EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system work better for society.

Rokasgrāmata

Pārvaldības brieduma modelis

	Izstrādājis	*Ratificējis*	*Apstiprinājis*
Vārds, uzvārds	*S. D'ALBERTANSON*	*M. SCHITTEKATTE*	*C. CARR*
Amats	Projekta koordinators	Projekta vadītājs	Nodaļas vadītājs
Datums	29.06.2018.	29.06.2018.	29.06.2018.
Paraksts			

Dokumenta vēsture

Redakcija	*Datums*	*Piebildes*
1.0	29.06.2018.	Galīgā versija publicēšanai

Šis dokuments ir juridiski nesaistoša Eiropas Dzelzceļu aģentūras rokasgrāmata. Tas neskar lēmumu pieņemšanas procesus, ko paredz ar piemērojamiem ES tiesību aktiem. Turklāt ES tiesību aktu saistoša interpretācija ir tikai Eiropas Savienības Tiesas kompetencē.

120 Rue Marc Lefrancq | BP 20392 | FR-59307 *Valenciennes Cedex*
Tālr.: +33 (0)327 09 65 00 | era.europa.eu

1 Ievads

Pēc vienotā drošības sertifikāta vai drošības atļaujas piešķiršanas valsts drošības iestādes (VDI) pārrauga, vai tas, ko vienotā drošības sertifikāta vai drošības atļaujas pieteikuma iesniedzējs norādījis kā savu drošības pārvaldības sistēmu *(SMS)*, tiek faktiski īstenots un turpina atbilst juridiskajiem pienākumiem. Citiem vārdiem sakot, VDI ir jānodrošina dzelzceļa pārvadājumu uzņēmuma vai infrastruktūras pārvaldītāja darbību uzraudzības līmenis, lai nodrošinātu, ka pieteikumā vienotā drošības sertifikāta vai drošības atļaujas saņemšanai norādītais atspoguļo realitāti.

Eiropas Savienības Dzelzceļu aģentūra (turpmāk tekstā arī – "Aģentūra") ir izstrādājusi šo Pārvaldības brieduma modeli (PBM), lai palīdzētu VDI novērtēt dzelzceļa uzņēmumu un infrastruktūras pārvaldītāju *SMS* to uzraudzības laikā.

Pārvaldības brieduma modeļa izmantošana var arī būt kā "logs" uz organizācijas drošības kultūru un palīdzēt VDI un organizācijām, kas tās reglamentē, apspriežot jautājumu, kā šīs organizācijas var uzlabot savu *SMS*.

Aģentūra ir ieviesusi šo modeli kā vadlīnijas. VDI var to izmantot vai neizmantot pēc izvēles. Ja VDI ir savs modelis vai cits līdzeklis, kā novērtēt, cik laba ir kāda *SMS*, tad tā var izmantot savu metodi. Nekas šajā dokumentā neliek apšaubīt pastāvošos modeļus, ar ko sasniedz tādus pašus mērķus.

Jebkurš dzelzceļa pārvadājumu uzņēmums vai infrastruktūras pārvaldītājs var, ja to vēlas, jebkurā laikā brīvi izmantot Pārvaldības brieduma modeli savā organizācijā. Vadlīnijas un rīks, kas nepieciešams rezultātu radara kartes izveidei, ir brīvi pieejami un lejupielādējami no Aģentūras tīmekļa vietnes. Tīmekļa vietnē un pakalpojumos *Apple store* un *Google Play* ir pieejama arī lietotne, kas satur brieduma modeļa novērtēšanas rīku, kuru ir vieglāk izmantot faktu vākšanā uz vietas. Aģentūra ierosina, ka dzelzceļa pārvadājumu uzņēmums vai infrastruktūras pārvaldītājs visā piecu gadu periodā izmanto modeli, lai veiktu savu novērtējumu, pamatojoties uz pārraudzības darbību informāciju, un pārskata konstatējumus, atjaunojot pieteikumu vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. Patlaban to var izmantot, lai izceltu jebkuras vājās vietas *SMS*, kas dzelzceļa pārvadājumu uzņēmumam vai infrastruktūras pārvaldītājam varētu būt, un dotu viņiem iespēju novērst jebkādus trūkumus pirms pieteikuma iesniegšanas jauna vienotā drošības sertifikāta vai drošības atļaujas saņemšanai.

1.1 Rokasgrāmatas mērķis

Šis vadlīniju dokuments sniedz VDI vienkāršu modeli, kas ļaus tām novērtēt, cik labi dzelzceļa pārvadājumu uzņēmumi un infrastruktūras pārvaldītāju *SMS* darbojas.

Modeļa mērķis ir, izmantojot vienkāršus līmeņus un pamatojoties uz uzraudzības laikā gūtajiem pierādījumiem, klasificēt *SMS* sniegumu vai iespējas, lai varētu pamatoti precīzi novērtēt organizācijas *SMS* vai kādas tās daļas rādītājiem – atkarībā no tā, ko VDI nolemj pārbaudīt uzraudzības laikā.

Jānorāda, ka modelis tiek piemērots uzraudzības laikā un uzraudzība var notikt tikai tad, ja ir piešķirts vienotais drošības sertifikāts vai atļauja. Tādēļ modeļa atšķirīgie līmeņi sākas no brīža, kad organizācija vairs neatbilst minimālajām prasībām, kas nepieciešams vienota drošības sertifikāta vai atļaujas piešķiršanai. Ja organizācija nonāk 1. līmenī, VDI, kas veic uzraudzību, vajadzētu rīkoties, lai novērstu šo situāciju; ārkārtas gadījumos tas varētu ietvert vienotā drošības sertifikāta vai drošības atļaujas atsaukšanu vai lietas nodošanu drošības sertifikācijas iestādei izskatīšanai. Tas ir tāpēc, ka, darbojoties šādā līmenī, iesniegtais pieteikums atjaunot vienotu drošības sertifikātu vai drošības atļauju tiktu noraidīts.

1.2 Rokasgrāmatas adresāti

Šā dokumenta adresāti ir:

- *valsts drošības iestādes, novērtējot dzelzceļa uzņēmumu un infrastruktūras pārvaldītāju* SMS *to uzraudzības laikā;*
- *valsts drošības iestādes, izstrādājot savu uzraudzības stratēģiju un plānu(-s);*
- *valsts drošības iestādes, savā starpā daloties informācijā par drošības pārvaldības sistēmas rādītājiem attiecīgajā dalībvalstī, ja pastāv kopīga vai koordinēta uzraudzība;*
- *valsts drošības iestādes, daloties informācijā ar Aģentūru pēc tam, kad ir saņemts atjaunošanas vai precizēšanas pieteikums, ja Aģentūra ir atbildīga par vienotā drošības sertifikāta izdošanu; un*
- *dzelzceļa pārvadājumu uzņēmumi un infrastruktūras pārvaldītāji – kā pašnovērtējuma uzdevumu, lai novērtētu savu* SMS *sniegumu, jo īpaši pirms vienotā drošības sertifikāta vai drošības atļaujas atjaunošanas pieteikuma iesniegšanas vai pašuzraudzības ietvaros.*

1.3 Piemērošanas joma

Valsts drošības iestādēm praktiski jāizmanto līdzekļi *SMS* kvalitātes novērtēšanai atbilstoši teorijai, kas sniegta vienotā drošības sertifikāta vai drošības atļaujas (infrastruktūras pārvaldītāja gadījumā) pieteikuma iesniegšanas posmā. Aģentūras Pārvaldības brieduma modelis var apmierināt šo vajadzību, tomēr jebkura atsevišķa VDI var brīvi izstrādāt savu metodi, kā sniegt šādu pārraudzības informāciju Aģentūrai.

Šis modelis nav paredzēts kā galīgā atbilde uz jautājumu par to, cik laba ir jebkura atsevišķa *SMS*, bet drīzāk kā līdzeklis, lai nodrošinātu zināmu precizitāti un struktūru VDI vērtējumam par to.

1.4 Rokasgrāmatas struktūra

Šis dokuments ir to Aģentūras rokasgrāmatu krājuma daļa, kas paredzētas dzelzceļa pārvadājumu uzņēmumu, infrastruktūras pārvaldītāju, valstu drošības iestāžu un Aģentūras atbalstam, veicot savus pienākumus un uzdevumus saskaņā ar Direktīvu (ES) 2016/798.

1. attēls. Aģentūras rokasgrāmatu krājums

Aģentūras Pārvaldības brieduma modelis izmanto tādu pašu pamata struktūru kā Komisijas Deleģētās regulas (ES) 2018/762 I un II pielikums, lai izveidotu spriedumu par organizācijas *SMS* kvalitāti. Trīs prasību virsraksti nedaudz atšķiras, lai pielāgotos rīka lietotnes versijai, taču katras brieduma modeļa prasības nolūks ir tāds pats kā attiecīgajām *SMS* prasībām. Tas arī atbilst VDI vajadzībai pēc instrumenta, ko var izmantot, lai izpildītu prasības, kas noteiktas Komisijas Deleģētās regulas (ES) 2018/761 7. panta 1. punktā, lai novērtētu SMS efektivitāti, un tās pašas regulas 5. panta 2. punktā, lai novērtētu dzelzceļa pārvadājumu uzņēmuma vai infrastruktūras pārvaldītāja drošības pārvaldības sniegumu. Pieeja, ko paredz 5. panta 2. punkts, ir vērsta uz to, lai izveidotu ciešu saikni starp novērtēšanu un turpmāko uzraudzību, uzlabotu informācijas apmaiņu starp VDI un starp VDI un Aģentūru (t. i., starp tiem, kas veic uzraudzību, un tiem, kas veic novērtēšanu), un visbeidzot, ienes dzelzceļa nozarē vairāk skaidrības, lai saprastu, kā viņu pašu sniegtie drošības rādītāji informē VDI uzraudzību (piemēram, uzraudzības pasākumu prioritāšu noteikšana jomām, kurās ir vislielākais drošības risks).

Katrai modeļa daļai ir mērķis izskaidrot, par ko ir šī daļa, un dažos gadījumos arī dažas ievada piebildes, lai sniegtu papildu paskaidrojumus. Katrai daļai ir norādīti pieci līmeņi: nepietiekams – 1. līmenis, pamata – 2. līmenis, konsekvents – 3. līmenis, prognozēšana – 4. līmenis un izcilība – 5. līmenis. Katram no šiem līmeņiem ir teksts, kurā izskaidrots, kāda šajā līmenī ir veiktspēja salīdzinājumā ar kritērija elementu. Lietotājiem ir jānovērtē pierādījumi, ko viņi ir guvuši no intervijām, dokumentu pārskatīšanas u. tml., un jāizlemj, kuram konkrētam līmenim tie vislabāk atbilst. Sākot ar 2. līmeni, tekstā norādīts, ka sniegums jāizvērtē salīdzinājumā ar iepriekšējo līmeni un nākamo līmeni, tādēļ 4. līmenī ir ietverti 3. līmeņa elementi, kā arī papildu elementi 4. līmenim. Tas ir tāpēc, ka 2. līmenis ir pirmais līmenis, kurā sniegums tiek uzskatīts par juridiski atbilstošu.

Lai izveidotu līmeņus, salīdzinot ar katru prasību, un saņemtu rezultātu atspoguļojumu diagrammas veidā, lietotājam jāaizpilda modelim pievienotā *Excel* izklājlapa, kas ir pieejama Aģentūras tīmekļa vietnē, vai arī lietotājs var lejupielādēt Aģentūras *SMS* lietotni, kurā šī funkcija jau ir ietverta. Ievadot skaitļus izklājlapā vai lietotnē, aizpildīsies radara karte / zirnekļa diagramma, kuras piemērs ir parādīts 2. attēlā (skat. 3.2. sadaļu). Pēc pabeigšanas iegūto diagrammu var iekopēt ziņojumā dzelzceļa pārvadājumu uzņēmumam / infrastruktūras pārvaldītājam.

1. tabulā (skat. 3.2. sadaļu) ir parādīts cits veids, kā atspoguļot tos pašus datus vienkāršā tabulā, kas ļauj noteikt līmeņus, izmantojot luksoforu sistēmu. Arī to var aizpildīt pēc vajadzības un, kad tabula ir aizpildīta, iekopēt galīgajā ziņojumā dzelzceļa pārvadājumu uzņēmumam / infrastruktūras pārvaldītājam. Katra VDI (vai katrs dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs) var izvēlēties, vai izmantot vienu vai otru, vai abus rezultātu atspoguļošanas veidus.

1.5 Četri aspekti, kas jāzina pirms modeļa izmantošanas

Izmantojot šādu modeli, jāņem vērā četri norādījumi.

1) Tas ir jebkādas izskatāmās *SMS* daļas "momentuzņēmums".
2) Skaitlisko rādītāju līmenis ir mazāk svarīgs nekā vērtējums, ar ko pavēsta, cik labi *SMS* darbojas.
3) Tā kā atsevišķu SMS daļu revīziju/pārbaužu rezultāti varētu mainīties, *konstatējumus var izmantot kā rādītājus, lai sniegtu informāciju vispārējam spējas novērtējumam* par dzelzceļa pārvadājumu uzņēmuma vai infrastruktūras pārvaldītāja *SMS vidējo sniegumu.* Ja modeli piemēro labi apmācīts personāls, tas sniedz priekšstatu par atsevišķas *SMS* veiktspēju un tādējādi pievērš uzmanību to jomu uzlabošanai, kuras darbojas sliktāk. Valsts līmenī modeļa izmantojums arī sniegs VDI vispārēju priekšstatu par to, kur vērst ierobežotus resursus, lai uzlabotu drošību, jo tas varētu parādīt, piemēram, sistēmisku vājumu dzelzceļa nozarē vienā konkrētā drošības pārvaldības jomā. Piemēram, ja visi dzelzceļa uzņēmuma rezultāti liecina par zemu risku novērtējuma līmeni, tas varētu būt nozīmīgs ieguldījums VDI uzraudzības stratēģijas izstrādē.
4) attiecībā uz modeļa izmantošanu ir būtiski, ka, vienojoties par novērtējuma apjomu, gan VDI, gan novērtējamā organizācija ļoti skaidri norāda iejaukšanās apjomu un līmeni. Tas ir ļoti svarīgi, jo tas atspoguļos pārliecības līmeni, ko var piedēvēt VDI novērtējumiem.

Saturs

1 Ievads ... 2
1.1 Rokasgrāmatas mērķis ... 2
1.2 Rokasgrāmatas adresāti ... 3
1.3 Piemērošanas joma ... 3
1.4 Rokasgrāmatas struktūra ... 3
1.5 Četri aspekti, kas jāzina pirms modeļa izmantošanas ... 5
2 Pārvaldības brieduma modelis un riska kontrole ... 8
2.1 Kādu modelī sasniegto līmeni VDI uzskata par pieņemamu? ... 8
2.2 Modeļa piemērošana valstu drošības iestādēs ar atšķirīgām juridiskām pilnvarām ... 8
2.3 Ziņojumi ... 8
2.4 Priekšnoteikumi modeļa izmantošanai ... 9
2.5 Kā izmantot šo modeli? ... 9
3 Modeļa līmeņi ... 13
3.1 Sasniegumu līmeņu noteikšana ... 13
3.2 Ziņojumi par modeļa rezultātiem ... 14
4 Pārvaldības brieduma modelis ... 18
4.1 C – organizācijas konteksts ... 18
4.1.1 C1 – organizācijas konteksts ... 18
4.2 L – līderība ... 20
4.2.1 L1 – līderība un ieguldījums ... 20
4.2.2 L2 – drošības politika ... 23
4.2.3 L3 - Funkcijas, pienākumi un pilnvaras ... 24
4.2.4 L4 – apspriešanās ar personālu un citām pusēm ... 25
4.3 PL – plānošana ... 27
4.3.1 PL 1 – riska novērtējums ... 27
4.3.2 PL2 – drošības mērķi un plānošana ... 29
4.4 S – atbalsts ... 31
4.4.1 S1 – resursi ... 31
4.4.2 S2 – kompetence ... 32
4.4.3 S3 – informētība ... 34
4.4.4 S4 – Informācija un komunikācija ... 35
4.4.5 S5 – dokumentēta informācija ... 36
4.4.6 S6 – cilvēkfaktora un organizatorisko faktoru integrēšana ... 38
4.5 OP – ekspluatācija ... 40
4.5.1 OP1 – darbības plānošana un kontrole ... 40

4.5.2 OP 2 – aktīvu pārvaldība 42
4.5.3 OP3 – darbuzņēmēji, partneri un piegādātāji 44
4.5.4 OP4 – pārmaiņu pārvaldība 46
4.5.5 OP5 – ārkārtas situāciju pārvaldība 47
4.6 PE – darbības rādītāju novērtējums 49
4.6.1 PE1 – uzraudzība 49
4.6.2 PE2 – iekšējā revīzija 51
4.6.3 PE3 - pārvaldības pārskatīšana 52
4.7 I – uzlabošana 53
4.7.1 I1 – mācīšanās no negadījumiem un starpgadījumiem 53
4.7.2 I2 – pastāvīga uzlabošana 54
Pielikums – līmeņu definīcijas 57

2 Pārvaldības brieduma modelis un riska kontrole

SMS novērtējums darbojas kā pamats, lai novērtētu organizācijas spēju kontrolēt riskus, ko rada tās dzelzceļa darbības. Ja *SMS* darbojas labi, ir loģiski pieņemt, ka organizācijas darbības riski tiek labi kontrolēti. Ja organizācijas *SMS* ir vājās vietas, tas norāda uz to, ka riski šajās jomās netiek pienācīgi kontrolēti, un tādēļ ir iespējams, ka šajās jomās ir vislielākā iespēja rasties apstākļiem, kas ļauj notikt negadījumam vai starpgadījumam salīdzinājumā ar citām jomām, kur *SMS* darbojas labi. Tāpēc, jo augstāks ir PBM rādītājs, jo labāka ir riska kontrole.

2.1 Kādu modelī sasniegto līmeni VDI uzskata par pieņemamu?

Aplūkojot turpmāk redzamo modeli, var uzskatīt, ka, tiklīdz organizācija ir to sasniegusi (3. līmeni), tā parasti darbojas tā, lai panāktu, ka *SMS* nodrošina attiecīgu riska pārvaldības un kontroles līmeni. Tas, protams, ir līmenis, kas pārsniedz līmeni, kurā tiek panākta minimālā atbilstība tiesību aktiem (2. līmenis). Tam ir labs iemesls. Minimālās atbilstības tiesību aktiem ievērošanas līmenī pastāv risks noslīdēt līdz 1. līmenim, kas ir zemāks par to. Pret 3. līmeni, protams, zemāks būtu 2. līmenis, tādējādi pastāv zināms norobežojums no nepieņemama rādītāju līmeņa. Tomēr būtu nepareizi, ja organizācijas uzskatītu par to mērķi sasniegt 3. līmeni. Modeļa nolūks ir palīdzēt VDI diskusijā ar dzelzceļa pārvadājumu uzņēmumu vai infrastruktūras pārvaldītāju jomās, kurās viņu *SMS* ir vājas vietas un kur viņi var veikt **uzlabojumus**. Katrā ziņā no VDI viedokļa tai vajadzētu koncentrēt resursus uz vislielākā riska jomām: konstatējot, ka kāds dzelzceļa uzņēmums vai infrastruktūras pārvaldītājs darbojas augstākajos modeļa līmeņos, tā varētu nolemt uz laiku samazināt šīs organizācijas uzraudzību, salīdzinot ar dzelzceļa uzņēmumu vai infrastruktūras pārvaldītāju, kas darbojas zemākos līmeņos un kam ir nepieciešams uzlabojums. Tas var būt stimuls dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem mēģināt uzlabot savu *SMS*, lai viņi varētu sasniegt šo augstāko spektra galu. Ir arī vērts atzīmēt, ka, ņemot vērā dažu VDI pieredzi, kas izmanto šādus modeļus, dažādu līmeņu izmantošana rada konkurenci starp dzelzceļa pārvadājumu uzņēmumiem, mudinot panākt vislabāko sniegumu drošības pārvaldības jomā, un tas var palīdzēt veicināt drošības uzlabojumu dalībvalstī. Tas var arī ietekmēt viņu iespējas nākotnē iegūt jaunus līgumus atkarībā no uzņēmējdarbības iespējām, kas pieejamas atsevišķās dalībvalstīs.

2.2 Modeļa piemērošana valstu drošības iestādēs ar atšķirīgām juridiskām pilnvarām

Pašreizējais modelis ir paredzēts, lai palīdzētu VDI novērtēt dzelzceļa pārvadājumu uzņēmumu un infrastruktūras pārvaldītāju *SMS* saskaņā ar Dzelzceļa drošības direktīvu un ar to saistītajām regulām. Tomēr jāatzīmē arī tas, ka, ievērojot to, VDI darbojas arī atbilstoši pilnvarām, kas tām piešķirtas ar valsts tiesību aktiem. Tas nozīmē, ka, piemēram, dažām VDI ir pienākums nodrošināt, lai dzelzceļa pārvadājumu uzņēmumi un infrastruktūras pārvaldītāji savā dalībvalstī pienācīgi risinātu arodveselības jautājumus, bet dažām nav. Turpmāk sniegtajā modelī arodveselības jautājumi nav ietverti norāžu tekstā. Tomēr, ja VDI izvēlas piemērot šo modeli drošības un arodveselības jautājumos, turpmāk minētie pamatprincipi ir viegli piemērojami šiem elementiem.

2.3 Ziņojumi

Kad novērtējums ir veikts, var uzrakstīt ziņojumu, kurā apkopoti iegūtie rezultāti. Ziņojumā ir jāsniedz sīki dati par pierādījumiem, kuru dēļ nonāk pie atzinuma par konkrētu līmeni. Konstatējumus var uzrādīt vai nu kā radara karti / zirnekļa diagrammu, vai luksofora tabulu. Ziņojuma mērķis ir identificēt stiprās un vājās puses un nodrošināt pamatu diskusijai ar organizāciju par to, kuras jomas tā uzlabos vienotā drošības sertifikāta vai drošības atļaujas darbības laikā. Rakstot ziņojumu, novērtējuma dziļums būtu skaidri jānosaka sākumā, lai būtu izpratne par to, cik lielā mērā VDI ir izpētījusi *SMS* pasākumus noteiktā jomā.

2.4 Priekšnoteikumi modeļa izmantošanai

Visiem VDI darbiniekiem, kuri izmanto modeli, vajadzētu būt kompetentiem tā lietošanā. Izmantojot šo modeli, VDI darbiniekiem jāizprot *SMS* daļas, kā noteikts Drošības pārvaldības sistēmu kopīgo drošības metožu (KDM) I un II pielikumā attiecībā uz drošības pārvaldības sistēmām, kā arī pašu modeli. Darbiniekiem vajadzētu būt kompetentiem arī attiecīgās intervēšanas un pārbaudes metodēs un spējīgiem gūt dažādu informāciju no dažādiem avotiem un to izplatīt attiecīgajās *SMS* sadaļās. Praksē, ja iespējams, dokumentu pārskatīšana būtu jāveic pirms intervijām uz vietas. PBM ir paredzēts, lai to izmantotu viena kompetenta persona, tomēr, ņemot vērā loģistikas grūtības, kas rodas, veicot vairākas intervijas, un, lai sniegtu papildu pārliecību par konstatējumiem, laba prakse ir izmantot vairākas kompetentas personas, kuras var cita citu atbalstīt uzraudzības laikā.

