

Riepnieku iela 2, Rīga, LV-1050, tālr. 67234308, 67234335, fakss 67234333, e-pasts pasts@vdzti.gov.lv, www.vdzti.gov.lv

Rīgā, 16.01.2023. Nr.1-1/4-1

**Uzraudzības rokasgrāmata**

Izmaiņu reģistrs[[1]](#footnote-1):

|  |  |  |  |
| --- | --- | --- | --- |
| **Versija**  | **Datums** | **Izmaiņas** | **Ierosinātājs** |
| V-1.0. | 29.11.2022. | Rokasgrāmatas izstrāde | Linda GailīteDirektora vietniece, Attīstības daļas vadītāja |
| V-1.0. | 13.12.2022. | Brieduma modeļa izveide | Jeļena StepanovaAttīstības daļas vecākā eksperte |
| V-1.0. | 27.12.2022. | Teksta pārskatīšana | Inese SaulīteAttīstības daļas vecākā eksperte/analītiķe |
| V-1.1. | 16.01.2023. | Audita grupas reglamenta iekļaušana rokasgrāmatāProcedūras pārskatīšana | Linda GailīteDirektora vietniece, Attīstības daļas vadītājaInese SaulīteAttīstības daļas vecākā eksperte/analītiķe |
|  |  |  |  |

**Saturs**

[1. Ievads 3](#_Toc124503195)

[1.1.Izmantošanas sfēra 3](#_Toc124503196)

[1.2. Rokasgrāmatā lietotie termini, definīcijas un saīsinājumi 3](#_Toc124503197)

[2. Dokumentu pārvaldība 5](#_Toc124503198)

[3. Uzraudzība 6](#_Toc124503199)

[3.1. DPS audits 6](#_Toc124503200)

[3.1.1. DPS 6](#_Toc124503201)

[3.1.2. Audita dokumentēšana, audita lieta 7](#_Toc124503202)

[3.1.3. Komunikācija ar auditējamo 9](#_Toc124503203)

[3.1.4. Audita grupa 9](#_Toc124503204)

[3.1.5. Audita posmi 11](#_Toc124503205)

[3.1.6. Audita plānošana 12](#_Toc124503206)

[3.1.7. Ievada sanāksme 14](#_Toc124503207)

[3.1.8. Sākotnējā dokumentu pārbaude 15](#_Toc124503208)

[3.1.9. Pirms pārbaudes sanāksme 16](#_Toc124503209)

[3.1.10. Komunikācija pārbaudes, vizītes laikā 17](#_Toc124503210)

[3.1.11. Praktiskās pārbaudes 17](#_Toc124503211)

[3.1.12. Audita konstatējumi 19](#_Toc124503212)

[3.1.13. Audita ziņojuma sagatavošana un apstiprināšana 19](#_Toc124503213)

[3.1.14. DPS daļu vērtējums un brieduma pakāpes noteikšana 21](#_Toc124503214)

[3.1.15. Audita noslēguma sanāksme 21](#_Toc124503215)

[3.1.16. Audita noslēguma ziņojuma nosūtīšana 22](#_Toc124503216)

[3.1.17. Rīcības plāni 22](#_Toc124503217)

[3.1.18. Pēcpārbaude 23](#_Toc124503218)

[3.1.19. Audita lietas slēgšana 23](#_Toc124503219)

[3.2. Praktiskās darbības novērtēšanas un punktveida pārbaudes 23](#_Toc124503220)

[3.2.1. Pārbaudes plānošana un sagatavošanās pārbaudei 24](#_Toc124503221)

[3.2.2. Pārbaudes uzsākšana, pārbaudes laika noteikšana 24](#_Toc124503222)

[3.2.3. Komunikācija ar pārbaudāmo organizāciju 25](#_Toc124503223)

[3.2.4. Pārbaude uz vietas 25](#_Toc124503224)

[3.2.5. Pierādījumu savākšana un novērojumu aprakstīšana 25](#_Toc124503225)

[3.2.6. Pārbaudes protokola nosūtīšana 27](#_Toc124503226)

[3.2.7. Korektīvās darbības 27](#_Toc124503227)

[3.2.8. Pārbaudes lietas slēgšana 28](#_Toc124503228)

[4. Dzelzceļa satiksmes negadījumu uzraudzība 28](#_Toc124503229)

[4.1. Informācijas saņemšana un izbraukšana uz negadījuma vietu 28](#_Toc124503230)

[4.2. Negadījuma vieta 28](#_Toc124503231)

[4.3. COR lietošana un dzelzceļa satiksmes negadījumu izmeklēšana 29](#_Toc124503232)

[5. Administratīvie lēmumi 30](#_Toc124503233)

[6. Kompetences 30](#_Toc124503234)

[1. pielikums Kritēriji vispārīgā līmeņa noteikšanai 31](#_Toc124503235)

[2. pielikums Kritēriji DPS daļu vērtējumiem pa līmeņiem 33](#_Toc124503236)

* [Organizācijas konteksts (O) 33](#_Toc124503237)
* [Līderība (L) 34](#_Toc124503238)
* [Plānošana (PL) 41](#_Toc124503239)
* [Atbalsts (A) 44](#_Toc124503240)
* [Ekspluatācija (E) 53](#_Toc124503241)
* [Darbības rādītāju novērtējums (N) 61](#_Toc124503242)
* [Uzlabošana (U) 65](#_Toc124503243)

# 1. Ievads

##  Izmantošanas sfēra

Šī uzraudzības rokasgrāmata (turpmāk- rokasgrāmata) nosaka Valsts dzelzceļa tehniskās inspekcijas (turpmāk – Inspekcija) Kustības drošības daļas (turpmāk- KDD) uzraudzības pārvaldības principus, metodes un nosaka iekšējos procesus, lai nodrošinātu atbilstošu uzraudzību.

Šī rokasgrāmata attiecas uz visām Inspekcijas struktūrvienībām, kas iesaistītas kustības drošības uzraudzībā, sniedz novērtējumu par sistēmām un izvērtē riskus un kā ir noteikts tieši piemērojamos Eiropas Savienības (turpmāk-ES) tiesību aktos:

* KOMISIJAS DELEĢĒTĀ REGULA (ES) 2018/762 (2018. gada 8. marts),ar ko saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/798 izveido kopīgas drošības metodes, kas attiecas uz prasībām drošības pārvaldības sistēmām, un atceļ Komisijas Regulas (ES) Nr. 1158/2010 un (ES) Nr. 1169/2010 (turpmāk- Regula 2018/762);
* KOMISIJAS DELEĢĒTĀ REGULA (ES) 2018/761 (2018. gada 16. februāris), ar ko izveido kopīgas drošības metodes uzraudzībai, ko valstu drošības iestādes veic pēc vienotā drošības sertifikāta vai drošības atļaujas izdošanas saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/798, un atceļ Komisijas Regulu (ES) Nr. 1077/2012 (turpmāk - Regula 2018/761);
* KOMISIJAS ĪSTENOŠANAS REGULA (ES) Nr. 402/2013 (2013. gada 30. aprīlis) par kopīgo drošības metodi riska noteikšanai un novērtēšanai un par Regulas (EK) Nr. 352/2009 atcelšanu;
* Komisijas Īstenošanas regula (ES) 2019/779 (2019. gada 16. maijs), ar ko paredz sīki izstrādātus par ritekļu apkopi atbildīgo struktūru sertifikācijas sistēmas noteikumus saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/798 un atceļ Komisijas Regulu (ES) Nr. 445/2011;
* KOMISIJAS REGULA (ES) Nr. 1078/2012 (2012. gada 16. novembris) par kopīgo drošības metodi pārraudzībā, kas jāveic dzelzceļa pārvadājumu uzņēmumiem, infrastruktūras pārvaldītājiem pēc drošības sertifikāta vai drošības atļaujas saņemšanas un par tehnisko apkopi atbildīgajām struktūrvienībām.

Rokasgrāmata apraksta uzraudzības procesus un pielietojamās metodes, īpašu uzmanību pievēršot drošības pārvaldības sistēmu (turpmāk - DPS) uzraudzībai. Rokasgrāmatā ir arī ietverti skaidrojumi par aktivitātēm, kas jāņem vērā plānojot uzraudzību.

Uzraudzība ietver dažādu uzraudzības metožu pielietošanu, plānošanu, ziņojumu apkopošanu un datu ievadi. Ziņojumi var ietvert informāciju par neatbilstībām, t.sk., atskaites par korektīvajām darbībām un neatbilstību novēršanas pārbaudi.

Uzraudzības process ir cieši saistīts ar kompetenču pārvaldību, ietverot vecāko inspektoru vai ekspertu darbības (kompetences un izpildījuma) novērtējumu un kompetences paaugstināšanas un uzturēšanas apliecinājumus. Kompetenču jautājumi ir atainoti Inspekcijas Kompetenču pārvaldības sistēmā[[2]](#footnote-2).

## 1.2. Rokasgrāmatā lietotie termini, definīcijas un saīsinājumi

Rokasgrāmatā lietotie termini un definīcijas izriet no tieši piemērojamiem ES tiesību aktiem, Dzelzceļa likuma un normatīviem aktiem.

Zemāk uzskaitīti ir rokasgrāmatā biežāk pielietotie termini un definīcijas, lai nodrošinātu ērtāku dokumenta lasāmību un pielietojumu.

