodes, lai iegūtu un	pārņemtā risku pārvaldības modeļa/ standartu prasībām (kritērijiem). Turklāt riska informācijas ziņošanai ir tālredzīgs skatījums, lai proaktīvi atbalstītu augstāko vadību lēmumu pieņemšanas darbībās.

2.5. Ziņošana augstākai vadībai (uzraudzība)				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
			ziņotu nozīmīgu informāciju par riska kultūru.	

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

2.6. Risku pārvaldības sistēmas pārskatīšana un pilnveidošana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Saskaņā ar iekšējā audita struktūrvienības stratēģiju un gada plānu, iestādes iekšējais audits novērtē risku vadības aspektus auditējamās sistēmās.	• Pārskatīšana galvenokārt tiek veikta reaktīvā veidā. • Atsevišķos gadījumos tiek izvērtēti/ pārskatīti atsevišķi risku novēršanas prakses aspekti, lai pārliecinātos par atbilstību ārējā	• Iestādē ir mēģināts novērtēt/pārskatīt risku vadības politikas/stratēģijas īstenošanu, risku vadības procesu un tā pievienoto vērtību iestādei. Novērtēšanai ir izstrādāti	• Risku vadības dokumentācija, procesa/prakses un spēju efektivitāte tiek sistemātiski (piemēram, reizi gadā) detalizēti, visaptveroši mērīta/novērtēta, kā arī	• Risku vadība iestādē ir izveidota kā ciklisks, nepārtraukts process (sākot ar vides izpēti, beidzot ar risku vadības novērtēšanu un pilnveidošanu).

2.6. Risku pārvaldības sistēmas pārskatīšana un pilnveidošana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
	normatīvajā regulējumā noteiktajām pamatprasībām. Tomēr netiek izvērtēts, cik efektīva ir izveidotā risku novēršanas kārtība un kādu pievienoto vērtību tā sniedz iestādei. • Risku novēršanas prakse tiek pārskatīta arī pie notikumiem ar lielu ietekmi vai ja iestādei ir nodarīts nopietns reputācijas kaitējums. Izmaiņas parasti aprobežojas ar konkrēta jautājuma vai konkrētas jomas risināšanu, nevis ar sistēmiskiem jautājumiem.	atsevišķi vērtēšanas pamatkritēriji. Risku vadības sistēmas vērtēšanai vēl nav sistemātiskuma raksturs. • Balstoties uz novērtēšanas pārskatiem un tajos sniegtajiem ieteikumiem, augstākā vadība izstrādā rīcības plānus un uzrauga to ieviešanu. • Risku vadības dokumentācija tiek pārskatīta un atjaunināta saskaņā ar ieteikumiem. • Par risku vadības sistēmas darbību tiek periodiski (piemēram, reizi trīs līdz piecos gados) sagatavots neatkarīgs iekšējā audita struktūrvienības ziņojums.	salīdzināta ar citām iestādēm. Izvērtējuma rezultāti tiek izmantoti risku vadības pilnveidošanai. • Risku vadības novērtēšanas/mērīšanas kritēriji regulāri tiek pārskatīti un pilnveidoti. • Risku vadības sistēmas novērtēšanas rezultāti tiek atspoguļoti regulāros ziņojumos augstākajai vadībai. Svarīgākā informācija tiek nokomunicēta līdz struktūrvienību līmenim. • Iekšējā audita struktūrvienība periodiski sniedz neatkarīgu ieskatu un novērtējumu par risku vadības gaitu iestādē. Tā ieteikumi ir vērsti risku vadības sistēmas kvalitātes un efektivitātes paaugstināšanu.	• Risku vadības sistēmas izpilde tiek pastāvīgi mērīta, vērtējot, cik efektīvi tā veicina iestādes mērķu sasniegšanu. Iestāde arī vērtē kontroļu atbilstību jaunākajām tendencēm, sasniegumiem risku jomā. Tiek īstenota salīdzināšana ar vadošo praksi. • Risku vadības sistēmas analizēšanā tiek izmantoti IT rīki. • Risku vadības sistēmas novērtēšanas rezultāti ir pilnībā integrēti ziņojumos par darbības rezultātiem iestādes augstākai vadībai. • Risku vadības sistēmas pilnveidošanu atbalsta pietiekami un savlaicīgi piešķirti resursi.

2.6. Risku pārvaldības sistēmas pārskatīšana un pilnveidošana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
			• Augstākā vadība apstiprina resursus, kas nepieciešami, lai sasniegtu uzlabojumus risku vadībā.	

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

3. RISKU VADĪBAS PROCESS[43]

Iestādes darbojas mainīgos ārējās vides apstākļos, tāpēc ir svarīgi regulāri pētīt, analizēt, izprast ārējās vides draudus un iespējas un ņemt vērā risku vadībā. Risku vadības process sastāv no secīgām, savstarpēji saistītām un koordinētām aktivitātēm, sākot no risku identificēšanas līdz to

[43] Risku vadības procesa novērtējums sniegs pierādījumus tam, vai iestādē apstiprinātā risku vadības politika/stratēģija un metodoloģija tiek īstenota praksē – vai noteiktās prasības ir pietiekami izprastas, atbilstošas, loģiskas, efektīvas, vai ir nepieciešams aktualizēt, pilnveidot risku vadības dokumentāciju un vai ir nepieciešama papildus/turpmāka darbinieku izglītošana?

novēršanas/mazināšanas pasākumu noteikšanai un īstenošanai. Risku vadību atbalsta vertikāla un horizontāla komunikācija un dažādi IKT rīki, informācijas sistēmas.

3.1. Ārējās vides iespēju un draudu analīze				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	***5*** ***Optimizēts, progresīvs***
• Netiek veikts ārējās vides izpētes monitorings, bet ārējo iespēju un draudu izvērtējums tiek veikts virspusēji un neregulāri (saistībā ar iestādes darbības plāniem, stratēģijas izstrādi vai konkrētu incidentu/problēmu novēršanu).	• Iestādē atsevišķās jomās ir veikta ierobežota apjoma (atsevišķu aspektu) ārējās vides izpēte/ analīze. Izpētes rezultātu apkopojums tiek dokumentēts, tomēr tas ir virspusējs.	• Ārējās vides izpēte notiek periodiski, tās rezultāti tiek izmantoti iestādes darbības stratēģiskajā plānošanā, kā arī vadības lēmumu pieņemšanā.	• Ārējās vides izpēte notiek pastāvīgi. Ārējās vides tendenču analīze tiek veikta un tiek izmantota iestādes visu līmeņu darbību risku vadības procesā.	• Iestāde izmanto progresīvas tehnoloģijas ārējās vides analīzei. Rezultātus izmanto arī galvenās ieinteresētās puses (piemēram, ministrija, citas iestādes).

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

3.2. Risku identificēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Iestādē tiek apzināti incidenti un problēmas. Risku vadības process ir nākotnes ieceres līmenī. • Iestādes funkcijās/procesos riskus identificē iekšējā audita struktūrvienība, veicot pārliecības sniegšanas pakalpojumus vai konsultatīvos pakalpojumus.	• Galvenokārt tiek dokumentēti atsevišķās iestādes jomās/procesos, lielajos projektos identificētie riski, piemēram, IKT drošības riski, krāpšanas/korupcijas riski u.tml. • Nepastāv koordinēta, saskaņota, konsekventa pieeja – risku identificēšana un dokumentēšana ir atsevišķu struktūrvienību vadītāju ziņā. Ir grūtības apsvērt savstarpēji saistītus riskus. Nav standartizēta risku reģistra forma. • Risku identificēšanas un uzskaites kvalitāte ir dažāda/nevienāda. • Risku identificēšanu apgrūtina nepietiekami aprakstīti iestādes procesi	• Iestādē riski tiek identificēti regulāri, izmantojot standartizētu procesu (gan iestādes, gan struktūrvienību līmenī). Risku vadības speciālists/struktūrvienība nodrošina nepieciešamo procesa koordināciju. • Vispārīgi iestādē (jomās/procesos) identificētie riski tiek klasificēti noteiktās kategorijās. • Risku reģistri ir standartizēti, strukturēti, un riski tiek identificēti visās funkcijās/procesos un visos līmeņos, kas atspoguļots struktūrvienību plānos un mērķos. • Risku identificēšanas precizitāte katrā struktūrvienībā būs atšķirīga. Bieži tiek apsvērta saikne starp	• Riski tiek identificēti sistemātiski, konsekventi un standartizētā veidā katrā iestādes līmenī, ņemot vērā iepriekšējos notikumos gūto pieredzi. Informācija ir pilnīga, kvalitatīva, izmaiņas izsekojamas. • Risku identifikācija ir integrēta parastajās ikdienas darbībās, un šo informāciju papildina periodiskas savstarpējās starp struktūrvienību risku identifikācijas darbības, lai nodrošinātu pilnīgumu un precizitāti. • Tiek piemēroti atbilstoši rīki un paņēmieni (piemēram, procesa dokumentēšana, scenāriju analīze, riska un kontroles pašnovērtēšanas semināri), lai identificētu iespējamos riskus.	• Tiek izmantots plašs iekšējās un ārējās informācijas avotu klāsts, lai proaktīvi identificētu un centralizēti novērtētu riskus visos iestādes līmeņos, izmantojot uzlabotus rīkus, piemēram, datu analīzi, mākslīgo intelektu. • Jauni vai mainīgi riski tiek proaktīvi identificēti reāllaikā, tostarp tāpēc, ka mainās riska apetīte un risku savstarpējā saistība visās iestādes jomās/procesos. • Identificētie riski un to savstarpējās saistības tiek regulāri pārskatītas un pārbaudītas visos iestādes līmeņos.

3.2. Risku identificēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
	(procesu vadībā ir nepilnības).	dažādām jomām, taču to parasti struktūrvienības veic neatkarīgi/ individuāli. • Risku identificēšanu veicina/atvieglo attīstīta procesu vadība iestādē. • Periodiski tiek atjaunināti risku reģistri. Ir noteikta kārtība, kādā ziņo par informācijas atjaunināšanu risku reģistros, tomēr procesā ir kļūdas, kavēšanās.	• Iestādes risku identificēšana ietver apsvērumus par riskiem no visām struktūrvienībām un to savstarpējo saistību, un tas tiek veikts kopīgā procesā, kaskadējot visā iestādē iekļaušanai plānos visos iestādes līmeņos. • Koordinēta regulāra informācijas atjaunināšana risku reģistros.	

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

3.3. Risku analīze un novērtēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Tiek analizēti un vērtēti notikušie incidenti, problēmas, tostarp noskaidrojot to cēloņus, bet netiek vērtēti riski. • Riskus novērtē iekšējā audita struktūrvienība pārliecības sniegšanas pakalpojumu vai konsultāciju ietvaros.	• Risku analīze un novērtēšana tiek veikta tikai atsevišķās iestādes jomās/procesos, lielajos projektos identificētajiem riskiem, piemēram, IKT drošības riski, krāpšanas/korupcijas riski u.tml. • Analīze ir daļēji standartizēta, tās forma ir samērā vienkārša, kuras pamatā lielākoties ir subjektīvi un plaši vērtējumi, kas var ievērojami atšķirties starp struktūrvienībām un lielā mērā ir atkarīgi no vadības iesaistīšanās. • Risku lieluma mērījumu iegūst, izmantojot kvalitatīvos varbūtības un ietekmes kritērijus. • Riski galvenokārt tiek prioritizēti augsta līmeņa/sarežģītības un	• Risku analīzes, novērtēšanas process ir aprakstīts/reglamentēts un darba veidlapas ir izstrādātas, un šis process un veidlapas tiek piemērotas visās struktūrvienībās/funkcijās / procesos iestādē. • Process ir jāpilnveido, nav pietiekami detalizēts, skaidrs. Nav pietiekamu rīku, lai nodrošinātu, ka risku novērtēšana ir konsekventa visās funkcijās/procesos (piemēram, līdzīgu risku iespējamās ietekmes novērtējums atšķiras). • Tiek nodrošināts risku vadības speciālista regulārs atbalsts/konsultācijas, lai mazinātu kļūdas, veicinātu padziļinātāku izpratni un nodrošinātu	• Risku analīzes, novērtēšanas process ir integrēts kā daļa no visiem iestādes procesiem. • Risku analīzes, novērtēšanas procesa ieviešanā un darba veidlapu pielietošanā praksē ir vērojama konsekventa pieeja visās struktūrvienībās iestādē. Darbiniekiem ir skaidra, padziļināta izpratne, kas tiek panākta arī ar risku vadības speciālista/struktūrvienības uzraudzību un atbalstu. • Kvantitatīvās pieejas tiek arvien vairāk izmantotas, lai gūtu praktisku ieskatu par riskiem. Scenāriju analīze un simulācijas tiek izmantotas konsekventi un regulāri.	• Risku analīze tiek veikta, izmantojot integrētu riska novērtēšanas sistēmu, kuras pamatā ir plašs kvalitatīvu un kvantitatīvu datu klāsts (gan iekšējie, gan ārējie). Tiek izmantoti progresīvi tehnoloģiskie rīki (piemēram, mākslīgais intelekts), lai kartētu cēloņu un seku sakarības, ieskaitot ietekmi uz savstarpēji saistītiem riskiem. • Iestādes prioritāro risku saraksts tiek atjaunināts, un arvien vairāk tiek ņemti vērā riski, kas saistīti ar citām iestādēm un valdības prioritātēm.