2.5 Kā izmantot šo modeli?

PBM modelis neaizstāj uzraudzību veicošās personas spriedumu. Tas drīzāk ir atbalsts vērtējuma izdarīšanai, kas ļauj koncentrēt uzmanību un rast labāku saikni starp to, pierādījumiem, uz kuriem tas balstīts, un *SMS* elementiem. Tāpēc tas palīdzēs uzraudzītājiem sniegt savus konstatējumus dzelzceļa uzņēmumiem un infrastruktūras pārvaldītājiem, kā arī dzelzceļa uzņēmumiem un infrastruktūras pārvaldītājiem saprast, kāpēc šie konstatējumi ir radušies. Piemēram, ja intervijas, dokumentu pārskatīšana un faktu vākšana uz vietas liecina, ka organizācijai nav stingras dokumentu pārvaldības sistēmas, VDI, kas veic uzraudzību, to var atzīmēt kā *SMS* trūkumu, un pierādījumus tam var apspriest ar organizāciju un vienoties par korektīviem pasākumiem. Valsts drošības iestāde var arī izmantot organizācijas vadības dokumentu sistēmas trūkumus, lai uzsvērtu iekšējās revīzijas un uzraudzības problēmas, jo tām būtu jākonstatē šīs problēmas.

Dažādi modeļa virsraksti atbilst dažādām *SMS* daļām, kā izklāstīts Drošības pārvaldības sistēmas prasību KDM I un II pielikumā attiecībā uz Drošības pārvaldības sistēmas prasībām. Tas nozīmē, ka pastāv tieša saikne starp šo modeli, ko izmanto uzraudzībā, un VDI vai Aģentūras (kas darbojas kā drošības sertifikācijas iestāde) veikto novērtējumu pirms vienota drošības sertifikāta vai drošības atļaujas piešķiršanas. Tas arī nozīmē, ka ar rūpīgu un plānotu šā modeļa kā VDI veiktās uzraudzības dokumenta izmantošanu var nodrošināt pārbaudi, vai organizācijai, kurai piešķirts vienots drošības sertifikāts vai drošības atļauja, ir *SMS*, kas nodrošina to, kas apgalvots, iesniedzot pieteikumu vienotā drošības sertifikāta vai drošības atļaujas termiņa laikā. Tādējādi PBM rezultāts ir svarīga informācija organizācijai un drošības sertifikācijas iestādei, jo tas būs svarīgs pieteikumiem vienotā drošības sertifikāta vai drošības atļaujas atjaunošanai. Tāpat ir atzīmēts, ka atsevišķie *SMS* elementi, kas izklāstīti modelī, ir saistīti, veidojot vienotu veselumu. Tas nozīmē, ka, apsverot kopējos konstatējumus, VDI var izskatīt jautājumu par atsevišķu *SMS* elementu rādītājiem, turklāt var arī apsvērt, ko tas nozīmē tās kopējiem rādītājiem.

VDI var izmantot PBM uzreiz pēc tam, kad ir izsniegts vienotais drošības sertifikāts vai drošības atļauja, lai sniegtu pamata priekšstatu par drošības pārvaldības sistēmas veiktspēju vienotā drošības sertifikāta vai drošības atļaujas termiņa sākumā. Šajā posmā iegūtā informācija pēc tam var veidot pamatu plānotajai uzraudzībai attiecībā uz atlikušo vienotā drošības sertifikāta vai drošības atļaujas termiņu. Šī pieeja varētu būt piemērota, ja iesaistītajai organizācijai iepriekš bijis *SSC/SA*, un tādēļ tai ir zināma pieredze darbā ar savu *SMS*. Jaunam tirgus dalībniekam bez iepriekšējas *SMS* pieredze tūlītēja uzraudzība, izmantojot PBM, nevar sniegt daudz vairāk informācijas, kā tika uzzināts vērtēšanas posmā, jo *SMS* ir jauna un nav izmēģināta. Vai arī – tiklīdz tiek piešķirts vienotais drošības sertifikāts vai drošības atļauja – uzraudzības iestāde, izmantojot vērtētāju iesniegto informāciju par uzraudzību interesējošām jomām, var plānot PBM izmantošanu visā vienotā drošības sertifikāta vai drošības atļaujas darbības laikā, ņemot vērā, ka ir jānodrošina zināms laiks, lai organizācijas *SMS* tiktu izmēģināta praksē.

VDI ir ieteicams izmantot PBM rezultātus kā ieguldījumu tās uzraudzības stratēģijā (un līdz ar to uzraudzības plānos). Praksē tas varētu nozīmēt to, ka organizācijām vai organizāciju daļām, kurām ir augsts PBM līmenis,

tiek veltīta mazāka uzraudzība nekā tām, kam kopumā vai atsevišķās jomās tiek piešķirti zemāki līmeņi. Tomēr, lai gan šī pieeja ir iegūtās informācijas likumīga izmantošana, lai noteiktu riska prioritāti, tas jānosaka, salīdzinot ar kopējo operācijas relatīvo risku. Piemēram, kravu pārvadājumu uzņēmums, kas specializējas bīstamo kravu pārvadājumos, PBM var sasniegt 4. un 5. līmeni, un tādēļ varētu uzskatīt, ka tam ir ļoti izstrādāta *SMS*, bet tomēr joprojām būtu lietderīgi to rūpīgi uzraudzīt, ņemot vērā ar šo darbību saistīto risku raksturu.

Piešķirot līmeni kādam elementam, pamatojoties uz pierādījumiem, visticamāk, ka uzraudzība identificēs gan pozitīvās, gan negatīvās puses. Tādēļ ir jāpieņem lēmums par to, vai piešķirt augstāku vai zemāku līmeni. Ir jāpieņem lēmums par pieejamo pierādījumu līdzsvaru. Ja tas drīzāk ir augstāks, nevis zemāks līmenis, tas jāatspoguļo pieņemtajā lēmumā. Ja pierādījumi ir neskaidri, tad vai nu personai, kura veic uzraudzību, mērķtiecīgu pašreizējo un/vai turpmāko uzraudzības darbību laikā būtu jāiegūst vairāk pierādījumu (piemēram, realitātes pārbaudes / pārbaudes), lai iegūtu precīzāku vērtējumu, vai būtu jāizmanto zemāks līmenis, pamatojoties uz to, ka nav pierādījumu, lai atbalstītu augstāku. Kad notiek noslēguma sanāksme ar dzelzceļa uzņēmumu / infrastruktūras pārvaldītāju, grūtības lēmuma pieņemšanā vienmēr var tikt pārrunātas, un dzelzceļa pārvadājumu uzņēmumam / infrastruktūras pārvaldītājam dota iespēja sniegt papildu pierādījumus. Tomēr, to darot, būtu jāuzmanās, lai šāda rīcība nekļūtu par normu, bet gan būtu ārkārtas notikums, jo, atļaujot papildu pierādījumus, dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs šajā stadijā varētu sākt risināt jautājumus, nevis nodarboties ar tiem rīcības plāna ietvaros pēc uzraudzības darbības.

Uz jautājumu par to, cik daudz pierādījumu ir nepieciešams, lai sniegtu precīzu vērtējumu, ir grūti atbildēt. Pierādījumi būs interviju, dokumentāru pierādījumu, novērojumu uz vietas un starpgadījumu/negadījumu izmeklēšanas rezultātu kopums attiecīgajā laikā, datumos un atrašanās vietās vairumā gadījumu. Vērtējuma pamatā jābūt atrastajiem pierādījumiem. Tātad, ja dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs apgalvo, ka konstatētais nav reprezentatīvs, tas nemaina rezultātu, jo kas tika konstatēts, tas tika konstatēts. Tas, ka bija iespējams atklāt situāciju, kuru dzelzceļa uzņēmums / infrastruktūras pārvaldītājs neatzīst, norāda uz problēmām, kas saistītas ar *SMS* darbību, un ka dzelzceļa uzņēmums / infrastruktūras pārvaldītājs to apstrīd, arī ir signāls tam, ka viss nav tā, kā tam jābūt. Ja vairāki pierādījumi liecina par to, ka pārbaudāmā joma ir labi pārvaldīta, tad būtu likumīgi pārtraukt turpmāku pierādījumu meklēšanu šajā brīdī. Ja savukārt pierādījumi nenodrošina šo pārliecību, tomēr nav iespējams secināt, kāpēc tas tā ir, tad ir jāmeklē papildu pierādījumi. Nav nepieciešams pārbaudīt visus procesus un procedūras no augstākā līmeņa līdz sīki izstrādātajām darba instrukcijām, lai izdarītu secinājumus par to, vai sistēma darbojas efektīvi. Jāiegūst pietiekami daudz informācijas no dokumentu izskatīšanas un intervijām, lai gūtu pietiekamu pārliecību, kāda ir situācija praksē. . Jāatceras, ka noslēguma ziņojums, izmantojot PBM, ir ziņojums, ko sagatavojusi kompetenta persona, izmantojot modeli, lai pamatotu savu profesionālo spriedumu, un tas ir pamatots ar dokumentu paraugiem, intervijām un citu informāciju, kas, visticamāk, nevar būt absolūta aina, jo tas prasītu pārskatīt katru informācijas daļu, kas attiecas uz organizāciju, un intervēt ikvienu, kas tur strādā, un visas organizācijas, kas ar to saskaras.

Parasti tiek meklēti pierādījumi tam, ka pārbaudāmā joma: a) tiek droši pārvaldīta, b) šī pārvaldība ir saskaņota un saistīta ar veidu, kādā *SMS* ir paredzēts darboties saskaņā ar sākotnējo pieteikumu vienota drošības sertifikāta vai drošības atļaujas saņemšanai, un c) organizācija zina, kas notiek. Ja a) pastāv bez b) vai c), var teikt, ka drošību pārvalda veiksme, nevis saskaņots plāns, kas nepārprotami nozīmē nepilnīgu *SMS*.

Sniedzot atzinumus organizācijai, kas tika vērtēta, ļoti svarīgi ir skaidri parādīt, kāds ir novērtējuma līmenis. Ziņojumā ir jānorāda redzētie pierādījumi un intervētās personas. Ja atrodami nepilnīgu dokumentāciju piemēri, tie arī jāpievieno ziņojumam.

Ja modeli izmanto, lai novērtētu konkrētas *SMS* daļas, pētījuma apjomā ir skaidri jānorāda nevērtētās jomas, un gala ziņojumā tām nav jānorāda līmenis, ja vien no jomām, kas ir pētījuma apjomā, neizriet pietiekami pierādījumi to komentēšanai. Piemēram, veicot pētījumu par aktīvu pārvaldību, kļūst skaidrs, ka pastāv vāja

kompetenču pārvaldības sistēma. Šajā gadījumā ir likumīgi piešķirt līmeni šai jomai, lai gan tai nebija pievērsta galvenā uzmanība revīzijā, izmantojot modeli.

Personai vai personām, kuras veic uzraudzību, ir jāveic pietiekami daudz interviju / dokumentu pārskatīšanu / faktu vākšanu uz vietas, lai pārliecinātos, ka viņiem ir labs priekšstats par notiekošo. Ainai nav jābūt pilnīgai, tomēr ir jāapkopo pietiekami daudz pierādījumu, lai pamatotu dzelzceļa pārvadājumu uzņēmuma / infrastruktūras pārvaldītāja izvietojumu modelī. Maza dzelzceļa pārvadājumu uzņēmuma / infrastruktūras pārvaldītāja galveno vadošo darbinieku un nedaudzu atlasītu citu darbinieku intervēšana varētu būt pietiekama, lai noteiktu, piemēram, kāda ir situācija organizācijā attiecībā uz līderību. Attiecībā uz lielu dzelzceļa pārvadājumu uzņēmumu / infrastruktūras pārvaldītāju ar vairākām bāzēm un daudzpakāpju pārvaldības struktūru būs grūtāk iegūt šādu pilnīgu priekšstatu, un būs vairākas izvēles, ko intervēt augstākajā līmenī. Šādos apstākļos būtu pamatoti izskatīt organizāciju vertikālā griezumā, iespējams, ik gadu, katru reizi aplūkojot dažādas jomas un intervējot attiecīgu darbinieku skaitu katrā vadības līmenī, lai varētu veidot pārdomātu viedokli par aplūkojamo jomu.

Lielām organizācijām ar sarežģītu struktūru būtu lietderīgi izmantot modeli, lai gūtu vispārēju priekšstatu par organizācijas vadību, piemēram, izskatot augsta līmeņa dokumentus un intervējot augstākā līmeņa vadītājus pirms modeļa izmantošanas, lai izskatītu to darbības noteiktus aspektus, piemēram, transportlīdzekļu tehnisko apkopi vairākos objektos. Tādā gadījumā labi pārvaldītai organizācijai ar labu *SMS* būtu iespējams redzēt, ka augsta līmeņa skatījums/dokumentācija tiek atspoguļota vienā un tajā pašā veidā katrā tehniskās apkopes depo. Tas nenozīmē, ka starp pašiem depo nevar būt atšķirības vienkārši tādēļ, ka to galveno elementu kopējā struktūra ir vienāda un tos vada vienādi. Tāpat arī attiecībā uz organizāciju ar sliktiem darbības rādītājiem varētu sagaidīt atšķirības starp viedokli, kāds kopējai līderībai ir par to, kā organizācija darbojas tehniskās apkopes depo līmenī, kā arī būtiskas atšķirības starp pašiem depo, kas varētu izvērsties drošības riskā, piemēram, salīdzināmu transportlīdzekļu pārbaudes periodiskuma atšķirības bez paskaidrojuma, kāpēc tas tā ir, lai gan līderība vienlaikus atzīst tikai vienu šādu tehniskās apkopes struktūru.

Modelī esošā numerācijas sistēma ir paredzēta, lai palīdzētu kategorizēt pārvaldības briedumu. Noteikta rezultāta iegūšana nav jāuzskata par pašmērķi. Iepazīstinot ar konstatējumiem dzelzceļa pārvadājumu uzņēmumu / infrastruktūras pārvaldītāju, ir ļoti svarīgi pievērst uzmanību un uzsvērt to, ka rezultāts ir personas, kura izdara uzraudzību, vērtējums, pamatojoties uz pierādījumiem, kas redzami noteiktā laikā un vietā.

No dzelzceļa uzņēmumiem vai infrastruktūras pārvaldītājiem var sagaidīt iebildumus, apstrīdot "līmeni", un tādā gadījumā ir svarīgi uzsvērt, ka VDI viedoklis ir balstīts uz redzētajiem un uzklausītajiem pierādījumiem, un tiem ir tiesības uz citu viedokli, pamatojoties uz savām zināšanām par organizāciju. Ja dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs mēģina risināt šo jautājumu, sniedzot vairāk pierādījumu, būs jāizvēlas, vai pieņemt tos, kā iepriekš norādīts, un mainīt secinājumus, vai norādīt, ka konstatējumi ir tādi, kādi tajā laikā tika izdarīti. Visus pierādījumus, kas iesniegti pēc uzraudzības un sniedz labvēlīgāku viedokli, parasti vajadzētu iesniegt kā daļu no pierādījumiem, lai izpildītu rīcības plānu, par kuru vienojušās organizācija un VDI.

Noslēguma sanāksmē jāuzsver, ka uzdevuma mērķis ir palīdzēt dzelzceļa pārvadājumu uzņēmumam / infrastruktūras pārvaldītājam uzlabot tā *SMS*. Jāidentificē rīcības pasākumi, lai novērstu visus trūkumus, kas saistīti ar juridisko prasību izpildi, t. i., 1. līmeni, un uzlabošanas pasākumi, kas noteikti 2. līmenim un augstākam. Par tiem būtu jāvienojas ar dzelzceļa pārvadājumu uzņēmumu / infrastruktūras pārvaldītāju, un dzelzceļa pārvadājumu uzņēmumam / infrastruktūras pārvaldītājam vajadzētu apņemties izstrādāt termiņa ierobežotu rīcības plānu, norādot informāciju, kas par ko atbildēs un līdz kuram laikam jāveic šīs izmaiņas, lai VDI pēc nepieciešamības var to pārbaudīt.

Modelis ir paredzēts, lai palīdzētu veikt uzraudzību, nevis lai aizstātu profesionālu vērtējumu. Tas nepretendē uz to, ka precīzi atbild uz to, kas atklāts uzraudzības laikā, kā arī nenorāda, kas ar to ir jādara. Izmantojot modeli, VDI var izlemt par izpildes darbību, kas var sekot uzraudzībai, pamatojoties uz tai piešķirtajām

juridiskajām pilnvarām, tomēr noteikti izmantojot pierādījumus, kas atklāti PBM revīzijā. Lai palīdzētu VDI izlemt, kāda izpildes darbība varētu būt piemērota, Aģentūra ir izstrādājusi Izpildes pārvaldības modeļa rokasgrāmatu.

Šo modeli var arī izmantot, lai izskatītu negadījumu izmeklēšanas vai uzņēmumu revīzijas ziņojumu konstatējumus. Šajā gadījumā jāanalizē ziņojuma rezultāti, lai redzētu, ko tie liecina par *SMS*. Kad ir identificēts attiecīgais prasību elements, izmantojot modeli, var veikt organizācijas brieduma novērtējumu, pamatojoties uz konstatējumiem revīzijas vai negadījuma izmeklēšanas ziņojumā. Viens ziņojums varbūt neko daudz nepateiks par organizāciju drošības pārvaldības spējām, taču, ja to veic regulāri reizi gadā vai katru otro gadu, kad var pārbaudīt vairākus ziņojumus, tas var būt spēcīgs instruments, lai noteiktu tās jomas organizācijas *SMS*, kur joprojām rodas problēmas.

3 Modeļa līmeņi

Izmantotā struktūra ir skala no 1 līdz 5, kur “1” nozīmē pārvaldības sistēmas darbības zemus rādītājus un '5' attēlo lieliskus pārvaldības rādītājus.

3.1 Sasniegumu līmeņu noteikšana

1. līmenis – nepietiekams

Šajā līmenī organizācijai, kuru novērtē, ir drošības pārvaldības sistēma, taču ir skaidrs, ka pastāv trūkumi, kuru dēļ rādītāju līmenis ir zemāks par tiesību aktos noteikto minimumu, kas vajadzīgs, lai piešķirtu vienotu drošības sertifikātu vai drošības atļauju. Pastāv procedūras un norādījumi, lai pārvaldītu drošības pasākumus, bet uzraudzības laikā ir skaidrs, ka pastāv nopietnas problēmas to saskaņotībā kopumā. Atsevišķi riski tiek kontrolēti, tomēr kopējais process, kas to pārvalda, ir vājš. Organizācija praksē darbojas tādā veidā, ka, šķiet, pastāv būtiskas neatbilstības tam, kas aprakstīts *SMS*. Šķiet, ka politika, procedūras un instrukcijas tiek piemērotas tādā veidā, kas neatbilst *SMS* izklāstītajam veidam, un tāpēc organizācijas vai tās darbuzņēmēju veikto darbību riski netiek obligāti pietiekami kontrolēti. Šajā līmenī VDI ir jāapsver nepieciešamā rīcība, lai atjaunotu organizācijas atbilstību tiesību aktu prasībām (lai iegūtu detalizētu informāciju par to, kā šis process varētu darboties, skat. *Aģentūras rokasgrāmatu par Izpildes vadības modeli*).

2. līmenis – pamata

Šajā līmenī organizācija darbojas minimālas tiesību aktu atbilstības līmenī, t. i., *SMS* darbojas līmenī, kas bija pietiekams, lai novērtējuma posmā tiktu piešķirts vienots drošības sertifikāts vai drošības atļauja. Rakstveida drošības pārvaldības sistēma pastāv un tiek izmantota, lai kontrolētu drošības riskus, tomēr trūkst struktūras un koordinācijas. Sistēma kopumā ir saskaņota, tomēr dažādās jomās pastāv trūkumi, pieejas nesaskaņotība un nekonsekvence. Pamatā organizācija labi tiek galā ar saviem pienākumiem drošības jomā, bet ne vairāk. Daudz netrūkst, lai rastos būtiska problēma un tā atgrieztos 1. līmenī, jo procedūras un riska pārvaldības integrācijas trūkums var kļūt par nozīmīgu problēmu tehnisku, operatīvu un organizatorisku risku gadījumā. Dažas darbības jomas drošības pārvaldības ziņā darbojas labāk nekā citas. Riskus vairāk kontrolē ar organizācijā strādājošo indivīdu darbību, nevis *SMS* izmantošanu. Ugunsdrošības pieeja riska pārvaldībai ir ierasta parādība, kas rosina uzņēmumu reaģēt uz negadījumiem vai starpgadījumiem, nevis proaktīvi veikt pasākumus to profilaksei.

3. līmenis – konsekvents

SMS ir izstrādāta, lai izveidotu sistemātisku un konsekventu pieeju riska pārvaldībai. Visi elementi ir vietā un darbojas, un tiek ņemti vērā visi drošības aspekti. Zināma uzmanība tiek pievērsta drošības kultūras uzlabošanai organizācijā, izstrādājot drošības kultūras uzlabošanas stratēģiju. Kaut arī organizācija ir konsekventa, tā nemēģina iepriekš prognozēt riskus, kā arī kultūra tajā nav pietiekami attīstīta riska pārvaldības procesa nodrošināšanai. Ugunsdrošības pasākumi ir snieguši pamatu pārdomātākai riska pārvaldības pieejai, tomēr daudz netrūkst (piemēram, nespēja pārvaldīt galvenos procesus vai procedūras laika gaitā), lai organizācija atgrieztos pamata darbību režīmā.

4. līmenis – prognozēšana

Tas ir tāds pats kā 3. līmenis, un papildus tam *SMS* pastāvīgi pārvalda riskus proaktīvi. Šeit organizācija uzrauga riska prekursorus un pēc iespējas rīkojas, lai novērstu bīstamus negadījumus. Organizācija ir apņēmusies attīstīt drošības kultūru, darbinieki ir iesaistīti darbībā, pārvaldot drošību saskaņotā un tālredzīgā veidā. Šajā līmenī pastāv organizācijas augstākā līmeņa vadības patiesa līderība, un tās darbinieki tic tai un ievēro vadības pieeju. Daudz pūļu tiek veltīts regulārai rādītāju pārskatīšanai un centieniem izprast tos riskus, ar kuriem organizācija saskaras, to raksturu un ko šajā jomā var darīt.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam drošības pārvaldības rakstveida sistēma ir veidota tā, lai to varētu pastāvīgi uzlabot. Organizācija aktīvi meklē iespējas uzlabot drošību un pilnveidot savu drošības kultūru, izmantojot informāciju, kas pieejama gan dzelzceļa nozarē, gan ārpus tās. Organizācija salīdzina savus rādītājus ar citiem gan dzelzceļa nozarē, gan ārpus tās. Pastāv pierādījumi, ka organizācija apzinās problēmas, kas tai ir vai var būt nākotnē, un aktīvi cenšas tās risināt, izmantojot *SMS*. Šajā līmenī organizācija ir pārliecināta par tās spēju pārvaldīt riskus, ar kuriem tā saskaras, un cenšas arī ārpus tās izglītot tos, ar kuriem tai mijiedarbība, un papildus tiecas mācīties no citu jomu pieredzes, ko var iekļaut savā darbībā. Drošība ir organizācijas darbības neatņemama daļa.