**1.tabula Definīcijas**

| **Termini**  | **Definīcijas** |
| --- | --- |
| **Audits** | Sistemātisks, neatkarīgs un dokumentēts process pierādījumu iegūšanai un to objektīvai novērtēšanai, ar mērķi gūt pietiekamu pārliecību, ka ieviestās DPS ir adekvātas, tiek izmantotas un nepārtraukti pilnveidotas, kā arī novērtētu DPS veiktspēju un efektivitāti  |
| **Auditējamais**  | Dzelzceļa sistēmas dalībnieks, kas tiek auditēts  |
| **Auditors**  | Nodarbinātais, kuram ir atbilstošas uzraudzības kompetences veikt auditu, un kurš ir nozīmēts audita veikšanai audita grupā |
| **Audita grupa** | Vairāki auditori, kuri veic auditu, nepieciešamības gadījumā pieaicinot tehniskos ekspertus |
| **Audita apjoms**  | Audita apmērs un robežas (audita norises laika periods, norises vietas, struktūrvienības, auditējamā auditējamo darbību un procesu apraksts) |
| **Audita mērķis**  | Vispārīgi formulēts audita sasniegums  |
| **Audita programma** | Informācijas kopums, kas nepieciešams audita plānošanai, organizēšanai un īstenošanai |
| **Audita plāns**  | Audita darbību un plānojuma apraksts, kuru nosūta auditējamam pirms audita veikšanas  |
| **Audita kritēriji**  | Politiku, procedūru un prasību kopums, ar kuriem salīdzina iegūtos audita pierādījumus  |
| **Audita lieta**  | Audita dokumentācijas kopums (paziņojums par auditu, audita plāns, auditoru kontrolsaraksti, atklāšanas un noslēguma sapulces protokoli un dalībnieku saraksts, audita ziņojums un ziņojums par neatbilstībām)  |
| **Audita lietas slēgšana**  | Audita lietas nobeigums, kad visas, paredzētās korektīvās darbības ir pabeigtas, neatbilstības ir novērstas un šo darbību izpilde ir pārbaudīta  |
| **Audita atklājumi**  | Novērtēšanas rezultāti atkarībā no auditu kritērijiem Audita atklājumi var norādīt uz atbilstību vai neatbilstību audita kritērijiem vai uz iespējamiem uzlabojumiem  |
| **Atbilstība** | Spēja pietiekamā līmenī nodrošināt darbības saskaņā ar auditējamā politikām, plāniem, procedūrām, likumiem, noteikumiem un līgumiem ievērošanu |
| **Audita novērojumi jeb atklājumi** | Kvantitatīvā vai kvalitatīvā rakstura informācija, pieraksti, faktu konstatēšana, kas balstās uz audita novērojumiem un kuru patiesums ir pārbaudāms. Audita pierādījumi var norādīt uz atbilstību vai neatbilstību audita kritērijiem vai uz iespējamiem uzlabojumiem  |
| **Audita slēgšana**  | Audita nobeigums, kad audita darbi ir pabeigti, ir apstiprināts audita ziņojums un apstiprinātais audita ziņojums ir nosūtīts auditējamam  |
| **Drošības novērtējums**  | Demonstrējums un pierādījums, ka piedāvātās izmaiņas sistēmā (tai skaitā funkcionālajā) var īstenot atbilstoši mērķiem vai standartiem, kas noteikti esošajā regulatīvajā sistēmā saskaņā ar drošības prasībām  |
| **Drošības rādītājs**  | Rādītājs, ko izmanto drošības uzraudzībai un novērtēšanai.  |
| **Drošības uzraudzība**  | Funkcija, kuru veic Inspekcija, lai pārbaudītu, ka drošības uzraudzības mērķi tiek sasniegti un prasības tie adekvāti izpildītas  |
| **Neatbilstība**  | Audita vai pārbaudes kritēriju neizpilde  |
| **Novērojums**  | Audita atklājums, kurš nav uzskatāms par standartu, noteikumu vai procedūru neizpildi, bet kuru var uzskatīt par kvalitātes un drošības pārvaldības sistēmas uzlabošanas potenciālu (potenciālās neatbilstības)  |
| **Organizācija** | Fiziska persona, juridiska persona vai personu apvienība |
| **Pārbaude** | Produktu, pakalpojumu, darbības procesu pārbaude un šo procesu atbilstības noteikšana pēc specifiskām prasībām vai pēc vispārējām prasībām uz profesionāla vērtējuma pamata  |
| **Pārbaudes kritēriji**  | Prasību un procedūru kopums  |
| **Pārbaudes atklājumi**  | Pieraksti, faktu izklāstījums, un cita informācija, kas saistīti ar pārbaudes kritērijiem un kurus var pārbaudīt  |
| **Pārbaudes atklājumi**  | Pārbaudes pierādījumu novērtēšanas rezultāti atkarībā no pārbaudes kritērijiem  |
| **Pārbaudes slēdziens**  | Pārbaudes izejas dati, ko iesniedz inspektors pēc pārbaudes mērķu realizācijas un visiem pārbaudes novērojumiem  |
| **Vecākais inspektors**  | Persona, kurai ir uzraudzībai piemērojamas kompetences, un kura ir nozīmēta uzraudzības veikšanai  |
| **Kompetence**  | Personāla īpašības un spējas izmantot zināšanas un prasmes |
| **Korektīvā darbība**  | Darbība, kuru veic, lai likvidētu konstatētas neatbilstības cēloni  |
| **Uzraudzība**  | Pastāvīga pārbaude, ko kompetentā iestāde veic vai ko kompetentās iestādes vārdā veic, lai pārliecinātos, ka šīs regulas un uz to pamata pieņemto deleģēto un īstenošanas aktu prasības, uz kuru pamata izdots sertifikāts vai attiecībā uz kurām sniegta deklarācija, joprojām ir izpildītas  |

# Dokumentu pārvaldība

Visas prasības dokumentu uzglabāšanai, pieejamībai un izsekojamībai nodrošina atbilstoši Inspekcijas Dokumentu pārvaldības kārtībai[[3]](#footnote-3). Inspekcija nodrošina uzraudzības dokumentu (pārskatu, ziņojumu, pierādījumu, u.c.) uzglabāšanu un pieejamību visiem KDD un atsevišķiem Attīstības daļas (turpmāk-AD) nodarbinātajiem. Uzraudzības procesā piemēro dokumentu pārvaldības procedūras un arhīva pārvaldības procedūras.

Uzraudzības procesā uzkrāj šādus dokumentus:

2.1. lietotāju rokasgrāmatas;

2.2. kompetenču pārvaldības procedūras;

2.3. nodarbināto apmācības, kvalifikācijas un apstiprināšanas dokumentāciju;

2.4. ar uzdevumu nodošanu citām struktūrvienībām saistīto dokumentāciju un informāciju par uzticētajiem uzdevumiem;

2.5. sertificēšanas dokumentāciju;

2.6. ES Dzelzceļu aģentūras:

2.6.1. dokumentāciju;

2.6.2. ieteikumus;

2.6.3. rokasgrāmatas;

2.6.4. sistēmas.

2.7. visu veikto uzraudzības metožu:

2.7.1. ziņojums;

2.7.2. veiktās korektīvās darbības;

2.7.3. audita laikā konstatētos novērojumus;

2.7.4. dienesta ziņojumus;

2.7.5. pārbaudes protokolus;

2.7.6. citu ar drošību saistītu dokumentus;

2.8. veikto izpildes nodrošināšanas pasākumu dokumentus;

2.9. dzelzceļa negadījumu statistiku;

2.10. korektīvo darbību efektivitātes novērtēšanas pasākumu dokumentus;

2.11. citus dokumentus, kas tiek ietverti uzraudzības procesā.

Inspekcija nodrošina visu dzelzceļa sistēmas dalībnieku (organizāciju un fizisko personu) saraksta izveidi. Saraksti tiek uzskaitīti un glabāti Elektroniskajā dokumentu pārvaldības sistēmā.

Visi dokumenti tiek aprakstīti un uzglabāti atbilstoši lietu nomenklatūrā noteiktajiem termiņiem. Personu dati tiek uzglabāti ievērojot personu datu aizsardzības prasības.

Nodarbināto kvalifikācijas un apmācību dokumentācijas glabāšana tiek nodrošināta nodarbināto personas lietās līdz darba vai civildienesta attiecību beigām.

# Uzraudzība

Uzraudzības procesā KDD piemēro jebkuru uzraudzības metodi un to piesaista pie noteiktas DPS daļas. Šajā sadaļā tiek aprakstīts uzraudzības process, ja tiek nodrošināts audits vai praktiskās darbības novērtēšanas pārbaude.

##  DPS audits

DPS audits ir audits, ko veic Inspekcija, lai iegūtu pārliecību, ka organizācijai darbojas efektīva sistēma drošības jomā un atbilst nepieciešamajām drošības prasībām, nodrošinot drošus pakalpojumus.

Organizācija nodrošina efektīvu drošības pārvaldību saskaņā ar spēkā esošajiem tiesību aktiem, ieviešot atbilstošu organizācijas politiku, mērķus, atbildību un procesus. Inspekcija nodrošina, ka, veicot DPS auditus, tie tiek organizēti tā, lai Inspekcija iegūtu visu nepieciešamo informāciju, kas nepieciešama, lai izdarītu slēdzienu par DPS veiktspēju, kā arī drošības prasību izpildi un kvalitāti.

Audita mērķis ir:

* iegūt un uzturēt pārliecību par auditējamās organizācijas spējām sniegt pieņemami drošus pakalpojumus;
* atbilstība normatīvo aktu un tieši piemērojamo ES tiesību aktu prasībām, it īpaši Regulas 2018/762 prasībām;
* veicināt uzlabojumus auditējamās organizācijas pārvaldības sistēmā.

Inspekcija nodrošina, ka uzraudzības auditi tiek efektīvi vadīti un organizēti plānotā un sistemātiskā veidā.

Lai sasniegtu Regulas 2018/761 mērķus, Inspekcija, kā valsts pārvaldes un reizē uzraudzības iestādei, ir tiesības sniegt organizācijām neatkarīgu, kvalitatīvu konsultēšanas (skaidrošanas) pakalpojumu un veikt/organizēt dažāda veida apmācības un seminārus, kas neietekmē Inspekcijas darbinieku objektivitāti, veicot kontroles funkcijas.

Labā prakse ir uz metožu, procesu un tehnikas balstīts veids kā sasniegt vēlamo rezultātu, nodrošinot tā sasniegšanu ar minimālām problēmām vai sarežģījumiem.

