

VAS "Latvijas Pasts"
Reģ.Nr.40003052790
Ziemeļu iela 10,
Lidosta "Rīga",
Mārupes novads,
LV-1000

info@pasts.lv
www.pasts.lv

+371 2700 8001



APSTIPRINĀTS

VAS "Latvijas Pasts"
2025.gada 02.septembrī
valdes sēdē ar lēmumu Nr.6.1.
(protokols Nr.41/2025)

APSTIPRINĀTS

VAS "Latvijas Pasts"
2025.gada 25.septembrī
padomes sēdē ar lēmumu Nr.5.1.
(protokols Nr.16/2025)

Risku vadības politika

Pasts

*DOKUMENTS PARAKSTĪTS AR DROŠU ELEKTRONISKO
PARAKSTU UN SATUR LAIKA ZĪMOGU

Saturs

I. Lietoto jēdzienu un terminu skaidrojums	2
II. Vispārīgie noteikumi	5
III. Risku vadības mērķi	6
IV. Risku vadības ietvars un principi	6
V. Risku vadībā iesaistītās puses un to atbildība	8
VI. Risku grupas	9
VII. Risku apetīte un tolerance	11
VIII. Iekšējās kontroles sistēma	12
IX. Incidentu vadība	16

I. Lietoto jēdzienu un terminu skaidrojums

Termins	Skaidrojums
Atlikušais risks	Riska vērtība pēc RMP un kontroļu īstenošanas.
COSO ERM un IC	Starptautiski atzītie ASV Tredveja komisijas sponsorējošo organizāciju komitejas (<i>The Committee of Sponsoring Organizations</i>) izstrādātie modeļi: COSO ERM – uzņēmuma risku pārvaldības modelis (<i>Enterprise Risk Management</i>) un COSO IC – iekšējās kontroles modelis (<i>Internal Control – Integrated Framework</i>).
Darbības nepārtrauktības plāns	Plāns, kas nosaka, kā tiek nodrošināta nepārtraukta LP kritisko procesu izpilde un kritisko resursu pieejamība un tiek veikti preventīvie pasākumi kritisko procesu nepārtrauktas izpildes nodrošināšanai ārkārtas situācijās, t.sk. kā kritiskās infrastruktūras objektam valsts apdraudējuma gadījumā.
Iespējas	Apstākļu un faktoru nenoteiktība, kas pozitīvi ietekmē LP mērķu sasniegšanu.
IKS	Iekšējās kontroles sistēma – pasākumu kopums, kas darbojas kā vienots, savstarpēji atbalstošs mehānisms, un palīdz nodrošināt: <ul style="list-style-type: none"> • darbības efektivitāti – uzlabot resursu izmantošanu un procesus; • atbilstību normatīvajiem aktiem – palīdz ātri reaģēt uz izmaiņām un integrēt normatīvo aktu prasības ikdienas procesos; • finanšu pārskatu precizitāti – novērš kļūdas un krāpšanu; • aktīvu aizsardzību – rada klientu, partneru un sabiedrības uzticamību.

Termins	Skaidrojums
	Iekšējās kontroles sistēma ir būtiska LP korporatīvās pārvaldības un risku vadības daļa.
Incidents	Iestājies/noticis riska realizācijas notikums, kas var izraisīt LP darbības vai konkrēta (noteikta) pakalpojuma sniegšanas pārtraukumu vai traucējumus, finansiālus vai reputācijas zaudējumus, apdraudējumu cilvēku veselībai/dzīvībai vai darbības nepārtrauktībai.
Jomas atbildīgais	Darbinieks (parasti LP struktūrvienības vadītājs), kas nosaka riska pārvaldības prasības jomā, kuru regulē ārējie normatīvie akti – prasības muitas, IKT drošības, sankciju, NILLTPFN, ESG un citās jomās. Jomas atbildīgais izstrādā un periodiski pārskata attiecīgā riska pārvaldības politiku un novērtēšanas metodoloģiju, Risku apetīti, toleranci un IKS saturu procesos, kā arī uztur attiecīgā riska reģistru. Jomas atbildīgajam ir tiesības veikt savas jomas atbilstības pārbaudes citās struktūrvienībās un viņš atbilstoši Kārtībā noteiktajam atskaitās LP valdei un padomei par riskiem un kontrolēm savā jomā.
Kārtība	VP03-02 "Risku vadības kārtība".
Kontrole	<p>Kontrole, kā pretdarbība riska cēloņiem un sekām, ir mērķu sasniegšanas mehānisms un riska mazināšanas paņēmieni, kuru raksturo divas komponentes: kontroles dizains un kontroles operacionālais izpildījums.</p> <p>Kontroles dizains – process, kurā Riska īpašnieks vai Jomas atbildīgais izstrādā, tai skaitā iekšējos normatīvajos aktos, un strukturē iekšējās kontroles, lai efektīvi pārvaldītu riskus.</p> <p>Kontroles operacionālais izpildījums – izstrādāto kontroļu īstenošana praksē, ko nodrošina Kontroles īpašnieks, un kas parāda, vai kontroles darbojas tā, kā paredzēts, un vai tās efektīvi ietekmē riskus.</p> <p>Kontroles efektivitātes novērtēšanai var izmantot rādītājus, kas parāda, cik lielā mērā kontrole mazina vai novērš risku.</p>
Kontroles īpašnieks	LP darbinieks vai struktūrvienība, kas ir atbildīga par kontroles ieviešanu, operacionālo izpildi un uzturēšanu, kā arī sadarbībā ar Risku īpašnieku vai Jomas atbildīgo novērtē kontroles efektivitāti, uzrauga tās darbību un veic nepieciešamos uzlabojumus.
KRVD	Kvalitātes un risku vadības daļa.
LP	VAS "Latvijas Pasts".
Politika	VP03-01 "Risku vadības politika".