3.2 Ziņojumi par modeļa rezultātiem

Modeļa rezultātus var parādīt kā radara karti vai kā luksofora sistēmu. Radara karte, **Error! Reference source not found.** un 1 tabula. turpmāk parāda *SMS* prasības, ko izvirza Komisijas Deleģētā regula (ES) 2018/762 pieciem veiktspējas līmeņiem, ievietojot attiecīgo veiktspējas līmeni, lai iegūtu izteikti vizuālu priekšstatu par organizācijas drošības sniegumu.

2. attēls.: Radara kartes / zirnekļa diagrammas piemērs modeļa rezultātu atspoguļošanai.

Radara karti var izveidot, izmantojot Aģentūras mobilo lietotni *ERA SMS*, kas ir pieejama pakalpojumos *Apple store* un *Google Play* vai noklikšķinot uz saites Aģentūras tīmekļa vietnē. Tās vietā var izmantot arī *Excel* izklājlapu, kas ir pieejama Aģentūras tīmekļa vietnē.

1 tabula. Luksofora sistēma pa līmeņiem

Drošības pārvaldības sistēmas PDCA elementi	*1. līmenis*	*2. līmenis*	*3. līmenis*	*4. līmenis*	*5. līmenis*
Organizācijas situācija					
Līderība					
Līderība un ieguldījums					
Drošības politika					
Funkcijas, pienākumi un pilnvaras					
Apspriešanās ar personālu un citām pusēm					
Plānošana					
Riska novērtējums					
Drošības mērķi un plānošana					
Atbalsts					
Resursi					
Apzināšanās					
Informācija un komunikācija					
Dokumentēta informācija					
Cilvēkfaktora un organizatorisko faktoru integrācija					
Darbības					
Darbību plānošana un kontrole					
Aktīvu pārvaldība					
Darbuzņēmēji, partneri un piegādātāji					
Pārmaiņu pārvaldība					
Ārkārtas situāciju pārvaldība					
Veiktspējas izvērtēšana					
Uzraudzība					
Iekšējā revīzija					

1 tabula. Luksofora sistēma pa līmeņiem

Drošības pārvaldības sistēmas PDCA elementi	*1. līmenis*	*2. līmenis*	*3. līmenis*	*4. līmenis*	*5. līmenis*
Pārvaldības pārskatīšana					
Uzlabošana					
Mācīšanās no negadījumiem un starpgadījumiem					
Pastāvīga uzlabošana					

Tomēr jāsaprot, ka robežas starp dažādiem līmeņiem tiek definētas pārejā no 1. līmeņa uz 2. līmeni, jo 1. līmenis nav minimālās tiesību aktu atbilstības līmenis, bet 2. līmenis ir. Tomēr pārejai no dzeltenas krāsas uz zaļu, pārejot no 2. līmeņa uz 3. līmeni, ir daudz neskaidrāka robeža, jo organizācija ir juridiski atbilstoša, tomēr uzlabo savas *SMS* kvalitāti un sniegumu.

Lai izmantotu šo modeli, uzraudzītajai organizācijai ir jābūt drošības sertifikātam, jouzraudzība var notikt vienīgi pēc sertifikāta piešķiršanas. Tas, ko ar modeli cenšas panākt, ir palīdzēt personai, kura veic uzraudzību, novērtēt, cik labi praksē darbojas drošības pārvaldības sistēma. Uzskata, ka 1. līmenis ir zemāks par minimālo atbilstību tiesību aktiem, un tādēļ to uzskata par līmeni, kurā ir vajadzīgi uzlabojumi, lai izvairītos no VDI sankciju piemērošanas par to nosacījumu neizpildi, saskaņā ar kuriem tika piešķirts vienotais drošības sertifikāts vai drošības atļauja.

Sākot ar 2. līmeni (no minimālās tiesību aktu atbilstības līmeņa uz augstāku līmeni), notiek attīstība no viena līmeņa uz otru. Šā iemesla dēļ nākamajā sadaļā 2. līmeni neuzskata par kumulatīvu, savukārt no 3. līmeņa līdz 5. līmenim – to uzskata par kumulatīvu, t. i., sasniedzot 2. līmeni, organizācija atbilst juridiskajām pamatprasībām. Nonākot 3. līmenī organizācija ir sasniegusi pieņemamu un konsekventu drošības pārvaldības sistēmas līmeni, spēj to saglabāt laika gaitā un var balstīties uz to, lai sasniegtu augstākos līmeņus. Izmantojot luksofora sistēmu, kopumā var viegli redzēt, ka 1. līmenis (sarkanā krāsa) atbilst sliktam sniegumam, 2. līmenis (dzeltenā krāsa) ir pietiekams un sniegums kļūst konsekvents līdz izcils, pārvietojoties uz 3., 4. un 5. līmenī (zaļā krāsa).

Pielikumā parādīta piecu līmeņu sistēma, kas skaidrības labad salīdzināta ar luksoforu un iekļauj vispārīgus apgalvojumus, kas norāda, kāds ir katrs līmenis praktiski. Ar bultiņa zem tabulas atgādina, ka robežas starp līmeņiem nav fiksētas:

- **zaļš**, ja pakāpe ir vienāda ar 3., 4. un 5. līmeni, un rādītājus uzskata par konsekventiem, prognozējošiem vai izciliem;
- **dzeltens** 2. līmenim, kur rādītājus uzskata par pamata;
- **sarkans** 1. līmenim, kur rādītājus uzskata par nepietiekamiem.

4 Pārvaldības brieduma modelis

4.1 C – organizācijas konteksts

Mērķis

Lai iegūtu vienotu drošības sertifikātu vai drošības atļauju, pieteikuma iesniedzējam jāapraksta savas darbības veids, apjoms un joma, jāparāda, kā tas nosaka nopietnus riskus, ar kuriem saskaras, jāidentificē "iesaistītās puses", jānorāda, kā tas pilda juridiskos drošības pienākumus un kādi tie ir, kā arī jāpaskaidro *SMS* joma. Šīs prasības mērķis ir noteikt vērtētāja darbības jomu un apjomu. Attiecībā uz uzraudzību būs svarīgi pārbaudīt, vai pieteikuma iesniedzēja sniegtās garantijas šajā jomā, piemēram, izpratne par risku un kā tas tiek novērsts ar *SMS*, tiek atspoguļotas reālajā ikdienas darbībā.

Ievada piebildes

Ir ļoti svarīgi, ka organizācija spēj paziņot uzraudzības iestādei savas darbības pareizo veidu, apjomu un jomu. Tas ir saistīts ar darbības robežu noteikšanu ar šiem elementiem, un tie ir jāatspoguļo organizācijas *SMS*. Šā iemesla dēļ šis elements ir pirmais starp lēmumu pieņemšanas kritērijiem, jo ar to nosaka visu, kas notiek pēc tam. Tāpēc attiecībā uz uzraudzību ir ļoti svarīgi, ka darbības realitāte precīzi atspoguļo novērtēšanas laikā paziņoto stāvokli, jo, ja tā nenotiek, tas nozīmē, ka novērtēšana veikta, izmantojot nepilnīgu informāciju. Skaidrojums par organizācijas vispārējo kontekstu var arī liecināt, kā tiek pārvaldīts cilvēkfaktors un organizatoriskie faktori.

Pastāv procedūras un norādījumi, lai pārvaldītu drošības pasākumus, bet uzraudzības laikā kļūst skaidrs, ka pastāv nopietnas problēmas to saskaņotībā kopumā. Tas palīdz noteikt organizācijas kontekstu un parāda vērtējošajai iestādei organizācijas izpratni par vidi, kurā tā darbojas. Citu pušu, kas nav dzelzceļu sistēmas daļa, rīcība var arī ietekmēt darbību drošību, un tāpēc tā arī jāņem vērā riska novērtējumā.

4.1.1 C1 – organizācijas konteksts

1. līmenis – nepietiekams

Šajā līmenī pastāv pamata apraksti, un darbības veids, apjoms, joma un/vai raksturs ir pietiekami skaidri, tomēr praksē ir vērojamas atšķirības starp SMS *jomu un novērtējumu, kā arī pastāv šaubas, vai visi nopietnie riski ir pienācīgi reģistrēti. Pastāv šaubas, ka organizācija efektīvi ievēro visas tiesību normas, kā tā apgalvo. Šķiet, ka ne visas iesaistītās puses ir pienācīgi atspoguļotas SMS pasākumos.*

2. līmenis – pamata

Šajā līmenī pastāv visi apraksti, tomēr ir bažas, ka darbības joma un apjoms nav pienācīgi aprakstīti. Ir apzinātas tiesiskās un citas prasības, kas ietekmē iesaistītās puses, tomēr šajā jomā ir sarežģījumi. Ir konstatētas dažas iesaistītās puses, kas nav iekļautas sākotnēji iesniegtajā SMS*, un pastāv pierādījumi, ka dažkārt nopietni riski netiek pienācīgi kontrolēti, kas attiecīgi ietekmē* SMS *efektivitāti.*

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam šajā līmenī darbības, SMS *un sastopamo nopietno risku apraksts atbilst praksē redzamajam. Organizācija skaidri apzinās, ko dara, un zina virzienu, kurā virzās. Pastāv skaidrs priekšstats par to, kuri tiesību akti ir piemērojami un kas ir iesaistītās puses.*

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam organizācija cenšas attīstīties un iemācīties labāk prezentēt sevi iesaistītajām pusēm, kā arī sadarboties ar tām, lai izstrādātu drošākas procedūras un procesus SMS *ietvaros. Tā vietā, lai tikai uzskaitītu tiesību aktus, kas jāievēro, organizācija aktīvi cenšas sadarboties ar attiecīgajām*

regulatīvajām iestādēm, lai izstrādātu stratēģijas tiesisko prasību ievērošanai. Robežas ar citām darbības daļām ir skaidri saprastas un tiek pārvaldītas.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam organizācija ir paraugs citām organizācijām attiecībā uz sevis prezentēšanu. Organizācijai ir skaidrs tās raksturs un juridiskie pienākumi, kā arī tā cenšas attīsties, pamatojoties uz savām stiprajām pusēm un izmantojot pieredzi, kas iegūta ne tikai dzelzceļa nozarē, bet arī ārpus tās.

4.2 L – līderība

Mērķis

Nodrošināt, ka organizācija tiek efektīvi pārvaldīta un vadīta.

Nodrošināt, ka drošības politika skaidri pauž augstākā līmeņa vadības ieceres, precīzi definējot, ko organizācija vēlas sasniegt, kā to panāks (ar līderības demonstrētajām darbībām) un kā vadība uzzinās par šīs ieceres sasniegšanu. Efektīvu līderību var uzskatīt par tādu, kas nosaka virzienu, organizāciju, resursus un spēju ieviest atbilstošu kultūru uzņēmējdarbībā vēlamo mērķu sasniegšanai. Vadībai ir efektīvi jāvada darbība, lai konkurējošās prioritātes neietekmētu drošības mērķus. Vadībai ir skaidri jānorāda darbiniekiem, kādi ir drošības mērķi un kā tie tiks sasniegti.

Nodrošināt, ka organizācija (īpaši valde) efektīvi nosaka, vai drošības politika un ar to saistītā darbība ir atbilstošas, ieviestas un efektīvas. Pārliecināties, ka paziņojumi ir konsekventi, skaidri un sagatavoti tā, lai radītu labāko vidi drošības pārvaldībai.

Ievada piebildes

Vāja līderība ir izraisījusi daudzas ievērojamas drošības kļūmes. Organizācijas pieeja drošībai bieži vien atspoguļo to darbinieku attieksmi, kuri pieņem ar darbību saistītus lēmumus, un tā nosaka organizācijā strādājošā personāla viedokļus un attieksmi.

Augstākā līmeņa vadības noteiktā vispārējā politika, saistītās procedūras un izrietošā drošības gaisotne ir ļoti svarīgas, lai noteiktu un saglabātu organizācijas pieeju drošībai. Ar politiku vajadzētu sniegt skaidru izpratni par to, kā organizācija paredz pārvaldīt drošību. Augstākā līmeņa vadībai un citiem vadītājiem ir arī jārāda piemērs un jārīkojas tā, lai pastiprinātu politikā ietvertos paziņojumus. Dzelzceļa drošības pasākumi ir integrēti darbībā.

4.2.1 L1 – līderība un ieguldījums

Līderība un ieguldījums attiecas uz organizācijas augstāko vadību, kas nosaka virzienu un pozitīvu, uz nākotni vērstu darba kārtību saviem darbiniekiem risku pārvaldībai visos darbības procesos. Augstākā vadība nosaka toni un kultūru uzvedībai organizācijā, kā arī tiem, kas ar to ir mijiedarbojas. Tiem darbiniekiem, kuri ieņem vadošus amatus, ir vislielākā ietekme uz organizācijas kultūru, organizācijas struktūru un tās efektīvu vadību. Tāpēc ir būtiski, ka viņi var darīt zināmus savus uzskatus tiem, kuri strādā organizācijas labā. Novērtējot šo jomu uzraudzības laikā, VDI darbiniekiem, ja iespējams, ir jāizvērtē, vai starp drošības pārvaldību un citiem darbības procesiem nav pretrunīgu prioritāšu.

1. līmenis – nepietiekams

Procedūras un drošības mērķi ir novecojuši vai nav paziņoti organizācijā, un ir maz pierādījumu par to izpratni.

Nav pierādījumu par apspriedēm ar darbiniekiem par drošības jautājumiem, un darbiniekiem nav saiknes ar vadību.

Drošības pārvaldības sistēma pastāv ļoti vienkāršotā līmenī (piemēram, lai gan cilvēkfaktoru ņem vērā, šim nolūkam lietotā sistēma ir vāja), un tā ir nodalīta no organizācijas ikdienas darbības.

Nav daudz pierādījumu vadības ķēdes interesei par drošības jautājumiem, jo ikdienas darbs ir svarīgāks. Ir grūti atrast resursus riska pārvaldības jautājumu risināšanai, jo organizācija nenovērtē, cik svarīgi ir tos izmantot šim nolūkam.

Nozīme, kāda cilvēkiem ir drošas, efektīvas un kvalitatīvas darbības nodrošināšanā, ir maz atzīta.

Trūkst vadības ieguldījuma drošības kultūrā, un organizācijā ir maz zināšanu par drošības kultūru un kāpēc tā ir svarīga, lai panāktu drošu un efektīvu organizācijas darbību. Drošība tiek uztverta atsevišķi no organizācijas

darbības mērķiem un tiek definēta, pamatojoties uz atbilstību noteikumiem un tehniskajiem vai procesuālajiem risinājumiem. Drošību pārvalda un vada atsevišķa drošības nodaļa, ko uzskata par galveno atbildīgo par organizācijas drošības kultūru. Vadības ieguldījums drošības mērķos un prioritātēs, kā arī ziņošana par to notiek tik ierobežoti, ka organizācijā par to nekā nezina. Drošību uzskata par kaut darāmu, nevis par labumu organizācijai. Pozitīvas drošības kultūras īstenošanā ir maz līderības.

Attiecībā uz starpgadījumiem un negadījumiem dominē fatālistiska kultūra, ka tie tāpat notiks. Kritiskā situācijā par iemeslu vienmēr atzīst cilvēka kļūdu, nemēģinot veikt turpmāko izmeklēšanu. Taisnīguma kultūra nepastāv, un starpgadījumos un negadījumos iesaistītos darbiniekus padara par grēkāžiem. Vadība un darbinieki parasti nav ieinteresēti drošībā un var izmantot drošību vienīgi kā pamatu citiem argumentiem, piemēram, darba samaksai, darbalaikam u. tml.

Darbības rādītāji ir zemāki par minimālajām prasībām atbilstībai tiesību aktiem, un tāpēc VDI ir jāapsver, kā uzlabot organizācijas rādītājus līdz noteiktajam minimālajam līmenim.

2. līmenis – pamata

Nepastāv saikne starp procesiem, kas saistīti ar drošību, un darbības procesiem.

Augstākā vadība nodrošina resursus, tomēr ar tiem nepietiek, lai izpildītu apņemšanos veikt pozitīvu ieguldījumu organizācijas drošībā un kultūrā.

Līderību atzīst par nozīmīgu drošības pārvaldībā, tomēr tās atspoguļojums SMS *šķiet nedaudz pretrunīgs un neskaidrs.*

Drošību uzskata par darbības risku, kas var nelabvēlīgi ietekmēt organizācijas finansiālos mērķus. Drošību definē, pamatojoties uz atbilstību noteikumiem un tehniskajiem vai procesuālajiem risinājumiem. Vispārējā pieeja drošībai ir stihiska no augstākā līmeņa vadības līdz zemākajam līmenim. Vadības ieguldījums ir uzskatāms par negribīgu, reaģējot, kad kaut kas nav izdevies, nevis, lai veiktu aktīvus pasākumus situācijas uzlabošanai.

Augstākā vadība ir apstiprinājusi cilvēkfaktora un organizatorisko faktoru stratēģiju, un to reizēm pārskata. Taču tas tiek darīts, lai ievērotu tiesību aktus, nevis tāpēc, ka būtu aptverts, cik svarīgi ir pārvaldīt cilvēkfaktoru un organizatoriskos faktorus, lai uzturētu un pilnveidotu uzņēmuma darbības rādītājus. Tāpēc resursi un cits atbalsts, kas vajadzīgi, lai īstenotu stratēģiju, faktiski nav pieejami.

Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienota drošības sertifikāta vai drošības atļaujas piešķiršanai.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam darbiniekus aktīvi iesaista drošības politikas un drošības mērķu pārskatīšanā un pārstrādāšanā, kā arī to piemērošanā.

Novērojams pozitīvas drošības kultūras attīstības sākums. Izstrādājot organizācijas darbības procesus, sāk sistemātiski izmantot zināšanas par cilvēkfaktoru un organizatoriskajiem faktoriem un ar tiem saistītās metodes. Vadība izmanto konsekventu un lielākoties pozitīvu pieeju diskusijās par resursiem, kas nepieciešami ar cilvēkfaktoru un organizatoriskajiem faktoriem saistīto jautājumu risināšanai, un to nodrošināšanai.

Vadība uzskata, ka drošība ir svarīga, tomēr dažreiz ikdienas darbs kļūst par prioritāti. Drošības pamatprincipi ir izstrādāti, un organizācija pievēršas aktīvai profilakses perspektīvai, nevis atbilstībai tiesību normām. Organizācija apzinās, ka turpmāko uzlabojumu veikšanai ir svarīga visu darbinieku iesaistīšana, un vairākums darbinieku vēlas sniegt pozitīvu ieguldījumu. Lielākā daļa darbinieku uzņemas personisku atbildību par savu drošību. Drošību veicina kampaņas un uzraudzības kontrole, galvenokārt no augstākā līmeņa lejup, tomēr ar darbinieku iesaistīšanu.

Drošības pārvaldības sistēma ir konsekventa, kontrolējot lielāko daļu risku, kam ir pakļauta organizācija.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam drošības mērķus atbalsta ikviena vadības ķēdes darbinieka rīcība.

Ir veikts ieguldījums pastāvīgā riska kontroles produktivitātes un efektivitātes uzlabošanā. Pastāv pierādījumi plašai sadarbībai visā vadības ķēdē. Pastāv pierādījumi, ka, analizējot darbības risku, tiek ņemti vērā drošības riski.

Politika augstākajā līmenī ir šāda:

- *pārskatīta un pārstrādāta, lai panāktu uzlabojumus paredzamā veidā; un*
- *vienādi interpretēta visās organizācijas daļās, kas to piemēro.*

Uz āru un uz uzlabojumiem vērsta, organizācijas kultūra kopumā ir pozitīva, un atsevišķās jomās darbiniekiem ir iespējas dot proaktīvu ieguldījumu drošības pārvaldības sistēmas izstrādē.

Ir pieejami resursi drošības pārvaldībai, tomēr pastāv daži maznozīmīgi ierobežojumi.

Vadība saprot, ka drošība un produktivitāte ir savstarpēji saistītas, un šaubu gadījumā drošībai ir pirmā prioritāte. Vadība rūpējas par drošību un piešķir ievērojamus resursus aktīviem drošības pasākumiem, piemēram, riska novērtēšanai, starpgadījumu un negadījumu izmeklēšanai, kā arī pārmaiņu procesu pārvaldībai. Visā organizācijā atzīst drošības svarīgumu un darbiniekus pozitīvi iesaista drošības iniciatīvās. Drošības rezultāti balstās uz apsteidzošajiem un atpaliekošajiem rādītājiem, izmantojot visus pieejamos datus.

Ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītie jautājumi ir integrēti visās organizācijas darbībās, un augstākā vadība to atbalsta.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam drošības politikā ietver korporatīvās drošības mērķus, kam organizācijā ir kaskādes princips. Pastāv pietiekamu cilvēkresursu, ekonomisko un tehnisko resursu piešķiršanas procedūras, lai atbalstītu šo mērķu sasniegšanu, un augstākā vadība uzrauga nepieciešamo drošības prasību īstenošanu. Drošības politikas efektivitāti novērtē, un rezultātus ņem vērā nākamajā pārskatīšanā. Drošības mērķus izmanto, lai panāktu, ka organizācija sasniedz darbības rādītājus un pārvalda darbības riskus atbilstoši labākā snieguma organizāciju augstākajiem rādītājiem dzelzceļa nozarē un ārpus tās.

Tiek atzīts, ka drošības risku pārvaldība nav atsevišķa funkcija, bet produktīvas, konkurētspējīgas un rentablas organizācijas neatņemama daļa.

Drošības riskus atzīst par risku visiem darbības rādītājiem, un drošības pārvaldības sistēma ir efektīva, kontrolējot pašreizējos un prognozējot jaunus riskus.

Drošs ikdienas darbs ir galvenā prioritāte, un drošība ir saistīta ar darbības rādītājiem. Vadības ieguldījums drošībā ir liels, un organizācija pieliek visas pūles, lai rastu spēcīgākus un ilgtspējīgākus risinājumus drošības problēmām. Iegūto pieredzi izmanto ikdienā. Darbinieki izprot un atbalsta drošības iniciatīvas un drošību kā dzīvesveidu. Organizācija veicina drošību darbā un mājās, un šim nolūkam piešķir attiecīgus resursus.

Organizācijas vadības darbinieki tiek uzskatīti par līderiem ar cilvēkfaktoru un organizatoriskajiem faktoriem saistīto jautājumu pārvaldības pilnveidošanā gan visā uzņēmumā, gan arī plašāk nozarē.

4.2.2 L2 – drošības politika

Ar efektīvu drošības politiku nosaka skaidru virzienu, kas organizācijai jāievēro. Tajā ņem vērā visus darbības rādītāju aspektus, kas ir daļa no ieguldījuma pastāvīgos uzlabojumos. Drošības politika ir svarīgs dokuments, kas parāda, kā organizācija pārvalda savus pienākumus drošības jomā, kā arī līderību un ieguldījumu pienācīgā drošības pārvaldībā.

1. līmenis – nepietiekams

Politikas izklāsts ir novecojis vai nav darīts zināms organizācijā.

Nav pierādījumu, ka notiek apspriešanās ar darbiniekiem.

Netiek pienācīgi atzīta cilvēku nozīme, nodrošinot drošu un efektīvu darbības līmeni.

Drošības politikā nav apņemšanās ievērot regulatīvos standartus.