3.3. Risku analīze un novērtēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
	liela budžeta projektos, kas saistīti ar nozīmīgiem reputācijas, krāpšanas riskiem.	lielāku konsekvenci iestādē. • Pakāpeniski tiek izmantotas standartizētas kvantitatīvās riska analīzes metodes, lai visaptveroši konsekventi papildinātu kvalitatīvo analīzi visā iestādē. Augsta riska zonās arvien vairāk tiek izmantota scenāriju analīze un/vai simulācijas, lai pārbaudītu un uzlabotu riska analīzes kvalitāti un uzticamību. • Augstākā vadība ir skaidri noteikusi riskus ar augstāko prioritāti, kas var ietekmēt iestādes mērķus un iespējas, kā arī struktūrvienību mērķu sasniegšanu.	• Augstākā vadība uztur iestādes prioritāro risku sarakstu, kas tiek novērtēts saistībā ar iestādes mērķiem. Riski programmas vai procesa līmenī ļauj pieņemt lēmumus, pamatojoties uz pilnīgu izpratni par lejupējiem un augšupējiem riskiem un savstarpēji saistītiem riskiem. • Pastāv zināma tehnoloģiju izmantošana, lai uzlabotu risku analīzes, novērtēšanas procesa konsekvenci un kvalitāti.	
Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):				
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:				

3.3. Risku analīze un novērtēšana				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:				
Ir/nav nepieciešamība paaugstināt brieduma līmeni:				
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):				
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:				

3.4. Risku apstrāde[44]: reaģēšana uz risku, mazināšana un rīcības plāni				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Iestādē ir iedibināta prakse risināt un novērst notikušos incidentus un problēmas, balstoties uz to cēloņu apzināšanu. Iestādes augstākās vadības līmenī tiek pārrunāti risinājumi līdzšinējo problēmu	• Risku analīzes, novērtēšanas rezultātā tiek sagatavoti risku apstrādes/mazināšanas plāni. Plāni ir izstrādāti galvenokārt atsevišķās iestādes jomās/procesos, lielajos projektos identificētiem un novērtētiem riskiem,	• Risku apstrādes/mazināšanas plāni tiek izstrādāti standartizēti un par datiem vairākos iestādes līmeņos, koordinējot struktūrvienības. Šajos plānos tiek ņemts vērā iestādes konteksts/vide (iekšējā un ārējā);	• Visas iespējamās risku apstrādes/mazināšanas iespējas, tostarp attiecībā uz savstarpēji saistītiem riskiem, tiek rūpīgi apsvērtas un pārbaudītas, lai nepieciešamības gadījumā izvēlētos atbilstošāko risku apstrādes pieejas.	• Risku apstrādes/mazināšanas iespējas ir noteiktas, izmantojot integrētu risku novērtēšanas sistēmu, kas izmanto progresīvus tehnoloģiskos rīkus (piemēram, mākslīgo intelektu) izmaksu un ieguvumu aprēķināšanai.

[44] Risku apstrāde – *Risk Treatment*

3.4. Risku apstrāde[44]: reaģēšana uz risku, mazināšana un rīcības plāni				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
atkārtotai nepieļaušanai nākotnē. • Iekšējā audita struktūrvienība novērtē iedibināto kontroļu atbilstību un efektivitāti identificēto risku mazināšanai, kā arī sniedz ieteikumus nepieciešamo papildu kontroles pasākumu ieviešanai un kopējās IKS stiprināšanai.	piemēram, IKT, krāpšanas/korupcijas riski u.tml. • Risku apstrādes/mazināšanas plāni tiek izstrādāti struktūrvienību līmenī daļēji standartizētā formātā, kurā nepieciešams izmaksu un ieguvumu novērtējums un apstrādes izvēles paskaidrojums. Tas bieži tiek darīts subjektīvi un ir ļoti atkarīgs no augstākās vadības iesaistīšanās. Rezultātā var būt dažādas/plašas variācijas. • Risku apstrādes/mazināšanas plāni tiek nokomunicēti augstākai vadībai. • Risku mazināšanas pasākumi no efektivitātes viedokļa pamatā netiek vērtēti. Konkrēti risku mazināšanas pasākumi, to	izmaksas un ieguvumi; pienākumi un gaidas; risku prioritātes noteikšana; riska apetīte; riska smagums un atlikušais risks. • Augstākā vadība regulāri centralizēti izskata risku apstrādes priekšlikumus, koncentrējoties uz iestādes līmeni un augstāka riska projektiem. Iestādes līmeņa risku apstrādes/mazināšanas plāni tiek apkopoti, taču tos nevar regulāri koplietot iestādē. • Tiek nodrošināts risku apstrādes/mazināšanas pasākumu uzraudzības process – vai kontroles mazina riskus, vai to īstenošana sasniedz to izveidošanas mērķi, vai kontroles ir lietderīgas. Kontroļu vērtēšana notiek atbilstoši noteiktiem	• Reakcijas uz riskiem (kontroles) ir proporcionālas riska līmenim, ieskaitot iestādes noteikto riska apetīti un tolerances līmeni. • Visu struktūrvienību risku apstrādes/mazināšanas plānu apstiprināšanu veic pēc vienotas kārtības. • Sistemātiski tiek pārbaudīta risku apstrādes efektivitāte. Atsevišķi tiek apsvērti gadījumi, kad risku apstrāde var prasīt iestādes darbības stratēģijas vai mērķu pārskatīšanu.	• Risku apstrādes/mazināšanas iespējas tiek pastāvīgi uzraudzītas, ņemot vērā jaunāko informāciju, tostarp par to efektivitāti un attiecībā uz ierosinātajām izmaiņām iestādes darbības stratēģijā, mērķos un uzvedībā. • Lai izvairītos no dublēšanās un nevajadzīgām izmaksām, tiek izskatītas riska apstrādes/mazināšanas iespējas, kas var novērst vairākus riskus.

3.4. Risku apstrāde[44]: reaģēšana uz risku, mazināšana un rīcības plāni				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
	īstenošana tiek pārskatīta, ja iestādē rodas problēma un tās atrisināšanai noteiktais pasākums vai to kopums ir jāpilnveido.	kritērijiem, un izvērtējuma rezultātā, ja nepieciešams, kontroles tiek pilnveidotas.		
Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):				
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:				
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:				
Ir/nav nepieciešamība paaugstināt brieduma līmeni:				
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):				
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:				

3.5. Risku informācija un komunikācija				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Iestādē iekšienē ir iedibināta horizontālā un vertikāla komunikācija incidentu un problēmu novēršanas risināšanai.	• Informācija par riskiem tiek iegūta atsevišķās iestādes darbības jomās, lielajos projektos – galvenokārt struktūrvienību līmenī, un	• Iekšējā regulējumā ir noteikta riska datu/informācijas vākšanas un apkopošanas, iekšējās komunikācijas (informācijas apmaiņas)	• Risku informācija ir analītiska, būtiska, atbilstošā detalizācijas pakāpē, pietiekama, kvalitatīva, uzticama un savlaicīga.	• Progresīva datu analīze, piemēram, izmantojot mākslīgo intelektu, tiek izmantota, lai apkopotu, pārveidotu un analizētu lielu datu apjomu skaidrā

3.5. Risku informācija un komunikācija				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Iestādes komunikācija ar ieinteresētajām pusēm (piemēram, ministrija, citas iestādes utt.) incidentu/ problēmu novēršanas jomā ir neregulāra, un komunikācijas iniciatore ir cita institūcija (piemēram, saņemts informācijas pieprasījums).	apjoms un nozīmīgums ir atkarīgs no vadības iesaistes un kompetences konkrētās darbības jomās, kā rezultātā ir atšķirīga/mainīga un lielākoties reaktīva pieeja risku vadībā. • Dati tiek glabāti elektroniskā formā (galvenokārt, MS Word un/vai MS Excel programmās). Datu apkopošana par riskiem ir manuāla un darbietilpīgs process. • Informācija par riskiem ir bieži nepilnīga, neprecīza, nekonsekventa attiecībā uz detaļām, pretrunīga vai novecojusi. • Risku jautājumos dominē "vertikālā" komunikācija (informācijas apmaiņa) – tā pamatā notiek pēc iestādes vadības	kārtība (process u.tml.) risku vadības ietvaros (piemēram, sadarbība risku novērtēšanā, risku mazināšanas pasākumu plānošanā, incidentu gadījumos, ziņojumu sniegšanā u.tml.), kā arī darbinieku pienākumi, atbildība komunikācijas procesā (piemēram, ziņojumu iesniegšanā). • Ir noteikti riska informācijas standarti, un ir pieejami dažādi kanāli, lai paziņotu informāciju par risku tiem, kam ir noteikti/deleģēti risku vadības pienākumi. • Iestādē identificēti un atsevišķi ir izdalīti komunikācijas riski. • Risku vadībā iesaistītie darbinieki savstarpēji komunicē (horizontālā komunikācija) savas	• Informācija par riskiem, to ietekmi un mazināšanas pasākumiem, iestādes darba plāniem un darbības rezultatīvajiem rādītājiem ir strukturēta vienkopus datu bāzē. • Nodarbinātie apspriež labāko praksi un tendences risku vadībā un savstarpēji dalās pieredzē. • Iestāde dalās pieredzē, komunicē ar citām iestādēm risku vadības jautājumos. No ieinteresētajām pusēm iestādē saņemtie viedokļi, ierosinājumi, bažas risku jomā tiek ņemtas vērā risku vadības procesā (piemēram, risku izvērtēšanā, pasākumu noteikšanā u.tml.).	un viegli saprotamā risku vadības informācijā. • Analītiskā informācija arvien vairāk ir pieejama darbiniekiem visā iestādē. • Iestādē tiek izmantotas IKT tehnoloģijas ar risku vadību saistītās informācijas sniegšanā, iniciatīvu ierosināšanā, veicinot visu iestādes darbinieku aktīvu iesaisti risku vadībā. • Iestāde un ieinteresētās puses komunicē par specifiskiem risku vadības jautājumiem. Ieinteresētajām pusēm ir augsta uzticamība attiecībā uz iestādes riska vadību.

3.5. Risku informācija un komunikācija				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
	iniciatīvas, kad konkrēti jautājumi nonāk vadības darba kārtībā. • Komunikācija ar ieinteresētajām pusēm risku jautājumos notiek nepieciešamības gadījumos (piemēram, informācijas sniegšana citai institūcijai u.tml.). Retos gadījumos iestāde ir iniciatore ārējā komunikācijā risku jautājumos.	kompetences ietvaros (piemēram, par risku novēršanas pasākumu īstenošanas gaitu, problēmām). • Iestādē noteikta kārtība (process) iestādes sadarbībai risku vadības jomā ar ieinteresētajām pusēm (t.i., ārējā komunikācija). Nepieciešamības gadījumā iestāde risku vadības jautājumos sadarbojas ar citām iestādēm.		

Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):	
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:	
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:	
Ir/nav nepieciešamība paaugstināt brieduma līmeni:	
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):	
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:	

3.6. Integritāte ar struktūrvienību vadības informācijas sistēmām				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
• Uzkrāta un apkopota informācija ir par notikušiem incidentiem, problēmām, to novēršanu. Šī informācija pamatā glabājas darbinieku, kas tika iesaistīti problēmu/ incidentu novēršanā, datoros. Atsevišķos gadījumos informācija ir pieejama lietvedības (dokumentu vadības) sistēmā (piemēram, darba plānā ar problēmas novēršanu saistīts uzdevums, kā arī informācija par uzdevuma izpildi darba plāna izpildes kontroles kontekstā).	• Informācija risku jomā tiek apstrādāta, apkopota un saglabāta atsevišķā, risku vadībai veltītā, direktorijā (piemēram, koplietošanas mapē, MS Word un/vai MS Excel programmās izveidotās informācijas sistēmās (tabulās)), kurai piekļuve ir darbiniekiem, kuru kompetencē ietilpst risku mazināšanas jautājumi. • Savukārt iestādes lietvedības (dokumentu vadības) sistēmā ietilpst iekšējās/ ārējās sarakstes dokumenti risku jomā, ar risku mazināšanu saistīti uzdevumi un informācija par to izpildi.	• Par risku vadības īstenošanu atbildīgie darbinieki risku vadības procesa ietvaros daļēji izmanto informācijas sistēmu (-as) funkcionalitāti. No risku vadībā izmantojamās informācijas sistēmas datus apstrādei, analīzei nepieciešamības gadījumā iespējams migrēt uz citām informācijas sistēmām.	• Risku vadībā izmantotā informācijas sistēma ir sasaistīta ar citām iestādes informācijas sistēmām, un ir pieejama lietošanai (atbilstoši kompetencei) visiem risku vadības procesā iesaistītajiem darbiniekiem.	• Risku vadībā izmantotā informācijas sistēma nodrošina darbības iespējas tiešsaistē. Darbinieki informācijas sistēmā redz visu aktuālo informāciju par pastāvošiem riskiem visās darbības jomās/procesos. • Darbiniekiem informācijas sistēmā ir iespēja sniegt priekšlikumus, idejas, ziņot par novirzēm procesos.
Brieduma pašnovērtējums – norāda esošo līmeni (veselos skaitļos no 1 līdz 5):				
Norādīt galvenās pazīmes, dokumentu nosaukumus, ka iestāde atbilst pašnovērtējumā norādītajam esošajam līmenim:				

3.6. Integritāte ar struktūrvienību vadības informācijas sistēmām				
1 **Sākotnējs**	**2** **Pamata**	**3** **Definēts, ieviests**	**4** **Integrēts, vadīts**	**5** **Optimizēts, progresīvs**
Nepieciešamās aktivitātes, lai pilnveidotu pašnovērtējumā norādīto esošo līmeni:				
Ir/nav nepieciešamība paaugstināt brieduma līmeni:				
Norādīt iestādei vēlamo brieduma līmeni (kuru iestāde vēlētos sasniegt) (veselos skaitļos no 1 līdz 5):				
Nepieciešamās aktivitātes, lai sasniegtu vēlamo brieduma līmeni:				

Brieduma modeļa izstrādē izmantotie avoti:

1. LR Finanšu ministrijas, Izglītības un zinātnes ministrijas, Labklājības ministrijas un Tieslietu ministrijas iekšējā audita struktūrvienību prakse.
2. Comcover Risk Management Benchmarking Program: Risk Management Capability Maturity Model, Australian Government, 2021.
3. Commonwealth Risk Management Capability Maturity Model, Australian Government, 2016.
4. Enterprise Risk Management: A “risk-intelligent” approach, Deloitte, 2015.
5. IPPF – Practice Guide: Assessing the Risk Management Process, Global IIA, 2019.
6. OECD Tax Administration Maturity Model Series: Enterprise Risk Management Maturity Model, OECD, 2021.
7. Risk Management Maturity Assessment Tool, Audit Office of New South Wales, 2015.
8. Risk Management Assessment Framework: a tool for departments, HM Treasury, 2009.
9. Risk Management Maturity Assessment at Central Banks, IMF Working Paper, International Monetary Fund, 2019.
10. The All-of-Government Enterprise Risk Maturity Assessment Framework, New Zealand Government, 2020.

2. pielikums

2. Pārbaudes jautājumu lapa par esošās risku vadības situācijas novērtējumu

Iestādes nosaukums: Lai ievadītu tekstu, noklikšķiniet vai pieskarieties šeit.