Termins	Skaidrojums
Riska grupa	Risku klasifikācija pēc to rašanās jomas – operacionālie, atbilstības/juridiskie, finanšu, sociālie, IKT u.tml.
Riska īpašnieks	LP darbinieks vai struktūrvienība, kas īsteno Riska vadību. Riska īpašnieks ir atbildīgs par iekšējo normatīvo aktu sagatavošanu un aktualizēšanu atbilstoši ārējo normatīvo aktu prasībām, tādējādi nodrošinot attiecīgā riska pārvaldību IKS ietvaros, kontroļu dizaina izstrādi, kā arī sadarbībā ar Kontroļu īpašnieku rūpējas par kontroļu efektivitāti.
Riska mazināšanas pasākumi (RMP) un kontroles	Pasākumi, kas tiek īstenoti, lai pārvaldītu identificētos riskus – mazinātu riska varbūtību un/vai riska ietekmi. No risku mazināšanas pasākumiem var tikt izveidots risku pārvaldības plāns ar atbildīgajiem par tā īstenošanu un izpildes termiņiem.
Riska tolerance	Maksimālā novirze no Risku apetītes, ko LP ir gatavs pieņemt.
Riska uzraudzības rādītāji	Pazīmes vai indikatori, kas kvantitatīvi parāda, vai riska vērtība ir mainījies. Rādītājus nosaka, ņemot vērā Risku apetīti. Rādītājus izsaka absolūtos vai relatīvos skaitļos, to novērtē trīs pakāpju skalā: zema, vidēja vai augsta.
Risks	<p>Apstākļu un faktoru nenoteiktība, kas negatīvi ietekmē LP mērķu sasniegšanu. Risku raksturo tā varbūtība, ietekme un vērtība.</p> <p>Riska varbūtība ir iespējamība, ka risks iestāsies (tai skaitā kā Incidents) tuvāko 12 mēnešu laikā.</p> <p>Riska ietekme ir riska iestāšanās radīto seku ietekme uz LP resursiem, procesu mijiedarbību un mērķu sasniegšanu.</p> <p>Riska vērtība ir riska varbūtības un riska ietekmes reizinājums.</p>
Risku apetīte	Risku apjoms un veids, ko LP vēlas un ir gatavs pieņemt savā darbībā, lai sasniegtu mērķus. Risku apetīte ietekmē kopējo risku vadības kultūru, darbu un resursu plānošanu, kā arī lēmumu pieņemšanas procesu, savukārt Riska tolerance nosaka robežas pieņemamām snieguma variācijām attiecībā uz konkrētiem mērķiem.
Risku portfelis	Strukturēta visu risku kopa, kas piemīt pakalpojumiem, produktiem un projektiem, un kuru nosaka gan LP līmenī kopumā, gan katrā struktūrvienībā atsevišķi. Risku portfelis palīdz sistemātiski identificēt, novērtēt, noteikt prioritātes, pārvaldīt riskus un resursus.
Risku reģistrs	Identificēto risku saraksts, ko izmanto kā risku pārvaldības rīku un kuru pārvaldībā iesaistās arī LP valde un padome. Tajā iekļauj būtiskos riskus, kuri var izraisīt LP darbības vai konkrēta (noteikta) pakalpojuma sniegšanas pārtraukumu vai traucējumus, finansiālus vai reputācijas zaudējumus, apdraudējumu cilvēku veselībai/dzīvībai vai darbības nepārtrauktībai. Risku reģistra

Termins	Skaidrojums
	<p>saturu un aizpildīšanas prasības nosaka VP03-02 "Risku vadības kārtība".</p> <p>Risku reģistrs un risku pārvaldības plāni, kas var tikt iekļauti reģistrā vai izstrādāti atsevišķi, ir LP komercnoslēpums Komercnoslēpuma aizsardzības likuma izpratnē.</p>
Risku vadība	<p>Nepārtraukts un sistemātisks process, kas ir integrēts gan LP stratēģijas izstrādē un ieviešanā, gan struktūrvienību ikdienas operatīvajā darbā un ietver risku identificēšanu, novērtēšanu, RMP un kontroļu ieviešanu un īstenošanu, to efektivitātes novērtēšanu, analīzi, atskaišu sagatavošanu un komunikāciju par riskiem. Proaktīvā pieeja ļauj identificēt iespējamās problēmas vai iespējas pirms to rašanās un izstrādāt plānu to negatīvo seku mazināšanai vai pozitīvās ietekmes palielināšanai.</p>
Sākotnējais (inherent) risks	<p>Hipotētisks, dabisks, konkrētam procesam, nozarei vai videi piemītošais risks, kas pastāv pirms RMP un kontroļu ieviešanas. Tā novērtēšanā neņem vērā iekšējās kontroles vai aizsardzības mehānismus un tas palīdz noteikt, kur nepieciešamas kontroles un cik spēcīgām tām jābūt. Ja netiek īstenoti nekādi RMP vai kontroļu pasākumi, tad Sākotnējā riska vērtība ir vienāda ar Atlikušā riska vērtību.</p>
Trīs aizsardzības līniju modelis	<p>Starptautiski atzīts risku vadības un iekšējās kontroles modelis, kurā uzņēmuma risku vadība nosacīti tiek sadalīta trīs aizsardzības līnijās: primārā risku vadība visās biznesa jomās, risku vadības procesa uzraudzība un kontrole un neatkarīgas pārlicības sniegšana, veicot iekšējā audita pārbaudes.</p>

II. Vispārīgie noteikumi

1. Lai aizsargātu un radītu pievienotu vērtību, sasniedzot uzņēmuma mērķus un attīstot savu potenciālu tirgū, LP uzņemas dažāda veida riskus. Risku vadība ir izpratne par to, kas varētu notikt, un rīkoties, lai palielinātu panākumu apjomu un iespējamību.
2. Riski tiek vērtēti un risku vadība tiek pilnveidota atbilstoši LP misijai, vīzijai un aktuālās vidēja termiņa darbības stratēģijas mērķiem.
3. Risku vadības procesa norise un prasības noteiktas Kārtībā.
4. Riskiem, kuru uzraudzības un vadības prasības nosaka ārējo normatīvo aktu regulējums, Jomas atbildīgie nodrošina, ka risku novērtēšana tiek veikta atbilstoši ārējo normatīvo aktu prasībām, izstrādājot attiecīgu metodoloģiju un iespēju robežās izmantojot Politikā un Kārtībā noteikto risku novērtēšanas ietvaru.
5. KRVD novērtē un pilnveido risku vadības sistēmas brieduma līmeni.
6. Politika ir saistoša visiem LP darbiniekiem, LP valdes un padomes locekļiem.
7. Politika tiek pārskatīta un aktualizēta pēc nepieciešamības vai atbilstoši vispārējai iekšējo normatīvo aktu pārskatīšanas kārtībai, lai nodrošinātu atbilstību aktuālajai LP vidēja

termiņa darbības stratēģijai, ārējiem un iekšējiem normatīvajiem aktiem un starptautiski atzītiem standartiem, kā arī novērstu identificētos procesa trūkumus.