Darbības rādītāju līmenis neatbilst minimālajām standartam, kas jāievēro.

2. līmenis – pamata

Drošības politika ir atjaunināta un darīta zināma organizācijā, tomēr vietējiem vadītājiem un uzraudzītājiem nav saskaņotas pieejas vai interpretācijas. Tādējādi organizācijā politiku piemēro atšķirīgi.

Politiku neuzskata par būtisku drošības uzturēšanai.

Zināmā mērā atzīst, ka indivīda nozīmes izpratnes uzlabošana var veicināt darbību, tomēr tas nenotiek konsekventi.

Drošības politikā ir apņemšanās ievērot tiesību aktu prasības.

Darbības rādītāju līmenis atbilst minimālajām prasībām, kas noteiktas, lai piešķirtu vienotu drošības sertifikātu vai drošības atļauju.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam izmanto drošības politiku un citas saistītās politikas kā orientieri vadītājiem, tādēļ visi darbinieki tās interpretē vienādi.

Darbinieki aktīvi iesaistās drošības politikas pārskatīšanā un pārstrādāšanā.

Organizācijā nepārprotami pievērš uzmanību cilvēkfaktora jautājumiem un atzīst indivīda būtisko nozīmi drošas un efektīvas organizācijas nodrošināšanā un darbības mērķu sasniegšanā.

4. līmenis – prognozēšana

Drošības politika atbilst ikviena darbinieka, kurš darbojas vadības ķēdē, rīcībai.

Drošības politikā ietver apzinātu ieguldījumu pastāvīgā riska kontroles produktivitātes un efektivitātes uzlabošanā. Pastāv pierādījumi plašai sadarbībai visā vadības ķēdē, atzīstot indivīda vērtību uzlabotu rādītāju nodrošināšanā.

Cilvēkfaktora potenciālu mēra, pielāgo un samēro atbilstoši organizācijas briedumam un sarežģītībai, orientējoties uz uzlabojumiem laika gaitā.

Drošības politika un saistītās politikas ir šādas:

- *savstarpēji saskaņotas;*
- *pārskatītas un pārstrādātas, lai panāktu uzlabojumus paredzamā veidā; un*
- *vienādi interpretētas visās organizācijas daļās, kas tās piemēro.*

5. līmenis – izcilība

Drošības politiku izmanto, lai panāktu, ka organizācija sasniedz darbības rādītājus, kas atbilst labākā snieguma organizāciju rādītājiem.

Drošības politikā atzīst, ka drošības risku pārvaldība ir nevis atsevišķa funkcija, bet gan produktīvas, konkurētspējīgas un rentablas organizācijas neatņemama daļa.

Drošības riskus atzīst par darbības rādītāju risku.

Indivīda nozīmi atzīst par organizācijas panākumu neatņemamu daļu un ņem vērā katrā operatīvās darbības un darbības attīstības pārskatīšanā.

Organizācija ir vērsta uz āru un meklē ārējās iespējas produktivitātes un efektivitātes uzlabošanai, kā arī to darot, ņem vērā cilvēkfaktora jautājumus.

4.2.3 L3 - Funkcijas, pienākumi un pilnvaras

Šīs prasības mērķis ir panākt, lai organizācija, kas tiek uzraudzīta, parādītu, ka organizācija ir strukturēta un kā tiek sadalīti pienākumi, lai sasniegtu organizācijas kopējos mērķus un īstenotu drošības politiku. Iespējams, ka ir darba līmeņi, kas to atbalsta, raugoties no politikas un stratēģiskās perspektīvas.

Riska kontrole ir pārdomāti jāiekļauj pārvaldības struktūrās, lai būtu skaidrs, kas par to atbild. Tām arī vajadzētu atpazīt un efektīvi novērst riskus, ko rada mijiedarbība ar darbuzņēmējiem, partneriem un piegādātājiem.

Tie ir svarīgākie elementi, kas ļauj saprast, cik labi organizācijas drošības pārvaldības sistēma kontrolē risku. Pieteikuma iesniedzējam jāparāda, kā viņi norīko kompetentus darbiniekus darbībām, kā nodrošina šo darbinieku skaidru izpratni par funkcijām un pienākumiem un kā no šiem speciālistiem prasa atbildību par viņu sniegumu. Tāpat jāpierāda, ka organizatoriskā struktūra un indivīda funkcijas un pienākumi nodrošina līdzsvaru starp atbilstību un drošības kultūru – domāšanas kultūru, nevis atbilstību drošībai, ko ievēro vienīgi atbilstības dēļ.

1. līmenis – nepietiekams

Organizācijas pārvaldības struktūras nav saistītas ar drošības mērķiem, tāpēc personāla pienākumus un atbildību ir viegli sajaukt.

Ja pienākumus deleģē, personālam netiek piešķirtas pilnvaras vai resursi to pildīšanai. Atsevišķi darbinieki, kuriem uzticēti pienākumi, var tos nezināt vai arī viņiem var nebūt nepieciešamās kompetences to pildīšanai. Darba aprakstos precīzi neatspoguļo, kā darbinieki faktiski pilda savus amatus un pienākumus.

Funkciju un pienākumu sadalījums organizācijā netiek koordinēts un nav saistīts ar organizācijas darbības mērķiem.

Darbības rādītāju līmenis ir zemāks par līmeni, kas ir noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Pastāv organizācijas struktūras apraksts, tostarp funkciju un pienākumu sadalījums drošības pārvaldības sistēmā. Pastāv plāni, lai noteiktu, kā organizācijā faktiski tiek veikts darbs.

Organizācijas struktūra nozīmē, ka lielāko daļu risku pārvalda darbinieki vai komandas, kas veic darbu, tomēr daži riski ir sadalīti tā, ka pastāv vai varētu pastāvēt pretrunas starp drošības un citiem mērķiem.

Šķiet, ka pastāv ļoti niecīga saskaņotība starp atsevišķām struktūrvienībām vai ar organizācijas darbības uzdevumu plašākiem mērķiem.

Šķiet, ka pastāv ļoti niecīga saskaņotība organizatoriskajās struktūrās, pienākumu sadalē un saistītajā kultūrā, kas nepieciešama to efektīvai īstenošanai.

Organizācija atbilst minimālajam atbilstības līmenim, kāds noteikts, lai piešķirtu vienotu drošības sertifikātu vai drošības atļauju.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam dažādu elementu organizatoriskā struktūra atbilst pienākumiem, kas ir skaidri sadalīti struktūrvienībās.

Vispārējā politika un procedūras attiecībā uz funkcijām un pienākumiem atbilst attiecīgo struktūrvienību politikai un procedūrām.

Pastāv kritēriji pienākumu un uzdevumu deleģēšanai un sadalei, ja ir noteikta nepieciešamā kompetence un prasmes. Šie kritēriji tiek piemēroti, un tāpēc drošības uzdevumi ir skaidri sadalīti, un darbiniekiem, kuri tos veic, ir attiecīga kompetence, pilnvaras un resursi to izpildei.

Pienākumu deleģēšanas gadījumā pastāv sistemātiska pieeja, kā to darīt. Darbinieki ir kompetenti, un viņiem piešķir pietiekamus resursus un pilnvaras pienākumu veikšanai.

Ja ir paredzētas jaunas vai mainītas funkcijas un pienākumi, tiek analizēti ar cilvēkfaktoru saistīti jautājumi attiecībā uz pārmaiņām un veids, kā organizācijā faktiski tiek pildīti pienākumi.

4. līmenis – prognozēšana

Tāds pats kā iepriekš norādītajā 3. līmenī, tomēr ar skaidru saikni starp organizatoriskās struktūras elementiem no organizācijas augšējā līmeņa līdz apakšējam līmenim, ne tikai darba līmeņos.

Vispārējā politika un procedūras ir izstrādātas tā, lai struktūrvienības tās viena otru papildina, lai veicinātu organizācijas stratēģisko mērķu īstenošanu.

Atbildību par sniegumu no darbiniekiem, kuri atbild par drošību, prasa godīgi un konsekventi. Organizācijas kultūra ļauj par drošību atbildīgajiem darbiniekiem ietekmēt uzdevumu izpildi un uzlabojumu veikšanu.

Pamatojoties uz izpratni par darba faktisko veikšanu, pastāv individuālo un kolektīvo centienu saskaņošana ar darbības rādītāju mērķiem.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam pastāv organizācijas struktūras, funkciju un pienākumu efektīva pārskatīšana visos līmeņos, salīdzinot ar stratēģisko un darbības mērķu sasniegšanu.

Pastāv formāls pārskatīšanas process, lai nodrošinātu, ka funkcijas un pienākumi paliek spēkā, ir aktuāli un tiek integrēti mainīgajā organizācijā, stratēģijā un vidē. Organizācija savā sistēmā konsekventi uzskata indivīdu par pārskatīšanas procesa standarta daļu.

4.2.4 L4 – apspriešanās ar personālu un citām pusēm

Veiksmīgas organizācijas aktīvi iesaista darbiniekus, lai mudinātu viņus izmantot zināšanas un pieredzi un veikt ieguldījumu kopīgu mērķu sasniegšanā. Šādas organizācijas dažādos veidos aktīvi atbalsta un veicina iesaistīšanos un apspriešanos.

Šā aspekta pārbaude arī norāda uzraudzības iestādei, kāda ir drošības kultūra organizācijā un cik aktīvi tā iesaista attiecīgās trešās puses drošības pārvaldībā jomās ar kopīgu risku.

1. līmenis – nepietiekams

Apspriešanās notiek reti vai nenotiek nemaz.

Darbinieki nesaprot, kā viņi veicina savu drošību un to cilvēku drošību, ar kuriem viņi kopā strādā.

Organizācija neatbilst standartam, kas noteikts minimālajai atbilstībai tiesību aktiem.

2. līmenis – pamata

Darbinieki saprot, ka viņi ir atbildīgi par savu un kolēģu drošību, tomēr organizācijā tas nenotiek konsekventi.

Notiek apspriešanās par veselības un drošības jautājumiem, tomēr, šķiet, ka tas nenotiek sistemātiski un neaptver visus darbiniekus.

Organizācija atbilst minimālajām tiesību normām, kas būtu jāievēro vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam organizācijā pastāv procedūras, lai nodrošinātu, ka ar darbiniekiem apspriežas par drošības jautājumiem.

Darbinieki saprot, kā viņi veicina savu drošību un dzelzceļa drošību, un saņem atgriezenisko saiti par savu ieguldījumu.

Darbinieki ar līdzīgām funkcijām organizācijā piemēro standartus vienādi.

4. līmenis – prognozēšana

Organizācijai ir politika, kuras mērķis ir iesaistīt darbiniekus visos organizācijas līmeņos, un pastāv skaidra struktūra, ar kuru šo politiku var darīt zināmu. Notiek apspriešanās ar strādniekiem un darbiniekiem, kad tiek pieņemti lēmumi par riska kontroles pasākumiem.

Organizācija regulāri apspriežas ar darbiniekiem dažādos veidos, piemēram, veicot aptaujas, rīkojot darbsemināru, sanāksmes ar vadītājiem un drošības ekskursijas.

Darbinieki ir motivēti sasniegt darbības mērķus un demonstrē konsekventu izpratni par to, kā tos sasniedz.

Darbinieki spēj pieņemt lēmumus mērķu izvirzīšanas sistēmā.

Darbinieki ar līdzīgām funkcijām organizācijā piemēro standartus konsekventi.

Personāls saprot pārmaiņu nepieciešamību un apstiprina, ka ar viņiem konsultējas par pārmaiņu ieviešanu.

5. līmenis – izcilība

Organizācija pilnībā izmanto darbinieku un citu ieinteresēto pušu potenciālu un aktīvi iesaista viņus, lai izveidotu kopīgotas vērtības un uzticēšanās, atklātības un pilnvarošanas kultūru.

Organizācija izmanto darbinieku iesaistīšanos, lai apkopotu idejas uzlabošanai un īstenotu tās praksē.

Darbinieki parāda, ka izprot, kā viņi palīdz sasniegt organizācijas mērķus. Šī izpratne atbilst attiecīgajai organizācijas politikai un augstākā līmeņa vadības attīstības koncepcijai.

Darbinieki demonstrē apņemšanos pārsniegt šos mērķus, sekojot pašreizējiem procesiem un norādot, kur tos var uzlabot.

4.3 PL – plānošana

Mērķis

Pārliecināties, ka organizācija spēj definēt un īstenot riska kontroli, kas ļauj uzņēmumam darboties droši. Pārliecināties, ka organizācija plāno drošas darbības un pienācīgi ņem vērā savu darbinieku un pārējo, kurus ietekmē tās darbības, labklājību.

Ievada piebildes

Laba plānošana ir sākuma punkts riska pārvaldīšanai. Organizācijai ir jāizstrādā attiecīgas procedūras, lai organizācija var izpildīt savus juridiskos pienākumus un darboties kā uzņēmums, kas sasniedz savus mērķus produktīvi un efektīvi. Laba plānošana ievērojami uzlabo veidu, kā organizācija pārvalda drošību, nodrošinot, ka ir pieejami nepieciešamie resursi, tostarp kompetenti darbinieki uzdevumu veikšanai. Tas nodrošinās efektīvu riska kontroli un produktīvu darbu.

4.3.1 PL 1 – riska novērtējums

Šis elements attiecas uz *SMS* būtību, un tā mērķis ir ļaut pieteikuma iesniedzējam parādīt, kā organizācijas sistēmas identificē un kontrolē riskus, ar kuriem tā saskaras. Uzraudzība jāizmanto, lai ļautu pieteikuma iesniedzējam parādīt, kā organizācija praksē izmanto riska novērtējuma rezultātus, lai uzlabotu riska kontroli, un kā to laika gaitā pārbauda. Ir svarīgi atcerēties, ka šis elements tieši neattiecas uz risku pārvaldību pārmaiņu dēļ (kas ir vēl viens elements), bet ir saistīts ar to. Jānorāda, ka ir īpaša prasība risku novērtēšanas gaitā risināt jautājumus, kas ir saistīti ar cilvēka veiktspēju, piemēram, darba uzdevuma izstrāde un noguruma riska pārvaldība. Tāpēc no uzraudzības viedokļa ir jāiegūst pierādījumi par šo jautājumu risināšanu riska novērtēšanas procesā.

Sistēmas, kas saistītas ar riska kontroles plānošanu un tās ieviešanu, ir jākoordinē, lai pārliecinātos, ka tās atbilst attiecīgajiem likumiem un ļauj organizācijai produktīvi un efektīvi sasniegt savus mērķus.

1. līmenis – nepietiekams

Uzņēmumam ir process risku novērtēšanai, bet tas netiek konsekventi pielāgots un atjaunināts, tādēļ tiek izmantoti vecie darbības noteikumi vai prakse riska kontrolei, kad risks jau ir mainījies.

Riska novērtējums nav pabeigts vai pārskatīts attiecībā uz visiem attiecīgajiem darbības pasākumiem.

Riska novērtējumi neatbilst paredzētajam lietojumam. Skaidrs, ka nav saprasti riska novērtēšanas mērķi un kā to veikt.

Riska kontroles pasākumus izmanto nepietiekami, un neveic esošo kontroles pasākumu efektivitātes uzraudzību.

Šķiet, ka riska novērtēšanā netiek ņemti vērā riski, kas saistīti ar cilvēkfaktora jautājumiem. Uzņēmumam nav nepieciešamības risināt šos jautājumus.

Organizācijas darbības rādītāju līmenis ir zemāks par līmeni, kas ir noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

Riska novērtēšanas procesā ir maz pierādījumu, ka, pārvaldot pārmaiņas, pienācīgi ņem vērā drošības riskus, tostarp tos, kas saistīti ar cilvēkfaktoru un organizatoriskajiem faktoriem.

2. līmenis – pamata

Riska novērtējums ir pabeigts, bet par vispārējo koordināciju ir bažas.

Kontroles pasākumos kādas darbības ietvaros ne vienmēr iekļauj riska novērtējumā identificētos pasākumus.

Riska novērtēšanu bieži izmanto tikai tādēļ, lai parādītu, ka esošie riska kontroles pasākumi ir pietiekami.

Riska novērtējumus izmanto tikai, lai noteiktu, kur ir nepieciešama riska kontrole, bet organizācija pietiekami neizmanto kontroles pasākumus.

Apmācība par riska novērtējumu ir nodrošināta visiem darbiniekiem, kuriem tas vajadzīgs, attiecīgā līmenī, kāds nepieciešams dažādiem atbildības līmeņiem.

Pastāv pierādījumi par riska kontroles pasākumu izmantošanu un to uzraudzību.

Tiek atzīts, ka riska novērtēšanā ir jāņem vērā cilvēkfaktora jautājumi, bet veids, kā tas notiek, rada bažas. Tādēļ šie jautājumi netiek kontrolēti tik labi, kā vajadzētu, izmantojot SMS*.*

Pastāv daži pierādījumi, ka pārmaiņu pārvaldības procesā ņem vērā drošības riskus, tostarp ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītos jautājumus.

Organizācijas darbības rādītāji atbilst minimālajam atbilstības līmenim, kāds noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam organizācijai ir skaidra politika attiecībā uz riska novērtējumu izmantošanu un to, kādi riski ir pieļaujami un kāpēc tas ir pieņemami.

Riska pārvaldību konsekventi izmanto dažādās organizācijas daļās, tostarp pārmaiņu pārvaldības procesā. Vadītāji izprot savu funkciju šajā procesā.

Tiek efektīvi izmantota risku kontrole un risku novēršana to rašanās vietā.

Vērtējumu saskaņošana ir konsekventa un tiek regulāri pārskatīta.

Riski un ar tiem saistītie kontroles pasākumi tiek skaidri paziņoti personālam.

Riska novērtēšanas procedūras ir pārmaiņu pārvaldības procesa daļa.

Pastāv vienkārša sistēma, lai pārbaudītu efektivitāti risku kontroles pasākumiem, kas ieviesti risku regulāras novērtēšanas rezultātā.

Pastāv konsekventi procesi, lai identificētu riskus, kas saistīti ar cilvēkfaktoru un organizatoriskajiem faktoriem, riska novērtēšanas procesā. Lai to atvieglotu, uzņēmums var izmantot speciālistu zināšanas, ja nepieciešams.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam riska novērtējumi ir iekļauti citos darbības aspektos, lai nodrošinātu sistemātisku pieeju riska kontrolei.

Visu līmeņu darbinieki un ārējās organizācijas var veicināt riska novērtēšanu.

Riska novērtējums, ieskaitot riska novēršanu tā izcelsmes vietā, ir pārmaiņu procesa un organizācijas kultūras daļa.

Pārskatīšana ir riska novērtējuma procesa daļa.

Riska pārvaldības principus saprātīgi piemēro visos līmeņos.

Pastāv sarežģīta sistēma, lai pārbaudītu efektivitāti risku kontroles pasākumiem, kas ieviesti regulāras risku novērtēšanas rezultātā .

Cilvēkfaktora un organizatorisko faktoru jautājumi ir pilnībā integrēti SMS *procesos riska novērtēšanai un pārmaiņu pārvaldībai. Personām, kuras atbild par riska novērtēšanu, tiek sniegta atgriezeniskā saite par viņu sniegumu.*

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam riska novērtējums tiek izmantots, lai vadītu pastāvīgu organizācijas riska profila uzlabošanu.

Riska pārvaldības pieeja ir iekļauta, un to konsekventi piemēro visā organizācijā. Riskus rūpīgi novērtē un apsver savlaicīgi pirms jebkādām pārmaiņām.

Riska novēršana tā rašanās vietā ir konsekventas pieejas daļa un ir atspoguļota organizācijas politikā.

Ir izveidotas aktīvas procedūras riska kontroles pasākumu izstrādei sadarbībā ar citām iestādēm, kas ir atbildīgas par riska kontroli, ja pastāv starpnozaru jautājumi.

Cilvēkfaktora un organizatorisko faktoru informāciju no riska novērtēšanas izmanto visā uzņēmumā, lai veicinātu nepārtrauktu drošības uzlabošanu. Novērtējumu rezultātus attiecīgos gadījumos kopīgo ar darbuzņēmējiem, partneriem un piegādātājiem, lai uzlabotu šo organizāciju darbību efektivitāti.

4.3.2 PL2 – drošības mērķi un plānošana

Lai panāktu organizācijas atbilstību tiesiskajām prasībām un nodrošinātu nepārtrauktu drošības uzlabošanu, vadība uzskata un paziņo darbiniekiem, ka nepieciešams, lai drošības mērķi atbilst *SMART* prasībām (skat. turpmāk).

Organizācijai ir jāpierāda, ka tai ir jēgpilni mērķi un process, lai īstenotu un uzraudzītu panākumus šo mērķu sasniegšanai to pastāvēšanas laikā. Drošības mērķiem jābūt "konkrētiem, izmērāmiem, sasniedzamiem, reālistiskiem un noteiktā laikā paveicamiem" *(SMART)*. Līdztekus plašākiem darbības mērķiem ir jānosaka gan īstermiņa, gan ilgtermiņa mērķi, kā arī jādefinē to prioritāte. Konfliktējošas prioritātes jāpārvalda tā, lai netiktu apdraudēti drošības mērķi salīdzinājumā ar citām darbības vajadzībām. Mērķi, kas noteikti dažādos līmeņos vai dažādām organizācijas daļām, jāsaskaņo, lai tie atbalstītu organizācijas politikas vispārējos mērķus. Arī ar atsevišķām personām var vienoties par personīgiem mērķiem, lai būtu pārliecība par ka organizācijas mērķu sasniegšanu.

1. līmenis – nepietiekams

Drošības mērķu ir maz vai to nav.

Visi pastāvošie drošības mērķi neatbilst SMART *principiem vai tiem nav noteikta prioritāte.*

Tiek pieļauts, ka drošības mērķi netiek sasniegti un netiek veikti nekādi pasākumi, lai novērstu trūkumus to sasniegšanā.

Personīgie mērķi nav saistīti ar organizācijas vispārējās politikas mērķiem.

Organizācijas darbības rādītāju līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Drošības mērķi pastāv. Daži no tiem var atbilst SMART *principiem, un to prioritātes var būt noteiktas, bet mērķi dažādās organizācijas daļās nav skaidri saskaņoti un var būt pretrunīgi, un tādējādi ne vienmēr atbalsta organizācijas politikas vispārējos mērķus.*

Personīgie mērķi pārsvarā ir saskaņoti ar organizācijas vispārējās politikas mērķiem.

Tiek veiktas drošības pārbaudes, lai sasniegtu drošības mērķus.

Organizācija atbilst minimālajām prasībām, kas jāievēro, lai sasniegtu atbilstību tiesību aktiem.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam ir noteikti drošības mērķi un pastāv drošības plāns, kas parāda, kā organizācija sasniegs tās mērķus.

Noteiktajos drošības mērķos ievēro piemērojamās tiesiskās un citas prasības.

Ir mēģināts noteikt SMART *mērķus un izvirzīt prioritātes mērķiem un uzdevumiem, kā arī savstarpēji saskaņot tos.*

Pastāv sistēmas, lai sekotu mērķu sasniegšanai.

Mērķu sasniegšana nav pienācīgi saskaņota ar pārskatīšanas procesu, t. i., pārskatos neņem vērā izvirzītos mērķus.