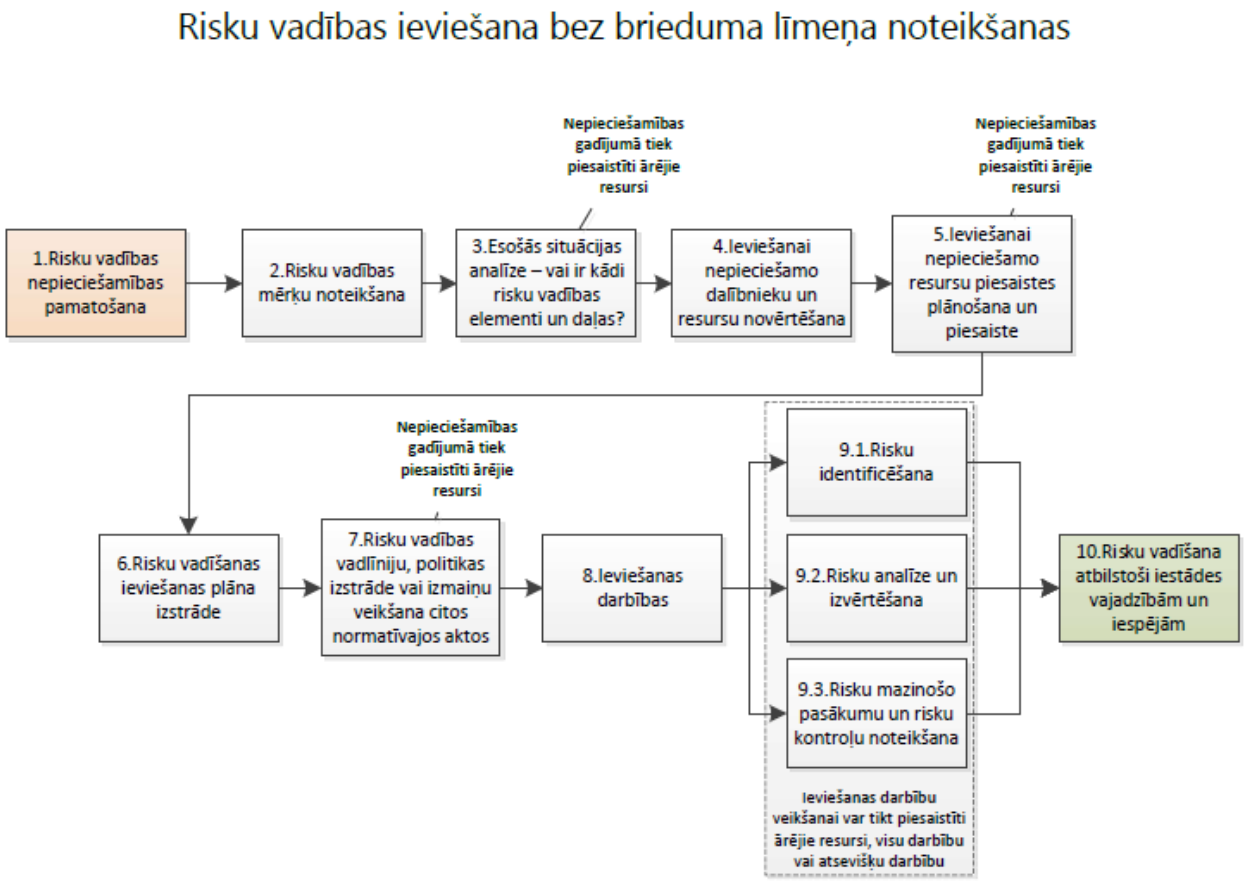
Novērtējuma datums:	Noklikšķiniet vai pieskarieties, lai ievadītu datumu.

Nr.	Jautājums	Jā	Nē	Daļēji	Piezīmes
1.	2. (*Šajā kolonnā iekļauti jautājumi par risku vadības brieduma pamatelementiem*)	3.	4.	5.	6. (*Šajā kolonnā iekļauj piezīmes, ja daļēji atbilst kādam no apgalvojumiem, norādot, kas konkrēti atbilst un kas būtu uzlabojams), atsauces uz dokumentu, saites, u.tml.*)
1	Noteiktas risku vadības lomas, atbildības un pienākumu sadalījums (rīkojums, nolikums, amata apraksts, struktūra)	☐	☐	☐	
2	Noteikts atbildīgais par risku vadību (rīkojums, amata apraksts)	☐	☐	☐	
3	Izveidota risku vadības ieviešanas darba grupa (rīkojums, nolikums)	☐	☐	☐	
4	Iestādes augstākā vadība izdevusi rīkojumu par risku vadības ieviešanu	☐	☐	☐	
5	Izstrādāts un apstiprināts risku vadības ieviešanas plāns	☐	☐	☐	
6	Iestādē ieviests ISO 9001	☐	☐	☐	
7	Iestādē ieviests ISO 31 000:2018	☐	☐	☐	
8	Iestādē ieviests COSO ERM	☐	☐	☐	
9	Iestādē ieviesti citi standarti vai vadlīnijas, kuru prasības paredz risku vadību vai tās elementus	☐	☐	☐	
10	Iestādē tiek vērtēti stratēģiskie riski, darbības riski, finanšu riski, atbilstības riski un/ vai citi riski	☐	☐	☐	

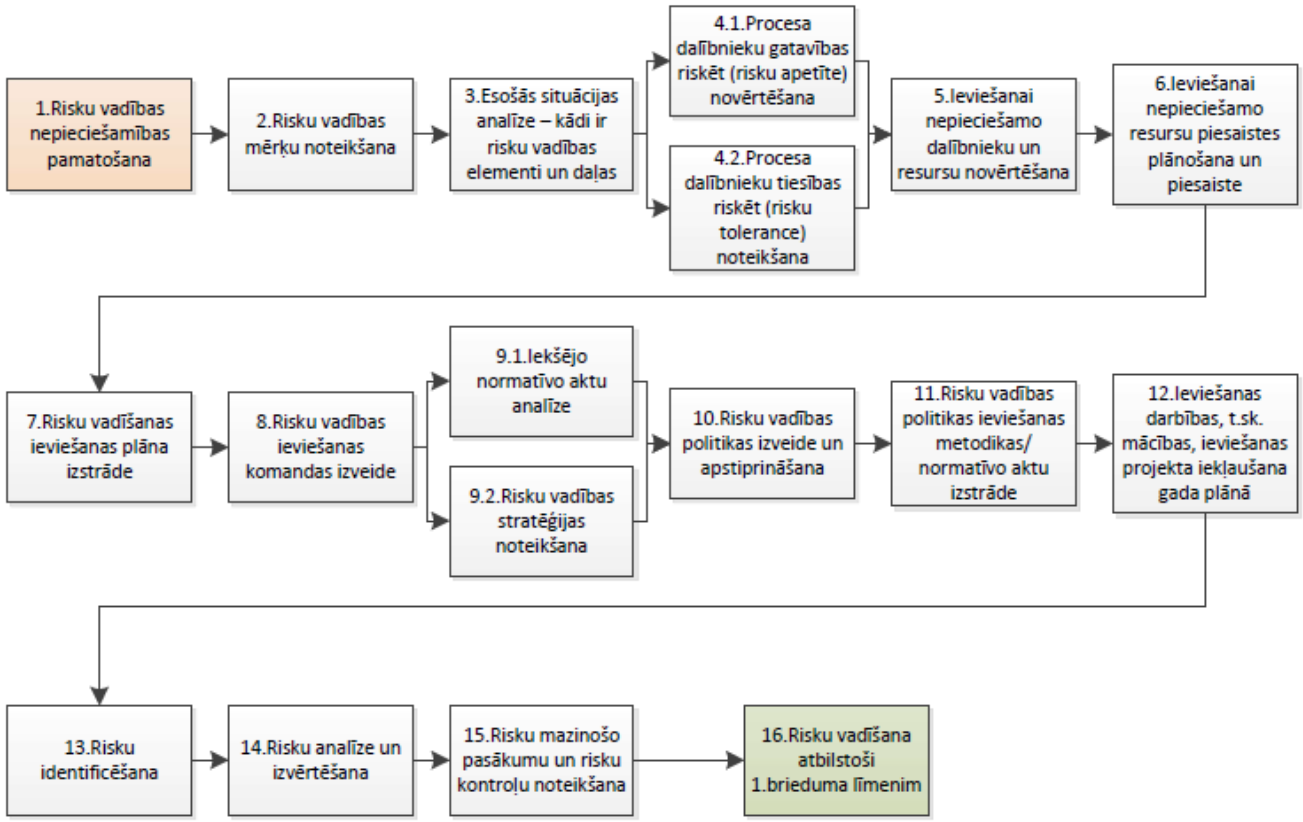
Nr.	Jautājums	Jā	Nē	Daļēji	Piezīmes
1.	2. (*Šajā kolonnā iekļauti jautājumi par risku vadības brieduma pamatelementiem*)	3.	4.	5.	6. (*Šajā kolonnā iekļauj piezīmes, ja daļēji atbilst kādam no apgalvojumiem, norādot, kas konkrēti atbilst un kas būtu uzlabojams), atsauces uz dokumentu, saites, u.tml.*)
11	Iestādē ieviesta Iekšējā kontroles sistēma (IKS)	☐	☐	☐	
12	Riski tiek vērtēti (nav noteikta risku vadības metodika)	☐	☐	☐	
13	Tiek sagatavoti protokoli, pieraksti, dokumentācija par risku vērtēšanu	☐	☐	☐	
14	Izveidots risku vadības process	☐	☐	☐	
15	Izveidots risku reģistrs	☐	☐	☐	
16	Izveidota metodika, veidlapas risku vērtēšanai	☐	☐	☐	
17	Darbiniekiem ir veiktas mācības par risku vadību	☐	☐	☐	
18	Par riskiem tiek ziņots iestādes augstākajai vadībai	☐	☐	☐	
19	Struktūrvienības novērtē (identificē, analizē un izvērtē) riskus, ņemot vērā izstrādāto/ apstiprināto risku vadības metodiku	☐	☐	☐	
20	Noteikti risku īpašnieki	☐	☐	☐	
21	Risku mazinošo pasākumu izpilde tiek uzraudzīta/notiek regulāra ziņošana par risku kontroles pasākumu ieviešanas progresu	☐	☐	☐	

Esošās situācijas risku vadībā novērtējums palīdz izprast risku vadības pilnveidojamās jomas, kas palīdzētu sasniegt ceļa kartē minētos brieduma līmeņa.