### DPS

DPS ietver šādas daļas un apakšsadaļas:

* **Organizācija (O)**;
* **Līderība (L)**:
	+ līderības ieguldījums (L1)- augstākās vadības līderība ieviest, uzturēt un uzlabot drošību;
	+ drošības politika (L2) - tās saderība ar stratēģiju;
	+ funkcijas, pienākumi un pilnvaras (L3);
	+ organizācijas apspriešanās (L4) - ar personālu par personāla kompetencēm, pienākumiem un pilnvarām un citām pusēm;
* **Plānošana (PL)**:
	+ riska novērtēšana un izmaiņu plānošana (PL1);
	+ drošības mērķu noteikšana (PL2);
* **Atbalsts (A)**:
	+ resursi (A1);
	+ kompetences (A2)- kompetenču pārvaldības sistēma;
	+ apzināšanās (A3)- personāla apzināšanās un drošība;
	+ komunikācija (A4)- informācija un saziņa;
	+ dokumentēta informācija (A5) - informācijas dokumentēšana, aprite un kontrole;
	+ cilvēkfaktoru un organizatorisko faktoru integrēšana (A6);
* **Ekspluatācija (E):**
	+ ekspluatācijas plānošana un kontrole (E1);
	+ aktīvu pārvaldība (E2);
	+ darbuzņēmēji, partneri un piegādātāji (E3);
	+ pārmaiņu pārvaldība (E4);
	+ ārkārtas situāciju pārvaldība (E5);
* **Darbības rādītāju novērtējums (N)**:
	+ pārraudzība (N1);
	+ iekšējā revīzija (N2);
	+ pārvaldības pārskatīšana (N3) - procesu pārskatīšana;
* **Uzlabojumi (U)**:
	+ mācīšanās no negadījumiem un starpgadījumiem (U1) - negadījumi, to izmeklēšana, analīze un cēloņu noteikšana un drošības ieteikumu izvērtēšana un īstenošana;
	+ pastāvīgi uzlabojumi (U2).

Kritēriji vispārīgā līmeņa noteikšanai ir norādīti 1. pielikumā. DPS daļu un apakšsadaļu kritēriji vērtējumiem pa līmeņiem ir aprakstīti 2. pielikumā.

### 3.1.2. Audita dokumentēšana, audita lieta

Lai nodrošinātu kvalitatīvu auditu un atvieglotu audita gaitā uzkrāto darba dokumentu apkopošanu un sistematizēšanu, kā arī, lai trešā persona varētu pārliecināties par audita norisi, visus audita darba dokumentus apkopo vienā audita lietā.

Visas ar auditu saistītās sanāksmes tiek dokumentētas.

Visu audita procesu dokumentē. Pierakstus veic, lai demonstrētu audita programmas izpildi. Izdala šādus dokumentu veidus:

* audita plāns – audita plānu sagatavo vadošais auditors un apstiprina direktors. Audita plānā norāda plāna sastādīšanas datumu;
* dokumentu pārbaudes protokols – uzsāk vadošais auditors, pēc tam secīgi auditori;
* kontrolsaraksti (ja tādi ir nepieciešami) – nodrošina auditori;
* pierakstu lapas informācijas atzīmēšanai un pierādījumiem – sagatavo katrs auditors atsevišķi;
* sanāksmju protokoli – sagatavo audita grupas sekretārs;
* audita atklājumi jeb audita ziņojums par neatbilstībām un novērojumiem – sagatavo audita grupa.

Audita darba dokumenti ir viss DPS audita gaitā uzkrāto dokumentu kopums, kas attiecas uz noteikto auditu, raksturo DPS audita procesu un ir nepieciešami kvalitatīva un objektīva audita ziņojuma sagatavošanai.

Darba dokumentus, ieskaitot audita laikā veiktos pierakstus, saglabā līdz audita lietas slēgšanai. Dokumentu uzglabāšanu pēc audita pabeigšanas un aprakstīšanu nosaka Inspekcijas Dokumentu pārvaldības kārtība. Dokumentus, kas saistīti ar konfidenciālu informāciju, uzglabā atbilstoši normatīvo aktu prasībām.

Lai nodrošinātu, ka DPS audita lieta pilnīgi un precīzi atspoguļo auditu, auditors dokumentē audita gaitu un ievieto lietā visu iegūto informāciju, kas sniedz pierādījumus par konstatētajiem faktiem, nepilnībām, neatbilstībām, secinājumiem un ieteikumiem.

Dokumentus ievieto hronoloģiskā secībā atbilstoši to saņemšanas vai sagatavošanas datumam.

Katrai audita lietai tiek piešķirts identifikācijas numurs, kurš tiek izmantots visos dokumentos. Ja ir nepieciešams, kā papildu numurs var tikt norādīts auditēšanas gads vai DPS daļas numurs. Audita dokumentu reģistrē un ievieto elektronisko dokumentu pārvaldības sistēmas “Organizācijas failā”.

Audita lieta var sastāvēt gan no dokumentiem papīra formātā, gan no elektroniskiem dokumentiem (hibrīdlieta).

Audita lietu un visus audita dokumentus kārto KDD pēc izveidota lietas satura. Ja dokuments ir elektroniski parakstīts, audita lietas saturā to norāda.

**2.tabula Audita lietas satura paraugs**

| **Nr.p.k.** | **Audita lietas saturs** | **Dokumenta veids** |
| --- | --- | --- |
|  | **Plānošana**Audita plāns un programmaSākotnējais dokumentu pārbaudes protokols Nr.\_\_\_\_\_\_SaraksteProtokoliAudita plāns un programma (koriģēta) | Elektronisks dokumentsPapīra dokuments |
|  | **Pārbaudes veikšana**SaraksteAuditā iesaistīto personu sarakstsPārbaudes protokols Nr.ProtokoliCiti darba dokumenti | Elektronisks dokumentsPapīra dokuments |
|  | **Audita ziņojums**Audita ziņojuma Nr.\_\_\_\_ projektsAudita ieteikumu ieviešanas plāna Nr.\_\_\_ projektsSarakste, komentāriProtokoliApstiprinātais audita gala ziņojums Nr.\_\_\_\_Audita slēgšana | Elektronisks dokumentsPapīra dokuments |
|  | **Korektīvo darbību īstenošana**SaraksteDokumentāli pierādījumiAudita lietas slēgšanas dokuments Nr.\_\_\_\_ | Elektronisks dokumentsPapīra dokuments |

Dokumentus, kas saistīti ar konfidenciālu informāciju, Inspekcijas inspektori glabā atbilstoši normatīvo aktu prasībām. Dokumentu glabāšana vai iznīcināšana notiek saskaņā ar Inspekcijas Dokumentu pārvaldības kārtības prasībām.

### 3.1.3. Komunikācija ar auditējamo

Audita grupas vadītājs ir atbildīgs par sākotnējo kontaktu nodibināšanu ar auditējamo, pirms tiek uzsākts plānotais audits. Komunikāciju ar auditējamo uztur, lai:

* noteiktu komunikācijas kanālu ar auditējamo;
* paziņotu auditējamam informāciju par audita plānu un audita grupu;
* pieprasītu auditam nepieciešamos dokumentus, ieskaitot pierakstus;
* informētu par nepieciešamību audita laikā nodrošināt pieeju attiecīgajām auditēšanas vietām, personām un dokumentiem, ieskaitot pierakstiem;
* noteiktu pieņemamus drošības pasākumus darbības vietā;
* informētu par nepieciešamību inspektorus nodrošināt ar pavadītājiem.

Audita grupas vadītājs rakstiski informē auditējamo, sagatavojot oficiālu vēstuli ar audita paziņojumu ne mazāk kā desmit darba dienas pirms plānotā audita veikšanas dienas.

### 3.1.4. Audita grupa

Mērķis audita grupas izveidei ir nodrošināt neatkarību lēmumu pieņemšanā, noteiktu un atbilstošu pienākumu sadalījumu, atbildību un tiesības, piesaistītu kompetentākos ekspertus un nodrošinātu atbilstošu veiktspējas novērtējumu, kas sniedz pilnvērtīgu novērtējumu par komersanta spēju darboties droši.

Audita grupa atbild par uzraudzības laikā gūto pietiekamo un objektīvo pierādījumu novērtējumu, uz kura pamata tiek balstīts ziņojums.

Audita grupā ir šāds “lomu” sadalījums:

* lēmuma pieņēmējs atbild par gala ziņojuma izdošanu un ir kompetents:
* ES tiesību akti dzelzceļa transporta jomā (uzraudzības kompetences 3.līmenis);
* nacionālais tiesību aktu regulējums ( uzraudzības kompetences 3.līmenis);
* drošības pārvaldības (SMS) vai citas sistēmas (uzraudzības kompetences 3.līmenis);
* dzelzceļa sistēmas darbība (uzraudzības kompetences 3.līmenis);
* problēmu risināšana (uzraudzības kompetences 3.līmenis);
* novērtējums (uzraudzības kompetences 3.līmenis);
* audita grupas vadītājs atbild par audita pārvaldību un tā savlaicīgu īstenošanu un ir kompetents:
* ES tiesību akti dzelzceļa transporta jomā (uzraudzības kompetences 3.līmenis);
* nacionālais tiesību aktu regulējums (uzraudzības kompetences 3.līmenis);
* drošības pārvaldības (SMS) vai citas sistēmas (uzraudzības kompetences 3.līmenis);
* dzelzceļa sistēmas darbība (uzraudzības kompetences 3.līmenis);
* komandas vadīšana (uzraudzības kompetences 3.līmenis);
* plānošana un organizēšana (uzraudzības kompetences 3.līmenis);
* intervēšana (uzraudzības kompetences 3.līmenis);
* problēmu risināšana (uzraudzības kompetences 2.līmenis)
* novērtējums (uzraudzības kompetences 3.līmenis);
* audita grupas vadītāja vietnieks atbild par audita pārvaldību un tā savlaicīgu īstenošanu un ir kompetents:
* ES tiesību akti dzelzceļa transporta jomā (uzraudzības kompetences 2.līmenis);
* nacionālais tiesību aktu regulējums (uzraudzības kompetences 2.līmenis);
* drošības pārvaldības (SMS) vai citas sistēmas (uzraudzības kompetences 3.līmenis);
* dzelzceļa sistēmas darbība (uzraudzības kompetences 3.līmenis);
* komandas vadīšana (uzraudzības kompetences 2.līmenis);
* kritiskās analīzes spējas jeb analītiskā domāšana (uzraudzības kompetences 2.līmenis);
* komunikācija (uzraudzības kompetences 3.līmenis);
* plānošana un organizēšana (uzraudzības kompetences 2.līmenis);
* intervēšana (uzraudzības kompetences 3.līmenis);
* problēmu risināšana (uzraudzības kompetences 2.līmenis);
* novērtējums (uzraudzības kompetences 3.līmenis);
* vērtētāji atbild par uzticētā novērtējuma noteikto daļu vai daļām un ir kompetenti:
* ES tiesību akti dzelzceļa transporta jomā (uzraudzības kompetences 2.līmenis);
* nacionālais tiesību aktu regulējums (uzraudzības kompetences 2.līmenis);
* drošības pārvaldības (SMS) vai citas sistēmas (uzraudzības kompetences 2.līmenis);
* dzelzceļa sistēmas darbība (uzraudzības kompetences 3.līmenis);
* kritiskās analīzes spējas jeb analītiskā domāšana (uzraudzības kompetences 3.līmenis);
* komunikācija (uzraudzības kompetences 3.līmenis);
* darbs komandā (uzraudzības kompetences 3.līmenis);
* plānošana un organizēšana (uzraudzības kompetences 3.līmenis);
* intervēšana (uzraudzības kompetences 3.līmenis);
* problēmu risināšana (uzraudzības kompetences 2.līmenis);
* novērtējums (uzraudzības kompetences 2.līmenis);
* pieaicinātie eksperti atbild par uzticētā novērtējuma noteikto daļu vai daļām un ir kompetenti:
* ES tiesību akti dzelzceļa transporta jomā (uzraudzības kompetences 2.līmenis);
* nacionālais tiesību aktu regulējums (uzraudzības kompetences 2.līmenis);
* drošības pārvaldības (SMS) vai citas sistēmas (uzraudzības kompetences 2.līmenis);
* dzelzceļa sistēmas darbība (uzraudzības kompetences 3.līmenis);
* kritiskās analīzes spējas jeb analītiskā domāšana (uzraudzības kompetences 3.līmenis);
* komunikācija (uzraudzības kompetences 3.līmenis);
* darbs komandā (uzraudzības kompetences 3.līmenis);
* plānošana un organizēšana (uzraudzības kompetences 3.līmenis);
* intervēšana (uzraudzības kompetences 3.līmenis);
* dokumentu pārbaudītājs atbild par dokumentu pārbaudi un pietiekamību un ir kompetents:
* drošības pārvaldības (SMS) vai citas sistēmas (uzraudzības kompetences 2.līmenis);
* dzelzceļa sistēmas darbība (uzraudzības kompetences 2.līmenis);
* komunikācija (uzraudzības kompetences 3.līmenis);
* darbs komandā (uzraudzības kompetences 3.līmenis);
* plānošana un organizēšana (uzraudzības kompetences 3.līmenis).

Audita grupa nodrošina konfidencialitāti, neizpaužot nekādu komerciālu informāciju par organizāciju, ievērojot Inspekcijas ierobežotas pieejamības informācijas aprites un aizsardzības kārtību.

### 3.1.5. Audita posmi

**1.shēma Audita posmi**



Auditu iedala šādos posmos:

* audita plānošana:
	+ mērķu noteikšana;
	+ audita apjoma noteikšana;
	+ audita grupas nozīmēšana, pienākumu sadale audita grupā;
	+ audita paziņojuma sagatavošana;
	+ audita grafika/plāna sastādīšana un nosūtīšana auditējamajam;
	+ ievada sanāksmes (kick-off) organizēšana ar auditējamo;
* sākotnējā Inspekcijas rīcībā esošo dokumentu pārbaude:
	+ auditējamā dokumentācijas pārskatīšana;
	+ darba dokumentu sagatavošana;
	+ plāna precizēšana;
	+ papildus informācijas pieprasīšana;
* vizīte auditējamā struktūrvienībās:
	+ pirms vizītes sanāksme ar auditējamo un informācijas sniegšana par audita apjomu, vizītes laiku un vietu, u.c. jautājumiem;
	+ pārbaudes, intervijas, inspekcijas, uz vietas esošo dokumentu pārbaude;
* audita rezultātu apkopošana:
	+ rezultātu noformēšana;
	+ novērojumu apkopošana;
	+ secinājumu izstrāde;
	+ audita ziņojuma projekta sagatavošana;
	+ auditējamā informēšana par audita ziņojuma projektu un tā secinājumiem;
	+ auditējamā komentāri par gala ziņojuma projektu un auditējamā korektīvo darbību ieviešanas plāns;
	+ sanāksme un diskusija ar auditējamo par audita ziņojuma projektu un korektīvo darbību izpildes plānu;
* audita gala ziņojuma apstiprināšana, ieteikumu ieviešanas plāna parakstīšana un audita slēgšana;
* pēcpārbaude - korektīvo darbību izpildes uzraudzība un nepieciešamības gadījumā vizīte uz vietas;
* audita lietas slēgšana.

### 3.1.6. Audita plānošana

Lai noteiktu auditā iekļauto daļu riska novērtējumu, attiecībā uz DPS daļām, Inspekcija katram auditējamajam izvērtē šādus faktorus:

* iesaistāmais resursu apjoms;
* izmaiņas/reorganizācija sistēmā;
* kompetenču pārvaldība;
* DPS sarežģītība;
* laiks no pēdējā veiktā audita.

Audits var tikt iedalīts kā:

* daļa no pastāvīgās drošības uzraudzības, kurā izvērtē pastāvīgo atbilstību prasībām un ir veicams saskaņā ar uzraudzības stratēģiju un plāniem;
* praktiskās darbības pārbaude, kas ietver pēc sertifikācijas laikā konstatēto problēmu uzraudzību vai uzraudzību pēc sūdzības, negadījuma, u.c.

Auditā ietilpst arī pēcpārbaudes, kas tiek veikta, lai pārliecinātos, ka korektīvās darbības tiek ieviestas un tās ir efektīvas.

Plānojot auditu, KDD vadītājs izveido audita grupu, kura sastāv no:

* lēmuma pieņēmējs;
* audita grupas vadītājs;
* audita grupas vadītāja vietnieks;
* vērtētāji;
* dokumentu pārbaudītājs.

Audita grupas locekļu pienākumu un atbildības sadalījumu, kā arī kompetences nosaka Audita grupas reglaments. Audita grupa atbild par kvalitatīvi veiktu auditu un pārbaudēm.

Audita mērķis ir DPS efektivitātes novērtēšana, kurā:

* nosaka DPS atbilstību tiesību aktu prasībām;
* konstatē par DPS iespējamo uzlabojumu veikšanu;
* pārbauda auditējamā atbilstību Regulas 2018/763[[4]](#footnote-4) kopējām prasībām;
* iegūst un uztur pārliecību par auditējamo spējām sniegt pieņemami drošu pakalpojumu;
* veicinauzlabojumu ieviešanu auditējamo organizācijas pārvaldības sistēmā;
* novērtē dzelzceļa negadījumu izmeklējumu rekomendāciju ieviešanu.

Plānojot auditu:

* nosaka audita apjomu un sfēru, piemēram:
	+ organizācija, kura tiks pakļauta auditam;
	+ DPS apjoms (lielums);
	+ DPS sarežģītības pakāpe;
	+ pēc vajadzības, ņemot vērā arī audita mērķi, nepieciešamo laiku, veikšanas biežumu, procesu skaitu un sarežģītību;
* nodrošina attiecīgo auditu veikšanai nepieciešamo dokumentu savākšanu, piemēram:
	+ sertificēšanas dokumenti;
	+ saņemtā operatīvā informācija;
* piemēro atbilstošāko metodi, piemēram:
	+ intervija;
	+ inspekcija;
	+ anketēšana;
	+ faktisko darbību pārbaude;
* novērtē auditējamā brieduma pakāpi, piemēram:
	+ auditējamam kopumā;
	+ atsevišķām DPS daļām;
* izvēlās kompetentāko personālu, ņemot vērā nodarbināto kompetences, piemēram:
	+ DPS daļām;
	+ visai sistēmai kopumā;
* ņem vērā laiku pārbraucieniem;
* atbilstošākos resursus.

KDD vadītājs seko līdzi, lai tiktu nodrošināta audita programmas izpilde, analizē un nepieciešamības gadījumā to uzlabo.

KDD nodrošina, ka uzraudzības auditi tiek efektīvi vadīti un organizēti plānotā un sistemātiskā veidā.

Pirms audita uzsākšanas tiek organizēta audita grupas sanāksme. Izvērtējot nepieciešamos resursus, DPS stratēģisko plānu un gada plānu, tiek sastādīts auditējamā DPS audita plāns.

Audita plānu sagatavo audita grupas vadītājs. Plānam jābūt elastīgam, lai pieļautu izmaiņu iespējas, kuras var būt nepieciešamas veicot praktiskās pārbaudes uz vietas.

Audita grupas vadītājs nosaka katra auditora atbildību par audita veikšanu. Audita grupas vadītājs ņem vērā auditoru priekšlikumus, kompetences un lomas. Izmaiņas var veikt audita laikā, lai nodrošinātu audita mērķa sasniegšanu.

Plānojot audita laiku, tajā ieskaita sanāksmi ar auditējamās organizācijas vadību un audita grupas sanāksmes. Audita plānu paziņo auditējamai organizācijai ievada (*kick-off*) sanāksmē. Plānu var precizēt ievada sanāksmes laikā, tajā veiktajām korekcijām jābūt dokumentētām protokolā.