III. Risku vadības mērķi

8. Risku vadība ir neatņemama LP kvalitātes vadības sistēmas sastāvdaļa.
9. Ieviešot vienotu pieeju risku pārvaldībai, LP:
 - 9.1. nodrošina lielāku gatavību notikumiem, kas varētu radīt finansiālus zaudējumus vai kaitējumu reputācijai, videi vai varētu būtiski ietekmēt pakalpojumu pieejamību;
 - 9.2. identificē ar esošajiem biznesa apstākļiem saistītas jaunas iespējas un izaicinājumus, vienlaikus uzlabojot veiktspēju, palielinot priekšrocības un samazinot negatīvus pārsteigumus;
 - 9.3. visos pārvaldības līmeņos atvieglo lēmumu pieņemšanu un darbu plānošanu;
 - 9.4. uzlabo resursu sadali un izmantošanu saskaņā ar Risku apetīti;
 - 9.5. uzlabo uzņēmējdarbības noturību un spēju reaģēt uz pārmaiņām;
 - 9.6. uzlabo reputāciju kā uzticams sadarbības partneris ar izcilu klientu apkalpošanas servisu.
10. LP nosaka risku vadības procesā iesaistīto LP struktūrvienību un darbinieku pienākumus, pilnvaras un atbildību.
11. Īstenojot risku vadību, LP stiprina vertikālo un horizontālo sadarbību starp dažādiem vadības līmeņiem, struktūrvienībām, leksējā audita daļu un ārējām uzraugošajām institūcijām.

IV. Risku vadības ietvars un principi

12. Risku pārvaldību LP īsteno divos līmeņos:
 - 12.1. operacionālajā (funkciju) līmenī – lai nodrošinātu objektīvu un kvalitatīvu risku novērtēšanu, risku pārvaldība tiek veikta vienas jomas, funkcijas vai procesu Risku īpašnieku un Jomu atbildīgo līmenī un atbildīgā valdes locekļa pārraudzībā;
 - 12.2. stratēģiskajā un taktiskajā līmenī – LP līmenī, kur pārvalda tikai būtiskos riskus, kuri var negatīvi ietekmēt LP funkciju veikšanu vai stratēģisko mērķu sasniegšanu.
13. LP risku vadība balstās uz COSO ERM modeli un ietver šādas komponentes:



14. **Pārvaldība un kultūra** nosaka organizācijas toni, uzsverot uzņēmuma risku pārvaldības nozīmi un uzraudzības pienākumus, rūpējas par ētiskajām vērtībām, vēlamu uzvedību un risku vadības izpratni LP.
15. Risku vadībā LP izmanto **Trīs aizsardzības līniju modeli**, kur:
- 15.1. Pirmā aizsardzības līnija ir visas LP struktūrvienības, kas ir atbildīgas par riskiem un to vadību savās ikdienas darbībās, tai skaitā, efektīvi izpildot Risku īpašnieku paredzētās kontroles. Risku identificēšanai, novērtēšanai, pārvaldībai, uzraudzībai un ziņošanai par riskiem, lai nodrošinātu, ka tie nepārsniedz noteikto Risku apetīti attiecīgajā jomā, ir izstrādāti iekšējie normatīvie akti un atbilstoši procesi ar iekšējām kontrolēm.
- 15.2. Otrā aizsardzības līnija ir KRVD un Jomu atbildīgie, kas veido risku vadības ietvaru un nosaka, kā identificēt, vērtēt, mērīt, uzraudzīt, pārvaldīt un ziņot par riskiem. Otrā aizsardzības līnija izvērtē un pārbauda pirmās aizsardzības līnijas riska vadību un kontroli. Otrā aizsardzības līnija ir neatkarīga no pirmās un neveic operacionālās darbības, lai saglabātu neatkarību uzraudzības un kontroles veikšanā.
- Ja struktūrvienībā tiek veiktas gan pirmās, gan otrās aizsardzības līnijas funkcijas, otrās aizsardzības līnijas neatkarību nodrošina atbildīgā valdes locekļa, pārvaldes vadītāja vai struktūrvienības vadītāja iesaiste risku vadībā.
- 15.3. Trešā aizsardzības līnija ir LP iekšējā audita daļa, kura ir neatkarīga no pirmās un otrās aizsardzības līnijas un ir atbildīga par pirmās un otrās aizsardzības līnijas pārvaldības, riska vadības un IKS procesu efektivitātes novērtēšanu.
16. **Stratēģija un mērķu noteikšana** nozīmē, ka LP risku vadība, stratēģija un mērķu noteikšana darbojas kopā stratēģiskās plānošanas procesā. Organizācija nosaka Risku apetīti, identificē un novērtē riskus, vienlaikus izstrādājot biznesa mērķus dažādos līmeņos, tas atbalsta stratēģiju un ļauj LP reaģēt uz riskiem.
17. **Stratēģijas izpildes uzraudzība** ietver risku, kas var ietekmēt stratēģijas un biznesa mērķu sasniegšanu, identificēšanu, prioritizēšanu saskaņā ar Risku apetīti, novērtēšanu un rezultātu ziņošanu galvenajām riska ieinteresētajām pusēm.
18. **Stratēģijas pārskatīšanas un papildināšanas** ietvaros LP, analizējot savu darbību, novērtē, cik labi darbojas risku vadības komponentes, ņemot vērā būtiskas izmaiņas, un kādas pārskatīšanas ir nepieciešamas.

19. **Informācijas apmaiņa, komunikācija un ziņošana** tiek īstenota kā nepārtraukts informācijas iegūšanas un apmaiņas process no iekšējiem un ārējiem avotiem, kas caurvij visus LP līmeņus.

V. Risku vadībā iesaistītās puses un to atbildība

20. LP padome:

- 20.1. nosaka pienākumu sadali un informācijas apmaiņu starp padomi un valdi;
- 20.2. apstiprina pirmā līmeņa organizatorisko struktūru, Politiku, Risku apetītes līmeņus;
- 20.3. pārrauga un gūst pārliecību, ka risku vadības funkcija LP ir atbilstoši ieviesta un strādā saskaņā ar Politiku;
- 20.4. kontrolē valdes nodrošināto IKS izveidi un darbības efektivitāti;
- 20.5. izskata ļoti augsta riska gadījumus un stratēģiskos riskus, nepieciešamības gadījumā pieņemot lēmumus.