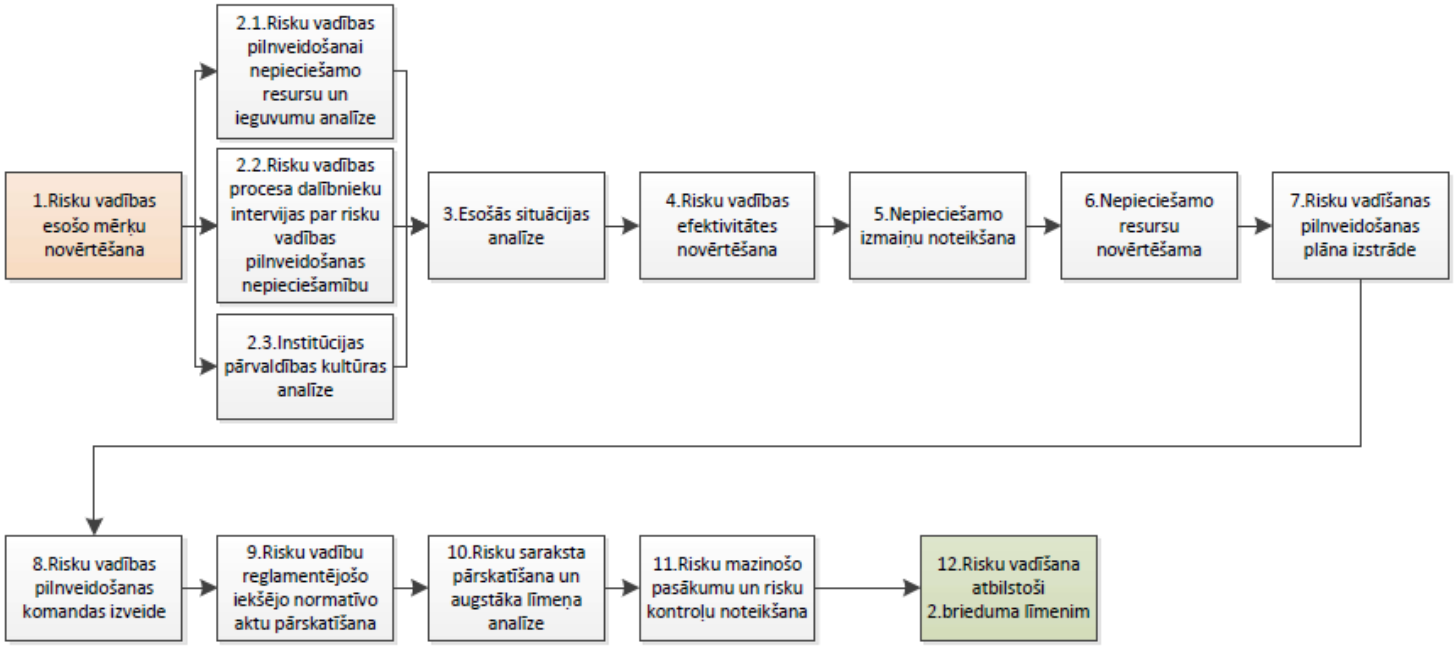
3. Ceļa kartes



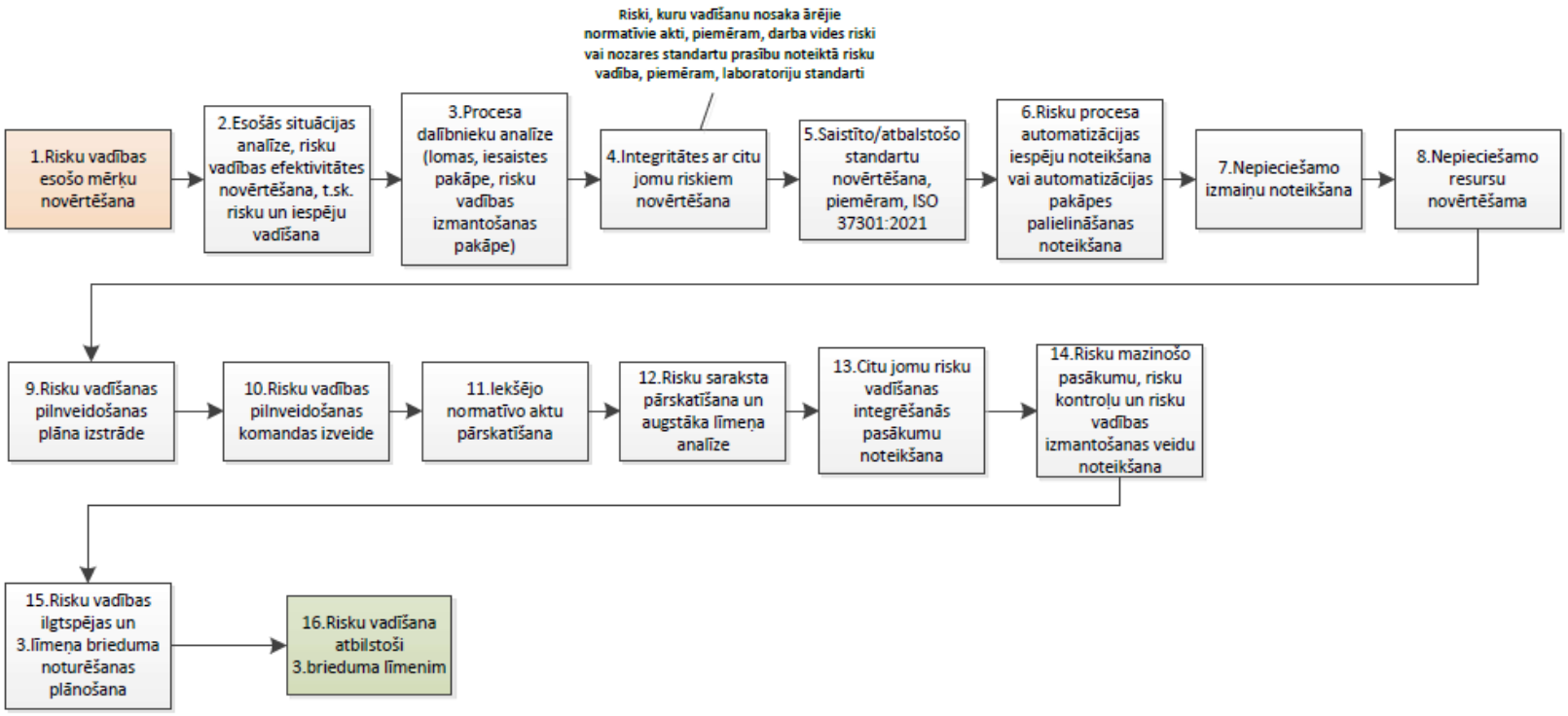
Risku vadības ieviešanas uzsākšana līdz pirmajam brieduma līmenim



Risku vadības pilnveidošana no pirmā brieduma līmeņa līdz otrajam brieduma līmenim



Risku vadības pilnveidošana no risku vadības otrā brieduma līmeņa līdz trešajam brieduma līmenim



4. Risku vadības standarti

Risku vadības standartu raksturojums:

Dokuments, dokumenta veids, pieejamība	Raksturojums				Izplatība
	Risku vadības mērķi	**Risku vadības ieguvumi**	**Risku vadības process**	**Risku vadības metodes un rīki**	
ISO 31000:2018 Starptautisks standarts *Ierobežota, maksas, publiski pieejams priekšskatījums*	Aizsargāt organizāciju vērtības, pieņemot lēmumus, nosakot un sasniedzot mērķus un uzlabojot sniegumu.	Stratēģijas noteikšana, mērķu sasniegšana un apzināta lēmumu pieņemšana.	Risku vadības plānošana. Risku novērtēšana. Risku vadīšana.	Standartā IEC 31010, Risku vadība – Risku vadība – Risku novērtēšanas metodes (*Risk management — Risk assessment techniques*).	Augsta izplatības pakāpe, iekšējo normatīvo aktu izstrādē, pētījumos.
COSO Uzņēmumu risku vadības ietvars – integrēšana ar stratēģiju un sniegumu *(COSO Enterprise Risk Management Framework - Integrating with Strategy and Performance)*	Nodrošināt, lai organizācijā uzlabojas lēmumu pieņemšana pārvaldībā, stratēģiskajā vadībā, mērķu noteikšanā un ikdienas darbību veikšanā. Palīdzēt uzlabot sniegumu, sasaistot stratēģiju un mērķus, ņemot vērā riskus un iespējas, vienlaikus veicinot vērtību veidošanu un saglabāšanu.	Risku vadības prakse integrēta stratēģijas noteikšanā un snieguma vadībā, kas nodrošina resursu zaudējumu samazināšanu. Risku apzināšana un vadīšana visā organizācijā.	Risku identificēšana. Risku ietekmes (*severity*) noteikšana. Risku prioritizēšana. Reaģēšana uz risku. Risku portfeļa skatījuma veidošana. Uzraudzības nodrošināšana. Komunikācija un ziņošana.	Kvantitatīva un kvalitatīva risku analīze.	Augsta izplatības pakāpe, iekšējo normatīvo aktu izstrādē, pētījumos.

Dokuments, dokumenta veids, pieejamība	Raksturojums				Izplatība
	Risku vadības mērķi	**Risku vadības ieguvumi**	**Risku vadības process**	**Risku vadības metodes un rīki**	
Portfeļu, programmu un projektu risku vadības standarts (*The Standard for Risk Management in Portfolios, Programs, and Projects*) Projektu vadības standarts *Ierobežota, maksas*	Risku vadības mērķis projektos ir nodrošināt iespēju izmantošanu un draudu ierobežošanu.	---	---	---	Izplatīts, lielākā izplatības joma projektu vadībā.
Oranžā grāmata (*The Orange Book, Management of Risk – Principles and Concepts*) *Publiski pieejama, bezmaksas*	Risku vadības mērķis ir atbalstīt atvērtību, izaicinājumus, inovācijas un izcilību mērķu sasniegšanā.	Pārvaldības un vadības procesu uzlabošana. Atbalsts lēmumu pieņemšanā par mērķiem.	Risku identificēšana un novērtēšana/analīze. Reaģēšana uz riskiem/ risku mazināšana. Risku uzraudzība. Atskaitīšanās.	Risku klasificēšana. Analīzes process.	Izplatīts, lielākā izplatības joma valsts pārvaldē, īpaši Nāciju Sadraudzības valstīs.

5. Iestādes iekšējo un ārējo vidi ietekmējošie elementi (veidlapas piemērs aizpildīšanai)

Iestādes nosaukums: Lai ievadītu tekstu, noklikšķiniet vai pieskarieties šeit.

Novērtējuma datums:	Noklikšķiniet vai pieskarieties, lai ievadītu datumu.

Ārējo videi ietekmējošie faktori	Iestādē:	Iekšējo vidi ietekmējošie faktori	Iestādē:
1. (*Šajā kolonnā jāiekļauj ārējās vides ietekmējošos faktorus, kurus iestādei iespējams izvērtēt, ja tie ir attiecināmi uz iestādi*)	2. (*Šajā kolonnā jāiekļauj pierādījumi, kas liecina, ka ārējās vides ietekmējošie faktori ir attiecināmi uz iestādi un kā tie ietekmējuši iestādi?*)	3. (*Šajā kolonnā jāiekļauj iekšējās vides ietekmējošie faktori, kurus iestādei iespējams izvērtēt, ja tie ir attiecināmi uz iestādi*)	4. (*Šajā kolonnā jāiekļauj pierādījumi, kas liecina, ka iekšējās vides ietekmējošie faktori ir attiecināmi uz iestādi un kā tie ietekmējuši iestādi?*)
Sociālie, kultūras, politiskie, juridiskie, reglamentējošie, finanšu, tehnoloģiskie, ekonomiskie un vides faktori – starptautiskā, valsts, reģionālā vai vietējā mērogā		Iestādes vīzija, misija un vērtības	
Galvenie virzītājspēki un tendences, kas ietekmē iestādes mērķus		Pārvaldības organizācija, organizatoriskā struktūra, lomas un atbildības sadalījums	
Tiesību akti, kas reglamentē iestādes darbību		Politikas plānošanas dokumenti, kuri saistoši iestādei	
Ārējo ieinteresēto pušu (sabiedrība, Ministru kabinets, NVO) uztvere, vērtības, vajadzības un gaidas		Iestādes darbības mērķi	
Esošās līgumattiecības un saistības pret trešajām pusēm, sadarbības partneri		Iestādes vajadzības	
Saziņas tīklu sarežģītība un atkarība no saziņas tīkliem		Iestādes kultūra	
Klientu uzvedība un gaidas no iestādes rīcības		Iestādes iekšējie normatīvie akti, saistošie piemērojamie standarti, metodikas, vadlīnijas	
		Funkcijas, procesi, tehnoloģijas	
		Cilvēkresursi un intelektuālais īpašums (zināšanas, pieredze)	
		Iedibinātā prakse (dokumentētā un nedokumentētā)	
		Dati, informācijas sistēmas un informācijas plūsmas	

Ārējo videi ietekmējošie faktori	Iestādē:	Iekšējo vidi ietekmējošie faktori	Iestādē:
		Attiecības ar iekšējām ieinteresētajām pusēm, ņemot vērā viņu uztveri un vērtības	

6. Iestādes Risku klasifikācija (piemērs)

Risku grupa	Riska apakšgrupa
Stratēģiskie riski	Politiskie riski
	Stratēģisko mērķu noteikšanas un īstenošanas riski
	Makroekonomiskie riski
Finanšu riski	Budžeta plānošanas un finanšu pārvaldības riski
	Budžeta izpildes riski
Darbības (operacionālie) riski	Personāla riski
	Procesu riski
	Projektu riski
	IKT riski
	Juridiskie riski (atbilstības riski)
	Korupcijas krāpšanas riski (atbilstības riski)
	Specifiskie atbalsta riski (atbilstības riski)
	Darba vides drošības riski
Reputācijas riski	Nav apakšiedalījuma
Ārējie riski	Nav apakšiedalījuma

7. Publiskajam sektoram raksturīgākie/ tipiskākie riski

STRATĒĢISKIE RISKI	DARBĪBAS RISKI	FINANŠU RISKI	ATBILSTĪBAS RISKI
Politiskie riski: • Politisko lēmumu ietekmes risks • Attīstības prioritāšu svārstību/ izmaiņu risks **Stratēģisko mērķu noteikšanas un īstenošanas riski:** • Stratēģiskās plānošanas dokumentu kvalitātes risks • Stratēģijas īstenošanas risks **Reputācijas riski:** • Plašsaziņas līdzekļu neprognozējamās rīcības risks • Sabiedrības informētības risks **Makroekonomiskie riski:** • Demogrāfiskās situācijas izmaiņu risks	**Pārvaldības riski:** • Organizatoriskās struktūras risks • Darba plānošanas un uzraudzības risks **Personāla riski:** • Darbinieku pietiekamības risks • Darbinieku zināšanu risks • Darbinieku motivācijas risks **Procesu riski:** • Birokrātijas/ administratīvā sloga risks • Priekšizpētes risks **Projektu riski:** • Projekta vadības risks • Saistību izpildes risks **Pakalpojumu riski:** • Klientu apkalpošanas kvalitātes risks • Informācijas pieejamības risks **Infrastruktūras riski:**	**Budžeta plānošanas un finanšu pārvaldība riski:** • Budžeta izdevumu risks • Finansējuma avotu pieejamības risks • Finanšu resursu pārvaldības risks **Budžeta izpildes riski:** • Budžeta izpildes disciplīnas risks • Budžeta struktūras un uzskaites sarežģītības risks • Finanšu pārskatu risks	**Informācijas tehnoloģiju riski:** • Nesankcionētas piekļuves risks • Jaunu tehnoloģiju risks • Datu kvalitātes risks Korupcijas, krāpšanas riski: • Interešu konflikta risks • Krāpšanas risks **Specifiskie atbalsta riski:** • Personas datu aizsardzības risks • Sankciju risks • Iepirkuma risks • Darba vides risks

• Globālās ekonomiskās ietekmes risks	• Fiziskās drošības risks • Darbības nepārtrauktības risks • Īpašumu pārvaldības risks **Sadarbības riski:** • Dalības starptautiskajās organizācijās risks • Iestāžu sadarbības un informācijas apmaiņas risks • Atkarības no ārpakalpojuma sniedzēja risks • Deleģēšanas risks **Juridiskie riski:** • Likumu izmaiņu risks • Tiesiskuma nodrošināšanas risks		

STRATĒĢISKIE RISKI

☐ **Politisko lēmumu ietekmes risks**
Risks, ka politiskās ietekmes rezultātā var tikt pieņemti steidzīgi, nepārdomāti, subjektīvi, nepamatoti, pretrunīgi un nekoordinēti lēmumi, kā rezultātā tiek nelietderīgi tērēti iestādes resursi trūkumu novēršanai un skaidrojošā darba veikšanai. Politiskās ietekmes mazināšanai iestādes rīcībā nav iespēju un rīku, lai savlaicīgi veiktu nepieciešamo analīzi un sagatavotu atbilstošu pamatojumu pareizu lēmumu pieņemšanai. Normatīvo aktu izstrāde netiek līdzi politisko lēmumu pieņemšanas ātrumam, lai koordinēti skaidrotu sabiedrībai jaunā regulējuma nepieciešamību.

☐ **Attīstības prioritāšu svārstību/ izmaiņu risks**
Risks, ka, mainoties politiskajiem spēkiem, bez pietiekamas analīzes un pamatojuma tiek veiktas izmaiņas nozaru attīstības prioritātēs, kā rezultātā jaunās prioritātes var dot ieguvumus tikai šaurām iedzīvotāju grupām. Lēmumi ir ar īstermiņa ietekmi, netiek pabeigti iesāktie darbi, kuru atlikšana nākotnē var izmaksāt daudz dārgāk, var tikt neizpildītas uzņemtās saistības un rodas pretrunas starp dažādu nozaru politiskajiem uzstādījumiem / mērķiem. Mainoties prioritātēm, mainās arī iestādes darbības prioritātes, kas uz laiku var apturēt

Risks, ka budžeta līdzekļi tiek piešķirti pēc politiskās piederības, ne pēc faktiskās vajadzības un izvērtējot mērķauditoriju pēc objektīviem kritērijiem.

☐ **Stratēģijas īstenošanas risks**
Risks, ka iestāde nespēj īstenot stratēģiju, un tiek apdraudēta iestādes mērķu sasniegšana. Iestādes nespēja nodrošināt nepieciešamos resursus stratēģijas ieviešanai, jo stratēģiskie mērķi nepietiekami definēti un/vai pārspīlēti, nesasniedzami vai neatbilstoši iestādes specifikai, kultūrai. Iestādes nespēja savlaicīgi reaģēt uz izmaiņām. Neatbilstoši mērķu sasniegšanai izvēlēti sadarbības partneri.