**3.tabula. Audita plāna struktūra**

|  |  |
| --- | --- |
| Audita nosaukums | (nosaukums) |
| Audita identifikācijas numurs | (lietas indekss un gads) |
| Auditējamā rekvizīti  | (reģistrācijās numurs, nosaukums, adrese, tālrunis, e-pasts) |
| Auditējamā struktūrvienības (ja ir nepieciešamība) |  |
| Audita mērķis |  |
| Audita grupa: |  |
| Audita grupas vadītājs | (amata nosaukums, vārds uzvārds) |
| Audita grupas vadītāja vietnieks | (amata nosaukums, vārds uzvārds) |
| Auditori | (amata nosaukums, vārds uzvārds) |
| (amata nosaukums, vārds uzvārds) |
| **Audita programma** |  **Stundu skaits** | **Plānojamais termiņš** |
| Plānošana  |  |  |
| * Ievada sanāksmes (*kick-off*) organizēšana ar auditējamo
 |  |  |
| Dokumentu pārbaude (plāna precizēšana un papildus informācijas pieprasīšana un saņemtās informācijas izskatīšana) |  |  |
| * Pirms pārbaudes sanāksme auditējamam
 |  |  |
| Faktiskā pārbaude |  |  |
| Rezultātu apkopošana (rezultātu noformēšana, novērtēšana, audita ziņojuma projekta izstrādāšana, secinājumu, ieteikumu izstrāde) |  |  |
| * Sanāksme par audita ziņojuma projektu
 |  |  |
| Audita gala ziņojuma apstiprināšana un audita slēgšana (audita ziņojuma precizēšana, ieteikumu ieviešanas uzraudzība un nepieciešamības gadījumā pēcpārbaude) |  |  |
| **Kopā** |  |  |
| **Nr.p.k.** | **DPS daļas un apakšsadaļas** | **Ietilpst auditā (jā/nē)** | **Nozīmētais auditors/i** |
|  | (DPS daļu un apakšsadaļu nosaukumi, kurus plāno auditēt) |  | (vārds uzvārds) |
| Iepriekšējā audita novērojumu rezultāti un ieteikumu ieviešanas statusa (izpildes) izvērtēšana (ja tādi ir) |
|  |
| Cita informācija |
|  |

### 3.1.7. Ievada sanāksme

Inspekcija uzaicina auditējamo organizāciju uz ievada sanāksmi, lai informētu par audita mērķi, plānu, programmu un audita grupas sastāvu. Šajā sanāksmē Inspekcija lūdz komunikācijai norādīt auditējamās organizācijas kontaktpersonas.

Sanāksmē piedalās vadošais auditors un divi auditori, auditējamās organizācijas vadības pārstāvji un audita grupas sekretārs.

Ievada sanāksmes mērķis ir informēt auditējamo par:

* audita mērķi;
* audita plānu;
* audita programmu;
* audita grupas sastāvu;
* par to, kā tiks veiktas audita darbības;
* sniegt iespēju auditējamajam uzdot jautājumus.

Ievada sanāksmē apskata šādus jautājumus:

* dalībnieku iepazīstināšana, nosakot arī kādu darbību veikšana katram ir paredzēta konkrētā auditā laikā;
* audita mērķis, sfēras un kritēriji;
* audita grafiks;
* citas svarīgas vienošanās ar auditējamo, piemēram, noslēguma sanāksmes datums un laiks, kā arī jebkuras starpposma sanāksmes starp audita grupu un auditējamā vadību un jebkuras sekojošas izmaiņas;
* metodes un procedūras, kas tiks izmantotas pārbaudes laikā;
* informācija par audiopierakstu veikšanu[[5]](#footnote-5);
* oficiālo komunikācijas kanālu apstiprināšana starp auditējamo un audita grupu;
* auditā lietojamās valodas apstiprināšana, ja audits tiek nodrošināts ar citu dalībvalstu drošības iestādēm;
* apstiprinājums, ka audita laikā auditējamais tiks informēts par audita gaitu;
* apstiprinājums, ka resursi un aprīkojums, kas nepieciešami audita grupai ir pieejami;
* apstiprinājums jautājumiem par konfidencialitāti;
* apstiprinājums par darbu drošību audita laikā (darba drošības noteikumu ievērošana);
* informācija par neatbilstību klasifikāciju;
* informācija par apstākļiem, kuru dēļ audits var būt pārtraukts;
* informācija par apstrīdēšanu, audita izpildi un secinājumiem.

Audita sanāksme ir formāla un audita grupai ir jāsastāda ievada sanāksmes dalībnieku saraksts, kuru iekļauj un uzglabā audita lietā.

### 3.1.8. Sākotnējā dokumentu pārbaude

Auditori analizē informāciju, kas ir saistīta ar paredzamo auditu un sagatavo auditam nepieciešamos darba dokumentus, kuri būs nepieciešami audita veikšanai.

Pēc audita plāna sastādīšanas, Inspekcija nodrošina tās rīcībā esošo dokumentu izvērtēšanu. Visi grupas dalībnieki, lai izvairītos no informācijas dublēšanās, pēc kārtas aizpilda dokumentu izvērtēšanas veidlapu. Darba dokumentu izmantošana neierobežo audita darbības robežas, kuras var mainīties audita laikā iegūtās informācijas rezultātā.

**4.tabula. Dokumentu pārbaudes protokols**

|  |  |
| --- | --- |
| **Audita identifikācijas numurs** | lietu nomenklatūras indekss |
| **Auditējamais (tā struktūrvienība)** | (reģistrācijās numurs, nosaukums, adrese, tālrunis, e-pasts) |
|  |  |
| **Auditors (vārds, uzvārds)** | (vārds, uzvārds) |
| **Auditora amats** | (amata nosaukums) |
| **Pārbaudes datums** | (dd.mm.gggg.) |
| **DPS daļa** | DPS daļas nosaukums |
| 1. **Izskatītie dokumenti**
 |  |
| **Nr.p.k.** | **Dokumenta nosaukums** | **Identifikācijas numurs** | **Izdošanas datums** |
|  |  |  |  |
|  |  |  |  |
| 1. **Novērojumi**
 |  |
| **Nr.p.k.** | **Novērojumi** |
|  |  |
|  |  |

Audita grupa izskata DPS un ar tiem saistītos dokumentus, izvērtē citu pieejamo informāciju (dzelzceļa satiksmes negadījumu izmeklēšanas materiālus, sūdzības u.c.).

Ja nepieciešama papildus informācija, lai gūtu pārliecību par DPS darbību, audita grupa sagatavo auditējamai organizācijai pieprasījumu par papildu dokumentu vai skaidrojumu iesniegšanu. Auditā var izmantot arī citu informācijas avotu, piemēram, atgriezeniskā saite no klientiem, informācija no ārējām organizācijām, sistēmas, tīmekļvietnes, u.t.t.

Dokumentācijas izskatīšanas termiņu var noteikt individuāli atkarība no plānotā audita apjoma.

Auditori var arī izveidot pēc pašu auditoru brīva ieskata kontrolsarakstus un var papildināt ar auditam nepieciešamajiem daļām.

Pēc DPS dokumentācijas izvērtēšanas, tiek organizēta atkārtota audita grupas sanāksme, lai precizētu un koriģētu audita plānu. Nepieciešamības gadījumā tiek sagatavots koriģētais audita plāns.

### 3.1.9. Pirms pārbaudes sanāksme

Vismaz desmit darba dienas pirms vizītes, audita grupa organizē auditējamai organizācijai pirms pārbaudes sanāksmi, lai informētu par vizītes/inspekcijas norises gaitu, DPS audita apjomu, auditoru pienākumiem un tiesībām un audita procedūrām. Nepieciešamības gadījumā pirms pārbaudes sanāksmes laikā veic plāna precizēšanu. Veiktās korekcijas dokumentē un atzīmē audita plānā.

Pirms pārbaudes sanāksmē Inspekcija informē:

* kuri auditori veiks pārbaudes/inspekcijas;
* kurās struktūrvienībās vai vietās tiek plānotas pārbaudes, intervijas u.t.t.;
* kad tiek plānotas pārbaudes;
* ar kuriem auditējamās organizācijas pārstāvjiem tiek plānotas pārbaudes vai intervijas;
* kādi papildus dokumenti tiks skatīti, ja ir radusies papildus nepieciešamība.

Pirms pārbaudes sanāksmi dokumentē.

### 3.1.10. Komunikācija pārbaudes, vizītes laikā

Atkarībā no audita sarežģītības pakāpes var būt nepieciešamība veikt formālu komunikāciju starp auditējamās organizācijas pārstāvjiem un auditoriem paša audita laikā.

Ja rodas problēmas, auditors informē audita grupas vadītāju par problēmām audita laikā. Audita grupas vadītājs par problēmām rakstiski ziņo auditējamās struktūras vadītājam. Rakstiskais paziņojums var būt gan elektroniskais pasts, gan oficiāli sagatavots paziņojums (dienesta ziņojums) par konstatētajām problēmām pārbaudes jeb audita laikā.

Par pierādījumiem, kas ir savākti audita laikā un kuri sniedz informāciju par bīstamu risku (drošība, vide) auditors nekavējoties ziņo auditējamai organizācijai un audita grupas vadītājam. Šādā gadījumā tiek sagatavots pārbaudes protokols ar kritiskiem punktiem, kā dēļ ir nepieciešams ierobežot satiksmi vai to slēgt.

Gadījumos, ja audita pierādījumi norāda uz audita mērķa sasniegšanas neiespējamību auditors par to ziņo audita grupas vadītājam. Savukārt, audita grupas vadītājs ziņo auditējamai organizācijai. Šādā gadījumā audita grupas vadītājs pieņem lēmumu par nepieciešamām izmaiņām audita plānā vai audita pārtraukšanu. Audita plāna izmaiņas saskaņo ar auditējamo organizāciju.

### 3.1.11. Praktiskās pārbaudes

Pārbaudes laikā audita grupa uz vietas pārbauda auditējamās organizācijas praktisko procedūru izpildes atbilstību DPS noteiktiem pasākumiem, vai atbilst Regulas 2018/762 I un II pielikumam[[6]](#footnote-6) un, vai DPS ir efektīva.

Katrs audita grupas dalībnieks pārbaudes laikā aizpilda auditā iesaistīto auditējamās organizācijas personu sarakstu, kuru papildina katru dienu un katrā pārbaudes vietā. Sarakstā norāda auditējamās organizācijas pārstāvja vārdu, uzvārdu, struktūrvienību un pārbaudes dienu, par ko auditējamās organizācijas pārstāvis sarakstā parakstās.