21. LP valde:

- 21.1. nosaka LP mērķus un organizatorisko struktūru saskaņā ar stratēģiju;
- 21.2. apstiprina Politiku un citus iekšējos risku vadības normatīvos dokumentus;
- 21.3. nosaka LP Risku apetīti, saskaņojot to ar LP padomi;
- 21.4. izveido risku vadības sistēmu un pārvalda visaptverošu IKS;
- 21.5. īsteno Politiku, nosakot pienākumus, tiesības un atbildības risku vadības jomā;
- 21.6. atbild par LP risku vadības nodrošināšanu, tās nepārtrauktību, risku kultūras veidošanu un ievērošanu visās LP struktūrvienībās;
- 21.7. nodrošina LP darbībai piemītošo risku identificēšanu, novērtēšanu un pārvaldīšanu, tai skaitā, izmantojot RMP un ieviešot attiecīgas kontroles;
- 21.8. uzrauga RMP un kontroļu ieviešanu;
- 21.9. novērš IKS trūkumus un sniedz pārskatus par tās darbību padomei un akcionāram.

22. LP struktūrvienības:

- 22.1. Risku īpašnieki ir LP struktūrvienības un kā pirmā aizsardzības līnija veic primāro risku vadību savas atbildības jomas un kompetences ietvaros;
- 22.2. Jomu atbildīgie – LP struktūrvienību vadītāji un attiecīgās jomas speciālisti – pilda otrās aizsardzības līnijas pienākumus risku vadībā, nodrošinot IKS iekšējo normatīvo aktu izstrādi un veicot atbilstības pārbaudes savā atbildības jomā, uztur attiecīgā riska reģistru un atbilstoši Kārtībā noteiktajam atskaitās LP valdei un padomei par riskiem un kontrolēm savā jomā;
- 22.3. Jomu atbildīgie, Risku īpašnieki un Kontroļu īpašnieki saskaņā ar LP noteikto kārtību periodiski pārskata procesus un ieviestās kontroles, nodrošinot, ka tās ir efektīvas un samērīgas ar pārvaldāmā riska līmeni, t.i., to izmaksas nepārsniedz potenciālus zaudējumus;
- 22.4. pirmā līmeņa vadītāji atbildīgā valdes locekļa vai pārvaldes vadītāja pārraudzībā ir atbildīgi par savas struktūrvienības risku identificēšanu un novērtēšanu atbilstoši Kārtībā noteiktajam, nosaka risku attīstības tendences, atbild par RMP plānošanu, kontroles pasākumu izvēli atbilstoši novērtētajam riskam, par RMP un kontroļu

ieviešanas termiņu ievērošanu, rūpējas par esošo kontroļu darbību un to efektivitāti, kā arī atbild par LP Risku apetītes un IKS prasību ievērošanu;

- 22.5. struktūrvienību vadītājiem ir pienākums apkopot informāciju par Incidentiem, veikt to analīzi, novērst sekas, izstrādāt pret darbības pasākumus un ziņot par tiem atbilstoši noteiktajai kārtībai. Struktūrvienību vadītājiem jānodrošina, ka Incidentu analīze tiek veikta sistemātiski, identificējot cēloņus, ne tikai sekas, lai veiktu korektīvus un preventīvus pasākumus.

23. KRVD:

- 23.1. pilda otrās aizsardzības līnijas pienākumus, sadarbojoties ar LP struktūrvienībām un LP valdi, koordinē, pārrauga un objektīvi izaicina un apšaubā struktūrvienībās identificētos riskus, to novērtējumu, RMP un kontroļu pasākumu ieviešanu un efektivitāti;
- 23.2. veicina izpratni par risku vadību un atbildību visos LP struktūrvienību līmeņos, sniedzot LP struktūrvienībām, LP valdei un padomei nepieciešamo metodoloģisko un konsultatīvo atbalstu risku vadības jomā;
- 23.3. veido un attīsta vienotu iekšējo normatīvo ietvaru, nodrošina pārējos LP darbiniekus ar informāciju par risku vadības procesu, kā arī veic darbinieku apmācību;
- 23.4. sadarbībā ar Risku īpašniekiem un Jomu atbildīgajiem nodrošina risku identificēšanu, novērtēšanu un vadību;
- 23.5. uztur LP risku reģistru ar RMP un kontroļu ieviešanas uzdevumiem un termiņiem, kontrolējot to izpildi;
- 23.6. sagatavo LP valdei un LP padomei regulāras atskaites par risku vadības procesu un rezultātiem atbilstoši Kārtībā noteiktajam un LP valdes un padomes lēmumiem;
- 23.7. risku vadības sistēmas brieduma līmeņa noteikšanai vismaz reizi trijos gados veic sistēmas pašnovērtējumu saskaņā ar Finanšu ministrijas apstiprinātajām "Vadlīnijām risku vadības iekšējam auditam un konsultācijai" vai citu atbilstošu metodiku;
- 23.8. sadarbībā ar Jomu atbildīgajiem izstrādā risku novērtēšanas metodoloģijas un pārbažu paņēmienus.

24. Ikviens LP darbinieks ir atbildīgs par risku vadības sistēmas uzbūves principu zināšanu, ārējo un iekšējo normatīvo aktu ievērošanu un, nepieciešamības gadījumā, risku situācijas un/vai incidentu komunikācijas eskalāciju savā ikdienas darbā līdz tiešajam vadītājam.

25. Iekšējā audita daļa vai piesaistīta trešā puse (neatkarīgs ārējais konsultants) veic risku vadības procesa iekšējos auditus, tādējādi nodrošinot trešo aizsardzības līniju. Vēlamā iekšējo auditu veikšanas regularitāte ir vismaz viena reize trijos gados.