☐ **Plašsaziņas līdzekļu neprognozējamas rīcības risks**
Risks, ka masu mediju pārstāvji pārkāpj nevainības prezumpcijas principu, tādējādi negatīvi ietekmējot gan iestādes, gan tās darbinieku reputāciju bez pamatota iemesla un apgrūtinot iestādes darbību uz laiku līdz lietas apstākļu noskaidrošanai vai pat tiesas lēmumam. Arī risks, ka masu mediju provocētās sensācijas / ažiotāžas nebalstās uz patiesajiem faktiem, tomēr uzraugošās institūcijas šīs ziņas izmanto savā riska novērtējumā.

☐ **Demogrāfiskās situācijas izmaiņu risks**
Risks, ka, pasliktinoties demogrāfiskajai situācijai, ir jāveic būtiskas izmaiņas nozares politikā, iestādes darbības organizācijā un piešķirtā budžeta finansējuma lēmumu pieņemšanu, kā īslaicīgi vai ilglaicīgi rada papildu slodzi uz iestādes darbiniekiem.

☐ **Stratēģiskās plānošanas dokumentu kvalitātes risks**
Risks, ka valsts nozīmes un nozaru politikas attīstības plānošanas dokumentu izstrāde netiek pietiekami koordinēta, kā rezultātā attīstības prioritātes ir pretrunīgas, nav nodrošināta plānoto darbību pēctecība un biežo izmaiņu veikšana neļauj sasniegt stratēģiskos mērķus. Izstrādātie plānošanas dokumenti ir nepārskatāmi, sarežģīti formulēti un tajos nav nodrošināta sasaiste ar rādītājiem, kas ļauj uzraudzīt mērķu sasniegšanas virzību un pakāpi.

☐ **Sabiedrības informētības risks**
Risks, ka nepietiekamas informācijas sniegšana var radīt pret iestādi vērstu negatīvu komunikāciju, neizpratni sabiedrībā. Risks, ka valsts pārvaldes un ierēdniecības negatīvais tēls tiek apzināti popularizēts, tādējādi mazinot darbinieku motivāciju strādāt valsts pārvaldē un apgrūtinot valsts iestāžu sadarbību ar sabiedrību. Riski, ka iestādes klientiem, sadarbības partneriem, uzraudzības iestādēm un citām iestādes darbībā ieinteresētām personām var izveidoties negatīvs viedoklis par to un tas var negatīvi ietekmēt iestādes spēju uzturēt esošās vai izveidot jaunas attiecības ar tās klientiem un citiem sadarbības partneriem.

☐ **Globālās ekonomiskas ietekmes risks**
Risks, ka starptautiskajā politiskajā un ekonomiskajā vidē veidojas aizvien vairāk pārnacionālu institūciju un uzņēmumu, lēmumu pieņemšana kļūst aizvien attālāka

apjomā. Var straujāk samazināties vai palielināties iestādes klientu kopējais skaits vai noteiktas mērķauditorijas lielums. Iestādes personāls var novecot straujāk, kā rezultātā var būt grūtāk ieviest jauninājumus iestādes darbībā.

un grūtāk kontrolējama, kā arī jebkāda notikuma ietekme aptver daudz plašākas valstu, nozaru vai mērķauditoriju grupas.
Globalizācijas procesu attīstība un prasību paaugstināšanās, kas paātrina un sarežģī procesu un notikumu attīstību. Plaša mēroga vai globālas krīzes vienlaicīgi ietekmē dažādus piegādes ķēdes posmus, neļaujot savlaicīgu piekļuvi resursiem par samērīgu cenu. ‘

DARBĪBAS RISKI

☐ **Organizatoriskās struktūras risks**
Risks, ka iestādes organizatoriskā struktūra nav atbilstoša iestādes stratēģiskajiem uzdevumiem, nav optimāla un notiek funkciju pārklāšanās vai darbu neizpilde. Personāla resursi nav optimāli pārdalīti starp pamata procesiem un atbalsta procesiem. Funkciju optimizācija, centralizācija resora ietvaros vai nodošana ārpakalpojumā var nedod sagaidīto ietaupījumu ilgtermiņā un funkciju izpildes atjaunošanai ir nepieciešami papildu būtiski ieguldījumi.

☐ **Darbinieku pietiekamības risks**
Risks, ka iestādei nav pietiekami personāla resursi savlaicīgai un kvalitatīvai funkciju izpildei, ir vērojama augsta darbinieku mainība un esošo darbinieku pārslodze noteiktās funkcijās vai visā iestādē kopumā. Iestādei trūkst noteiktas jomas speciālisti, tie nav pieejami arī darbaspēka tirgū.

☐ **Darba plānošanas un uzraudzības risks**
Risks, ka darbu izpildes plānošana nav sasaistīta ar iestādes darbības mērķiem (mērķu kaskadēšana), nav noteiktas atbildīgās personas darbu izpildei, kā rezultātā darbu izpilde notiek haotiski un nelietderīgi patērē iestādes resursus. Risks, ka uzraudzība ir neracionāla, jo nav noteikti izpildes sasniedzamie rezultāti un efektivitātes kritēriji noteiktam periodam. Iestādes izstrādātie operatīvie plāni netiek komunicēti darba procesā iesaistītajiem darbiniekiem un, ja attiecināms, trešajām pusēm.

☐ **Darbinieku zināšanu risks**
Risks, ka iestādes darbiniekiem nav pietiekamas zināšanas, kas nepieciešamas patstāvīgai sava amata pienākumu izpildei. Darbiniekiem nav iespējas pastāvīgi pilnveidot savas profesionālās iemaņas un zināšanas, tirgū nav pieejamas nepieciešamās apmācību iespējas. Iestādei nepieciešami šauras specializācijas darbinieki,

kādi netiek sagatavoti vispārējā izglītības sistēmā un ar tirgū pieejamo apmācību palīdzību. Darbinieku darbaspējas ietekmē iepriekšējās pieredzes esamība vai neesamība. Darbinieku prasmes strādāt attālināti.

☐ **Darbinieku motivācijas risks**
Risks, ka valsts pārvaldes darbinieku atalgojums ir nesamērīgs ar darba tirgū piedāvāto atalgojumu, kā rezultātā iestādei nav iespējams piesaistīt nepieciešamās kvalifikācijas un specializācijas darbiniekus, kā arī pietiekami viņus motivēt darba attiecībām ilgtermiņā. Iestādē strādājošiem vadītājiem ir apgrūtinoši savākt motivētu un kompetentu vidēja un zemāka līmeņa vadības komandu. Vērojama šķelšanās starp ārvalstu finansējuma pārvaldīto iesaistīto un neiesaistīto darbinieku grupām pieejamo papildu labumu (apmācības, komandējumi, atalgojums u.tml.) dēļ.

☐ **Projekta vadības risks**
Risks, ka projektu vadība notiek haotiski, nestrukturēti ar nepietiekamu informācijas apmaiņu un sadarbības koordināciju, bez skaidri noteiktām atbildības un prioritāšu sfērām. Projekta vadības komanda nav optimāla un/vai lemt spējīga, kā arī nav skaidri noteikta projekta komandas komunikācija ar pārējo iestādes personālu, ja tas nepieciešams rezultāta sasniegšanai un lēmumu pieņemšanai. Projektu realizācijas jauda ir pārāk maza pieņemto lēmumu īstenošanai. Projekta ietvaros var rasties interešu sadursmes, kuras neizdodas sabalansēt rezultāta sasniegšanai. Risks, ka iestāde neveic projekta uzraudzību, lai nodrošinātu sagaidāmos ieguvumus un

☐ **Tiesiskuma nodrošināšanas risks**
Risks, ka normatīvo aktu nepilnības neļauj pietiekami pamatot iestāžu lēmumus un resursu trūkuma rezultātā pieņemtie lēmumi netiek izskaidroti iestādes klientiem, kā rezultātā pieaug pārsūdzību apjoms, kuru izskatīšanai tiek tērēti aizvien lielāki iestādes resursi.
Risks, ka ar iestādes lēmumiem saistītais tiesvedības process var tikt apgrūtināts, jo normatīvajos aktos ir nesakārtotas normas attiecībā uz atbildību. Risks, ka tiek nelietderīgi patērēti iestādes darbības resursi iestādes pārstāvniecībai tiesās, ja tiesu process tiek apzināti kavēts un šādai vilcināšanas rīcībai nav soda sankciju.

☐ **Saistību izpildes risks**
Risks, ka piegādātāji nepilda saistības savlaicīgi un pietiekamā kvalitātē paredzēto finansējuma apjomā.

novērstu nelietderīgu līdzekļu izmantošanu.

☐ **Birokrātijas/ administratīvā sloga risks**
Iekšējie procesi ir smagnēji, birokrātiski, neefektīvi, kas patērē vairāk resursu nekā nepieciešams un neļauj pietiekami ātri realizēt nepieciešamās darbības. Dokumentu apritē nav pietiekami izmantotas elektronizācijas/ automatizācijas iespējas. Iestādes klientiem tiek uzlikts riska līmenim nesamērīgs administratīvais slogs.
Risks, ka nav nodrošināta efektīva procesu darbības, lai būtu iespējams efektīvi veikt uzdevumus un tiktu sasniegti iestādes mērķi.

☐ **Klientu apkalpošanas kvalitātes risks**
Risks, ka procesi nav vērsti uz klientu apkalpošanas kvalitāti, nav definēts vienots klientu apkalpošanas standarts, personāls nav pietiekami kompetents klientu apkalpošanai, klientu apkalpotājiem ir dažādas pieejas un redzējums / normu interpretācija, netiek pilnvērtīgi uzraudzīta klientu apkalpošanas kvalitāte (piemēram, klientu sūdzību saturiskā analīze), lai pilnveidotu klientu apkalpošanu atbilstoši klientu vajadzībām. Nepilnvērtīgi ir identificētas iestādes klientu grupas, kuru vajadzībām pielāgot dažādos klientu apkalpošanas procesus. Risks, ka iestādes izveidotā klientu apkalpošanas sistēma nav optimāla no iestādes pieejamības, rindu pārvaldības, elektronizācijas pakāpes, apkalpošanas izmaksu

☐ **Priekšizpētes risks**
Risks, pirms darba uzsākšanas nav pietiekami kvalitatīvi veikta priekšizpēte par plānotā rezultāta (pakalpojuma, normatīvā regulējuma, projekta utt.) lietderību, finansiālo izdevīgumu, alternatīvām iespējām, ārējām prasībām, efektīvākiem ieviešanas variantiem utt., kā rezultātā var tikt nelietderīgi tērēti iestādes resursi strādājot pie rezultātiem, kas nenes sagaidāmo vērtību vai nesasniedz definētos mērķus. Risks, ka iestādei var nebūt pieejami aktuāli, pareizi, pietiekami dati, lai veiktu nepieciešamo problēmas analīzi, dati var tikt nepareizi izvēlēti un interpretēti, lai identificētu un raksturotu cēloni un problēmu, kā rezultātā iestādes vadība var pieņemt nepareizus lēmumus.

☐ **Informācijas pieejamības risks**
Risks, ka klientiem nav pietiekami un ērti pieejama visa nepieciešamā informācija par iestādes pakalpojumiem, tā ir kļūdaina, nav aktuāla, ir neskaidra vai grūti atrodama. Risks, ka nav pietiekama informācija par e-pakalpojumu pieejamību un procesu.

viedokļa u.tml. Risks, ka iestāde nespēj savlaicīgi, pilnā apjomā un efektīvi apkalpot iestādes klientus, jo nav pieejama attiecīga atbalsta informācijas sistēma.

☐ **Fiziskās drošības risks**
Risks, ka elektrības un interneta pārtraukumu, dabas stihiju, ugunsgrēku, plūdu, zādzību, vandālisma, pandēmijas u.tml. apdraudējumu rezultātā var tikt apdraudēta iestādes darbība vai noteiktu funkciju izpilde. Risks, ka iestādes rīcībā esošie pamatlīdzekļi un tehnoloģijas ir morāli un fiziski novecojušas, lai tās būtu piemērotas iestādes funkciju izpildei.

☐ **Īpašumu pārvaldības risks**
Risks, ka iestādes īpašumi var būt tās funkcijām neraksturīgi īpašumi, kuru uzturēšanai izmaksas pārsniedz ieņēmumus. Īpašumi netiek optimizēti to izmantošanas un uzturēšanas izmaksu ziņā. Risks, ka iestādei nav pietiekama finansējuma nekustamā un kustamā īpašuma saprātīgai un pietiekamai uzturēšanai, kā rezultātā iestādei piederošā īpašuma vērtība var strauji kristies. Risks, ka īpašuma adekvātai uzturēšanai var rasties neprognozēti un būtiski izdevumi, iespējams, ka iepriekš nav apzinātas iespējamās uzturēšanas izmaksas. Risks, ka iestāde nav pilnībā apzinājusi sev piederošos nekustamos un kustamos īpašumus, tie nav atbilstoši uzskaitīti un reģistrēti likumdošanā noteiktā kārtībā un to patiesajā vērtībā. Iestādes uzskaitē un valsts reģistros reģistrētie iestādes īpašumi vairs neeksistē vai ir zaudējuši savu vērtību bojājumu rezultātā. Risks, ka iestāde nav

☐ **Darbības nepārtrauktības risks**
Risks, ka iestāde nav apzinājusi būtiskos riskus un neveic profilaktiskos riska kontroles pasākumus iestādes darbības nepārtrauktības nodrošināšanai. Iestādē nav izstrādāts praktisks plāns darbības atjaunošanai, nav noteikts atbildības un pienākumu sadalījums, kā arī apmācīti darbinieki ātrai un optimālai iestādes darbības atjaunošanai. Nav definēti nosacījumi krīzes izsludināšanai un darbību koordinācijai ar valsts institūcijām krīzes novēršanai.

☐ **Tiesību aktu izmaiņu risks**
Risks, ka likumdošanas un/vai jebkuru citu ārējo normatīvo aktu izmaiņas radīs iespēju negatīviem notikumiem, kuru iestāšanās gadījumā iestādes mērķi netiek sasniegti vai ir būtiski jāmaina. Var tikt patērēti vairāk resursi, rodas papildus izmaksas. Ilgstoša starpinstitūciju saskaņošana. Risks, ka normatīvā akta izstrādes un saskaņošanas procesā tiek ieviestas vairākas būtiskas izmaiņas, kā rezultātā gala normatīvajā aktā ir daudz pretrunu un neskaidrību, nav pietiekamā apjomā paredzēta atbildība / pienākumi noteiktu darbību izpildei, ieviešanas mehānisms praksē nedarbojas. Iestādei jātērē vairāk resursu normatīvo aktu izskaidrošanai / interpretēšanai, kā arī precizējumu veikšanai.

apzinājusi visas iespējamās infrastruktūras uzturēšanas izmaksas.