**5.tabula Auditā iesaistīto personu saraksts**

|  |  |
| --- | --- |
| **Audita identifikācijas numurs** | (lietas indekss un gads) |
| **Auditējamais** | (reģistrācijās numurs, nosaukums, adrese, tālrunis, e-pasts) |
| **Auditors** | (vārds, uzvārds) |
| **Auditora amats** | (amata nosaukums) |
| **Nr.p.k.** | **Vārds, uzvārds** | **Struktūrvienība** | **Vieta** | **Datums** | **Paraksts** |
|  |  |  |  |  |  |

Auditā var būt piemēroti šādas uzraudzības metodes:

* intervija ar darbiniekiem;
* anketēšana;
* praktiskās darbības novērtēšanas pārbaude;
* punktveida pārbaude;
* darbību veidu, darba apstākļu un darba vides novērojumi;
* informācijas analīze un salīdzināšana (politika, mērķi, standarti, instrukcijas, licences, atļaujas, specifikācijas, līgumi, pasūtījumi u.c.), efektivitātes rādītāju novērtēšana, sistēmu, tīmekļvietņu datu analīze;
* inspicēšana - mērīšana un cita tehniskā kontrole, darbību veidu, darba apstākļu un darba vides novērojumi.

Katrs audita grupas dalībnieks, veicot pārbaudi, noformē pārbaudes lapu, kurā atspoguļo pārbaudes laikā visus izskatītos dokumentus, veiktās pārbaudes, intervijas un novērojumus un neatbilstības. Novērojumus pamato ar pierādījumiem un norāda piemērojamās prasības un/vai to īstenošanas mehānismus (auditējamā DPS dokumentācija, rokasgrāmatas utt.) saistībā ar kuriem audits veikts. Pārbaudes protokols un pārrunu protokols tiek aizpildīts elektroniski.

**6.tabula Pārbaudes protokols**

|  |  |  |  |
| --- | --- | --- | --- |
| **Pārbaudes/intervijas datums** |  |  |  |
| **Audita identifikācijas numurs** | (lietas indekss un gads) |
| **Auditējamā organizācija** | (reģistrācijās numurs, nosaukums, adrese, tālrunis, e-pasts) |
| **Auditējamās organizācijas struktūrvienība** | (struktūrvienības nosaukums) |
| **Auditors** | (vārds, uzvārds) |
| **Auditora amats** | (amata nosaukums) |
| **Auditora paraksts** | (elektroniskais paraksts) |
| **Pārbaudes/intervijas vieta** | (pārbaudes vieta) |
| **DPS daļa** | (daļas nosaukums) |
| 1. **Pārbaudes laikā izskatītie dokumenti**
 |
| **Nr.p.k.** | **Dokumenta nosaukums** | **Identifikācijas numurs** | **Izdošanas datums** |
|  |  |  |  |
|  |  |  |  |
| 1. **Pārbaudes**
 |
| **Nr.p.k.** | **Pārbaudes** |
|  |  |
| 1. **Pārrunu protokols**
 |
| **Intervējamais** |  |
| **Intervējamā amats** |  |
| **Nr.p.k.** | **Jautājums** | **Atbilde** |
|  |  |  |
|  |  |  |
| 1. **Neatbilstības (obligāti ieviešanas pasākumi)**
 |
| **Nr.p.k.** | **Neatbilstība**  | **Atsauce uz procedūru, dokumentu, u.c.** |
|  |  |  |
|  |  |  |
| 1. **Novērojumi (iespējamie pasākumi)**
 |
| **Nr.p.k.** | **Novērojums** |
|  |  |
|  |  |

Pārbaudes protokola pārbaužu daļā mērīšanas vai novērtēšanas rezultātus norāda, ja ir veikta:

* ritekļu pārbaude;
* infrastruktūras objekta pārbaude;
* tehniskā aprīkojuma pārbaude;
* darba vietas tehniskā aprīkojuma pārbaude;
* mācību tehnisko uzskates līdzekļu pārbaude;
* u.c. gadījumi.

Auditors katrā pārbaudes vietā gatavo atsevišķu pārbaudes lapu. Ja ir viena pārbaudes vieta vairākas dienas, gatavo vienu pārbaudes lapu.

Intervijas laikā uzdod korektus un precīzus jautājumus, lai intervējamais būtu spējīgs sniegt izsmeļošu atbildi. Cenšas uzdot netiešos jautājumus, lai gūtu pārliecību par personāla kompetenci.

Ja pārbaudes laikā tiek konstatēti trūkumi dzelzceļa infrastruktūrai vai ritekļiem, kas apdraud dzelzceļa satiksmes drošības stāvokli, cilvēku veselību, apkārtējo vidi, kuru dēļ jāaizliedz dzelzceļa infrastruktūras vai ritošā sastāva ekspluatācija, KDD nekavējoties pieņem lēmumu par dzelzceļa infrastruktūras vai ritošā sastāva ekspluatācijas apturēšanu, informējot par lēmumu auditējamās organizācijas pārstāvi un nodrošina pārbaudes protokola sastādīšanu.

### 3.1.12. Audita konstatējumi

Audita konstatējumus novērtē pēc audita mērķiem, sfēras un kritērijiem, lai iegūtu audita atklājumus (atbilstības, neatbilstības un novērojumus).

**2.shēma Audita konstatējumi**



Vajadzības gadījumā audita grupa tiekas, lai pārskatītu audita konstatējumus attiecīgajos audita posmos. Atbilstību audita kritērijiem apkopo, lai norādītu auditējamā aprakstītos procesus, kuri tika auditēti.

Neatbilstības pamato ar pierādījumiem un norāda vai piemērojamās prasības īstenojas auditējamā procesos (DPS, instrukcijas, rokasgrāmatas utt.), saistībā ar kuriem audits veikts.

### 3.1.13. Audita ziņojuma sagatavošana un apstiprināšana

Par katru auditu tiek sastādīts audita ziņojuma projekts.

Audita ziņojuma projektā norāda informāciju par audita izpildes laiku, audita mērķi, audita apjoma aprakstu, kopējos secinājumus, audita novērojumus un secinājumus (rīcības plānu).

**7.tabula. Audita ziņojuma saturs**

|  |
| --- |
| Auditējamās organizācijas nosaukumsDrošības pārvaldības sistēmas audita ziņojuma projekts Nr. |
| Vieta, datums |  |
| **Audita mērķis un apjoms** |  |
| Ievadteksts un auditoru sastāvs, laika periods, pārbaudes vietas un auditējamās DPS daļas.  |
| **Kopsavilkums** |
| 1. Vispārīgs apraksts
2. Galvenie secinājumi:
	1. Neatbilstības (norāda skaitu);
	2. Konstatējumi (norāda galvenos)
	3. Vispārīgais brieduma līmeņa vērtējums (zemākais no daļām).
 |
| **Audita novērojumi un secinājumi** |
| **Nr.p.k** | **DPS daļa** | **Pierādījumi** | **Neatbilstība vai novērojums** | **Vērtējums** | **Rīcības plāns** |
|  | DPS daļa | Atsauces uz dokumentiem, procedūru aprakstiem | Apraksts | Līmenis (0-4) | Apraksts, termiņš |
| **Novērtēšanas kritēriji** |

Audita noslēguma ziņojumā norāda neatbilstību un/vai novērojumu skaitu. Neatbilstības tiek pamatotas ar tādiem dokumentiem (bet ne tikai) kā:

* tiesību aktiem;
* politika, iekšējās procedūras;
* instrukcijas, rīkojumi, tehniskās apkopes žurnāli un pieraksti u.c.
* rokasgrāmatas;
* līgumsaistības un vienošanās;
* apmācības, kvalifikācijas vai medicīniskie pieraksti;
* pārbaudes protokoli;
* atsevišķos gadījumos testu un uzdevumu izpildes rezultāti;
* iekšējo auditu ziņojumi;
* citi līdzīgi dokumenti, kurus uztur un uzglabā auditējamais.

Audita ziņojuma projektu audita grupa gatavo kopīgi, organizējot iekšējās sanāksmesun diskusijas par konstatētajiem novērojumiem. Katrai neatbilstībai piešķir vērtējumu. Audita ziņojuma projekta neatbilstības vai novērojumu daļā norāda konstatējumus, gan par prasību izpildi, gan par neizpildi, gan ,,labas prakses” piemērus, gan paņēmienus, kuri rada bažas.

Audita kopsavilkuma daļā var arī norādīt slēdzienu par:

* par DPS atbilstību audita kritērijiem;
* par DPS ieviešanu, funkcionēšanu un uzlabošanas rezultātiem;
* organizācijas vadības spējām analizēt DPS procesus.

Ziņojuma noslēgumā informē par ziņojuma apstrīdēšanas iespējām.

### 3.1.14. DPS daļu vērtējums un brieduma pakāpes noteikšana

Inspekcijas uzdevums ir pārraudzīt dzelzceļa sistēmas dalībnieku DPS veiktspēju, proti, jāgūst pārliecība, vai norādītais atspoguļo realitāti un pasākumi ir efektīvi. Katram līmenim ir sastādīts veikstpējas kritēriju apraksts (skatīt pielikumā). Vērtējums kalpo tikai kā vizuālais rādītājs novērojumiem.

Vērtējumu līmeņos norāda pie audita ziņojuma novērojumiem un secinājumiem. Gūtos datus aizpilda tabulā, kas ļauj noteikt līmeņus. Kopējo rezultātu atspoguļojumu ataino diagrammas veidā ziņojuma kopsavilkumā. Mērķi, apraksts un kritēriji kopējā un DPS daļu vērtējumam ir atainoti pielikumā.

DPS vērtējums ir, lai novērtētu auditējamā spēju kontrolēt drošības riskus darbības laikā. Ja DPS darbojas labi, darbības riski tiek labi kontrolēti. Ja DPS ir vājās vietas, riski šajās jomās netiek pienācīgi kontrolēti, un ir iespējams, ka šajās jomās ir vislielākā iespēja rasties apstākļiem, kas ļauj notikt negadījumam vai starpgadījumam. Vērtējumu veic par katru DPS daļu.