VI. Risku grupas

26. Īstenojot risku vadību, riski tiek klasificēti vismaz, bet ne tikai, šādās riska grupās:

- 26.1. **atbilstības/juridiskie riski** ir risku grupa, kurā atbilstības risks ietver plašu standartu spektra ievērošanu, tostarp normatīvo prasību, līgumsaistību un ētikas normu pielāgošanu iekšējos normatīvajos aktos, turpretī juridiskais risks koncentrējas uz iespējamu tiesvedību, ja tiek pārkāpti likumi vai līgumu nosacījumi;
- 26.2. **ārpakalpojumu izmantošanas riski** rodas no iespējamības, ka trešās puses likumdošanas un līguma prasību pārkāpumi, tās pakalpojumu kvalitātes,

- pieejamības, drošības vai IKT risinājuma trūkumi vai slikta reputācija var negatīvi ietekmēt LP darbību, klientu apkalpošanu vai atbilstību normatīvajām prasībām;
- 26.3. **cilvēkresursu riski** ir risku grupa, kurā apvienoti ikdienas pārvaldības riski, kas saistīti ar nepieciešamo darbinieku plānošanu, atlasi, profesionālo sagatavošanu, kvalifikācijas pilnveidi un izaugsmes nodrošināšanu, kā arī darba devēja/LP konkurētspējas nodrošināšanu;
- 26.4. **darba vides drošības riski** attiecināmi uz iespēju gūt traumas vai slimības darba apstākļos. Grupa ietver fiziskos, ķīmiskos, bioloģiskos, ergonomiskos un psihosociālos apdraudējumus;
- 26.5. ESG (*Environment, Social, Governance*) riski: šos riskus veido vides, sociālie un uzņēmuma pārvaldības jautājumi:
- 26.5.1. **vides riski** ir LP darbība apkārtējā vidē, kas attiecas uz resursu izsīkšanu, piesārņojumu, emisijām, atkritumu veidošanos un klimata pārmaiņām;
- 26.5.2. **sociālie riski** ir saistīti ar LP ietekmi uz sociālajām jomām, kas skar darbiniekus, klientus, piegādātājus un sabiedrību kopumā. Riskā ir iekļauta darbinieku drošība, darba prakse, taisnīga atlīdzība, piegādes ķēdes pārvaldība, cilvēktiesības, daudzveidība, iekļaušana un sabiedrības veselība;
- 26.5.3. **uzņēmuma pārvaldības riski** ir saistīti ar uzņēmuma pārvaldības modeli, struktūru un procesiem. Pārredzamība, ētika, atbildību sadalījums, atbilstība likumdošanas prasībām, risku un IKS vadība, valdes dažādība un akcionāru tiesības ir daļa no uzņēmuma pārvaldības riskiem;
- 26.6. **finanšu riskus** veido ārējie tirgus apstākļi un ekonomiskie faktori, kas ir ārpus LP kontroles, ietekmējot uzņēmuma rentabilitāti, ieņēmumu un investīciju budžeta izpildi, piemēram, kredītrisks, likviditātes, tirgus cenas, valūtas, procentu riski;
- 26.7. **fizisko bojājumu riski** attiecas uz iespējamiem zaudējumiem vai bojājumiem aktīviem, ēkām, telpām, īpašumam vai personām fizisku notikumu vai apstākļu dēļ. Tos var izraisīt ugunsgrēks, plūdi, dabas katastrofa vai noziegumi, piemēram, zādzība vai vandālisms;
- 26.8. **IKT drošības riski** (izņemot IKT drošības operacionālos riskus) ietver plašu potenciālu draudu klāstu, kas var ietekmēt LP informācijas sistēmas un to datu konfidencialitāti, integritāti un pieejamību. Šie riski var rasties no dažādiem avotiem, tostarp ļaunprātīgiem darbiniekiem, ārējiem uzbrukumiem, dabas katastrofām un cilvēciskām kļūdām;
- 26.9. **IKT riski** (tai skaitā IKT drošības operacionālie riski) saistīti ar LP informācijas sistēmu un tehnoloģiju uzturēšanu, attīstību un IKT darbības nepārtrauktības nodrošināšanu;
- 26.10. **korupcijas un interešu konflikta riski** rodas no apdraudējuma, ka kāds no LP nodarbinātajiem vai amatpersonām, kam uzticēta vara vai atbildība noteiktu pilnvaru ietvaros, ar nodomu vai bez nodoma rīkojas savu vai citas personas materiālo interešu labā, gūstot sev vai nodrošinot citiem nepienākošos labumus un nodarot kaitējumu LP;
- 26.11. **krāpšanas riski** attiecas uz maldinošas un negodīgas darbības iespējamību nodarīt finansiālu vai citu kaitējumu LP. Tas ietver informācijas sagrozīšanas, manipulācijas un ievainojamību izmantošanas iespēju, lai maldinātu citus un gūtu personisku vai finansiālu labumu;

- 26.12. **NILLTPF riski** ir saistīti ar noziedzīgi iegūtu līdzekļu legalizāciju un terorisma un proliferācijas (t.i., masveida iznīcināšanas ieroču izgatavošanas, glabāšanas, pārvietošanas, lietošanas vai izplatīšanas) finansēšanu;
- 26.13. **operacionālie riski** izriet no ikdienas operāciju izpildes un norāda uz iespēju ciest zaudējumus neefektīvu vai slikti izstrādātu iekšējo procesu, cilvēku kļūdu, normatīvu aktu pārkāpšanas, informācijas sistēmu kļūmju, datu noplūdes vai ārēju notikumu dēļ;
- 26.14. **projektu riski** ietver tos pašus riskus, kādi piemīt procesiem. Būtiska nozīme projektu risku identificēšanā ir izpratnei par plānoto periodu, izpildes termiņiem, budžetu, komunikāciju un pārējiem aspektiem, kas raksturo projekta tvērumu;
- 26.15. **reputācijas riski** rodas no iespējas LP ciest zaudējumus saistībā ar negatīva sabiedrības viedokļa izveidošanos par uzņēmumu, tā pakalpojumiem un klientu apkalpošanu;
- 26.16. **sankciju riski** rodas no apstākļiem, ka LP var tikt izmantots sankciju pārkāpšanā vai apiešanā;
- 26.17. **stratēģiskie riski** ir saistīti ar stratēģisko mērķu noteikšanu un īstenošanu, LP darbības nodrošināšanu vidējā termiņā un ilgtermiņā;
- 26.18. **uzņēmējdarbības riski** izriet no LP vadītāju lēmumiem par produktu un pakalpojumu attīstību un virzīšanu tirgū.
27. Risku vadības procesa uzraudzība un kontrole ir KRVD darbinieku īstenots aktivitāšu kopums, lai koordinētu un pārraudzītu risku vadības procesa pilnveidošanu un norisi LP.