☐ **Dalības starptautiskajās organizācijās risks**
Risks, ka, piedaloties starptautiskajā organizācijā, var būtiski pieaugt normatīvā regulējuma un saistošo prasību apjoms, kā rezultātā iestādei ir nepieciešami papildus resursi prasību ievērošanai, nepieciešamā vadības un kontroles mehānisma nodrošināšanai, uzraudzības pasākumu veikšanai. Iestāde var neadekvāti interpretēt starptautisko organizāciju prasības, tādējādi radot nepamatotu administratīvo slogu saviem klientiem. Iestādes vietēji izvirzīto prasību neatbilstība starptautisko organizāciju prasībām var radīt zaudējumus.
Nepietiekamu resursu atvēlēšana vai iestādes darbinieku pašu nedrošība valsts interešu lobija veidošanai starptautiskās organizācijās var novest pie valstij nelabvēlīgu vai valsts mērogam neatbilstošu lēmumu pieņemšanas.

☐ **Iestāžu sadarbības un informācijas apmaiņas risks**
Risks, ka iestādes efektīvi nesadarbojos, lai kopīgi pārvaldītu vienoto procesu, kā arī aktīvi meklētu un novērstu problēmu cēloni / avotu. Risks, ka informācija netiek efektīvi (optimālā apjomā, kvalitatīvi, savlaicīgi) izplatīta, lai nodrošinātu pietiekošu sadarbību starp procesā iesaistītajiem. Nav pietiekami sistematizētas informācijas plūsmas (formalizācijas pakāpe, kanāli un adresāti) un izmantoti e-risinājumi informācijas apmaiņai. Iestādes rīcībā nav pietiekami efektīvi organizēts lēmumu un dokumentācijas saskaņošanas process.

☐ **Atkarības no ārpakalpojuma sniedzēja risks**
Risks, ka funkciju nodošana ārpakalpojuma sniedzējiem var būtiski ietekmēt (bremzēt, apgrūtināt, apturēt) iestādes darbību un tās attīstības iespējas, jo savu plānu realizācijā rodas atkarība no ārpakalpojuma sniedzēja veiktspējas, darba kvalitātes, cenas un piegādes nosacījumiem

☐ **Deleģēšanas risks**
Risks, ka, deleģējot iestādes funkciju izpildi trešajai pusei, nav pietiekami izvērtēta deleģēšanas lietderība - sagaidāmie ieguvumi, finansiālais izdevīgums, vienota izpratne par saprātīgu finanšu vadību, ieguldījums informācijas apmaiņā, optimāls pilnvarojuma sadalījums rīcībai ar budžeta līdzekļiem, samērīgas iespējas ietekmēt lēmumus, uzraudzības modelis.

FINANŠU RISKI

☐ **Budžeta izdevumu risks**
Risks, ka izmantotie budžeta līdzekļi nav sasaistīti ar noteiktu nozares politikas mērķu sasniegšanu, izvēlētie izpildes rādītāji neatspoguļo mērķus vai to sasnieguma pakāpi. Budžeta izmaksu sasaiste ar izpildes rādītājiem kā efektivitātes kritērijiem nav pietiekami elastīga, kā rezultātā budžeta līdzekļu izmaksas var tikt kavētas vai neveiktas rādītāju interpretācijas dēļ. Nav skaidras budžeta izpildes rādītāju ievērošanas kontroles, tādējādi nav sabalansēta atbildība starp iestādes vadītāju un kontrolētāju par budžeta izmantošanas lietderību un efektivitāti.

☐ **Budžeta izpildes disciplīnas risks**
Risks, ka, nesavlaicīgi veicot budžeta līdzekļu izmantošanu, neiztērētie budžeta līdzekļi var tikt zaudēti un iestādes nevar izpildīt uzņemtās saistības pret klientiem un citām trešajām pusēm.

☐ **Finanšu pārskatu risks**
Risks, ka finanšu pārskati nesniedz precīzu un ticamu informāciju par iestādes darbību. Finanšu uzskaites datu nekorekta ievade informācijas sistēmās, uzskaites neatbilstība faktiskajai situācijai, dati nav nepieejami, dati tiek sagrozīti vai nepilnīgi. Nav noteikti vienoti darījumu attaisnojošo dokumentu iesniegšanas principi, rezultātā risks, ka novēlota darījumu uzskaite vai dubultā uzskaite.
Risks par grāmatvedības prasību un standartu interpretāciju un neatbilstošu piemērošanu. Netiek veikti grāmatvedības sistēmas atjauninājumi un papildinājumi uzskaitei. Uzkrājumu uzskaites apjoma neatbilstība nākotnes darījumiem.
Risks, ka ministrijas konsolidētais gada pārskats varētu būt kļūdains, jo kļūdaini finanšu dati no padotības iestādēm, kā arī atšķirīgas uzskaites sistēmas.

☐ **Finansējuma avotu pieejamības risks**
Risks, ka politisku lēmumu rezultātā samazinās nozarei un attiecīgi iestādei pieejamais finansējums nozares attīstības mērķu sasniegšanai. Risks, ka, samazinoties valsts budžeta finansējumam, lielāka interese ir par iespējām piesaistīt ES finansējumu, kā rezultātā neprognozēti / neproporcionāli pieaug slodze uz ES fondu vadībā iesaistītajām institūcijām.
☐ Risks, ieņēmumi no valsts sniegtajiem maksas

☐ **Budžeta struktūras un uzskaites sarežģītības risks**
Risks, ka izveidotā budžeta līdzekļu uzskaites sistēma ir pārāk sadrumstalota, detalizēta, sarežģīta un neelastīga, lai spētu sagatavot saprātīgas finansējuma izlietošanas prognozes, kā arī ātri un vienkārši veikt izmaiņas. Risks, ka iestādes sagatavoto prognožu precizitāte tiek izmantota kā reputācijas mērs vai tālākā finansējuma pieejamības mērs. Risks, ka budžeta izmaksu uzskaites prasības ir pārspīlētas un nav samērīgas ar nepieciešamību nodrošināt izmaksu caurspīdīgumu,

pakalpojumiem un ar šo pakalpojumu sniegšanu netiek saistītie ar atbilstošiem izdevumiem, maksas pakalpojumu izcenojumu ir neaktuāli, netiek pārskatīti pakalpojumu izcenojumi.

Finanšu resursu pārvaldības risks
Risks, ka iestādes finanšu resursi netiek optimāli pārvaldīti, inflācijas rezultātā iestādei var pietrūkt brīvu un likvīdu naudas līdzekļu saistību segšanai. Risks, ka iestāde varētu neievērot visas ar nodokļiem saistīto likumdošanas aktu prasības, nepildīt visus maksājumu un deklarāciju iesniegšanas noteikumus, vai ievērojama apjoma darījumu nosacījumus, radot negatīvu nodokļu ietekmi, papildus izmaksas, kā arī reputācijas pasliktināšanos..

kā rezultātā tiek nelietderīgi tērēti iestādes resursi uzskaites veikšanai.
Risks, ka iestāde nespēj nodrošināt pilnvērtīgu grāmatvedības uzskaiti un digitālu rēķinu procesu.
Risks, ka iestāde, saņemot finansējumu no vairākiem finansējuma avotiem, nespēj efektīvi nošķirt katra finansējuma avota līdzekļu uzskaiti (dalīto grāmatvedību) atbilstoši to specifiskajām prasībām, kā rezultātā piešķirtie finanšu līdzekļi deklarēti vairākiem finansējuma avotiem radot dubultā finansējuma risku.

ATBILSTĪBAS RISKI

☐ **Krāpšanas risks**
Risks, ka iestādes klienti var sniegt nepatiesu informāciju, lai iegūtu likumdošanā paredzētos labumus.
Risks, ka publiskajos iepirkumos piegādātāji sniedz maldinošu informāciju vai izmanto negodīgas konkurences paņēmienus (dempinga cenas, mākslīgi palielinātas cenas, slēptas vienošanās u.tml.).
Risks, ka darbinieks sniedz apzināti nepatiesu vai nepilnīgu informāciju, vai tīši nav sniedzis informāciju, lai sagrozītu patieso situāciju.

☐ **Interešu konflikta risks**
Risks, ka lēmumu pieņemšanā par finanšu līdzekļu izmantošanu iesaistītie darbinieki ir/var kļūt neobjektīvi un pieņemt lēmumus savās vai sev pietuvināto grupu interesēs, kā rezultātā līdzekļi var tikt nelietderīgi izšķērdēti un netiek novirzīti paredzēto mērķu izpildei.

☐ **Darba vides risks**
Risks, ka darba drošības prasību ievērošana netiek ievērota, ka

☐ **Personas datu aizsardzības risks**
Risks, ka personas datu aizsardzības prasības netiek ievērotas. Risks, ka

piemērotas darba vides un darba drošības prasību pilna ievērošana var prasīt būtiskus papildu resursus vai arī darba drošības prasību neievērošana var radīt zaudējumus uzlikto sodu vai kompensāciju darbiniekiem nomaksai. Risks, ka iestādē nav izstrādāts vai ir neaktuāls civilās aizsardzības pasākumu plāns, tas nav sakoordinēts ar valsts un pašvaldību iestāžu civilās aizsardzības plāniem, atbildīgie darbinieki par pasākumu realizāciju nav atbilstoši apmācīti, nav pieejama vai nedarbojas nepieciešamā infrastruktūra un aizsardzības līdzekļi, kā rezultātā iestādes darbinieku veselība un dzīvība var tikt apdraudēta.

☐ **Iepirkuma risks**

Iestādes darbiniekiem nav pietiekamas kompetences kvalitatīvai iepirkuma dokumentācijas izstrādei atbilstoši iestādes vajadzībām un likumdošanas prasībām. Risks, ka iestādē netiek veikta pietiekami detalizēta vajadzību apzināšana un analīze, lai precīzāk un atbilstošāk iestādes vajadzībām definētu iepirkuma priekšmetu un izvairītos no nelietderīgiem iepirkumiem. Iepirkumi nav pietiekami optimizēti, lai iegūtu maksimāli izdevīgāko piedāvājumu un piegāžu grafiks būtu atbilstošs vajadzību rašanās momentam. Centralizēto iepirkumu pārvaldība nav efektīva, lai nodrošinātu konkurētspējīgas cenas. Konkurence var saasināties, kā rezultātā pieaug par iepirkumu konkursiem iesniegto sūdzību skaits un iepirkumu process būtiski paildzinās, jo likumdošanā nav paredzēta arī atbildība par nepamatotu sūdzību iesniegšanu. Risks, ka konkurences tirgus dalībnieki veikuši aizliegtas vienošanās, radījuši negodīgas iestāde nerīkojas pietiekami, lai novērstu tūlītēju datu drošības apdraudējumus. Risks, ka personas dati var kļūt pieejami neautorizētām trešajām personām iestādes darbinieku tīšas vai netīšas rīcības rezultātā vai trešo pušu ļaunprātīgas rīcības rezultātā, tādējādi negatīvi ietekmējot sabiedrības uzticību iestādei, iestādes reputāciju un radot finansiālus zaudējumus uzlikto sodu un noteikto kompensāciju nomaksai.

☐ **Sankciju risks**

Risks, ka iestāde atbilstoši prasībām neievēro starptautiskās publiskajās tiesībās noteiktos ierobežojošos pasākumus jeb ierobežojumus vai aizliegumi pret valsti, režīmu vai personu (fizisku vai juridisku) par starptautisko tiesību pārkāpšanu. Netiek veikti novērtējumi sankciju regulējuma apiešanas identificēšanai.

☐ **Datu kvalitātes risks**

Risks, ka citu iestāžu rīcībā esošās informācijas sistēmas un dati nav pieejami pārējām valsts pārvaldes iestādēm, kā arī šo iestāžu klientiem, ja attiecināms. Risks, ka valsts pārvaldē tiek uzturētas vairākas līdzīgas informācijas sistēmas ar līdzīgiem datiem un tiek patērēti papildu resursi gan datu dubultai ievadei, gan sistēmu uzturēšanai un modernizācijai.

Risks, ka dati ir neprecīzi, nepareizi, neaktuāli, nepietiekami, kļūdaini, novēloti, sagrozīti, izdzēsti, neatbilstoši uzskaitīti, nav pārbaudāmi. Nav iespēja vai prasmes efektīvi apkopot un analizēt liela apjoma datus.

konkurences apstākļus. Risks, ka iestāde zaļā publiskā iepirkuma principu, prasību un to kārtību piemēro neatbilstoši.

☐ **Nesankcionētas piekļuves risks**
Risks, ka kiberuzbrukumu, ielaušanās vai nesankcionētas piekļuves rezultātā trešās puses iegūst personas datus, ierobežotas pieejamības informāciju, konfidenciālu informāciju vai informāciju par valsts noslēpumu, tiek sagrozīti/izdzēsti svarīgi iestādes rīcībā esošie dati, vai arī apdraudēta iestādes rīcībā esošo informācijas sistēmu veiktspēja, kā rezultātā iestādes darbība tiek apgrūtināta vai tai rodas zaudējumi saistībā ar uzlikto sodu un kompensāciju nomaksu. Risks, ka iestādes rīcībā esošās ierobežotas pieejamības informācijas (komercnoslēpums, atbalsta saņēmēju dati, autortiesību objekts, konfidenciāla informācija, valsts noslēpums u.tml.) nodošana trešajām personām bez attiecīga tiesību īpašnieka saskaņojuma var radīt būtiskus zaudējumus valsts budžetam un zaudējumus iestādei kompensāciju nomaksai, kā arī negatīvi ietekmēt iestādes reputāciju.

☐ **Jaunu tehnoloģiju risks**
Risks, ka jaunu informācijas sistēmu izveidei nav aplēsts viss nepieciešamais iestādes ieguldījuma apjoms (personāla laiks darbam ar izstrādātāju, infrastruktūras iepirkums, uzturēšanas izmaksas nākotnē, papildinājumu izstrādes izmaksas utt.). Nepietiekami ir novērtēti arī jaunas informācijas sistēmas ieviešanas vai paplašināšanas / modernizācijas projektā iesaistītie riski. Risks, ka iestāde iegādājas jaunākās tehnoloģijas, kuras iestādes nespēj apgūt un pareizi ekspluatēt, kuras neatbalsta visas nepieciešamās iestādes noteiktās funkcionalitātes, vai kuras nedarbojas vai darbojas kļūdaini un ražotājs ilgstoši nespēj novērst kļūdu cēloni. Risks, ka jaunās tehnoloģijas ir pārāk atvērtas trešajām pusēm un drošības nodrošināšanai ir jātērē papildu resursi. Risks, ka iestāde iegādājas aparatūru un programmnodrošinājumu, kas nav savietojamas ar jau esošo nodrošinājumu, kā rezultātā rodas papildus izmaksas aparatūras vai programmnodrošinājuma pilnīgai vai daļējai nomaiņai vai to savietojamības nodrošināšanai.