Darbinieki apzinās savas darbības nozīmīgumu un nozīmi, kā arī veidu, kā viņi palīdz sasniegt drošības mērķus un plāno pārvaldīt drošības riskus.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam ir SMART *mērķi, kam ir noteikta prioritāte un kuri ir savstarpēji saistīti, lai atbalstītu vispārējo politiku.*

Ar drošības pārvaldības sistēmu nodrošina drošības mērķu noteikšanu un sasniegumu novērtēšanu.

Mērķu sasniegšanu vai to nesasniegšanu reģistrē un izmanto pastāvīgai uzlabošanai.

Ir izveidotas sistēmas, lai uzraudzītu potenciālo un faktisko drošības mērķu sasniegšanu.

5. līmenis – izcilība

Tāds pats kā turpmāk 4. līmenis, un papildus organizācija salīdzina savus veiktspējas rādītājus ar citiem rādītājiem dzelzceļa nozarē un ārpus tās, lai pārliecinātos par mērķu atbilstību izcilībai.

4.4 S – atbalsts

Mērķis

Šīs prasības mērķis ir nodrošināt, lai organizācija piešķirtu pietiekamus resursus, tostarp kompetentu personālu, lai tās *SMS* var kontrolēt risku saskaņā ar tās mērķiem.

Norādīt funkcijas un pienākumus, lai izpildītu organizācijas drošības mērķus.

Nodrošināt svarīgas informācijas pieejamību lēmumu pieņēmējiem.

Pārliecināties, ka organizācijas pasākumi un darbības veicina kultūru, kas ļauj panākt izcilu riska kontroli.

Ievada piebildes

Drošības pārvaldības sistēmas dokumentācija ir stingri jāpārrauga, jāpārvalda un regulāri jāpārskata, lai pašreizējā apritē tiktu izmantota tikai jaunākā katra drošības kontroles dokumenta versija. Jebkādas izmaiņas dokumentācijā, kas izveidota, pastāvīgi uzlabojot riska kontroli, ir jāizdara savlaicīgi.

Ir ļoti svarīgi drošības pārvaldības sistēmā ietvert un ieviest visaptverošu kompetences pārvaldības sistēmu un attiecīgus informācijas apmaiņas pasākumus gan no vadības personālam, gan otrādi, kā arī citiem, kuri paļaujas uz komunikāciju no organizācijas puses savu organizāciju drošības pārvaldībai. Tas ir tādēļ, ka šie elementi atbalsta *SMS* produktivitāti un efektivitāti. Ar kompetentu darbinieku atrašanos amatā, veicot no tiem prasītos pienākumus, samazina kļūdu risku sprieduma izdarīšanā, kas iedragā *SMS* darbību. Tajā pašā laikā jāpārliecinās, ka informācijas apmaiņas sistēma gan no augšas lejup, gan no apakšas augšup organizācijā nodrošina, ka atbildīgie darbinieki saņem svarīgākās ziņas savlaicīgi.

4.4.1 S1 – resursi

Efektīva resursu izmantošana ir galvenais jebkuras drošības pārvaldības sistēmas elements. Nepietiek ar to, ka procesi pastāv, tiem arī ir jāstrādā, un tādēļ ir jānodrošina pietiekami resursi konstruktīvai un efektīvai to norisei.

1. līmenis – nepietiekams

Organizācija nodrošina resursus, kas ļauj drošības pārvaldības sistēmai darboties, bet tas netiek darīts sistemātiski, drīzāk šķiet, tā ir fragmentāra pieeja. Tādēļ resursu izplatība visā organizācijā ir nevienmērīga, dažām daļām ir pietiekami daudz resursu un dažām pārāk maz.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Šajā līmenī organizācija spēj labāk pārvaldīt resursus, lai varētu īstenot uzdevumus. Resursu piešķiršana tiek uzskatīta par svarīgu drošības pārvaldības sistēmas elementu. Organizācijas augstākā vadība regulāri pārskata resursus.

Organizācija darbojas pamata līmenī, kas ir jāsasniedz vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam organizācija var pierādīt, ka resursi ir pietiekami un to sadalījums ir konsekvents visās darbības daļās. Atsevišķu darbinieku prombūtne nav nozīmīgs jautājums, jo to risina SMS *procesos. Organizācija sāk domāt par resursu efektīvāku izmantošanu.*

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, bet šeit organizācija prognozē savas nākotnes vajadzības, lai tā būtu jau iepriekš gatava gaidāmajām pārmaiņām un tai būtu nodrošināti resursi to pārvaldībai.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam organizācija resursu pārvaldību veic ļoti aktīvi, elastīgi izmantojot tos visā organizācijā lielākas drošības un efektivitātes sasniegšanai.

4.4.2 S2 – kompetence

Ir svarīgi, lai personāla vadība, kas atbild par drošību, laika gaitā organizētu kompetenču pārvaldības sistēmu, kas veido drošības pārvaldības sistēmas elementu. Tieši ar šo sistēmu darbinieku prasmes tiek vērtētas, attīstītas, uzturētas un uzraudzītas tā, lai netiktu apdraudēta drošība.

Organizācijām ir vajadzīga efektīva kompetenču pārvaldības sistēma, lai palīdzētu pārliecināties par personāla attiecīgām kompetencēm. Kompetenču pārvaldības sistēmas (KPS) būtiska daļa ir kompetences saglabāšana. Tas iekļauj visaptverošu nepārtrauktas profesionālās pilnveides (NPP) programmu, kurā vairāk pieredzējušie darbinieki var uzzināt par jauniem pasākumiem drošības jomā un nodrošināt to ievērošanu.

Kompetenču pārvaldības sistēmas darbība var atklāt daudz informācijas par organizācijas drošības kultūru. Pārdomātā kompetenču pārvaldības sistēmā iekļauj darbiniekus, kuri faktiski veic darbu un tādēļ vislabāk izprot uzdevumu un dod ieguldījumu KPS koncepcijas izstrādē, tādējādi palīdzot gan indivīdiem, gan organizācijai sasniegt labākus rādītājus. Funkcionējoša KPS ir galvenais drošības kultūras rādītājs organizācijā.

1. līmenis – nepietiekams

Kompetenču pārvaldības sistēma ir dokumentēta, bet nav skaidri īstenota un nav saistīta ar darba uzdevumu plānošanu. Pastāv neskaidra pieeja, kā pārvaldīt darbinieku kompetenci.

Darbinieki var būt vai nebūt kompetenti, bet nav konsekventa procesa kompetences identificēšanai.

Apmācības nepieciešamība tiek pārvaldīta nesistemātiski, un tūlītējas vajadzības ir svarīgākas pār ilgtermiņa attīstību.

Organizācijas darbības rādītāju līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

Kompetencēm, kas nepieciešamas, lai cilvēki varētu efektīvi pārvaldīt cilvēkfaktoru un organizatoriskos faktorus vai drošības kultūras jautājumus organizācijā, tiek pievērsts maz uzmanības vai netiek pievērsta nekāda uzmanība.

2. līmenis – pamata

Apmācība notiek atsevišķās struktūrvienībās, galvenokārt "strādājot darbavietā" kompetenču pārvaldības sistēmas ietvaros. Pastāv minimālais atbilstības līmenis tiesību aktu prasībām darbā pieņemšanai, atlasei un apmācībai. Ir izveidots atlases process drošībai svarīgām funkcijām.

Darbā pieņemšanas, atlases un apmācības politika nav saskaņotas sistēmas daļa un nav saistīta ar organizācijas stratēģiskajiem mērķiem, un tā ir tikai nedaudz plašāka par tiesību aktu prasību izpildi.

Apmācības vajadzības, tostarp tās, kas saistītas ar cilvēkfaktora, organizatorisko faktoru un drošības kultūras jautājumu risināšanu, ir identificētas, taču norīkošana uz apmācību bieži vien ir nejauša un atkarīga gan no apmācības, gan no attiecīgā personāla pieejamības, nevis veido strukturētas pieejas daļu.

Organizācija atbilst minimālajām atbilstības līmenim, kāds noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam organizācijai ir efektīva, dokumentēta kompetenču pārvaldības sistēma. Tā aptver kompetences, kas nepieciešamas, lai sasniegtu organizācijas stratēģiskos mērķus un pārvaldītu riskus. Organizācija spēj pilnībā izmantot savu darbinieku kompetences, ja tā tās zina.

Organizācija spēj noorganizēt un izstrādāt apmācības programmas darbiniekiem, kuri pilda drošībai svarīgus pienākumus, nodrošinot, ka attiecīgās vajadzības tiek apmierinātas un personāla kompetences uzturētas.

Ir paredzēti pasākumi personālam, kas atgriežas darbā pēc negadījumiem/starpgadījumiem vai ilgstošas prombūtnes, tostarp tiek noteikta nepieciešamība pēc papildu apmācības, ja nepieciešams.

Darbā pieņemšanas un atlases procesi ir visaptveroši (piemēram, psihometriski un uz uzdevumiem balstīti) un pārsvarā konsekventi, un tajos parasti izvēlas attiecīgus cilvēkus dažādām funkcijām.

Apmācību vada kompetenti speciālisti saskaņā ar noteiktu programmu, ņemot vērā attiecīgā amata vajadzības. Apmācībā ietver reaģēšanu normālas un sliktas darbības režīmos.

Pastāv izpratne par nepieciešamību saistīt kompetenču pārvaldības sistēmu ar darba uzdevuma plānošanu un izpildi.

Ir saprasts, kādas kompetences ir nepieciešamas cilvēkfaktora, organizatorisko faktoru un drošības kultūras jautājumu pārvaldīšanai, un tiek pieņemti darbā attiecīgi darbinieki ar vajadzīgajām prasmēm.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam politikai attiecībā uz darbā pieņemšanu, apmācību un atlasi ir skaidra saikne ar organizācijas stratēģiskajiem mērķiem, kuru zemākajos līmeņos ir darbinieku mērķi. Tie ir balstīti uz precīzu uzdevumu novērtējumu (uzdevumu analīzi), ar ko nodrošina skaidru un saskaņotu kompetenču pārvaldības sistēmu. Tiek izmantota mentorēšana, un funkciju izmaiņas ir labi pārdomātas.

Apmācības režīms ir visaptverošs un saistīts ar nepieciešamo kompetenci, kāda ir nepieciešama efektīvai darbībai konkrētos amatos.

Personāla atlases procesi ir visaptveroši un vērsti uz optimālu prasmju noteikšanu konkrētam amatam. Tos nodrošina ar periodiska pārskatīšanu (kā arī ar pārskatīšanu, kad darbinieki aiziet no organizācijas), lai pārliecinātos par piemērotu cilvēku pieņemšanu darbā, organizācijai mainoties un attīstoties.

Organizācija skaidri apzinās, kādas cilvēkfaktora, organizatorisko faktoru un drošības kultūras vajadzības tai ir jāapmierina, un tai ir procesi, kuros tā pārliecinās, ka tai ir darbinieki ar vajadzīgajām prasmēm un līdzekļi to uzturēšanai laika gaitā.

5. līmenis – izcilība

Tāds pats kā 4. līmenis ar papildinājumu, ka organizācija izprot sava personāla kompetenci un pilnībā izmanto darbinieku potenciālu. Organizācija tos aktīvi iesaista, pamatojoties uz kopīgotām vērtībām un uzticības, atklātības un iespēju palielināšanas kultūru.

Organizācija izmanto darbinieku iesaistīšanos, lai apkopotu idejas uzlabošanai un īstenotu tās praksē. Cilvēkresursu plānošana tiek veikta, lai nodrošinātu darbības nepārtrauktību.

Ir vērienīga un tālredzīga attīstības koncepcija ar mērķi nodrošināt, ka tiek pieņemti darbā piemēroti cilvēki un viņiem tiek nodrošināta attiecīga apmācība un attīstība, lai veicinātu prasmju kopumu uzturēšanu tādā līmenī, kas ļauj organizācijai augt un attīstīties, vienlaikus saglabājot un uzlabojot drošības rādītājus.

Organizācija ir līdere to savu darbinieku prasmju pilnveidošanā, kuras ir vajadzīgas, lai sasniegtu augstus rezultātus cilvēkfaktora, organizatorisko faktoru un drošības kultūras jautājumu risināšanā.

4.4.3 S3 – informētība

Informētība nozīmē darbinieku informēšanu par organizācijas drošības politiku un to, kā viņi veicina drošību organizācijā, par apdraudējumiem un riskiem, kas viņiem jāapzinās, kā arī negadījumu un starpgadījumu izmeklēšanas rezultātiem. Tas attiecas arī uz darbinieku informēšanu par sekām, ja netiek sniegts ieguldījums drošības pārvaldības sistēmas īstenošanā gan no viņu, gan no organizācijas puses. Tādēļ šis elements sniedz svarīgu informāciju par organizācijas drošības kultūru.

1. līmenis – nepietiekams

Šajā līmenī organizācija ir darījusi drošības politiku personālam pieejamu un sniedz zināmu pamatinformāciju par riskiem un apdraudējumiem. Negadījumu izmeklēšanas rezultāti netiek sistemātiski paziņoti visiem darbiniekiem, un nav saskaņotu mēģinājumu pārliecināties par darbinieku sapratni attiecībā uz viņu un organizācijas pienākumiem, tāpēc drošības kultūra ir slikta.

Organizācijas darbības rādītāju līmenis ir zemāks, nekā noteikts tā atbilstībai tiesību aktiem.

2. līmenis – pamata

Šajā līmenī darbiniekiem sniedz vairāk informācijas, taču šķiet, ka tās formāts nav konsekvents un sniegtie ziņojumi visā organizācijā nav skaidri. Organizācija cenšas nodrošināt darbinieku sapratni par viņu nozīmi drošības veicināšanā drošības pārvaldības sistēmas ietvaros.

Organizācijas darbības rādītāji atbilst minimālajam līmenim, kāds noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

Savāktā informācija liecina, ka organizācijas drošības kultūra ir vāja un tās līmenis dažādās organizācijas daļās ievērojami atšķiras.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam darbinieku informēšanas process par drošības politiku un informēšana par viņu funkcijām ir konsekvents un darbinieki saprot ziņojumus. Tiek veikts zināms uzraudzības process, lai pārliecinātos, ka darbinieki ir apguvuši informāciju un saprot, cik būtiska ir viņu nozīme SMS *efektīvas darbības nodrošināšanā.*

Organizācijas drošības kultūra šķiet konsekventa, bet joprojām pastāv daži trūkumi, un tā netiek pilnveidota.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam organizācija proaktīvi cenšas veicināt informētību par tās un personāla nozīmi un atbildību. Organizācija aktīvi cenšas uzsvērt ieguvumus pašiem darbiniekiem no uzlabotiem drošības rādītājiem.

Organizācija aktīvi veicina savas drošības kultūras uzraudzības pilnveidi un uzlabošanos, un tas ir viens no līdzekļiem, kā nodrošināt, ka SMS *gūst vajadzīgos rezultātus.*

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam organizācija cenšas uzlabot ne tikai savu darbinieku izpratni par organizāciju un viņu pienākumiem, bet arī informēt apakšuzņēmējus, piegādātājus un citus, ar kuriem tai ir mijiedarbība.

Organizācija tiek uzskatīta par līderi tādas pozitīvas drošības kultūras veidošanā, kāda tajā pastāv. Darbinieki iesaistās un saprot savus pienākumus un funkcijas, un proaktīvi atbalsta uzņēmumu ceļā uz tā mērķiem.

4.4.4 S4 – Informācija un komunikācija

Atbilstība šim elementam ir paredzēta, lai pierādītu, ka pieteikuma iesniedzējs savā pieteikumā ir pierādījis, ka viņam ir attiecīgi līdzekļi, lai dažādos līmeņos identificētu ar drošību saistītu informāciju un paziņotu to īstajā laikā un atbildīgajiem pārstāvjiem. Tā ir paredzēta, lai viņi pētītu nākotnes iespējas un pašreizējā riska kontrole joprojām būtu atbilstoša un aktuāla, varētu noteikt jaunus draudus un iespējas, ko rada ārējā ietekme (politiskā, sociālā, vides, tehnoloģiskā, ekonomiskā un juridiskā ietekme). Lai viņi varētu pārliecināties, ka informācija ir sasniegusi to attiecīgo speciālistu (jo īpaši drošībai svarīgo personālu) savā organizācijā, kuram ir jāreaģē uz to. Tas ietver būtiskas drošības informācijas sniegšanas veidu citām ieinteresētajām pusēm, ar kurām tie saskaras.

Ar pasākumiem jānodrošina, ka jebkuram darbiniekam, kurš pieņem lēmumu vai veic uzdevumu, ir pieejama pareiza informācija šādā veidā:

- korporatīvie ziņojumi par drošības nozīmīgumu;
- procedūras informācijas apmaiņai ar attiecīgajām ieinteresētajām pusēm;
- ar drošību saistītās procedūras un standarti;
- faktiskie dati un izlūkdati; kā arī
- norādījumi un ziņojumi.

1. līmenis – nepietiekams

Ir maz mēģinājumu sniegt attiecīgu drošības informāciju. Ja procedūras ir ieviestas, darbinieki pieņem lēmumus, pamatojoties uz savu spriedumu.

Maz informācijas par drošību tiek vākts vai kopīgots.

Vadītāji nerunā ar darbiniekiem, kuri nepilda administrācijas funkcijas, vai dara to neefektīvi.

Informācijas apmaiņa un komunikācija organizācijā ir nejauša un neizsekojama.

Trūkst apziņas, ka efektīvai komunikācijai ir svarīga nozīme, ietekmējot cilvēka uzvedību un līdz ar to arī drošības rādītājus.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. Līmenis - Pamata

Personāla rīcībā ir procedūras un standarti attiecībā uz riska kontroli.

Daļu informācijas, kas saņemta no personāla, izmanto lēmumu pieņemšanai.

Vadītāji dod norādījumus un saņem ziņojumus, kas attiecas uz risku kontroli, taču pastāv konsekvences trūkums.

Zināmā mērā tiek atzīta drošībai būtiskas komunikācijas nozīme, lai nodrošinātu drošu darba izpildi. Pastāv pierādījumi, ka tiek izstrādāti nodrošināšanas plāni, lai to pārbaudītu.

Organizācijas darbības rādītāji atbilst minimālajam līmenim, kāds noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam darbības rakstveida mērķu, standartu un būtisku risku kontroles un paziņošanas procedūru formāts ir piemērots lietotājiem.

Faktisko informāciju izmanto, lai dalītos pieredzē un vadītu turpmāko sniegumu un lēmumus.

Vadītāji dod norādījumus, kas pastiprina procedūras, lai palīdzētu sasniegt drošības mērķus.

Darbinieki ziņo par savu sniegumu un pieredzi, jo organizācija mudina viņus to darīt.

Komunikācija organizācijā ir regulāra un atbilst noteiktai kārtībai abos vadības ķēdes virzienos – augšup un lejup.

Speciālistu, kuriem ir pienākums sniegt informāciju visā organizācijā, uzdevumi un atbildība ir skaidri jādefinē.

Komunikācijas uzraudzība un novērtēšana notiek regulāri.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam viss atbilst galvenajām riska kontroles sistēmām.

Lēmumu pieņemšanai ir pieejama pareizā informācija.

Vajadzības gadījumā ir izveidotas efektīvas atgriezenisko saišu apkopošanas procedūras, lai pārliecinātos par komunikācijas saprotamību un par organizācijas izpratni attiecībā uz personāla reakciju uz paziņojumiem. Attiecīgajiem darbiniekiem tiek sniegta atgriezeniskā saite par viņu sniegumu pozitīvā un nediskriminējošā veidā.

Komunikācija tiek uzraudzīta, un rezultāti tiek izmantoti, lai sniegtu informāciju organizācijas mēroga komunikācijas programmai.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam komunikācijas kvalitāti un tās kārtību regulāri pārskata, salīdzinot ar apzināto labo praksi citās nozarēs. Informāciju proaktīvi kopīgo ar organizācijām, ar kurām uzņēmumam ir mijiedarbība, kā arī ar darbuzņēmējiem.

Informācijas apmaiņu dokumentē.

Pastāv koncepcija par uz āru vērstu komunikāciju, kurā notiek kopīgošana gan iekšēji, gan ārēji ar attiecīgiem partneriem, piegādātājiem un apakšuzņēmējiem.

Cilvēkfaktora nozīme komunikācijā ir skaidri saprotama, un organizācijai ir skaidrs mērķis pastāvīgi uzlabot komunikācijas rādītājus.

4.4.5 S5 – dokumentēta informācija

Izcilas organizācijas sniedz ticamu svarīgu lēmumu pārskatu un informāciju, kas apkopota gadu gaitā, lai pierādītu, ka tās kontrolē risku visos līmeņos.

Lai pārliecinātos, ka informācija par riska kontroli, darba procesiem un mācībām, kas gūtas no revīzijām un starpgadījumiem, tiek savlaicīgi un efektīvi paziņota attiecīgajiem darbiniekiem, organizācijā ir jābūt dokumentu pārvaldības un kontroles sistēmai, ar ko to nodrošina.

Šajā elementā ietilpst drošības pārvaldības sistēmas dokumentācija, dokumentu izveide un atjaunināšana, kā arī dokumentētas informācijas kontrole.

1. līmenis – nepietiekams

SMS *dokumentācija ir sagatavota. Tajā neietver visas uzņēmuma darbības, un to regulāri neatjaunina pēc jebkura veida pārmaiņām, kas to prasītu.*

Dokumentācija netiek pareizi izplatīta vai kopīgota. Organizācija neizmanto SMS *kā "darba instrukcijas", savukārt darbības prakse ir atšķirīga un bieži vien ir saistīta ar personāla un darbinieku personīgo atmiņu un vēsturisko praksi, neņemot vērā pagājušo laiku un pārmaiņas, kas tādēļ var būt nepieciešamas.*

Dokumentāciju izmanto tikai sertificēšanas/pilnvarošanas mērķiem.

Dokumentu kontroles sistēmas ir vājas, tāpēc dažādas uzņēmuma daļas izmanto dažādas dokumentu versijas.

Organizācijas darbības rādītāju līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Dzelzceļa uzņēmums / infrastruktūras pārvaldītājs parasti strādā saskaņā ar procedūrām un instrukcijām, kas izveidotas SMS*. Ir iespējamas dažas novirzes. Ir reģistrēta zināma informācija par svarīgiem riska kontroles pasākumiem, tomēr ieraksti ir nekonsekventi.*

Ikgadējais drošības ziņojumā, ko iesniedz valsts drošības iestādei, iekļauj organizatorisko struktūru, drošības mērķus nākamajam gadam un to izvēles argumentus. Tajā iekļauj arī informāciju par iekšēju negadījumu un starpgadījumu izmeklēšanu, detalizētu informācija par izvēlētajiem drošības rādītājiem, lai uzraudzītu sniegumu salīdzinājumā ar mērķiem, kā arī, vai ir jebkādi valsts izmeklēšanas iestādes atklāti pieejami ieteikumi.

Dokumentu kontroles sistēma parasti ir uzticama, taču pastāv problēmas ar versiju numerāciju un dokumentu sistemātisku atjaunināšanu.

Organizācijas darbības rādītāji atbilst minimālajam līmenim, kāds noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam ir reģistrēta galveno risku procesu un standartu informācija.

Svarīgu informāciju un lēmumus, kas varētu būt vērtīgi nākotnē, reģistrē.