VII. Risku apetīte un tolerance

28. LP darbība un mērķu sasniegšana ir saistīta ar riskiem un LP darbībā tiek apzināts, ka ne visus riskus ir iespējams mazināt un ka noteiktu risku tālāka mazināšana vai kontrole var būt nelietderīga.
29. Risku apetīti nosaka LP valde, saskaņojot to ar padomi, un pārskata ne retāk kā reizi gadā. Risku toleranču līmeņus nosaka Risku īpašnieki un Jomu atbildīgie, ņemot vērā Risku apetīti u.c. faktoros.
30. LP Risku apetītes un tolerances noteikšanā tiek izmantota vēsturiskā, aktuālā, kā arī sagaidāmā nākotnes informācija.
31. KRVD darbinieki sniedz metodoloģisku un informatīvu atbalstu LP valdei un padomei Risku apetītes un tolerances noteikšanā.
32. Risku īpašnieki un Jomu atbildīgie, kur tas ir iespējams, nosaka risku uzraudzības rādītājus. Riska rādītāja līmenim sasniedzot iepriekš noteikto augsto pakāpi jeb pārsniedzot Riska tolerances robežas, Riska īpašniekam vai Jomas atbildīgajam jābūt gatavam rīkoties pēc iepriekš pārdomātā scenārija (t.sk. Darbības nepārtrauktības plāna), lai nodrošinātu savas funkcijas vai procesa normālu darbību.
33. Ja potenciālais ieguvums pārsniedz iespējamus zaudējumus, Riska īpašniekam vai Jomas atbildīgajam ir jāpieņem risks tāds, kāds tas ir, neveicot tā samazināšanu.
34. RMP un kontroļu ieviešanai LP piemēro:
- 34.1. nulles Risku apetīti darba vides drošības riskiem, kas saistīti ar LP cilvēku dzīvību, korupcijas un interešu konflikta riskiem, krāpšanas, IKT drošības un sankciju riskiem;

- 34.2. minimālu Risku apetīti, pieļaujot nebūtiskas Riska vērtības, atbilstības/juridiskajiem riskiem, NILLTPF, ESG, IKT, reputācijas riskiem;
- 34.3. operacionālajam riskam Risku apetīte tiek noteikta iekšējos normatīvajos aktos;
- 34.4. pārējiem riskiem Risku apetīti nosaka LP valde saskaņā ar LP vidēja termiņa darbības stratēģiju.
35. Plānojot RMP un kontroļu pasākumus, LP struktūrvienības prioritāri mazina tos riskus, kurus LP valde un padome ir iekļāvusi Risku apetītes definīcijā.

VIII. Iekšējās kontroles sistēma

36. IKS ir būtiska risku vadības sastāvdaļa, to izstrādā, dokumentē un ievieš ar mērķi efektīvi samazināt riskus līdz Risku apetītei.
37. IKS izstrādā, ņemot vērā ārējo normatīvo aktu prasības, biznesa vajadzības un šo Politiku.
38. Īstenojot risku vadību, katram identificētajam riskam novērtē Riska varbūtību un Riska ietekmi, tādējādi nosakot Riska vērtību, un novērtē gan Sākotnējo risku, gan Atlikušo risku. IKS nenovērš visus riskus, bet nodrošina saprātīgu pārliecību, ka LP mērķi tiks sasniegti.
39. LP apzinās, ka nav iespējams pārvaldīt visus riskus: uzņēmuma rīcība ir neproduktīva, kad mērķu sasniegšanai paredzēti cilvēciskie, finanšu un laika resursi tiek iztērēti neatbilstošām vai pārmērīgām kontrolēm.
40. IKS ietver uzņēmējdarbības mērķu kategorijas, šo mērķu ieviešanas līmeņus un COSO modeļa elementus (skat. attēlu).



41. **Uzņēmējdarbības mērķu kategorijas** ir būtiskas tam, kā LP izveido un pārvalda savas iekšējās kontroles un risku vadības procesus:
- 41.1. **Stratēģiskie mērķi** – augsta līmeņa mērķi, kas atbilst LP misijai un vīzijai un palīdz radīt pievienoto vērtību.

- 41.2. **Operacionālie mērķi** attiecas uz LP darbības efektivitāti un resursu izmantošanas lietderību, tostarp snieguma mērķiem un aktīvu aizsardzību.
- 41.3. **Atskaitīšanās mērķi** koncentrējas uz iekšējās un ārējās ziņošanas uzticamību, ietverot gan finanšu, gan nefinanšu informāciju.
- 41.4. **Atbilstības mērķi** attiecas uz LP atbilstību piemērojamajām prasībām.
42. **Uzņēmējdarbības mērķu ieviešanas līmeņi** atbilst LP vidēja termiņa darbības stratēģijas mērķu kaskadēšanai un KPI sasniegšanai.
43. **IKS elementi:**
- 43.1. **Iekšējā vide**

Iekšējā vide ir IKS pamats. Tā ir organizācijas kultūra, vadības stils, ētikas principi, darbinieku kompetence un atbildība, izmantotās tehnoloģijas un resursi. Iekšējā vide veicina to, kā LP darbinieki uztver un risina riskus, tostarp risku pārvaldības filozofiju un Risku apetīti, integritāti un ētiskās vērtības, kā arī vidi, kurā tie darbojas. Efektīva kontroles vide novērš/ samazina riskus ikdienas procesos, t.sk. neidentificētos.

43.2. **Mērķu noteikšana**

Tā paredz, ka mērķiem jābūt noteiktiem pirms vadība sāk identificēt potenciālos risku notikumus, kas ietekmē mērķu sasniegšanu. Stratēģisko risku vadība nodrošina, ka LP ir ieviests process mērķu noteikšanai un ka izvēlētie mērķi atbalsta un atbilst LP misijai un ir saskaņā ar LP Risku apetīti. Tas nodrošina līdzsvaru, kad risks netiek pieņemts mazākā apjomā, nekā ir nepieciešams mērķu sasniegšanai, vai otrādi – pārāk lielā apjomā, pārsniedzot Risku apetīti. Analizējot stratēģisko mērķu sasniegšanas alternatīvas iespējas, vadība nosaka riskus, kas saistīti ar stratēģisko izvēli un izskata to iespējamās sekas.

43.3. **Notikumu identificēšana**

Tā nosaka, ka ir jāidentificē pagātnes un nākotnes iekšējie un ārējie apstākļi, faktori un Incidenti, kas ietekmē LP mērķu sasniegšanu, nošķirot riskus un iespējas. Draudi un iespējas tiek ņemtas vērā vadības stratēģijā un mērķu noteikšanas procesos. Lai noteiktu visus mērķu sasniegšanai nozīmīgus notikumus, to identificēšanai jānotiek neatkarīgi no notikumu realizācijas varbūtības un seku novērtējuma.