8. Incidentu reģistrs (piemērs - veidlapa)

Nr.p.k.	Incidenta apraksts	Incidenta reģistrēšanas datums	Incidenta cēlonis	Incidenta sekas	Incidenta prioritāte	Process	Incidenta novēršanas pasākumi	Risku, kas ir saistīti ar incidentu apraksts	Risku mazinošie pasākumi, atbildīgais un ieviešanas termiņš	Gūtās mācības pēc incidenta novēršanas
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.
1.	Notikusi klasificētas (ierobežotas pieejamības) informācijas noplūdeas procesā iepirkumu veikš, publicējot šo informāciju plašsaziņas līdzekļos	29.07.2023	Darbinieka zināšanu trūkums par informācijas klasificēšanu	Informācija publicēta plašsaziņās līzekļos. Cietusi iestādes reputācija, jo nav bijusi pietiekama klasificētas informācijas aizsardzība. Uzsākta tiesvedība pret iestādi par Informācijas atklātības likuma neievērošanu.		Iepirkumu veikšana	Veikta dienesta izmeklēšana par informācijas noplūdes cēloņiem, kā rezultāta konstatēts, ka dokumenta sagatavotājs nav veicis atzīmi par dokumenta klasifikāciju. Plašsaziņas līzekļos publicēta atvainošanās par izraisīto informācijas noplūdi. Darbinieks nosūtīts uz mācībām par Informācijas atklātības likuma un iestādes iekšējos normatīvajos aktos paredzētajām klasificētas informācijas aizsardzības prasībām.	Darbiniekiem, kuri sagatavo klasificētu informāciju var nebūt pietiekamas zināšanas par to pareizu aizsardzību, tostarp noformēšanu un var notikt atkārtotas klasificētas informācijas noplūdes	Sagatavot mācību materiālu par klasificētas informācijas aizsardzības prasībām un organizēt testus, lai pārbaudītu darbinieku zināšanu līmeni, Personāla departaments sadarbībā ar Juridisko departamentu, 31.12.2023.	Nepieciešams veikt regulāras (vismaz vienu reizi divu gadu laikā) darbinieku zināšanu pārbaudes par klasificētas informācijas aizsardzību.

9. Risku varbūtības skala (veidlapa aizpildīšanai)

Punktu skaitliskā vērtība	**Skaitliskās vērtības nozīme**	**Skaidrojums (I)** **(riska notikuma norises biežums laika periodā)**	**Skaidrojums (II)** **(riska notikuma īpatsvars no kopējo notikumu apjoma)**
1.	**2.** (*Iekļauj varbūtības skalas skaidrojumu. Iestādei iespējams to mainīt*)	**3.** (*Iekļauj skaidrojumu atbilstoši iestādes darbības specifikai*)	**4.** (*Iekļauj skaidrojumu atbilstoši iestādes darbības specifikai*)
1	Gandrīz neiespējams		
2	Maz ticams		
3	Iespējams		
4	Bieži		
5	Ļoti bieži		

10. Risku ietekmes skala (veidlapa aizpildīšanai)

Punktu skaitliskā vērtība	**Skaitliskās vērtības nozīme**	**Skaidrojums:**
1.	**2.** (*Iekļauj varbūtības skalas skaidrojumu. Iestādei iespējams to mainīt*)	**3.** (*Iekļauj skaidrojumu atbilstoši iestādes darbības specifikai*)
1	Ļoti zema	
2	Zema	
3	Vidēja	
4	Būtiska	
5	Katastrofāla	

11. Sākotnējais un atlikušais riska līmenis (piemērs - veidlapa)

Nr. p.k.	Saīsinātais riska apraksts	Risks, riska notikuma apraksts	Riska kategorija	Riska apakš-kategorija	Varbūtība	Ietekme uz stratēģiskajiem mērķiem	Ietekme uz reputāciju	Ietekme uz finansēm	Maksimālā ietekme (Max((7.);(8.);(9.))	Riska vērtība ((7.)*(10.))	Sākotnējais riska līmenis	Esošās kontroles, kas mazina riska līmeni	Varbūtība	Ietekme uz stratēģiskajiem mērķiem	Ietekme uz reputāciju	Ietekme uz finansēm	Maksimālā ietekme (Max((15.);(16.);(17.))	Riska vērtība ((14.)*(18.))	Atlikušais riska līmenis	Risku vadības stratēģija
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	Var nebūt ilgstoši aizpildītas vakances	Divas vakances Iepirkumu nodaļas vecākā eksperta amatā netiks ilgstoši (vairāk kā seši mēneši) aizpildītas (dēļ nekonkurētspējīgā atalgojuma), kas var izraisīt iepirkumu procesa ievērojamu (līdz 3 mēnešiem) īstenošanas kavēšanos un kvalitātes pasliktināšanos, kā arī var radīt ārējo klientu neapmierinātību	Darbības (operacionālais) risks	Personāla risks	5	1	2	2	**2**	10	**Augsts**	Noteikts minimālais atalgojuma līmenis atbilstoši amata kategorijai	3	2	2	2	**2**	6	**Vidējs**	Riska samazināšana
2	IT sistēmu funkcionalitāte var nebūt aktuāla un piemērota pamatdarbībai	IT sistēmu funkcionalitāte ir novecojusi un nav iespējama datu pārnese starp informācijas sistēmām, kā arī nav iespējams ģenerēt pārskatus	Darbības (operacionālais) risks	IKT risks	5	5	5	4	**5**	25	**Ļoti augsts**	Sagatavots un apstiprināts iekšējais normatīvais akts, kas paredz IKT uzturēšanas kārtību - IS administrēšanu	4	2	3	4	**4**	16	**Ļoti augsts**	Riska samazināšana

12.1. Risku reģistrs (1.variants - vienkāršotais risku reģistra piemērs - veidlapa)

Nr. p.k.	Saīsinātais riska apraksts	Risks, riska notikuma apraksts	Riska kategorija	Riska apakš-kategorija	Riska reģistrēšanas datums	Varbūtība	Ietekme uz stratēģiskajiem mērķiem	Ietekme uz reputāciju	Ietekme uz finansēm	Maksimālā ietekme (Max((7.);(8.);(9.))	Riska līmeņa vērtība ((7.)*(11.))	Riska līmenis	Risku vadības stratēģija	Pasākumi riska mazināšanai	Atbildīgais par pasākuma izpildi	Izpildes termiņš
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	Var nebūt ilgstoši aizpildītas vakances	Divas vakances Iepirkumu nodaļas vecākā eksperta amatā netiks ilgstoši (vairāk kā seši mēneši) aizpildītas (dēļ nekonkurētspējīgā atalgojuma), kas var izraisīt iepirkumu procesa ievērojamu (līdz 3 mēnešiem) īstenošanas kavēšanos un kvalitātes pasliktināšanos, kā arī var radīt ārējo klientu neapmierinātību	Darbības (operacionālais) risks	Personāla riski		3	2	2	2	2	6	**Vidējs**	Riska samazināšana	Palielināt un noteikt atalgojuma līmeni no zemākā uz vidējo	Personāla departaments	dd.mm.gggg.
2	IT sistēmu funkcionalitāte var nebūt aktuāla un piemērota pamatdarbībai	IT sistēmu funkcionalitāte ir novecojusi un nav iespējama datu pārnese starp informācijas sistēmām, kā arī nav iespējams ģenerēt pārskatus	Darbības (operacionālais) risks	IKT riski		4	2	3	4	4	16	**Ļoti augsts**	Riska samazināšana	1. Aktualizēt iekšējo normatīvo dokumentu, kas reglamentē informācijas sistēmu uzturēšanu, paredzot tajā informācijas sistēmu izmaiņu pieprasījumu sagatavošanas kārtību 2. Izvērtēt ieviešamos informācijas sistēmas funkcionalitātes pilnveidojuma risinājumus un sniegt priekšlikumus augstākajai vadībai par vispiemērotākā risinājuma ieviešanu; 3. Ņemot vērā augstākās vadības pieņemtos lēmumus, ieviest informācijas sistēmas funkcionalitātes pilnveidojumus.	Informācijas tehnoloģiju departaments	dd.mm.gggg.

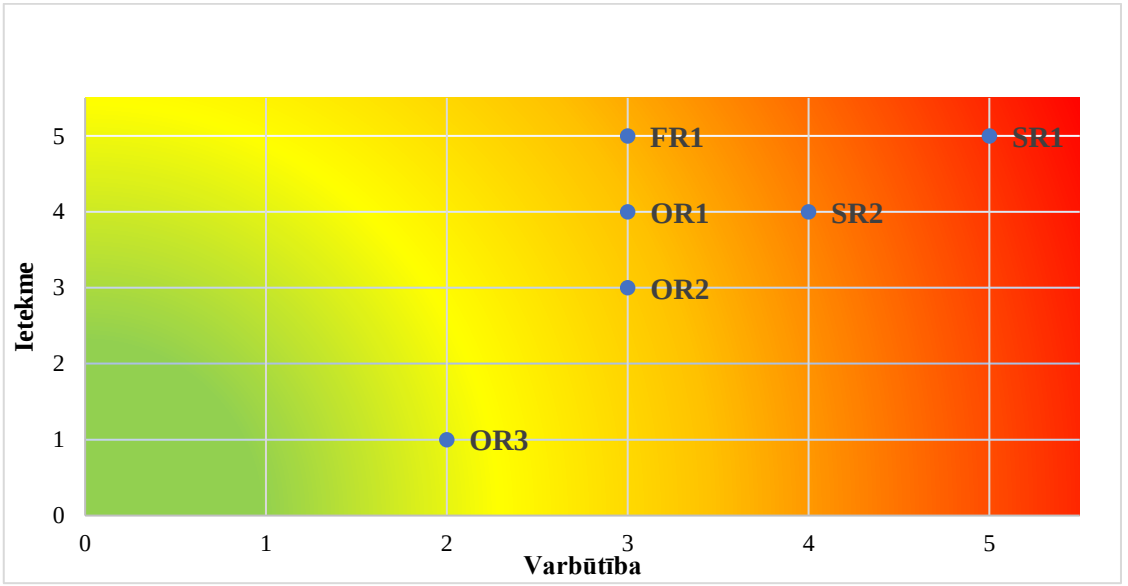
12.2. Risku reģistrs (2. variants - analītisks risku reģistra piemērs - veidlapa)

Nr. p.k.	Saīsinātais riska apraksts	Risks, riska notikuma apraksts	Riska kategorija	Riska apakš-kategorija	Riska reģistrēšanas datums	Riska cēlonis	Riska sekas	Procesa nosaukums	Riska īpašnieks	Būtiskākās esošās kontroles, kas mazina riska līmeni	Varbūtība	Ietekme uz stratēģiskajiem mērķiem	Ietekme uz reputāciju	Ietekme uz finansēm	Maksimālā ietekme (Max((12.);(13.);(14.))	Riska līmeņa vērtība ((12.)*(16.))	Riska līmenis	Risku vadības stratēģija	Pasākumi riska mazināšanai	Atbildīgais par pasākuma izpildi	Izpildes termiņš
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	Var nebūt ilgstoši aizpildītas vakances	Divas vakances Iepirkumu nodaļas vecākā eksperta amatā netiks ilgstoši (vairāk kā seši mēneši) aizpildītas (dēļ nekonkurētspējīgā atalgojuma), kas var izraisīt iepirkumu procesa ievērojamu (līdz 3 mēnešiem) īstenošanas kavēšanos un kvalitātes pasliktināšanos, kā arī var radīt ārējo klientu neapmierinātību	Darbības (operacionālais) risks	Personāla risks		Nekonkurētspējīgs atalgojums salīdzinājumā ar citām iestādēm	Iepirkumu procesa ievērojama (līdz 3 mēnešiem) īstenošanas kavēšanās. Stratēģiskie mērķi tiek ietekmēti, kavēsies dažu mērķa īstenošana līdz vienam gadam. Negatīva publicitāte nacionālajos un dažos starptautiskajos plašsaziņas līdzekļos ar ietekmi uz reputāciju.	Iepirkumu veikšana	Administratīvais departaments	Noteikts minimālais atalgojuma līmenis atbilstoši amata kategorijai	3	1	2	2	2	**6**	**Vidējs**	Riska samazināšana	Palielināt un noteikt atalgojuma līmeni no zemākā uz vidējo	Personāla departaments	dd.mm.gggg.
2	IT sistēmu funkcionalitāte var nebūt aktuāla un piemērota pamatdarbībai	IT sistēmu funkcionalitāte ir novecojusi un nav iespējama datu pārnese starp informācijas sistēmām, kā arī nav iespējams ģenerēt pārskatus	Darbības (operacionālais) risks	IKT risks		Iepriekšējā gada budžetā nebija pieejams pietiekams finansējums	Netiek nodrošināta atbilstība ārējiem normatīvajiem dokumentiem. Stratēģisko mērķu sasniegšana tiek ietekmēta, kavēsies dažu mērķa īstenošana 1 – 3 gadiem. Negatīva publicitāte nacionālajos un dažos starptautiskajos plašsaziņas līdzekļos ar ietekmi uz reputāciju Var rasties būtiski finansiālie zaudējumi valsts budžetā (100 000 – 500 000 EUR vai vairāk)	Informācijas sistēmu uzturēšana	Informācijas tehnoloģiju departaments	Sagatavots un apstiprināts iekšējais normatīvais akts, kas paredz IKT uzturēšanas kārtību - IS administrēšanu	5	2	5	3	5	**25**	**Ļoti augsts**	Riska samazināšana	1. Aktualizēt iekšējo normatīvo dokumentu, kas reglamentē informācijas sistēmu uzturēšanu, paredzot tajā informācijas sistēmu izmaiņu pieprasījumu sagatavošanas kārtību 2. Izvērtēt ieviešamos informācijas sistēmas funkcionalitātes pilnveidojuma risinājumus un sniegt priekšlikumus augstākajai vadībai par vispiemērotākā risinājuma ieviešanu 3. Ņemot vērā augstākās vadības pieņemtos lēmumus, ieviest informācijas sistēmas funkcionalitātes pilnveidojumus.	Informācijas tehnoloģiju departaments	dd.mm.gggg.