Pastāv darbību apraksts attiecībā uz drošības pārvaldības procesiem un šo procesu mijiedarbību SMS *ietvaros. Personāls konsekventi īsteno drošības pārvaldības procesus.*

Ir pārskats par līgumiskajiem procesiem un citiem darbības līgumiem, ieskaitot informāciju drošības risku kontroles veidu. Pastāv darbuzņēmēju, partneru un piegādātāju aktuāls saraksts ar sniegtā pakalpojuma veida un apjoma aprakstu, ko atjaunina ikreiz, kad piešķir jaunus uzdevumus.

Dokumentu pārvaldības sistēma ir uzticama un spēj nodrošināt, ka apritē atrodas tikai dokumenta jaunākā versija.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam lietotājiem un lēmumu pieņēmējiem ir pieejami visaptveroši dati par procesiem saistībā ar drošību, ar tiem saistītajiem riskiem un standartiem, lēmumiem un informāciju.

Dokumentu kontrole ir pietiekami attīstīta, lai signalizētu, kad dokumenti ir jāatjaunina un kurš par to ir atbildīgs.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam plašāk izmanto procesu, lai veicinātu pārvaldības sistēmas produktivitāti un efektivitāti. SMS *atspoguļo dzelzceļa uzņēmuma / infrastruktūras pārvaldītāja faktisko darbības praksi.* SMS *ir dokuments, kas nepārtraukti mainās un attīstās, lai uzlabotu drošību, nevis administratīvs slogs.*

Dokumentu kontroles sistēmas darbojas, lai uzlabotu un attīstītu SMS*, un tās tiek uzskatītas par noderīgu līdzekli* SMS *mērķa konsekvences nodrošināšanai.*

4.4.6 *S6 – cilvēkfaktora un organizatorisko faktoru integrēšana*

1. līmenis – nepietiekams

Pastāv COF stratēģija, taču ir daudz nepilnību, un ar to neaptver visus attiecīgos procesus. COF stratēģija nav pielāgota organizācijas struktūrai un procesiem. Dažās jomās ir dokumentēti COF procesi, tomēr ne visi, piemēram, nav metodes, kā integrēt COF riska analīzē vai negadījumu izmeklēšanā. Ir maz COF funkciju un pienākumu aprakstu, trūkst COF kompetences, un COF netiek piešķirti resursi. COF stratēģija un izveidotie COF procesi netiek pilnībā izmantoti praksē. Aprīkojuma, darbstaciju, darba sistēmu un rīku veidošanā maz tiek ņemtas vērā lietotāju vajadzības. Paļaujas uz komerciāli pieejamām ražotāju procedūrām, tās maz pielāgojot vai nemaz nepielāgojot uzņēmuma konkrētajām vajadzībām, un procedūras, neiesaistot lietotājus, izstrādā citas personas, nevis lietotāji. Par lietotāju vajadzībām darba vidē tiek domāts maz.

2. līmenis – pamata

Ir atzīts, ka jānosaka riski, kas saistīti ar cilvēku rīcību, bet tie netiek visā uzņēmumā konsekventi noteikti. Ar COF stratēģiju aptver visus attiecīgos procesus organizācijā, tomēr tās struktūra ir neskaidra un dažu COF jomu procesi ir labāk aprakstīti nekā citi. Nav skaidrs, kad un kā jāpiemēro COF. COF funkcijas un pienākumi Ir aprakstīti, taču nav piešķirti pietiekami resursi. Nav izpratnes par COF jēdzienu un to, kad un kā ir jāpiemēro COF metodes. Vajadzības gadījumā izmanto COF stratēģijas un COF procesus, tomēr tiek izvirzīti argumenti, ka tas nav nepieciešams. COF stratēģija netiek uzskatīta par svarīgu, lai panāktu organizācijas drošību un efektivitāti.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam tiek atzīts, kādu vērtību var dot speciālās zināšanas par cilvēkfaktoru un organizatoriskajiem faktoriem. Organizācijā visi izprot cilvēkfaktora un organizatorisko faktoru jēdzienu, un visi saprot, cik svarīgi ir izmantot sistemātisku pieeju cilvēkfaktoram un organizatoriskajiem faktoriem, lai panāktu efektīvu drošību organizācijā. Visās organizācijas daļās tiek piemērota sistemātiska COF pieeja. Pārsvarā izmanto COF stratēģiju, procesus un metodes, taču ne vienmēr, un COF tiek piešķirti resursi. COF kompetences prasības attiecībā uz dažādām funkcijām Ir aprakstītas un izpildītas. COF tiek ņemti vērā pārmaiņu pārvaldībā. COF koncepcija ir pazīstama ikvienam organizācijas loceklim, un ikviens saprot, ka ir svarīgi sistemātiski izmantot cilvēkfaktoru un organizatoriskos faktorus organizācijas drošības un efektivitātes sasniegšanai.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam sistemātisku COF pieeju konsekventi piemēro visās organizācijas daļās. COF pieeja ir neatņemama visu procesu daļa. Galvenā uzmanība nav pievērsta juridisko COF prasību izpildei, bet gan COF pieejas piemērošanai tādā veidā, kas atbilst uzņēmuma mērķiem. Organizācijā ikviens saredz COF pieejas piemērošanas priekšrocības attiecībā uz drošību, efektivitāti un kvalitāti. COF spējas tiek mērītas, pielāgotas un samērotas ar organizācijas briedumu un sarežģītību, un laika gaitā uzmanība tiek pievērsta uzlabojumiem. Izstrādes procesā izmanto cilvēkfaktora un organizatorisko faktoru pasākumus, lai validētu jaunus mijiedarbības veidus un rīkus, un izmaiņas automatizētajās funkcijās vai jaunas automatizētas funkcijas tiek novērtētas īpašos cilvēkfaktora pētījumos. Procedūru izstrādē un to struktūras un satura veidošanā tiek izmantotas cilvēkfaktora metodes, piemēram, uzdevumu analīzes un izmantojamības analīze, un reālsimulācijās tiek iesaistīti esošie operatīvie darbinieki, lai optimizētu procedūras. Ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītā spēja tiek mērīta, pielāgota un ir samērīga ar organizācijas brieduma un sarežģītības pakāpi un vērsta uz uzlabošanos laika gaitā.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam veids, kā organizācija sevi prezentē, ir gaismas signāls citām organizācijām. Organizācijai ir skaidrs tās raksturs un juridiskie pienākumi, kā arī tā cenšas attīsties, pamatojoties uz savām stiprajām pusēm un izmantojot pieredzi, kas iegūta ne tikai dzelzceļa nozarē, bet arī ārpus tās. Organizācija ir cilvēkfaktora jautājumu risināšanas nozīmīguma drošības pārvaldībā aktīva veicinātāja. Ir atzīts, ka cilvēki ir būtiski svarīgi organizācijas panākumu gūšanā, un to ņem vērā ikreiz, kad tiek pārskatīta darbības un uzņēmuma attīstība. Lietotāji ir izstrādes procesa centrā. Organizācija ir vērsta uz āru, mācās no ieinteresētajām personām un citām nozarēm un meklē ārējas iespējas, kā uzlabot savu efektivitāti un drošību, un, to darot, ņem vērā ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītos jautājumus.

4.5 OP – ekspluatācija

Mērķis

Pareiza operatīvo darbību, saskarņu un pārmaiņu pārvaldība ļaus organizācijai izpildīt savus juridiskos pienākumus, elastīgi reaģēt uz mainīgiem apstākļiem un nodrošināt darbinieku pozitīvu rīcību. Tas savukārt ļaus organizācijai sasniegt tās darbības mērķus un vajadzības.

Ievada piebildes

Šajā sadaļā ir ietvertas tās *SMS* daļas, kas attiecas uz mijiedarbību (piemēram, ar darbuzņēmējiem, piegādātājiem un avārijas dienestiem), aktīvu pārvaldību laika gaitā un pārmaiņu pārvaldību. Jebkurai organizācijai ir izšķiroši svarīgi konstruktīvi un efektīvi pārvaldīt šīs jomas visas darbības interesēs. Tā ir *SMS* daļa, kas nodarbojas ar dzelzceļa uzņēmuma vai infrastruktūras pārvaldītāja darbības praktiskajiem aspektiem. Šajā sadaļā ir skaidras saites ar vispārējo *SMS* efektivitātes uzraudzību. Šajā jomā ietilpst arī tās darbības daļas, kas visvairāk spēj izraisīt reputācijas zaudējumus, nepietiekami pārvaldot uzņēmējus, piegādātājus vai mijiedarbību. Šai sadaļai ir arī cieša saikne ar savstarpējas izmantojamības tehnisko specifikāciju attiecībā uz "satiksmes nodrošināšanas un vadības" apakšsistēmu (SITS-OPE), kas nosaka operatīvās pamatprocedūras, kas jāievēro visās funkcionālajās darbības jomās. Tā kā valsts drošības iestādēm ir jāapstiprina atbilstība SITS-OPE, šie elementi ir jāpārbauda uzraudzības laikā.

4.5.1 OP1 – darbības plānošana un kontrole

Mērķis

Organizācijai jānodrošina, ka tehniskās un ekspluatācijas prasībās, kas izriet no riska novērtēšanas, ņem vērā attiecīgās savstarpējas izmantojamības tehniskās specifikācijas, kas attiecas uz ekspluatāciju un satiksmes vadības apakšsistēmām. Ja ir piemērojami valsts noteikumi, tos izpilda, plānojot, īstenojot un pārskatot attiecīgos darbības procesus.

Augsta līmeņa organizācijā būs stabilas sistēmas, lai panāktu atbilstību tehniskiem un operatīviem norādījumiem, kā arī kultūra, kas to atbalsta, un tā vienmēr centīsies veikt uzlabojumus, apsverot inovācijas dzelzceļa nozarē un citās nozarēs.

1. līmenis – nepietiekams

Operatīvās darbības tiek veiktas, neņemot vērā ilgtermiņa stratēģijas un citas darbības vajadzības. Ja operatīvās darbības ir saistītas ar personāla kompetenci un pārvaldību, tās tiek risinātas nesistemātiski.

Riska novērtēšanas procesi netiek pareizi piemēroti operatīvajām darbībām. Procedūru, kas atspoguļo operatīvās kontroles jautājumus, ir maz vai tās nav izveidotas tā, lai atspoguļotu darba faktisko situāciju, nevis idealizētu versiju, tāpēc ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītie jautājumi faktiski nav ņemti vērā operatīvo darbību īstenošanā.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

Atbilstība SITS-OPE noteiktajiem darbības pamatprincipiem ir ierobežota vai netiek ievērota.

2. līmenis – pamata

Organizācija ņem vērā atbilstošās savstarpējas izmantojamības tehniskās specifikācijas un attiecīgā gadījumā valsts noteikumus, tomēr tas nenotiek sistemātiski un papildu pasākumi nav skaidri pamatoti ar riska novērtējuma rezultātiem.

Darbinieki apzinās vietējās funkcijas un atbildību par operatīvajām darbībām, kas tos ietekmē, bet neiesaistās to plānošanā vai organizēšanā.

Dažas operatīvās darba procedūras, jo īpaši drošībai būtiskās, tiek izstrādātas, taču tas nenotiek sistemātiski, tātad daži cilvēkfaktori un organizatoriskie faktori tiek ņemti vērā, bet parasti maz.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

SITS-OPE tiek ievērotas, bet tikai minimālajā pieņemamajā līmenī.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam riska novērtēšanas procesā, ko piemēro operatīvajām darbībām, pastāvīgi ņem vērā procesu un procedūru pārvaldību, kas paredzēta, lai nodrošinātu, piemēram, vilcienu ceļu pareizu plānošanu, nosedzot attiecīgi riskus saistībā ar personālu, kas tos ekspluatē.

Kompetenču pārvaldības, informācijas un komunikācijas procesus konsekventi piemēro operatīvās darbības procesiem.

Pastāv saskaņots process, lai nodrošinātu uzdevuma patiesās būtības atspoguļošanu procedūrās. Ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītie jautājumi tiek konsekventi ņemti vērā visā organizācijā.

SITS-OPE tiek konsekventi ievērotas organizācijas darbībā.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus ir operatīvo darbību pārvaldības sistēma, kuru pamatā ir riska novērtējums visā organizācijā. Šajās sistēmās ņem vērā dinamisko ietekmi, kāda operatīvajām darbībām vienā darbības jomā (piemēram, signalizācijas prasības ietekmē, kā notiks nepieciešamā sliežu ceļa tehniskā apkope) ir uz citu jomu, un mēģina to paredzēt riska novēršanai.

Organizācijas darbinieki pieņem kultūru, kas ļauj viņiem pozitīvi ietekmēt operatīvās darbības un visas tajās veiktās pārmaiņa.

Komunikācija un informācijas apmaiņa par operatīvajām darbībām ir stabila, un augstākā vadība uzrauga procesa efektivitāti.

Darbības procedūras ietver mijiedarbības pasākumus starp dažādiem uzdevumiem un tostarp darbuzņēmēju uzdevumiem. Notiek datu vākšana, kas tiek izmantota, lai noteiktu cilvēka veiktspēju. Visā organizācijā tiek izmantota proaktīva pieeja ar cilvēkfaktoru un organizatoriskajiem faktoriem saistīto jautājumu noteikšanā un pārvaldībā.

SITS-OPE izklāstītos darbības pamatprincipus sāk izmantot kā līdzekli dinamiska darbību elementa vadīšanai drošības pārvaldības sistēmā.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam organizācija nepārtraukti meklē veidus, kā uzlabot savas operatīvās darbības, veicot nākotnes iespēju izpēti dzelzceļa nozarē un ārpus tās. Visu līmeņu personāls tiek iesaistīts šajā procesā un var to veicināt.

Organizācija aktīvi, darbojas novērtējot panākumus izpratnē par procedūrām un uzdevumu patieso būtību, un mēģina to izmantot, lai uzlabotu savu darbību drošību un efektivitāti. Tāpēc cilvēkfaktors un organizatoriskie faktori tiek labi pārvaldīti un organizāciju uzskata par līderi šajā jomā.

SITS-OPE izklāstītie darbības pamatprincipi ir neatņemama drošas vilcienu ekspluatācijas daļa, un organizācija tos aktīvi izplata starp līdzīgiem uzņēmumiem kā labo praksi.

4.5.2 OP 2 – aktīvu pārvaldība

Veiksmīga aktīvu pārvaldība ir saistīta ar organizācijai piederošo aktīvu, ko tā pārvalda, identificēšanu. Tā iekļauj arī sistēmas, ar ko nodrošina, ka aktīvi to dzīves cikla laikā saglabājas labā stāvoklī un tiek izmantoti tikai paredzētajā darbības jomā, lai organizācija varētu droši, produktīvi un efektīvi sasniegt tās darbības mērķus. Šī sadaļa attiecas uz visiem drošībai būtiski nozīmīgajiem aktīviem. Šajā kontekstā atsauce uz aktīvu pārvaldību attiecas uz aktīvu dzīves cikla pārvaldību no to izveides līdz likvidācijai. Visbeidzot, organizācijai ir jāpierāda, ka tā ir izmantojusi uz indivīdu vērstu pieeju katrā aktīvu dzīves cikla posmā.

1. līmenis – nepietiekams

Aktīva un operatīva tehniskā apkope tiek veikta saskaņā ar grafikiem, bet nav visaptveroša aktīvu reģistra, tāpēc organizācija nevar būt pārliecināta, ka visi aktīvi tiek uzturēti drošā stāvoklī.

Aktīvi tiek veidoti, ierobežoti ņemot vērā turpmākās uzturēšanas vajadzības, cilvēkfaktora ietekmi vai spēju likvidēt aktīvus drošā veidā pēc to dzīves cikla beigām.

Jauna aprīkojuma plānošanai un izveidei ir maz vai nav kritēriju.

Aktīvu tehniskās apkopes plānā ir nepilnības, tāpēc nav iespējams pārliecināties par kāda aktīva pienācīgu uzturēšanu visā tā darbības laikā.

Notiek informācijas apmaiņa par aktīvu stāvokli, taču tā nav pilnīga.

Vajadzības gadījumā aktīvu pārvaldības sistēma pievērš uzmanību atbilstībai savstarpējas izmantojamības pamatprasībām.

Lai gan darbinieki tiek apmācīti, nav pietiekami daudz pierādījumu visaptverošas kompetenču pārvaldības sistēmas pastāvēšanai.

Aktīvu reģistra pārvaldība nav aktuāla.

Lietošanas ierobežojumu reģistrēšanai nav sistēmas, un sistēma objektu izņemšanai un atgriešanai pakalpojumā ir nepilnīga.

Aktīvu veidošana koncentrējas uz komerciālo pieejamību, nevis atspoguļo lietotāja vajadzības.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Lielākajai daļai aktīvu ir izstrādāti pārbaudes un tehniskās apkopes grafiki, tomēr ne visiem.

Pārbaužu biežums ir norādīts, bet ne vienmēr balstīts uz risku.

Pārbaužu biežuma neievērošana netiek skaidri pārvaldīta, un uzkrājas nepadarīti darbi.

Kopējā aktīvu pārvaldības politika nav skaidri paredzēta drošības uzlabošanai. Daži aktīvi ir izveidoti, ņemot vērā ieguvumus drošībā, tostarp risinot ar cilvēkfaktoru saistītus jautājumus, bet tie ir atsevišķi piemēri un nav visaptveroša plāna daļa.

Aktīvu pārbaudes process pats virza aktīvu pārvaldību, nevis aktīvu stāvoklis. Informācija tiek kopīgota, tomēr nesniedz pilnīgu priekšstatu par aktīvu pēc tā izveides. Informācija par to, kā un kad likvidēt aktīvu, ir ierobežota.

Pastāv labāks aktīvu reģistrs ar norādēm par ierobežojumu piemērošanu, kas attiecas uz iekārtām, kuras atgriežas pakalpojumā.

Aktīvu Izveides pamatā ir nevis strukturēta pieeja, bet gan veselā saprāta, darba pieredzes un personisko vēlmju apkopojums.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, bet papildus ir atjaunināts aktīvu reģistrs un pārbaudes un tehniskās apkopes grafiki ir balstīti uz risku, kā arī tos ievēro.

Pārbaudes var aizkavēties, taču to atzīst un pārvalda ar ieviestajiem riska mazināšanas pasākumiem.

Pārbaužu biežums tiek pārskatīts, un ir iespēja pielāgoties pārmaiņām aktīvu stāvoklī.

Aktīvus izmanto paredzētajam mērķim, vienlaikus saglabājot to paredzēto ekspluatācijas stāvokli un risinot ekspluatācijas problēmas gan normālos, gan traucētos darbības režīmos. Lielākajai daļai aktīvu ir projekta dokumentācija, kas ietver cilvēkfaktora ievērošanu, un šī informācija ir daļa no pamatinformācijas, atbilstoši kurai tiek veiktas pārbaudes. Lielākajai daļai aktīvu ir likvidācijas plāni ar skaidru norādi par pārvaldītu izslēgšanu no aktīvu bāzes.

Tiek izmantoti pieejamie projektēšanas standarti, ar kuriem ņem vērā cilvēkfaktora principus, un paraugprakse. Ir izveidots koncepcijas testa režīms, ietverot cilvēkfaktora jautājumus. Galalietotāji sniedz ieguldījumu prasību definēšanā un testēšanas procesā. Pārmaiņu procesu pārvaldība (skat. xxx "Pārmaiņu pārvaldība") ietver cilvēkfaktora jautājumus kā projekta izskatīšanas daļu.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam pārbaužu biežums tiek sistemātiski pārskatīts, ir balstīts uz riskiem un sistēma ļauj to elastīgi pielāgot pārmaiņām aktīvu stāvoklī īstermiņā un ilgtermiņā.

Izveides dati ir pieejami par visiem aktīviem, un tiem ir skaidri noteikts virziens uz pārvaldīto likvidāciju. Ir skaidrs mehānisms, kā aktīvu pārvaldīšanas procesā iekļaut informāciju par aktīvu stāvokļa pārmaiņām un likvidēt aktīvus, kuru dzīves cikls ir beidzies.

Tā vietā, lai reaģētu uz pārmaiņām aktīvu stāvoklī, organizācija vēlas iepriekš uzzināt par aktīvu stāvokļa pārmaiņām, izmantojot, piemēram, attālinātu aktīvu uzraudzību, un spēj izvietot nepieciešamos resursus to pārvaldībai.

Organizācijai ir skaidrs plāns nākotnes aktīvu izveidošanai un pārvaldībai, ar ko uzlabo drošību.

Galalietotāju atsauksmes par pašreizējām koncepcijām tiek izmantotas jaunu aktīvu plānošanai. Cilvēkfaktora apsvērumi ir neatņemama koncepciju izstrādes procesa daļa.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam pārbaudes biežumu un grafiku pārskatos ietver informāciju ārpus organizācijas vai dzelzceļa nozares.

Organizācija vēlas attīstīt savu aktīvu pārvaldības politiku, ievērojot nozares un labāko pasaules mēroga praksi šajā jomā.

Organizācijai ir visaptveroša aktīvu pārvaldības sistēma, kas seko aktīviem kopš to izveides, ekspluatācijas laikā un līdz likvidācijai. Organizācija piemēro jaunāko pieeju aktīvu pārvaldībai, lai nodrošinātu drošības uzlabošanos un attīstību laika gaitā.

Ar attālinātās aktīvu pārvaldības sistēmām sniedz detalizētu informāciju par visu aktīvu stāvokli, un tā nonāk organizācijas riska pārvaldības politikā, lai aktīvus uzturētu attiecīgā stāvoklī.

Pastāv visaptveroša kompetenču pārvaldības sistēma, kas veicina personāla, kurš atbild par aktīvu pārvaldīšanu, attīstību, nodrošinot tā attiecīgu apmācību un tam nepieciešamās zināšanas un prasmes, lai veiktu darbu, par kuru tas atbild.

Aktīvu koncepciju pamatā ir dziļas zināšanas par to, kas ir aktīvs un kā to izmanto. Organizācija cenšas izmantot cilvēkfaktora principa labāko praksi, lai apgūtu aktīvu izveidi, uzturēšanu un likvidāciju.

4.5.3 OP3 – darbuzņēmēji, partneri un piegādātāji

Organizācijām ir efektīvi jāuzlabo savu darbuzņēmēju, partneru un piegādātāju, kā arī to drošība, kurus ietekmē to darbības, neatkarīgi no šo darbību veikšanas vietas.

Tas nav tikai riska novērtēšanas jautājums, un tam nav arī nepieciešams visu risku vai attiecīgā riska kategoriju saraksts, bet pieteikuma iesniedzējam ir jāparāda, ka tā sistēmas un procedūras kopumā ir izstrādātas un organizētas tā, lai atvieglotu šo risku identificēšanu, novērtēšanu un kontroli. Labi sagatavotu līgumu izmantošana ir vispāratzīts veids risku pārvaldībai. Tomēr galvenais atbildīgais par darbuzņēmēju pārvaldību un to nodevumu pārbaudi saskaņā ar noteiktajām specifikācijām ir dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs. Darbuzņēmēju vai apakšuzņēmēju izmantošana nenozīmē, ka dzelzceļa pārvadājumu uzņēmums / infrastruktūras pārvaldītājs deleģē jebkuru no saviem pienākumiem nodrošināt līgumā paredzēto pakalpojumu izpildi saskaņā ar standartiem, kas noteikti pirms darbības.