Jo zemāks ir rādītājs, jo labāka ir risku kontrole un procesi tiek pastāvīgi pilnveidoti. Novērtējot dzelzceļa sistēmas dalībnieka darbību ar vērtējumu “4”, Inspekcija nekavējoties pieņem drošības pasākumus. Novērtējot dzelzceļa sistēmas dalībnieka darbību ar vērtējumu “3”, Inspekcija var piemērot pagaidu drošības pasākumus un Inspekcija saskaņo korektīvo darbību izpildi pēc iespējas īsākā termiņā, kurš nav ilgāks par 3 mēnešiem.

**Ja auditējamajam tiek piešķirts 3. vai 4.līmenis, Inspekcija var pieņemt pagaidu drošības pasākumus riska līmeņa samazināšanai**.

Pagaidu drošības pasākumi var būt:

* sertifikāta vai apliecības apturēšana;
* infrastruktūras vai ritošā sastāva ekspluatācijas aizliegumi;
* dzelzceļa speciālistu atstādināšana;
* sliežu ceļu slēgšana;
* ritošā sastāva atstādināšana;
* u.c.

Novērtējot dzelzceļa sistēmas dalībnieka darbību ar vērtējumu “2”, Inspekcija saskaņo korektīvo darbību izpildes termiņu ne ilgāku par 6 mēnešiem. Novērtējot dzelzceļa sistēmas dalībnieka darbību ar vērtējumu “1”, Inspekcija korektīvo darbību izpildi pārbauda, veicot nākamo plānoto uzraudzības darbību.

Brieduma modelis ļauj identificēt DPS vājās vietas un, kur nepieciešams, veikt uzlabojumus. Ja auditējamajam tiek konstatēts zems risks, Inspekcija var pieņemt lēmumu uz laiku samazināt šīs organizācijas uzraudzību, salīdzinājumā ar pārvadātāju un manevru darbu veicēju (turpmāk- pārvadātājs) vai infrastruktūras pārvaldītāju, kam piešķirts augstāks risks.

### 3.1.15. Audita noslēguma sanāksme

Par audita ziņojuma projektu Inspekcija informē auditējamo, organizējot sanāksmi un prezentējot galvenos secinājumus un nepieciešamos uzlabojumus par DPS elementu darbību. Audita grupa sagatavo prezentāciju.

Audita noslēguma sanāksmi vada direktors. Sanāksmē piedalās audita grupa un auditējamās organizācijas vadības pārstāvji.

Sapulci vada tā, lai audita atklājumi (neatbilstības, novērojumi) un slēdzieni auditējamajai organizācijai ir saprotami un sniedz informāciju, ka audita noslēguma un neatbilstību ziņojumi, auditējamajam tiks nosūtīti oficiālā vēstulē divu nedēļu laikā pēc audita noslēguma sanāksmes dienas, kā arī tiek izskaidrota korektīvo darbību saskaņošanas kārtība.

Noslēguma sanāksmē audita grupas vadītājs paziņo, ja tādi ir bijuši, par tiem šķēršļiem, kas radās audita laikā un kas varēja samazināt ticamību audita slēdzienam. Jebkuras domstarpības starp audita grupu un auditējamo organizāciju apspriež un pēc iespējas tās atrisina. Ja nav vienota atrisinājuma par audita atklājumiem un slēdzienu, visus viedokļus fiksē noslēguma sanāksmes protokolā. Sanāksmes protokolu pievieno audita lietai.

Nepieciešamības gadījumā var tikt organizēta sanāksme, lai precizētu audita ziņojuma projektā un audita ieteikumu ieviešanas plāna projektā ietverto informāciju. Papildus Inspekcija aicina auditējamo sagatavot dokumentus par auditējama skaidrojumiem un precizējumiem, ja tādi ir, lai gūtu pārliecību par dokumentu esamību un patiesumu. Audita ziņojuma projektu paraksta audita grupas vadītājs.

Pēc auditējamā auditējama komentāru saņemšanas tiek sagatavots audita gala ziņojums un audita ieteikumu ieviešanas plāns. Audita gala ziņojumu un ieteikumu ieviešanas plānu paraksta audita grupas vadītājs un visi auditori. Audita ziņojumu apstiprina direktors.

### 3.1.16. Audita noslēguma ziņojuma nosūtīšana

Ja ir nepieciešams, Inspekcija var organizēt sanāksmi, lai precizētu audita ziņojuma projektā un korektīvo darbību ieviešanas plāna projektā ietverto informāciju. Papildus Inspekcija aicina auditējamo organizāciju sagatavot dokumentus par auditējamās organizācijas skaidrojumiem un precizējumiem, ja tādi ir, lai gūtu pārliecību par dokumentu esamību un patiesumu.

Pēc auditējamās organizācijas komentāru saņemšanas tiek sagatavots audita gala ziņojums un rīcības pasākumu ieviešanas plāns. Audita gala ziņojumu un ieteikumu ieviešanas plānu paraksta audita grupas vadītājs un visi auditori. Audita ziņojumu apstiprina direktors.

### 3.1.17. Rīcības plāni

Inspekcija audita ziņojumā iekļautā aile par rīcības pasākumu plānu, ļauj auditējamai organizācijai lemt par korektīvo darbību ieviešanu un atbildīgo personu nozīmēšanu.

Pēc noslēguma sanāksmes audita noslēguma ziņojuma projektu nosūta auditējamai organizācijai, lūdzot sniegt komentārus un priekšlikumus par rīcības pasākumiem DPS daļas uzlabošanai un termiņiem.

Pēc pasākumu plāna aizpildīšanas auditējamā organizācija iesniedz to Inspekcijai. Inspekcija, ja tas ir nepieciešams, sniedz komentārus par korektīvo darbību ieviešanu un termiņiem.

Audita grupas vadītājs uzrauga rīcības pasākumu plānu ieviešanas gaitu un pieņem lēmumu, par audita lietas slēgšanu vai pagarināšanu, ja ieteikums nav ieviests noteiktā laikā. Visus ieteikumus reģistrē audita reģistrā.

Visi dokumentārie pierādījumu tiek reģistrēti un uzglabāti “Organizācijas lietā”.

### 3.1.18. Pēcpārbaude

Rīcības pasākumu plāna uzraudzība notiek pēc auditējamās organizācijas sniegtās informācijas par rīcības pasākumiem.

Pēcpārbaudes laikā auditori pārbauda auditējamās organizācijas rīcības pasākumu plānu izpildi, pārliecinoties vai organizācija nodrošina pārmaiņas, lai uzlabotu DPS darbību un drošību kopumā.

Ieviešanas pasākumu rezultativitāti pārbauda attiecīgais auditors, kurš ir veicis DPS daļas pārbaudi.

### 3.1.19. Audita lietas slēgšana

Audits ir noslēgts, ja:

* audita darbi ir pabeigti;
* audita ziņojuma projekts ir nosūtīts auditējamam, saskaņošanai;
* ir saskaņots audita ziņojums;
* saskaņotais audita ziņojums ir nosūtīts auditējamam;

Nesaskaņots audita ziņojums nerada ierobežojumus audita slēgšanai.

Audita lietu slēdz, kad no auditējamā ir saņemta informācija un apliecinājumi par visu ieteikumu ieviešanu.

## 3.2. Praktiskās darbības novērtēšanas un punktveida pārbaudes

Pārbaudes mērķis ir pārliecināties, ka uzraugāmais objekts vai organizācija atbilst darbības tiesību aktu vai labās prakses prasībām un noteiktās darbības procedūras tiek ievērotas.

**3.shēma Pārbaužu veikšanas process**



### 3.2.1. Pārbaudes plānošana un sagatavošanās pārbaudei

Kopējā uzraudzības plāna ietveros, katra uzraudzības metode, šajā gadījumā, pārbaude balstās uz definētiem mērķiem un Inspekcijas uzraudzības metodēs noteiktiem kritērijiem.

Mērķis nosaka, kas ir jāpārbauda pārbaudes laikā, un tas var būt:

* DPS daļas pārbaude;
* sistēmas atbilstības noteikšana pēc kritērijiem;
* sistēmas atbilstības noteikšana pēc normatīvo dokumentu prasībām;
* pārbaudāmā joma jeb sfēra.

Pārbaudes mērķi nosaka KDD vadītājs un/vai vecākais inspektors, kurš pieņem lēmumu par pārbaudes uzsākšanu.

Pārbaudes joma jeb sfēra nosaka objektu (infrastruktūra, ritošais sastāvs, dzelzceļa speciālisti, u.t.t.), kurš tiks pakļauts pārbaudei. Nozīmētais vecākais inspektors izanalizē informāciju, kas ir saistīta ar paredzēto pārbaudi un sagatavo pārbaudei nepieciešamos darba dokumentus, kuri būs nepieciešami kā izziņu materiāls pārbaudes gaitas fiksēšanai.

Nozīmētais inspektors izanalizē informāciju, kas ir saistīta ar paredzēto inspekciju un sagatavo inspekcijai nepieciešamos darba dokumentus, kuri būs nepieciešami kā izziņu materiāls inspekcijas gaitas fiksēšanai.

Pārbaudes veic atkarībā no uzraudzībai pakļautās jomas lieluma. Pārvadātājiem un infrastruktūras pārvaldītājam pārbaudes piesaista pie DPS daļas.

### 3.2.2. Pārbaudes uzsākšana, pārbaudes laika noteikšana

Saskaņā ar uzraudzības plānu attiecīgais KDD inspektors uzsāk plānot pārbaudi.

Pārbaudes apjoms ir atkarīgs no:

* pārbaudes mērķa un ilguma;
* pārbaudāmo procesu skaita, sarežģītības un svarīguma;
* pārbaudes kritērijiem;
* iepriekšējo pārbaužu rezultātiem un analīzes (riska novērtējums, korektīvās darbības, u.c.);
* izmaiņām pārbaudāmajā organizācijā;
* atļaujas darbības termiņa.