13. Risku mazinošo pasākumu plāns (piemērs - veidlapa)

NPK	Risks, riska notikuma apraksts	Riska līmenis	Riska mazināšanas pasākumi	Atbildīgais par pasākuma izpildi	Izpildes termiņš
1	2	3	4	5	6
1	Divas vakances Iepirkumu nodaļas vecākā eksperta amatā netiks ilgstoši (vairāk kā seši mēneši) aizpildītas (dēļ nekonkurētspējīgā atalgojuma), kas var izraisīt iepirkumu procesa ievērojamu (līdz 3 mēnešiem) īstenošanas kavēšanos un kvalitātes pasliktināšanos, kā arī var radīt ārējo klientu neapmierinātību	**Vidējs**	Palielināt un noteikt atalgojuma līmeni no zemākā uz vidējo	Personāla departaments	dd.mm.gggg.
2	IT sistēmu funkcionalitāte ir novecojusi un nav iespējama datu pārnese starp informācijas sistēmām, kā arī nav iespējams ģenerēt pārskatus	**Ļoti augsts**	1. Aktualizēt iekšējo normatīvo dokumentu, kas reglamentē informācijas sistēmu uzturēšanu, paredzot tajā informācijas sistēmu izmaiņu pieprasījumu sagatavošanas kārtību 2. Izvērtēt ieviešamos informācijas sistēmas funkcionalitātes pilnveidojuma risinājumus un sniegt priekšlikumus augstākajai vadībai par vispiemērotākā risinājuma ieviešanu; 3. Ņemot vērā augstākās vadības pieņemtos lēmumus, ieviest informācijas sistēmas funkcionalitātes pilnveidojumus.	Informācijas tehnoloģiju departaments	dd.mm.gggg.

14. Risku karte (piemērs, automatizēts risinājums)



SR 1 – Var netikt sasniegti iestādes stratēģiskie mērķi,

SR 2 – Var rasties ekonomiskā krīze,

FR 1 – Var nebūt pietiekams finansējums iestādes darbības plānā iekļautā pasākuma īstenošanai

OR 1 - Var būt kļūdaini dati gada pārskata sagatavošanai

OR 2 – Var rasties nesankcionēta datu noplūde

OR 3 – Var nebūt pietiekams attālinātā darba programmnodrošinājums pielikums

15. Risku karte (veidlapas aizpildīšanai, manuāls risinājums)[45]

		Iespējamība				
		1	2	3	4	5
Ietekme		Gandrīz neiespējams	Maz ticams	Iespējams	Bieži	Ļoti bieži
5	Katastrofāla					
4	Būtiska					
3	Vidēja					
2	Zema					
1	Ļoti zema					

[45] Iestāde sagatavo manuāli, iespējams mainīt risku zonas, ņemot vērā iestādes darbības specifiku, pieņemtos lēmumus par risku pieļaujamo līmeni (“zaļo” zonu). Krāsām iespējams mainīt diapazonu.

16.1. Risku matrica (1.variants)[46]

		Ietekme				
		1	2	3	4	5
Varbūtība		Ļoti zema	Zema	Vidēja	Būtiska	Katastrofāla
5	Ļoti bieži	5	10	15	20	25
4	Bieži	4	8	12	16	20
3	Iespējams	3	6	9	12	15
2	Maz ticams	2	4	6	8	10
1	Gandrīz neiespējams	1	2	3	4	5

[46] Iestāde sagatavo manuāli, iespējams mainīt risku zonas, ņemot vērā iestādes darbības specifiku, pieņemtos lēmumus par risku pieļaujamo līmeni (“zaļo” zonu). Krāsām iespējams mainīt diapazonu.

16.2. Risku matrica (2.variants) [47]

	Ietekme					
Varbūtība		1	2	3	4	5
		Ļoti zema	Zema	Vidēja	Būtiska	Katastrofāla
5	Ļoti bieži	Vidējs	Augsts	Ļoti augsts	Ļoti augsts	Ļoti augsts
4	Bieži	Vidējs	Augsts	Augsts	Ļoti augsts	Ļoti augsts
3	Iespējams	Zems	Vidējs	Augsts	Augsts	Ļoti augsts
2	Maz ticams	Zems	Vidējs	Vidējs	Augsts	Augsts
1	Gandrīz neiespējams	Zems	Zems	Zems	Vidējs	Vidējs

[47] Iestāde sagatavo manuāli, iespējams mainīt risku zonas, ņemot vērā iestādes darbības specifiku, pieņemtos lēmumus par risku pieļaujamo līmeni (“zaļo” zonu). Krāsām iespējams mainīt diapazonu.

17. Riska profils (Veidlapa aizpildīšanai)

Sagatavošanas datums:

Riska Nr.:	
Veidlapas aizpildīšanas datums:	
Riska kategorija:	
Riska notikuma apraksts:	
Riska īpašnieks:	
Nākamās pārskatīšanas datums:	
Riska veicinošie faktori:	
Varbūtības vērtējums (A)	
Ietekmes vērtējums (B)	
Riska līmeņa vērtība (A*B)	
Būtiskākās esošās kontroles, kas mazina riska līmeni:	

RISKA MAZINĀŠANAS PASĀKUMI			
Ierosinātie riska mazināšanas pasākumi:			
Nr.	**Apraksts**	**Datums:**	**Statuss:**
1.			

18. Apkopotā rezultātu karte (veidlapa aizpildīšanai)

Sagatavošanas datums:

Riska saīsināts apraksts	Riska kategorija	Riska notikuma apraksts	Individuālie vērtējumi	Varbūtības vērtējums (A)					Ietekmes vērtējums (B)				
				1	2	3	4	5	1	2	3	4	5
Risks X			**Persona 1**										
			Persona 2										
			Persona 3										
			Grupas vidējais vērtējums (A) un (B) atsevišķi										
			Kopējais vidējais riska novērtējums (A*B)										
Risks Y			**Persona 1**										
			Persona 2										
			Persona 3										
			Grupas vidējais vērtējums (A) un (B) atsevišķi										
			Kopējais vidējais riska novērtējums (A*B)										

IZMANTOTĀS LITERATŪRAS UN AVOTU SARAKSTS

1. ISO 9001:2015 – Quality management. International Organization for Standardization [2017. gada 16. marts]. Pieejams vietnē: http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm; https://www.lvs.lv/.
2. ISO 31 000:2018 – Risk management — Guidelines. International Organization for Standardization [2008. g. februāris]. Pieejams vietnē: https://www.lvs.lv/.
3. ISO Guide 73:2009 - Risk management — Vocabulary [November 2009].
4. Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework - Integrating with Strategy and Performance [2017]. Pieejams vietnē: https://www.coso.org/sitepages/internal-control.aspx?web=1.
5. Implementing the Commonwealth Risk Management Policy – Guidance [2016].
6. Starptautiskie Iekšējā audita profesionālās prakses standarti [2017].
7. Ministru kabineta 2012. gada 8. maija noteikumi Nr.326 "Noteikumi par iekšējās kontroles sistēmu tiešās pārvaldes iestādēs". Pieejams vietnē: https://likumi.lv/ta/id/247746-noteikumi-par-ieksejas-kontroles-sistemu-tiesas-parvaldes-iestades.
8. Finanšu un kapitāla tirgus komisijas normatīvie 2020. gada 3. novembra noteikumi Nr. 209 "Kapitāla un likviditātes pietiekamības novērtēšanas procesa izveides normatīvie noteikumi". Pieejams vietnē: https://likumi.lv/ta/id/318511-kapitala-un-likviditates-pietiekamibas-novertesanas-procesa-izveides-normativie-noteikumi .
9. Galandere - Zīle, I. [2017]. Valsts kases Kvalitātes un risku vadības departamenta direktore.
10. The Information Systems Audit and Control Association (ISACA). Pieejams vietnē: https://www.isaca.org/training-and-events/training-topics/browse-all-training?utm_source=google&utm_medium=cpc&utm_campaign=tyw&utm_content=sem_tyw_training-tyw-row-google&cid=sem_2007811&Appeal=sem&gad=1&gclid=Cj0KCQjwgLOiBhC7ARIsAIeetVCLuFDcqbkC6p48pqfRKq-F1SQcLODuuGpGdTd4TYfCmZcfZxgi18saAqowEALw_wcB#sort=relevancy&f%3ALanguage=%5BEnglish%5D .
11. Eiropas Sociālā fonda, Eiropas Reģionālā attīstības fonda un Kohēzijas fonda vadībā iesaistīto iestāžu ES fondu Risku pārvaldības stratēģija 2014.-2020. gada plānošanas periodā, ES fondu vadošā iestāde [2014. gada 19. decembris]. Pieejams vietnē: https://www.esfondi.lv/upload/14-20_gads/2014-12-19_Risku_parvaldibas_strategija_2014.-2020.gada_planosanas_perioda.pdf.
12. Practise Standart for Project Risk Management, Project Management Institute [2009]. Pieejams vietnē: https://www.pmi.org/-/media/pmi/documents/public/pdf/certifications/practice-standard-project-risk-management.pdf?v=1e0b5985-74af-4c57-963c-b91a9af6fecb.
13. Minimum Security Requirements for Federal Information and Information Systems National Institute of Standards and Technology (NIST), [March 2006], Pieejams vietnē: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf.
14. Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37, Revision 2,

National Institute of Standards and Technology (NIST), [December 2018], Pieejams vietnē: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.
15. "Trīs līniju modelis", Iekšējo auditoru institūts [2020. gada jūlijs] https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-latvian.pdf.
16. 2002. gada 6. jūnija Saeimas likums "Valsts pārvaldes iekārtas likums". Pieejams vietnē: https://likumi.lv/ta/id/63545-valsts-parvaldes-iekartas-likums.
17. 2012. gada 13. decembra Saeimas likums "Iekšējā audita likums". Pieejams vietnē: https://likumi.lv/ta/id/253680-iekseja-audita-likums
18. Ministru kabineta 2022. gada 26. aprīļa noteikumi Nr. 262 "Valsts un pašvaldību institūciju amatu katalogs, amatu klasifikācijas un amatu apraksta izstrādāšanas kārtība". Pieejams vietnē: https://likumi.lv/ta/id/332122-valsts-un-pasvaldibu-instituciju-amatu-katalogs-amatu-klasifikacijas-un-amatu-apraksta-izstradasanas-kartiba.
19. Risku kapacitāte. Pieejams vietnē: https://analystprep.com/study-notes/frm/part-1/foundations-of-risk-management/governance-of-risk-management/.
20. Iestādes risku profils un apetīte. Pieejams vietnē: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-0614.pdf.
21. Attieksmes, uzvedības un kultūras modelis, The Institute of Risk Management [2012]. Pieejams vietnē: https://www.theirm.org/media/7236/risk-culture-resources-for-practitioners.pdf.
22. Risku kultūras ietvars, The Institute of Risk Management [2012]. Pieejams vietnē: https://www.theirm.org/media/7230/risk-culture-resources-for-practitioners.pdf.
23. Eiropas Komisijas Zaļā grāmata par korporatīvo pārvaldību, LR Tieslietu ministrijas publikācija [2011. gada 17. maijs]. Pieejams vietnē: https://www.tm.gov.lv/lv/jaunums/zala-gramata-par-kapitalsabiedribu-korporativas-parvaldibas-principiem?utm_source=https%3A%2F%2Fwww.google.com%2F .
24. The Orange Book, Government Finance Function and HM Treasury [29 May 2013] Pieejams vietnē: Orange Book - GOV.UK (www.gov.uk).
25. The Orange Book, UK Government [2023. gada versija]: Pieejams vietnē: https://www.gov.uk/government/publications/orange-book
26. Finanšu ministrijas izstrādātajās Vadlīnijās risku vadības iekšējam auditam un konsultācijai.
27. Risku vadības sistēmas briedums valsts pārvaldē, Finanšu ministrija [2022. gada 21. oktobris]. Pieejams vietnē: PowerPoint Presentation (fm.gov.lv).
28. "Reformu plāns – valsts pārvaldes attīstības impulss" Ministru kabinets [2019]. Pieejams vietnē: https://www.mk.gov.lv/lv/jaunums/reformu-plans-valsts-parvaldes-attistibas-impulss.
29. Iekšējā audita profesionālās prakses starptautiskie standarti https://iai.lv/lv/standarti-un-noradijumi.
30. Korporatīvās pārvaldības kodekss (Tieslietu ministrija, Princips # 4 un 5) https://www.tm.gov.lv/sites/tm/files/media_file/korporativas-parvaldibas-kodekss_0.pdf.
31. Informācija par Trīs līniju aizsardzības modelis - Rokasgrāmatas 3.1. nodaļā.

IAI Trīs līniju modelis pieejams šeit: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-latvian.pdf

32. Iekšējā audita likums. Pieejams vietnē: https://likumi.lv/ta/id/253680-iekseja-audita-likums.
33. Ministru kabineta 2013.gada 9.jūlija noteikumi Nr. 385 "Iekšējā audita veikšanas un novērtēšanas kārtība". Pieejams vietnē: https://likumi.lv/ta/id/258270-iekseja-audita-veiksanas-un-novertesanas-kartiba.
34. Pieejamās vietnes:
35. vispārīgi

- RZMBJMZK (ibm.com)
- TPP 12-03a A risk management toolkit - Executive Guide (nsw.gov.au)
- TPP12-03b Risk management toolkit Volume 1 Guidance for Agencies (nsw.gov.au)
- TPP 12-03c Risk management toolkit Volume 2 - Templates (nsw.gov.au)
- 12-22_Risk_Management.pdf (nsw.gov.au)
- risk-management-guideline.pdf (gov.bc.ca)
- Framework for Enterprise Risk Management Version 3.0 - U.S. Department of Labor - Office of Inspector General (dol.gov)
- ISO
- bves-program-manual-final-edit-version-022218.pdf (ca.gov)
- Foreword (dhs.sa.gov.au)
- COSO
- https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf\
- https://www.coso.org/Shared%20Documents/CROWE-COSO-Internal-Control-Integrated-Framework.pdf
- https://www.issai.org/wp-content/uploads/2019/08/intosai_gov_9100_e.pdf
- The Orange book (faktiski visi linki / dokumenti)
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191516/Risk_management_assessment_framework.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191517/The_principles_of_mamaging_risks_the_public.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191518/Managing_risks_to_the_public_appraisal_guidance.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191519/Setting_and_communicating_your_risk_appetite.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191520/Managing_your_risk_appetite_a_practitioners_guide.pdf

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191521/Managing_your_risk_appetitie_good_practice_examples.pdf