Pieteikuma iesniedzējam ir jāpierāda, ka tam ir izstrādāti procesi, lai noteiktu darbuzņēmēju un citu piegādātāju kompetenci un novērtētu to drošības rādītājus kā daļu no iepirkuma procesa.

Galvenie darbuzņēmēja kontroles elementi ir šādi:

- skaidri definēti līguma nosacījumi;
- skaidri noteikta darba specifikācija;
- darbuzņēmēja izvēle;
- darbuzņēmēja iepazīstināšana ar objektu (ja nepieciešams);
- produktu drošības un kvalitātes kontrole;
- atļauja strādāt (ja nepieciešams);
- darba nodošana un pieņemšana tā beigās; un
- veiktspējas uzraudzība un pārskatīšana.

Kāda vai visu iepriekš minēto elementu trūkums vai nepilnīgums būs svarīgs rādītājs lēmumu pieņemšanā organizācijas brieduma līmenī.

1. līmenis – nepietiekams

Uzņēmuma potenciālā ietekme uz uzņēmuma drošības rādītājiem darbuzņēmēja izmantošanas jomā netiek novērtēta, un izrietošās organizatoriskās pārmaiņas netiek pienācīgi pārvaldītas. Organizācija īpaši necenšas identificēt vai sadarboties darbā ar citām organizācijām attiecībā uz kopīgotu risku kontroli. Darbuzņēmuma līgumi, ja tādi pastāv, neņem vērā drošības ierobežojumus, un darbuzņēmējs neapzinās savu atbildību par drošību. Procedūras, kā to panākt, ir vājas vai arī to nav. Kultūras ziņā pastāv tendence nekopīgot informāciju attiecībā uz risku kontroli.

Informācija netiek vākta vai kopīgota, un līguma noteikumi to neprasa.

Darbuzņēmējus nozīmē, kad nepieciešams. Tomēr, izvēloties darbuzņēmējus, ir maz ar izmaksām nesaistītu apsvērumu. Piemēram, līgumslēdzēja agrākie drošības rādītāji nav starp atlases kritērijiem iepirkuma procesā. Darbu maz plāno un maz uzmanības pievērš risku kontroles pienākumiem, lemjot par darba izpildes veidu.

Darbuzņēmēju uzraudzībai vai pabeigtā līguma pārskatīšanai tiek pievērsts maz uzmanības. Īstas cilvēkfaktora un organizatorisko faktoru stratēģijas nav, bet tas, kas ir, uz darbuzņēmējiem, partneriem un piegādātājiem neattiecas.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Ar procedūrām faktiski nosaka mijiedarbības starp struktūrvienībām darba līmenī. Sadarbība ar pārējām organizācijām ir saistīta ar īstenojamām procedūrām un standartiem, taču tā nav sistemātiska. Darbinieki to izmanto dažām kopīgotām risku pārbaudēm, kas šajā līmenī ir identificētas.

Daži risku kontroles sistēmas elementi ir paredzēti darbuzņēmēja kontrolei, taču šķiet, ka nav sistemātiska procesa no to atlases līdz pārskatīšanai pēc līguma.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

Cilvēkfaktora un organizatorisko faktoru stratēģija pienācīgi neaptver darbuzņēmējus, partnerus un piegādātājus.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus sistemātiski tiek identificēta organizatoriskā mijiedarbība ar darbuzņēmējiem, partneriem un piegādātājiem.

Ir ieviestas procedūras un standarti, lai kontrolētu kopīgus riskus, ar pusi, kas ir atbildīga par skaidri identificēto.

Pastāv rakstveidā definēti sistēmas drošības mērķi, un tos ņem vērā, izstrādājot līguma noteikumus.

Notiek regulāras diskusijas ar citām organizācijām, ar kurām ir mijiedarbība, lai vienotos par mērķiem, standartiem, procesiem un kārtību.

Pastāv veidi, kā kopīgot informāciju darba līmenī.

Komunikācija ārpus organizācijas ir pietiekama, lai pārliecinātos, ka ikvienam, kurš pieņem lēmumu par riska kontroli ar starporganizatoriskām robežām, ir pareizā informācija (procedūru un standartu veidā), faktiskie dati un izlūkdati, kā arī instrukcijas un ziņojumi.

Tiek atzīta darbuzņēmēju kontroles nozīme, un tas ir atspoguļots organizācijas attiecīgajā politikā.

Darbuzņēmējus izvēlas atbilstoši viņu spējai veikt darbu droši un apmierinošā līmenī.

Līguma izpildes laikā tiek uzraudzīts darbuzņēmēja sniegums, un, lai tam sekotu, tiek efektīvi izmantoti attiecīgi izpildes rādītāji.

Cilvēkfaktora un organizatorisko faktoru stratēģija aptver attiecīgus jautājumus, kas saistīti ar darbuzņēmējiem, partneriem un piegādātājiem, tāpēc ir skaidrs, kādas ir viņu funkcijas un pienākumi savu darbinieku pārvaldībā.

4. līmenis – prognozēšana

Lēmumi un pasākumi atbilst visai informācijai, kas sniegta 3. līmenī.

Visā organizācijā ir pasākumi informācijas apmaiņai, lai veicinātu efektīvu pārskatīšanu un pastāvīgu uzlabošanu.

Pastāv sistemātiska pieeja darbuzņēmēju kontrolei.

Efektīva atbilstības prasību sistēma izmanto līdzsvarotu pieeju, tostarp ņemot vērā potenciālo darbuzņēmēju drošības rādītājus.

Visos līguma darbības posmos ir skaidra atbildības izpratne. Labas darba attiecības starp pasūtītāju un visiem darbuzņēmējiem tiek nodrošinātas, izmantojot efektīvus mijiedarbības pasākumus, tostarp cilvēkfaktora un organizatorisko faktoru stratēģiju, caur kuras prizmu aplūko organizācijas attiecības ar tās darbuzņēmējiem, partneriem un piegādātājiem.

Ar darbības rādītāju izvērtējumu un pārskatīšanu pēc līguma izpildes nosaka lēmumus par līgumslēdzēju izvēli turpmākajam darbam.

Pastāv sistēma, ar ko nodrošina nepieciešamo attiecīgo lēmumu izsekojamību, komunikāciju u. tml.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam organizācija pievērš uzmanību citiem sektoriem un valstīm sistēmas drošības problēmu un sasniegumu identificēšanai, lai vajadzības gadījumā iekļautu tos savu darbuzņēmēju, partneru un piegādātāju pārvaldības pasākumos.

Lai labāk sasniegtu kopīgos mērķus, tiek izmantots uzņēmuma un tā darbuzņēmēju, partneru un piegādātāju komandas darbs.

Labu praksi kopīgo ar citām organizācijām, tostarp darbuzņēmējiem, partneriem un piegādātājiem.

Līgumslēdzēja piegādes ķēde nevainojami nodrošina visus organizācijas mērķus.

Darbuzņēmēja un organizācijas galvenie un drošības pasākumi ir saskanīgi.

Darbuzņēmēja darbinieku un uzņēmuma darbinieku attieksme neatšķiras, jo visi saņem vienādu apmācību un informāciju pārliecībai par savu drošību. Cilvēkfaktora un organizatorisko faktoru stratēģija ir veidota tā, ka to piemēro visām pusēm vienādi.

4.5.4 OP4 – pārmaiņu pārvaldība

Pārmaiņu pārvaldības mērķis ir nodrošināt, lai pārmaiņas organizācijā tiktu pienācīgi plānotas saskaņā ar ES prasībām un pārbaudītas, lai palīdzētu organizācijai sasniegt tās darbības mērķus. Ar efektīvu pārmaiņu pārvaldību kontrolē riskus, ko rada pārmaiņas, un palīdz organizācijai pieņemt pareizo lēmumu, lai uzlabotu savu darbību, nemazinot drošību.

Šim procesam ir jāļauj novērtēt riskus proporcionāli un stingri, vajadzības gadījumā iekļaujot cilvēkfaktora jautājumus, kā arī pieņemt attiecīgus kontroles pasākumus.

1. līmenis – nepietiekams

Daži pārmaiņu veidi ir atzīti, un to aspekti tiek pārvaldīti.

Nav identificēti visi riski, kas saistīti ar pārmaiņām, un tādēļ tos neņem vērā.

Pārmaiņu ietekme uz organizācijas kultūru netiek vērtēta.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Ir izprasta pārmaiņu pārvaldības nozīme, un ir zināma kontrole pār visu veidu pārmaiņām.

Pārmaiņas tiek plānotas, bet ne vienmēr ir piemērotas.

Pārmaiņu plānošanas sistēma nav skaidra, tāpēc risku identificē vai kontrolē pēc pārmaiņām, nevis pirms tās notiek.

Pārmaiņu ietekmi uz organizācijas kultūru ņem vērā ļoti minimāli.

Funkcijas un pienākumi attiecībā uz pārmaiņu pārvaldību un saistītie drošības riski nav skaidri definēti.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam ir efektīva pieeja visu procesu, organizatorisko un inženiertehnisko izmaiņu pārvaldībai.

Var būt izveidota strukturēta pieeja pārmaiņām, ietverot vairākus soļus pārmaiņu pārvaldības sistēmā.

Pastāv konsekventa pieeja riska novērtēšanai un riska kontrolei pirms un pēc pārmaiņu veikšanas. Riska novērtēšana ir pārmaiņu pārvaldības procesa būtiska daļa.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam pārskatīšanu veic pēc pārmaiņām, lai ņemtu vērā arī ietekmi, ko pārmaiņas atstājušas uz organizācijas kultūru.

Ir ieviests visaptverošs jautājumu reģistrācijas žurnāls, lai fiksētu attīstību, kas notiek pārmaiņu laikā.

Ir atzīts, ka, lai gūtu labumu, pārmaiņu procesā ir svarīgi iesaistīt darbiniekus.

Pastāv procedūra drošības pārvaldības sistēmas pārmaiņu plānošanai, ieviešanai un kontrolei, kad tās notiek pārmaiņu laikā.

Ir atzīts, ka, lai gūtu labumu, pārmaiņu procesā ir svarīgi iesaistīt darbiniekus.

Pārmaiņu pārvaldības process ietver ierosināto pārmaiņu ietekmi uz partneriem, piegādātājiem un citiem, ar kuriem organizācijai ir mijiedarbības.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus pastāv arī izpratne, ka pārmaiņas ietekmē citus darbības aspektus. Tādējādi darbības risks ir saistīts ar drošības risku jebkādu pārmaiņu laikā un to dēļ.

Pieņēmumus, kas izdarīti par pārmaiņām un to laikā, pārbauda, un tiek veikti atbilstoši ārkārtas pasākumi, ja pieņēmumi izrādās neprecīzi.

4.5.5 OP5 – ārkārtas situāciju pārvaldība

Stabilas plānošanas sistēmas ir būtiskas jebkurai atbildīgajai personai, un tajās ir jāiekļauj informācija, kas jāsniedz avārijas dienestiem, lai viņi varētu izstrādāt savus rīcības plānus avārijas situācijām.

Ārkārtas situāciju plānošanas elementi ietver:

- paredzamu ārkārtas situāciju identificēšanu;
- pasākumu izstrādāšanu rīcībai šādās ārkārtas situācijās;
- atbilstošas apmācības nodrošināšanu un pārliecināšanos, ka ir pieejami nepieciešamie resursi; un
- plānu pārbaudi, ja nepieciešams, ar citiem cilvēkiem un organizācijām.

1. līmenis – nepietiekams

Organizācija maz identificē iespējamās ārkārtas situācijas un kā rīkoties, ja tās rodas.

Organizācija paļaujas uz avārijas dienestiem, lai risinātu visus ārkārtas situācijas aspektus, un tai nav pasākumu plāna ar citiem dalībniekiem, kuri var būt iesaistīti avārijas pārvaldībā, izņemot aicināt viņus un ļaut viņiem tikt galā ar atgadījumu.

Organizācijas darbības līmenis ir zemāks, nekā noteikts konkrētajam vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Organizācija ievēro noteikumus un praksi, ko pieprasa ārējas struktūrvienības/organizācijas, piemēram, infrastruktūras pārvaldītājs vai citi dzelzceļa pārvadājumu uzņēmumi, un ir izveidota ārkārtas situāciju pārvaldības sistēma.

Ir identificētas avārijas situācijas, kas varētu rasties, un ir izstrādāti zināmi plāni, kā rīkoties to gadījumā.

Darbiniekus apmāca rīcībai ārkārtas situācijās tikai tad, ja tas ir absolūti nepieciešams.

Ir procedūras rīcībai ārkārtas gadījumos, ko bieži sagatavo citas iestādes/organizācijas un kas ir pieņemtas iekšēji.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam iespējamās ārkārtas situācijas, kas rodas no uzdevumiem, ir identificētas kā riska novērtējuma daļa.

Ir izstrādāti kontroles pasākumi, iekļaujot apmācību un resursus, lai risinātu ārkārtas situācijas un kopīgotu informāciju ar attiecīgajām pusēm.

Notiek mācības rīcībai ārkārtas situācijās kopīgi ar citām organizācijām, kas ir iesaistītas uzdevumā.

Ir pieejamas visaptverošas procedūras rīcībai ārkārtas situācijās, kurās vajadzības gadījumā ietver arī citas organizācijas, piemēram, avārijas dienestus vai vietējās iestādes.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam, pārskatot procedūras, ņem vērā atgriezenisko saiti no procedūru pārskatiem, lai nodrošinātu, ka pasākumi rīcībai ārkārtas situācijās ir aktuāli un efektīvi.

Notiekot smagiem starpgadījumiem, Starp organizāciju, avārijas dienestiem un citiem iesaistītajiem dalībniekiem notiek regulāra sadarbība, lai nodrošinātu, ka procesa/procedūru un tehnisko jautājumu pārmaiņas tiek pienācīgi ņemtas vērā un mainītas pārmaiņu pārvaldības procesā.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam organizācija pārņem labu praksi ārkārtas situāciju pārvaldībā, jo īpaši mijiedarbības koordinācijā, gan dzelzceļa nozarē, gan ārpus tās. Regulāra sadarbība ar avārijas dienestiem ir aktīva, ar mērķi izstrādāt labākus pasākumus kopīgai rīcībai turpmāku starpgadījumu gadījumā.

4.6 PE – darbības rādītāju novērtējums

Mērķis

Novērtējuma mērķis ir pārliecināties, ka riska kontroles pasākumi ir izveidoti un darbojas pareizi, sasniedzot organizācijas mērķus.

Ievada piebildes

Organizācijām ir jānovērtē riska kontroles efektivitāte, lai pārliecinātos, ka riski tiek identificēti un pārvaldīti praksē. Ir jāuzrauga droša darba sistēmas, lai pārliecinātos par to atbilstību un ievērošanu. Lai nodrošinātu, ka drošības pārvaldības sistēma darbojas pareizi, jābūt izveidotām sistēmām darbības rādītāju uzraudzībai, revīzijai un pārskatīšanai.

Revīzijā pārbauda, vai organizācija dara to, ko tā apgalvo. Tās atbalstam ir regulāri jāveic pārskatīšanas, lai pārliecinātos, ka organizācijas darbības mērķi ir pareizi. Pārskatot arī jāpārliecinās, vai pasākumi, kas ieviesti darbības mērķu sasniegšanai darbojas, kā plānots.

Uzraudzība, revīzija un pārskatīšana veido atgriezeniskās saites cilpu vispārējā drošības pārvaldības sistēmā un ir būtiskas pastāvīgas uzlabošanas un izcilības sasniegšanas programmu daļa.

4.6.1 PE1 – uzraudzība

Organizācijai jāspēj pierādīt, ka tā ir izveidojusi drošības pārvaldības sistēmas piemērošanas un efektivitātes uzraudzības procesu un ka šis process atbilst tās darbības apjomam, mērogam un veidam. Organizācijai ir jāpierāda, ka ar šo procesu var identificēt, novērtēt un izlabot jebkādus *SMS* darbības traucējumus.

1. līmenis – nepietiekams

Nav efektīva procesa drošības kritēriju noteikšanai, datu vākšanai un analīzei. Izpratne par to, vai esošie riska kontroles pasākumi darbojas efektīvi, Ir vāja vai tās nav vispār.

Nav izprasta uzņēmuma nepieciešamība pārvaldīt un novērtēt cilvēkfaktora un organizatorisko faktoru jautājumus. Ja tos ņem vērā, tad pēc ad hoc *principa.*

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

Nav atzīta vajadzība pārraudzīt organizācijas drošības kultūru.

2. līmenis – pamata

Uzraudzība tiek īstenota, bet tas bieži notiek ad hoc*: daži procesi tiek uzraudzīti un dažas iekārtas tiek pārbaudītas, tādējādi pieeja datu vākšanai ir nekonsekventa.*

Dokumentācija ir nodalīta un netiek analizēta uzņēmuma līmenī. Tā sekas ir pieeja rīcības plāniem, kas nav skaidri definēta un nav saskaņota uzņēmuma līmenī.

Nav skaidras saiknes starp drošības politiku, uzņēmuma drošības mērķiem un uzlabošanas rīcības plāniem.

Vadība neatzīst vajadzību uzraudzīt riska kontroli, un atsevišķu nodaļu vai vienību ziņā ir izlemt, kādu informāciju apkopot.

Ir atzīts, ka cilvēkfaktoram un organizatoriskajiem faktoriem ir nozīme uzņēmējdarbībā, tomēr to piemērošana nav konsekventa.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

Organizācijas drošības kultūra tiek uzraudzīta ierobežotā apmērā.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus organizācija mēģina izmantot piemērojamo kopīgās drošības metodi, lai pārbaudītu drošības pārvaldības sistēmas pareizu izmantojumu un visus tajā ietvertos procesus un procedūras, kā arī īsteno visus korektīvos pasākumus, kas nepieciešami identificēto neatbilstību dēļ.

Uzraudzību nosaka process, tāpēc būtiski svarīgās un neaizsargātās sistēmas nav prioritāras attiecībā uz mazāk būtisku vai neaizsargātu sistēmu uzraudzību. Rādītāju izvērtēšana notiek vērtēšanas pēc, nevis ar skaidri noteiktu mērķi.

Saikne ar riska novērtējumu aprobežojas ar riska kontroles pasākumu identificēšanu, kurus pēc tam uzrauga loģiskā veidā.

Uzraudzības stratēģija ir definēta, un ir izstrādāti plāni tās īstenošanai. Tādējādi pieeja datu vākšanai un analīzei ir konsekventa, un vadība izmanto informāciju, lai pieņemtu lēmumus un uzlabotu organizāciju.

Resursu piešķiršanai uzraudzībai nav noteiktas prioritātes saskaņā ar riska novērtējuma rezultātiem.

Darbības rādītāju novērtēšanā ir apstiprināts process, lai pārbaudītu cilvēkfaktora un organizatorisko faktoru jautājumu ietekmi SMS *darbībā. Tā novērtēšanai vajadzības gadījumā ir pieejamas speciālistu īpašās zināšanas.*

Ir ieviests konsekvents drošības kultūras uzraudzības process.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam ir izpratne par būtisko un viegli ievainojamo sistēmu uzraudzību.

Attiecīgās KDM tiek pilnībā piemērotas, un uzraudzība ir pilnībā balstīta uz risku. Būtiski nozīmīgiem procesiem ir noteikta prioritāte resursu piešķiršanā.

Vadītāji un uzraudzītāji ir labi apmācīti, un tiem ir nepieciešamie resursi, kā arī pastāv pierādījumi par pašreizējo darba sistēmu provocēšanu pieejas trūkumu noteikšanai.

Vidējā un augstākā līmeņa vadītāji uzrauga rezultātus, pamatojoties uz riska apsvērumiem, un rīcības plānus koordinē un apspriež uzņēmuma līmenī. Uzraudzības mērķis ir paredzēt drošības rādītāju pasliktināšanos un meklēt uzlabojamās jomas, nevis tikai novērtēt SMS *rezultātus.*

Ir specifiski rādītāji, kas ļauj novērtēt cilvēkfaktora un organizatorisko faktoru ietekmi uz SMS *piemērošanu un izsekot kontroles procesu.*

Drošības kultūras uzraudzības process tiek veikts regulāri, un tā rezultāti tiek izmantoti drošības kultūras stratēģijas uzlabošanā, lai nodrošinātu pastāvīgu uzlabošanos.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam tiek izmantoti uzlaboti uzraudzības rīki. Organizācijai ir rīki, kas palīdz darbiniekiem ziņot par atgadījumiem, un ierosināt risinājumus, kas jāapspriež rīcības plānos.

Datu analītiku uzskata par konkurences priekšrocību, un drošības rādītāju uzraudzība ir iekļauta visaptverošā uzraudzības procesā, ietverot visas struktūrvienības un nodaļas. Organizācijai ir visaptveroša datu pārvaldības sistēma, lai izsekotu tās aktīvu datubāzi un izmantošanas nosacījumus.

Uzņēmums apzinās, cik svarīgi ir izmantot riska modeļus un koplietot datus un informāciju ar citiem dzelzceļa operatoriem, lai paplašinātu savas datu kopas un uzlabotu datu kvalitāti riska novērtēšanai.

Atskaitīšanās ir laba prakse, un ir novatoriski projekti, kurus veicina drošības kultūras uzlabošanas stratēģija un ar kuriem atbalsta spēcīgu drošības un pārskatu sniegšanas kultūru uzņēmumā.

Uzraudzības procedūras tiek pārskatītas, lai pārliecinātos, ka tās joprojām atbilst organizācijas riska profilam.

Dati no cilvēkfaktora un organizatorisko faktoru jautājumu kontroles ir neatņemama nepārtrauktas uzlabošanas daļa organizācijā. Rezultātus pēc tam izmanto, pieņemot lēmumus par darbību un drošības uzraudzību. Iegūto informāciju kopīgo ar partneriem, piegādātājiem un līgumslēdzējiem.

Drošības kultūras uzraudzības process ir piemērs tam, kā šādi pasākumi būtu jāveic gan organizācijā, gan ārpus tās.

4.6.2 PE2 – iekšējā revīzija

Iekšējā revīzija ir būtiska neatkarīga un sistemātiska riska kontroles sistēmu un vadības pasākumu pārbaude ar mērķi nodrošināt darbības mērķu sasniegšanu. Iekšējās revīzijas nepieciešamību nosaka arī KDM attiecībā uz uzraudzību. Revīzijas parasti ir paredzētas, lai mēģinātu ierobežot subjektivitāti, atbalstot uz pierādījumiem balstītu pieeju. Revīziju sistemātiskums *SMS* kontekstā ir paredzēts, lai sniegtu augstākā līmeņa vadībai skaidrus pierādījumus, uz kuriem balstīt lēmumus drošības rādītāju uzlabošanai.

1. līmenis – nepietiekams

Ir maz pierādījumu par revīziju veikšanu, vai arī to nav vispār.

Veiktās revīzijas nav plānotas vai prioritāras, un uz to konstatējumiem netiek reaģēts.

Revidenti netiek konsekventi apmācīti, un saikne ar KDM procesu ir nepilnīga.

Revīzijas process nav strukturēts, starp revīzijām un pārbaudēm nav reālas atšķirības.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Revīzijas vispār notiek, bet izmantotajās metodēs un aptvertajās jomās neņem vērā konkrētās riska kontroles sistēmas būtību vai nozīmību.