43.4. **Risku novērtēšana**

Risku novērtēšana nozīmē potenciālo nākotnes risku, kas var ietekmēt LP mērķu sasniegšanu, identificēšanu un novērtēšanu, pamatojoties uz pagātnes statistikas un rādītāju datiem, novērojumiem, kā arī uz apstākļu un faktoru attīstību. Riski tiek novērtēti gan esošajiem LP procesiem, pakalpojumiem un produktiem, gan uzsākot jaunu projektu, pakalpojumu, produktu vai kritiskās biznesa funkcijas sadarbības partnerību, gan pārtraucot kāda pakalpojuma sniegšanu.

Risku novērtēšanas process nodrošina apzinātā riska identifikāciju, novērtēšanu un analīzi, lai noteiktu piemērotu riska vadības stratēģiju. Viens no galvenajiem riska novērtējuma mērķiem ir informēt LP valdi un padomi par risku jomām, kurās jāveic atbilstoši pasākumi, un noteikt šo pasākumu mīļiedarbību, piešķiramos resursus, budžetu un ieviešanas prioritāti, pēc nepieciešamības veicot izmaiņas plānošanas dokumentos.

Riski tiek izskatīti attiecībā uz visu LP kā uzņēmumu, nodrošinot, ka struktūrvienību Atlikušo Risku portfeļa kopējais novērtējums nepārsniedz kopējo LP Atlikušā riska pieņemamo līmeni.

43.5. **Reaģēšana uz riskiem**

Novērtējot iespējamu **riska ietekmi** uz LP mērķu sasniegšanu un ieguldījumus RMP īstenošanai, riska vadībai izmanto vienu no stratēģijām:

Izvairīšanās	Pilnībā atsakoties no darbības, kas rada risku, šādi izvairoties no riska un tā rašanās cēloņiem (<i>avoidance</i>).
Pārņemšana	Pārnesot vai dalot risku ar trešajām pusēm, izmantojot apdrošināšanu vai ārpakalpojumu (<i>transfer</i>).
Samazināšana	Ieviešot IKS, šādi samazinot riska rašanās cēloņus vai sekas (<i>mitigation</i>).
Dalīšana	Dalot risku ar partneriem vai iesaistītajām pusēm, saglabājot LP kontroli pār risku (<i>sharing</i>).
Pieņemšana	Pieņemot risku bez papildu RMP un kontroļu ieviešanas, t.sk. gadījumos, kad draudi nav apzināti vai netiek vadīti (<i>acceptance</i>).

Novērtējot iespējamu **iespēju ietekmi** uz LP mērķu sasniegšanu, riska vadībai izvēlas citas stratēģijas:

Pieņemšana	Pasīvi pieņemot iespēju un cerot, ka tā notiks, t.sk. gadījumos, kad iespējas nav apzinātas vai netiek vadītas (<i>acceptance</i>).
Izmantošana	Nodrošinot, ka iespēja notiek un tiek pilnībā izmantota (<i>exploitation</i>).
Pastiprināšana	Aktīvi palielinot iespējas iestāšanās varbūtību vai tās pozitīvo ietekmi (<i>enhancement</i>).
Koplietošana	Dalot iespēju ar trešajām pusēm partnerības ietvaros, lai, ieguldot summētos resursus, maksimizētu ieguvumus (<i>sharing</i>).

43.6. Kontroles pasākumi

Kontroles pasākumi ir konkrēti procesu posmi un procedūras, kas paredzēti risku novēršanai vai mazināšanai (piemēram, politikas, noteikumu un instrukciju izstrāde un izpilde, amatu apraksti, pienākumu sadale, autorizācija sistēmās, piekļuves kontrole, limitu noteikšana, uzskaites pārbaudes, inventarizācijas, "četrus acu" principa ievērošana, atskaišu iesniegšana, dokumentu saskaņošana, līgumu noslēgšana, *back-up* ierakstu nodrošināšana, apdrošināšanas polišu iegāde), ietekmējot tā iestāšanās varbūtību vai ietekmi.

Kontroles pasākumi regulāri tiek pārskatīti kopā ar risku novērtējumiem, lai nodrošinātu, ka riska profils, laika gaitā mainoties riska apstākļiem, joprojām ir derīgs un kontroles ir efektīvas neatkarīgi no riska cēloņu spēka un pārmaiņām.

Lai nodrošinātu kontroles pasākumu efektivitāti, tiem jābūt:

- atbilstoši – pareiza kontrole pareizā vietā un proporcionāla attiecīgajam riskam;
- pastāvīgi īstentiem saskaņā ar plānu visā periodā – visiem iesaistītajiem darbiniekiem tās rūpīgi jāpilda;
- rentabliem, lai novērstu nelietderīgu naudas līdzekļu, laika un cilvēkresursu patēriņu – ieguldījumi RMP un kontrolēs nedrīkst pārsniegt potenciālos zaudējumus;

d) visaptverošiem, saprātīgiem un tieši saistītiem ar kontroles mērķiem.

Ieviešot kontroli, vispirms izstrādā **Kontroles dizainu**, kas ietver šādas darbības:

- a) riska identificēšana – saprast, kādi riski pastāv konkrētā procesā vai darbībā;
- b) kontroles mērķu noteikšana – definēt, ko kontrolei vajadzētu novērst, atklāt vai labot, ņemot vērā riska cēloņus;
- c) kontroles veida izvēle:
 - preventīvās kontroles (novērš kļūdas vai pārkāpumus pirms tie notiek);
 - reaktīvās vai detektīvās kontroles (atklāj kļūdas vai pārkāpumus pēc to notikšanas);
 - kompensējošās kontroles (aizvieto citas kontroles, ja tās nav iespējamas);
 - kārtējās kontroles (risku stāvokļa pārbaudei);
- d) kontroles izstrāde – izveidot konkrētus mehānismus, piemēram, apstiprināšanas procedūras, piekļuves ierobežojumus, pienākumu sadali, pārskatu pārbaudes u.c.;
- e) atbildības sadalījums – noteikt, kurš ir atbildīgs par kontroles īstenošanu un uzraudzību.