Ir revīziju plāni, tomēr tie nav saskaņoti.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam ir pierādījumi par koordinētu, efektīvu un plānotu pieeju revīzijām. Revīziju darbība ir vērsta uz tiesību aktu ievērošanu un darbības mērķu sasniegšanu.

Revīzijas tiek sistemātiski dokumentētas, un rezultāti tiek reģistrēti. Organizācijas valde apzinās rezultātus un apspriež tos regulāro valdes sanāksmju laikā.

Kompetenču pārvaldības sistēmā ir ietverti noteikumi par revidentu apmācību. Tiek uzturēts kompetentu revidentu reģistrs.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam plāno revīzijas pasākumus un nosaka to prioritāti, ņemot vērā iepriekšējo revīziju un uzraudzības rezultātus.

Izmanto attiecīgu revīzijas metožu kombināciju, lai sniegtu informāciju par drošības rādītājiem salīdzinājumā ar darbības mērķiem.

Augstāko vadību informē par revīziju rezultātiem, lai tā var pārskatīt drošības pārvaldības sistēmu. Šajā līmenī SMS *noteiktais nepārtrauktais uzlabojums pats ir pakļauts analīzei, lai pārbaudītu, vai uzlabojumi patiešām sniedz gaidītos ieguvumus, vai arī ir jāmaina, lai uzlabotu rezultātus.*

5. līmenis – izcilība

Tāds pats kā 4. līmenis ar papildinājumu, ka darbības mērķi, ar ko salīdzina veiktās revīzijas rezultātus, ir daudz grūtāk sasniedzami, un tādēļ tos salīdzina ar labāko praksi.

Ir iekļauti līdzīgu organizāciju revīzijas mērķi.

4.6.3 PE3 - pārvaldības pārskatīšana

Lai organizācijas drošības pārvaldības sistēma darbotos konstruktīvi un efektīvi, kā arī turpinātu attīstīties laika gaitā, ir nepieciešama spēcīga drošības līderība no vadības. Organizācijai ir jāparāda, ka vadība aktīvi iesaistās drošības pārvaldības sistēmas darbības pārskatīšanā un tās izstrādē nākotnei. Vadības līmeņa pārskatīšanu var uzskatīt par daļu no uzraudzības, ko organizācija veic, lai nodrošinātu, ka ar tās procesiem un procedūrām sasniedz paredzēto rezultātu.

1. līmenis – nepietiekams

Augstākā vadība maz nodarbojas ar uzraudzības un revīziju konstatējumu analīzi. Tas tiek vairāk darīts struktūrvienības/nodaļas līmenī.

Darbības un drošības mērķi netiek regulāri pārskatīti.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Veiktās pārskatīšanas nav iekļautas sistemātiskā pieejā uzlabošanai. Tās bieži ir stihiskas un reti tiek plānotas kā pārvaldības cikla daļa.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam vadība automātiski izmanto uzraudzības un revīziju konstatējumus, lai pārskatītu organizācijas rādītājus un vajadzības gadījumā veiktu izmaiņas.

Pārskatīšanas ieteikumi ir skaidri sadalīti, izsekojami un parāda, ka ir ņemtas vērā plašākas sekas.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus ņem vērā pieredzi, kas gūta no starpgadījumiem citās organizācijās un citās nozarēs.

Vadība prasa personālam sniegt ieteikumus darbības procesu uzlabojumiem, un izskata tos, lai redzētu, vai tie mainītu darbību.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam vadība ievieš izlases kārtā pārskatu praksi konkrētās darbības jomās, lai pārbaudītu, vai procesi un procedūras joprojām atbilst mērķim.

Vadība nodarbojas ar nākotnes perspektīvu izpēti, lai identificētu jaunas tehnoloģijas vai idejas, kas var uzlabot darbību. Piemēram, pastāv uzskats, ka liela datu apjoma izmantošana uzlabo darbības efektivitāti un drošību.

4.7 I – uzlabošana

Mērķis

Organizācijām ir jāattīstās laika gaitā, jo, ja tās to nedara, tās stagnē un kļūst pārāk bezrūpīgas. Tas galu galā rada sekas drošības pārvaldībai. Organizācijai ir jāpieņem filozofija mācīties no savām un citu kļūdām, kā arī uzlabot savus drošības pārvaldības kontroles pasākumus. Uzlabojumu pamatā esošie pamatprincipi nozīmē orientāciju uz tālredzīgu domāšanu, cenšoties paredzēt organizācijas pārmaiņas nākotnē un nodrošināt *SMS* pozitīvu attīstību, kad tās notiek.

Ievada piebildes

Organizācijā var notikt uzlabojumi, mācoties no savu negadījumu un starpgadījumu (tostarp starpgadījumu un bīstamu situāciju) izmeklēšanas, kā arī mācoties no citiem notikumiem dzelzceļa nozarē vai citās rūpniecības nozarēs. Organizācijām ir jāizpēta arī gandrīz notikuši negadījumi ar tādu pašu pamatīgumu, kā viņi izmeklētu negadījumu, lai uzzinātu, kas gandrīz noticis, kā radās situācija un kā varētu izvairīties no līdzīga atgadījuma. Ar Izmeklēšanas kopsavilkumiem un to rezultātiem ir pēc iespējas jākopīgo visā organizācijā un ar citām līdzīgām organizācijām. Organizācijām jābūt aktīvām ar domu mācīties veikt uzlabojumus, ne tikai mācoties no negadījumiem un starpgadījumiem, bet arī izmantojot jebkuru citu atbilstošu pieejamu informācijas avotu, piemēram, uzraudzību un revīziju vai citu cilvēku pieredzi, kas tai varētu palīdzēt veikt uzlabojumus.

4.7.1 I1 – mācīšanās no negadījumiem un starpgadījumiem

Negadījumu un starpgadījumu izmeklēšanā ir jāpārskata drošības pārvaldības sistēmas darbības rādītāji pirms notikuma un jānoskaidro, kādas sistēmas daļas ir darbojušās labi un kādās jomās ir vajadzīgs uzlabojums, kā arī jāizvērtē gūtās atziņas par cilvēku veiktspēju. Organizācijai ir jācenšas arī mācīties no izmeklēšanas, ko veic valsts izmeklēšanas iestādes (VII) un citas VII visā ES, kā arī no starpgadījumu un negadījumu izmeklēšanas rezultātiem visā pasaulē.

1. līmenis – nepietiekams

Efektīvas izmeklēšanas pierādījumu ir maz, un organizācijas kultūra ir atrast kādu vainīgo. Nenotiek mācīšanās no starpgadījumu izmeklēšanas, kas tiek veikta ārpus organizācijas vai citās nozarēs. Personu, kas veic izmeklēšanu, kompetenci var apšaubīt.

Ir maz vai nav norāžu, ka pienācīgi ņem vērā indivīda funkciju negadījumos vai starpgadījumos.

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

2. līmenis – pamata

Starpgadījumus izmeklē, tomēr ir maz norādījumu par to, kā un ko izmeklēt.

Tiek izmeklēti tiešie cēloņi.

Izmeklēto starpgadījumu diapazons lielā mērā ir saistīts tikai ar negadījumiem, un ieteikumi, kas izriet no izmeklēšanām, aprobežojas ar to, lai novērstu tāda paša notikuma atkārtošanos. Ieteikumos nenorāda jomas, kurās ir jāveic plašāki uzlabojumi.

Notiek mēģinājumi mācīties no negadījumiem citās nozarēs.

Darbinieki, kuri veic izmeklēšanu, ir saņēmuši apmācību, taču viņi nav efektīvas kompetenču pārvaldības sistēmas daļa.

Tiek atzīts, ka negadījumos un starpgadījumos nozīme ir cilvēkfaktoram un organizatoriskajiem faktoriem, un izmeklēšanas gaitā tiek mēģināts izpētīt šo situāciju, tomēr tas bieži tiek aizmirsts, kad ziņojumus paraksta vadības līmenī.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam. Lai gan tiek atzīts, ka šiem jautājumiem var būt nozīme negadījumos un starpgadījumos, visbiežāk joprojām tiek vainotas atsevišķas personas, nevis novērsti sistēmiski organizatoriskie trūkumi.

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam ir standarta kārtība, kad un kā tiek veikta izmeklēšana.

Tiek izmeklēts negadījuma cēlonis, un izmeklēšana tiek veikta arī pēc negadījuma.

Darbinieki ir saņēmuši vispusīgu apmācību negadījumu un starpgadījumu izmeklēšanā un ir kompetenču pārvaldības sistēmas daļa.

Cilvēkfaktora un organizatorisko faktoru jautājumi ir nelaimes gadījumu un starpgadījumu izmeklēšanas procesa neatņemama daļa. Vadība uzskata to par tikpat svarīgu kā citus notikuma cēloņus un strādā, lai novērstu problēmas, ja tās rodas. Liels uzsvars tiek likts uz taisnīguma kultūras koncepciju, kur cenšas noteikt, kas noticis nepareizi, nevis atrast vainīgo.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam izmeklēšanas kvalitāte nodrošina ieteikumus, ko var piemērot gan organizācijā, gan ārpus tās.

Izpētīto starpgadījumu robežās vajadzības gadījumā ietver darba pārtraukumus un gadījumus, kad paredzētie rezultāti nav sasniegti.

Augstāko vadību informē par izmeklēšanas rezultātiem un ieteikumiem, kā arī nodrošina to īstenošanu atbilstoši apstākļiem.

Tiek pētīti starpgadījumu izmeklēšanas ieteikumi citos dzelzceļa uzņēmumos vai uzņēmumos ārpus organizācijas, lai noskaidrotu, vai šie rezultāti ir būtiski organizācijas darbībai.

Organizācija cenšas gūt atziņas saistībā ar cilvēkfaktoru un organizatoriskajiem faktoriem no savām un citām izmeklēšanām dzelzceļa nozarē un ārpus tās, kā arī risināt šīs problēmas savas SMS *ietvaros. Organizācija sevi pozicionē kā taisnīgu organizāciju, un realitātē vainošanas kultūra nepastāv.*

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam ir izpratne par citu organizāciju izmeklēšanas konstatējumu norādēm.

Ir gatavība mācīties no negadījumiem, mainot uzvedību visā darbībā.

Augstākā vadība iesaistās savas pieredzes izplatīšanā citiem uzņēmumiem dzelzceļa nozarē un ārpus tās, kā arī izmanto citu dzelzceļa uzņēmumu vai citu nozaru gūtās atziņas.

Organizācija cenšas nodot atziņas par cilvēkfaktoru un organizatoriskajiem faktoriem, ko tā gūst no negadījumiem un starpgadījumiem, un uzsvaru, ko tā liek uz taisnīguma un mācīšanās kultūru, saviem partneriem, piegādātājiem un līgumslēdzējiem, dzelzceļa nozarei kopumā un vēl plašāk.

4.7.2 I2 – pastāvīga uzlabošana

Organizācijai ir jāpierāda, ka tā cenšas visu laiku veikt uzlabojumus, mācoties no notikumiem, komunikācijas ar regulatoriem un citā veidā. Uzraudzības laikā sagaida, ka organizācijas parāda, ka tām ir process, lai

identificētu un īstenotu pozitīvas pārmaiņas savās *SMS*, tostarp, izmantojot drošības kultūras pastāvīgas uzlabošanas stratēģiju. Korektīvais pasākums ir saistīts ar tādu darbību definēšanu, noteikšanu un izpildi, kas pēc uzraudzības, izmeklēšanas, revīzijas un pārskatīšanas ir noteiktas kā nepieciešamas.

1. līmenis – nepietiekams

Neraugoties uz SMS *procesiem un procedūrām, uzraudzība, revīzijas un pārskatīšana dod niecīgas vai nesniedz nekādas pārmaiņās vai nu tāpēc, ka tās netiek veiktas, vai tāpēc, ka pēc tām nenotiek turpmākas darbības.*

Organizācijas darbības līmenis ir zemāks, nekā noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam.

Starpgadījumi un negadījumi "notiks" – dominē fatālistiska kultūra. Nav īstas stratēģijas drošības kultūras pastāvīgai uzlabošanai. Kritiskā situācijā par iemeslu vienmēr tiek atzīta cilvēka kļūda, nemēģinot veikt turpmāko izmeklēšanu. Taisnīguma kultūras nav, kā arī starpgadījumos un negadījumos iesaistītos darbiniekus bieži padara par grēkāžiem. Vadība un darbinieki parasti nav ieinteresēti drošībā un var izmantot drošību vienīgi kā pamatu citiem argumentiem, piemēram, darba samaksai, darba laikam u. tml.

2. līmenis – pamata

Vienkāršie konstatējumi no uzraudzības, izmeklēšanas, revīzijas un pārskatīšanas rada vienkāršas darbības un izmaiņas drošības pārvaldības sistēmas zemākajos līmeņos. Organizācijā notiek atsevišķi mēģinājumi meklēt notikumu pamatā esošās problēmas, sistemātiski pārskatot uzraudzības, izmeklēšanu un revīziju informāciju.

Organizācija atbilst tikai minimālajām tiesību aktu prasībām, kas noteiktas vienota drošības sertifikāta vai drošības atļaujas turētājam.

*Drošības nodaļu uztver kā atbildīgu par drošību, bet vadība iegulda laiku un pūles starpgadījumu un negadījumu profilaksei, jo uzskata tos par novēršamiem. Pastāvīgas drošības kultūras uzlabošanas stratēģija pastāv un attiecas uz pareizajām vispārējām jomām, tomēr korektīvie pasākumi galvenokārt risina darbinieku cilvēkfaktora kļūdas ar sodu vai citiem līdzekļiem, lai novērstu uzvedību, kas nav droša, jo uzskata viņus par starpgadījumu un negadījumu cēloņiem, tāpēc kultūra ne vienmēr ir taisnīga. Drošības rādītājus mēra ar atpalikušiem rādītājiem, piemēram, traumas dēļ zaudēto laiku, medicīniskām traumām, noskriešanu no sliedēm, braukšanu garām aizliedzošam signālam (*SPAD*) u. tml. Organizācijai ir vairāk nopietnu starpgadījumu un negadījumu nekā konkurentiem.*

3. līmenis – konsekvents

Tāds pats kā 2. līmenis, un papildus tam ir izveidots process, lai pārliecinātos, ka tiek īstenotas nepieciešamās darbības, kas noteiktas, veicot uzraudzību, revīziju un pārbaudes, un lai noteiktu, kurš ir atbildīgs par darbībām un to izpildes termiņiem.

Ir ieviestas procedūras, lai uzraudzītu drošības pārvaldības sistēmas piemērotību, atbilstību un efektivitāti, ņemot vērā piemērojamajā kopīgajā drošības metodē izklāstīto sistēmu, un ar tām nodrošina pastāvīgus rezultātus.

Korektīvie pasākumi notiek jebkurā drošības pārvaldības sistēmas līmenī.

Vadība atzīst, ka starpgadījumus un negadījumus izraisa vairāki faktori, no kuriem daži izriet no vadības lēmumiem. Tiek pētīti nopietni starpgadījumi un negadījumi, kā arī ir uzsākts sistemātisks secinājumu izdarīšanas process. Ir pastāvīga stratēģija drošības kultūras nepārtrauktai uzlabošanai, kas ir labi izveidota un kuras panākumus var attiecīgi novērtēt. Organizācijā valda taisnīguma kultūra.

4. līmenis – prognozēšana

Tāds pats kā 3. līmenis, un papildus tam ir mehānisms progresa izsekošanai un korektīvo pasākumu pabeigšanai.

Korektīvie pasākumi ir saistīti ar drošības pārvaldības sistēmā noteiktajiem mērķiem.

Drošības mērķu un plānošanas rezultāti, riska novērtējums, personāla un citu personu iesaistīšana, informācija un komunikācija, uzraudzība, revīzija, vadības pārskatīšana un mācīšanās no nelaimes gadījumiem un starpgadījumiem tiek izmantoti kā pamats, lai izstrādātu stratēģijas un plānus pastāvīgai uzlabošanai.

Pirmcēloņu analīzi veic attiecībā uz visiem starpgadījumiem un negadījumiem, un pieņem, ka lielākā to daļa izriet no vadības lēmumiem. Ir izpratne par ikviena atbildību ne tikai par savu drošību, bet arī par kolēģu drošību. Vadība un darbinieki ar cieņu izturas cits pret citu, un ir izveidota sistemātiska pieeja taisnīguma nodrošināšanai. Tiek veicināts veselīgs dzīvesveids un uzraudzīti negadījumi, kas nav saistīti ar darbu. Stratēģijā pastāvīgai drošības kultūras uzlabošanai un taisnīguma kultūras īstenošanai vadās no paraugprakses ar reāliem un izmērāmiem mērķiem.

5. līmenis – izcilība

Tāds pats kā 4. līmenis, un papildus tam ir korektīvie pasākumi, kas noved pie vadības veiktas līdzīgu procesu pārskatīšanas ārpus tiešās jomas, kurā noticis starpgadījums, lai konstatētu līdzīgus trūkumus un pārmaiņas, kas ir jāveic.

Starpgadījumu un negadījumu, kas izraisa fizisku vai psiholoģisku kaitējumu darbiniekiem vai trešām personām, profilakse ir organizatoriska prioritāte. Organizācija nav pieredzējusi nevienu reģistrējamu starpgadījumu vai negadījumu gadiem ilgi, tomēr nav pašapmierinātības sajūtas. Uzvedības vai organizatoriskas novirzes pastāvīgi tiek uzraudzītas, un tiek uzsāktas darbības to novēršanai. Organizācija veiktspējas uzraudzībai izmanto virkni pamatrādītāju. Vienādranga organizācijas uzskata drošības kultūras nepārtrauktas uzlabošanas stratēģiju un to, kā organizācija īsteno taisnīguma kultūru, par paraugu šajā jomā, kurš atbilst paraugpraksei dzelzceļa nozarē un ārpus tās.

Organizācijā pret visu izturas kritiski un pārmaiņas rūpīgi izvērtē.

Pielikums – līmeņu definīcijas

Brieduma līmeņi	1. līmenis	2. līmenis	3. līmenis	4. līmenis	5. līmenis
Nosaukums	Nepietiekams	Pamata	Konsekvents	Prognozēšana	Izcils
Īsa definīcija	Šajā līmenī organizācijai, ko novērtē, ir drošības pārvaldības sistēma, taču ir skaidrs, ka pastāv trūkumi, kuru dēļ rādītāju līmenis ir zemāks par to, kas vajadzīgs, lai piešķirtu vienotu drošības sertifikātu vai drošības atļauju. Pastāv procedūras un norādījumi, lai pārvaldītu drošības pasākumus, bet uzraudzības laikā kļūst skaidrs, ka pastāv nopietnas problēmas to saskaņotībā kopumā. Atsevišķus riskus kontrolē, tomēr kopējais process, ar ko to pārvalda, ir nepietiekams. Organizācija praksē darbojas tādā veidā, ka, šķiet, pastāv būtiskas neatbilstības tam, kas aprakstīts Drošības pārvaldības sistēmā (*SMS*). Šķiet, ka politika, procedūras un instrukcijas tiek piemērotas veidos, kas neatbilst *SMS* izklāstītajiem veidiem, un tāpēc organizācijas vai tās darbuzņēmēju veikto darbību riski netiek obligāti pietiekami kontrolēti. Šajā līmenī VDI ir	Šajā līmenī organizācija darbojas minimālas atbilstības tiesību aktiem līmenī, t. i., *SMS* darbojas līmenī, kas bija pietiekams, lai novērtējuma posmā tiktu piešķirts vienots drošības sertifikāts vai drošības atļauja. Rakstveida drošības pārvaldības sistēma pastāv un tiek izmantota, lai kontrolētu drošības riskus, tomēr trūkst struktūras un koordinācijas. Sistēma kopumā ir saskaņota, tomēr dažādās jomās pastāv trūkumi, pieejas nesaskaņotība un nekonsekvence. Pamatā organizācija labi tiek galā ar saviem pienākumiem drošības jomā, bet ne vairāk. Daudz netrūkst, lai rastos būtiska problēma un tā atgrieztos 1. līmenī, jo procedūras un riska pārvaldības integrācijas trūkums var kļūt par nozīmīgu problēmu tehnisku, operatīvu un organizatorisku risku gadījumā. Dažas darbības jomas drošības pārvaldības ziņā darbojas labāk nekā citas. Riskus vairāk	Drošības pārvaldības sistēma ir izstrādāta, lai izveidotu sistemātisku un konsekventu pieeju riska pārvaldībai. Visi elementi ir vietā un darbojas, un tiek ņemti vērā visi drošības aspekti. Drošības kultūrai organizācijā tiek pievērsta zināma uzmanība. Kaut arī organizācija ir konsekventa, tā nemēģina iepriekš prognozēt riskus, kā arī tajā nav pietiekami attīstītas kultūras riska pārvaldības procesu nodrošināšanai. Ugunsdrošības pasākumi ir snieguši pamatu pārdomātākai riska pārvaldības pieejai, tomēr daudz netrūkst (piemēram, nespēja pārvaldīt galvenos procesus vai procedūras laika gaitā), lai organizācija atgrieztos pamata darbību režīmā.	Tāds pats kā 3. līmenis, un papildus drošības pārvaldības sistēma pastāvīgi pārvalda riskus proaktīvi. Šeit organizācija uzrauga riska faktorus un rīkojas jau iepriekš, lai novērstu bīstamus negadījumus. Organizācija ir apņēmusies attīstīt drošības kultūru, darbaspēks ir iesaistīts darbībā, pārvaldot drošību saskaņotā un tālredzīgā veidā. Šajā līmenī pastāv organizācijas augstākā līmeņa vadības patiesa līderība, un tās darbinieki tic tai un ievēro vadības pieeju. Daudz pūļu tiek veltīts regulārai rādītāju pārskatīšanai un centieniem izprast tos riskus, ar ko organizācija saskaras, to raksturu un ko šajā jomā var darīt.	Tāds pats kā 4. līmenis, un papildus tam drošības pārvaldības rakstveida sistēma ir veidota tā, lai to varētu pastāvīgi uzlabot. Organizācija aktīvi meklē iespējas uzlabot drošību un pilnveidot savu drošības kultūru, izmantojot informāciju, kas pieejama gan dzelzceļa nozarē, gan ārpus tās. Organizācija salīdzina savus rādītājus ar citiem gan dzelzceļa nozarē, gan ārpus tās. Pastāv pierādījumi, ka organizācija apzinās problēmas, kas tai ir vai var būt nākotnē, un aktīvi cenšas tās risināt, izmantojot *SMS*. Šajā līmenī organizācija ir pārliecināta par tās spēju pārvaldīt riskus, ar kuriem tā saskaras, un cenšas arī ārpus tās izglītot tos, ar kuriem tai ir mijiedarbība, un tiecas mācīties no citu jomu pieredzes, ko var iekļaut tās darbībā. Drošība ir organizācijas darbības neatņemama daļa.

	jāapsver nepieciešamā rīcība, lai atjaunotu organizācijas atbilstību tiesību aktu prasībām (skat. Aģentūras "Izpildes rokasgrāmata", lai iegūtu sīkāku informāciju par to, kā šis process varētu darboties).	kontrolē organizācijā strādājošo indivīdu darbība, nevis *SMS* izmantošana. Ugunsdrošības pieeja riska pārvaldībai ir ierasta parādība, kas rosina uzņēmumu reaģēt uz negadījumiem vai starpgadījumiem, nevis proaktīvi veikt pasākumus to profilaksei.