Kontroles operacionālais izpildījums nodrošina iecerētā Kontroles dizaina īstenošanu, ievērojot šādus principus:

- a) kontroles ievērošana – vai darbinieki faktiski veic noteiktās kontroles darbības (piemēram, informācijas pārbaudes, apstiprinājumus, dokumentēšanu);
- b) kontroles biežums – vai kontroles tiek veiktas ar paredzēto regularitāti (piemēram, katru dienu, mēnesi, pēc katra darījuma);
- c) dokumentācija un pierādījumi – vai ir pieejami pierādījumi, ka kontrole ir veikta (piemēram, izdrukāti dokumenti, parakstīti pārskati, ir pieejami sistēmas žurnāli);
- d) atbildība – vai ir skaidri noteikts, kurš ir atbildīgs par kontroles veikšanu;
- e) efektivitāte praksē – vai kontrole faktiski novērš vai atklāj kļūdas, pārkāpumus vai krāpšanu kā bija iecerēts.

43.7. Informācija un komunikācija

Informācijas aprite veicina efektīvu atskaišu, pārskatu un ziņojumu sagatavošanu, kas savukārt nodrošina vadībai iespēju saņemt savlaicīgu, pareizu un pilnīgu informāciju, kas ir svarīga lēmumu pieņemšanai par resursu pārdalīšanu un mērķu koriģēšanu. LP veicina komunikāciju par risku vadības jautājumiem, ņem vērā LP darbinieku atbildības jomas un līmeņus, kā arī nodrošina, ka netiek izpausta informācija par kontrolēm, kas varētu mazināt to efektivitāti, izņemot gadījumus, kad to nosaka ārējie normatīvie akti, vienošanās vai uzraugošo institūciju pieprasījumi.

Efektīva komunikācija nodrošina informācijas plūsmu visos virzienos – horizontāli un vertikāli starp LP darbiniekiem, valdi un padomi, klientiem un ārējām ieinteresētajām pusēm, tas nodrošina, ka visi darbinieki saprot savus pienākumus un saņem nepieciešamo informāciju. LP tiek ievēroti atklātuma un darbinieku iesaistes principi, kas motivē darbiniekus sniegt informāciju vadītājiem par Incidentiem un atklāt potenciālos riskus.

43.8. Uzraudzība

Uzraudzība ir pastāvīga risku vadības un kontroles sistēmas efektivitātes novērtēšana un uzlabošana. Tā ietver struktūrvienību vadītāju pašnovērtējumu par struktūrvienības darbībām, lai nodrošinātu atbildībā esošo procesu atbilstību risku vadības sistēmas, t.sk. IKS, prasībām.

Uzraudzībā ikdienā tiek izmantoti Riska uzraudzības rādītāji, periodiski tiek veikti iekšējie un ārējie auditi, lai atkarībā no kontroles kritiskuma un LP risku vadības funkcijas brieduma līmeņa veikt kontroles efektivitātes pārbaudi.

Risku īpašnieki un Jomu atbildīgie ziņo valdei par konstatētiem LP risku vadības un kontroļu trūkumiem un iespējām, kas var ietekmēt uzņēmuma spēju izstrādāt un īstenot tā stratēģiju, noteikt un sasniegt mērķus.

IX. Incidentu vadība

44. Incidentu vadība ir cieši saistīta ar darbības nepārtrauktības plānošanu, jo savlaicīga reakcija uz Incidentiem var būt izšķiroša pakalpojumu nodrošināšanas nepārtrauktībai.
45. Incidentu vadība ietilpst IKS un nodrošina LP spēju identificēt, reaģēt un mācīties no notikumiem, kas, riskam iestājoties, var radīt nevēlamu ietekmi uz darba resursu pieejamību, procesu norisi, sniegto pakalpojumu kvalitāti vai uzņēmuma reputāciju.
46. LP izstrādā un uztur Incidentu pārvaldības procedūras, kurās ietverta iekšējā un ārējā Incidentu ziņošana, Incidenta detalizēta reģistrēšana, Incidenta seku novērtšana, cēloņu analīze, kā arī nepieciešamo izmaiņu veikšana IKS ietvaros, lai nepieļautu nākotnē atkārtotu Incidentu rašanos. LP vadība aktīvi iesaistās Incidentu pārvaldībā, piešķirot nepieciešamos resursus, nosakot atbildības un pilnvaras, kā arī sekmējot kultūru, kurā Incidentu ziņošana tiek uzskatīta par normu, nevis izņēmumu.
47. Incidentu vadības cikls ietver galvenos posmus:

47.1. Identificēšana/Atklāšana

Identificēšanas laikā tiek konstatēts, ka ir noticis novirzes gadījums no sagaidāmā procesa vai rezultāta. Ir svarīgi savlaicīgi pamanīt pazīmes, kas liecina par iespējamu risku realizēšanos, kas var izpausties kā negaidīts šķērslis procesa norisē un/vai sistēmas traucējumi.

47.2. Reaģēšana un Apziņošana

Reaģēšana ietver tūlītēju rīcību, lai mazinātu jebkura riska iestāšanās sekas, kā arī neļaujot Incidentam turpināties un paplašināties, ko nodrošina procesā paredzētas reaktīvās kontroles vai iepriekš definēto rīcības plānu aktivizēšana gan struktūrvienības līmenī, gan visā LP kā Darbības nepārtrauktības plāna vai krīzes komunikācijas scenāriju īstenošana, ja ir pieņemts attiecīgs LP valdes lēmums.

Apziņošanas komunikācija ir atbilstoša Incidenta sekām, var notikt vienlaicīgi ar reaģēšanas posmu un ir nepieciešama, lai maksimāli ātri brīdinātu potenciāli iesaistītos kolēģus, klientus un/vai sadarbības partnerus par notikušo, ja Incidents var ietekmēt viņu intereses vai LP sniegto pakalpojumu kvalitāti.

47.3. Izmeklēšana

Izmeklēšanas posmā struktūrvienību vadītāji veic padziļinātu analīzi, lai noskaidrotu Incidenta cēloņus, apstākļus un sekas – tie var būt saistīti gan ar RMP un kontroļu dizaina vai izpildes trūkumiem, gan ar iepriekš neidentificētajiem vai nepārvaldītajiem riskiem.

47.4. Uzlabošana

Uzlabošanas posmā struktūrvienību vadītāji kopā ar attiecīgajiem Risku īpašniekiem veic izmaiņas procesos, RMP vai kontrolēs, IKT sistēmās un apmāca darbiniekus rīkoties tā, lai novērstu līdzīgu Incidentu atkārtosanos.