KDD vecākais inspektors ieplāno noteiktus datumus pārbaudes veikšanai. Vismaz divas dienas pirms pārbaudes veikšanas informē organizācijas pārstāvjus par pārbaudi un tās mērķi (infrastruktūra, ritošais sastāvs, ekspluatācija, u.t.t.). Kontaktus ar pārbaudei pakļautās organizācijas struktūrvienības vadītāju nodibina attiecīgais vecākais inspektors vai KDD vadītājs. Komunikācijas laikā:

* apstiprina pārbaudes veikšanas pilnvaras;
* informē par pārbaudes grafiku un inspektoru, kurš veiks pārbaudi;
* pieprasa dokumentus, ja tādi ir nepieciešami pārbaudei;
* vienojas par pārbaudes kārtību;
* saskaņo pārbaudes laikā nepieciešamo pārbaudāmās organizācijas personālu, kas pavadīs vecāko inspektoru.

Ja pārbaudāmā organizācija nevar nodrošināt sava pārstāvja piedalīšanos pārbaudē, KDD vecākais inspektors nozīmē citu datumu tā paša mēneša vai nākamā mēneša ietvaros.

Ja ir jāveic pārbaude, kas prasa tūlītēju rīcību un tā nav ieplānota, KDD vadītājs nozīmē mutiski atbildīgo vecāko inspektoru. Atsevišķos gadījumos pēkšņās pārbaudes nepieciešamību var arī nozīmēt direktors.

### 3.2.3. Komunikācija ar pārbaudāmo organizāciju

Attiecīgais KDD vecākais inspektors ir atbildīgs par sākotnējo kontaktu nodibināšanu ar pārbaudāmo organizāciju, pirms tiek uzsākta plānotā pārbaude.

Komunikāciju ar pārbaudāmo organizāciju uztur, lai:

* noteiktu komunikācijas kanālu ar pārbaudāmo organizāciju;
* apstiprinātu pilnvaras veikt pārbaudi;
* paziņotu par pārbaudes sfēru un/vai pārbaudes mērķi;
* pieprasītu nepieciešamos dokumentus, ja tādi ir nepieciešami;
* informētu par nepieciešamību pārbaudes laikā nodrošināt pieeju attiecīgajiem objektiem vai vietām, personām un dokumentiem, ieskaitot pierakstiem;
* noteiktu pieņemamus drošības pasākumus darbības vietā;
* informētu par nepieciešamību vecāko inspektoru nodrošināt ar pavadītājiem.

### 3.2.4. Pārbaude uz vietas

Informācijas iegūšanas metodes ir:

* intervijas ar dzelzceļa speciālistiem un citām personām;
* darbību veidu, darba apstākļu un darba vides novērojums;
* dokumentu analīze (atklājumi, sertifikāti, atļaujas, instrukcijas, kārtības, tehnoloģiskie procesi, līgumi, u.t.t.);
* tehniskās kontroles, programmu realizācijas, mērījumu rezultātu pierakstu, sanāksmju protokolu, auditu ziņojumu u.c. izpēte;
* apkopojošo datu, tai skaitā negadījumu, analīžu rezultātu un efektivitātes rādītāju novērtēšana;
* informācijas iegūšana par pārbaudāmās organizācijas procesiem un sistēmām;
* citi informācijas avoti (atgriezeniskā saite no klientiem, informācija no ārējām organizācijām, piegādātāju novērtējuma pieraksti, negadījumu analīze, u.c.).

### 3.2.5. Pierādījumu savākšana un novērojumu aprakstīšana

Pārbaudes laikā savāc informāciju un pārbauda to atbilstību pārbaudes mērķiem, sfērai un kritērijiem (ieskaitot informāciju par pārbaudāmās organizācijas funkcijām, darbībām un procesiem). Šīs informācijas kopumu veido atklājumi. Atklājumus novērtē, salīdzinot tos ar pārbaudes mērķiem un kritērijiem, un salīdzināšanas rezultātā iegūst novērojumus.

Novērojumi var norādīt uz atbilstību vai neatbilstību noteiktiem kritērijiem. Tikai atklājumi, kas ir pārbaudāmi, kalpo par novērojumu. Visus atklājumus dokumentē pārbaudes protokolā. Pārbaudes rezultātā izveido slēdzienu par rezultātiem.

Visi novērojumi tiek dokumentēti un norādīti pārbaudes protokolā.

**8.tabula. Pārbaudes protokola paraugs**

|  |
| --- |
| Iestādes rekvizīti(sastādīšanas vieta) |
| **Pārbaudes protokols** |
| (dd.mm.gggg.) | Nr. (lietas indekss un numurs) |
|  |  |
|  | Organizācijas nosaukums |
|  | Organizācijas reģ.Nr. |
|  | Organizācijas adrese |
|  |  |
| **Pārbaudes metode:** |  |
| [ ]  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| drošības pārvaldības sistēmas audits | praktiskās darbības novērtēšanas pārbaude | punktveida pārbaude | informācijas analīze | anketēšana | intervijas ar dzelzceļa sistēmas dalībnieku darbiniekiem | neplānota pārbaude | pēcnegadījuma pārbaude |
|  |  |  |  |  |  |  |  |
| **Norise:** |  |  |  |  |  |  |  |
| **Vieta** | **Datums** |
|  |  |
|  |  |
| **Pārbaudes mērķis vai joma** |
|  |
|  |  |
| **Novērojumi** (apraksts)**:** |
|  |
| **Rezultāti** (secinājumi): |
| **Nr. p.k.** | **Secinājumi** | **Vērtējumi**  | **DPS daļa**  | **Inspekcijas ierobežojumi** |
|  | Apraksta atklājumi | Piešķir riska pakāpi (0-4) | Atsauce uz DPS daļu |  |

**Rīcība:**

**Korektīvās darbības** (aizpilda pārbaudāmā organizācija)**:**

| **Nr.p.k.** | **Korektīvās darbības** | **Ieviešanas datums** |
| --- | --- | --- |
| **1.** | organizācija apraksta savas korektīvās darbības |  |
| **2.**  |  |  |
| **3.**  |  |  |

**Organizācijas piezīmes, ja tādas ir:**

**Pārbaudi veica:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| (amats) |  | (paraksts vai e-paraksts\*) |  | (paraksta atšifrējums) |
|  |  |  |  |  |
| (amats) |  | (paraksts vai e-paraksts\*) |  | (paraksta atšifrējums) |

\*drošs elektroniskais paraksts, skatīt elektronisko parakstu un laika zīmogu

**Organizācijas pārstāvis:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| (amats) |  | (paraksts vai e-paraksts\*) |  | (paraksta atšifrējums) |
|  |  |  |  |  |
| (amats) |  | (paraksts vai e-paraksts\*) |  | (paraksta atšifrējums) |

\*drošs elektroniskais paraksts, skatīt elektronisko parakstu un laika zīmogu

**Organizācijas pārstāvja kontaktinformācija:**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| (tālrunis) |  | (e-pasts) |

Veicot vērtējumu, pārvadātājiem un infrastruktūras pārvaldītājam, piemēro riska brieduma modeli pie attiecīgās DPS daļas. Pārējiem dzelzceļa sistēmas dalībniekiem, balstoties uz neatbilstības nopietnību, nosaka tikai kopējo riska pakāpi visai organizācijas sistēmai kopumā. Kritiskās neatbilstības ir definētas Inspekcijas Uzraudzības metodēs[[7]](#footnote-7).

Sagatavojot kopējo slēdzienu, KDD vecākais inspektors izanalizē pārbaudes novērojumus un novērtē atbilstību pārbaudes mērķiem.

Pēc slēdziena sagatavošanas inspektors saskaņo pārbaudāmās organizācijas piedāvātās korektīvās darbības un īstenošanas termiņus (saskaņā ar Inspekcijas Uzraudzības metodēs noteikto).

Sagatavojot pārbaudes protokolu KDD vecākais inspektors ņem vērā:

* pārbaudes mērķi;
* pārbaudes jomu jeb sfēru (piemēram DPS daļa, riteklis, u.t.t.);
* kritērijus, kas definēti Inspekcijas uzraudzības metodēs;
* reālus korektīvo darbību īstenošanas termiņus;
* iebildumus vai domstarpības starp inspektoru un pārbaudāmo organizāciju.

### 3.2.6. Pārbaudes protokola nosūtīšana

Pārbaudes protokolu ar neatbilstībām (ja tādas tiek atklātas) sagatavo divos eksemplāros, ja dokuments ir papīra veidā vai vienā eksemplārā, ja dokuments tiek parakstīts ar elektronisko parakstu. Sagatavoto pārbaudes protokolu (novērojumi, novērtējums u.t.t.) nosūta no oficiālā vēstulē ne vēlāk kā 10 darba dienu laikā pēc inspekcijas veikšanas dienas vai e-pastā, ja dokuments ir parakstīt ar elektronisko parakstu.

### 3.2.7. Korektīvās darbības

Korektīvo darbību pabeigšanu un to rezultativitāti pārbauda atbildīgais KDD vecākais inspektors, kurš ir sastādījis pārbaudes protokolu ar novērojumiem. Šīs pārbaudes var būt nākošās pārbaudes vai audita daļa.

Pēc pārbaudes protokola nosūtīšanas, pārbaudāmās organizācija sniedz komentārus, priekšlikumus par korektīvām darbībām, termiņiem un nozīmētām atbildīgām personām audita ieteikumu ieviešanā.

Attiecīgais KDD vecākais inspektors seko līdzi korektīvo darbību ieviešanā, tai skaitā pievienojot pārbaudes lietai dokumentārus pierādījumus par korektīvo darbību ieviešanu.

Visi dokumentārie pierādījumu tiek reģistrēti un uzglabāti “Organizācijas failā”.

### 3.2.8. Pārbaudes lietas slēgšana

Pārbaudi uzskata par pabeigtu, kad organizācija ir īstenojusi korektīvās darbības, un to ir pārbaudījis Inspekcijas inspektors.

Inspekcija var veikt pārbaudi objektā, lai pārliecinātos par korektīvo darbību īstenošanu un to efektivitāti, ja rodas pamatotas bažas par formālu attieksmi pret korektīvo darbību īstenošanu.

# 4. Dzelzceļa satiksmes negadījumu uzraudzība

Inspekcija uzrauga negadījumu izmeklēšanu, lai izvērtētu, vai tiek pienācīgi veikta cēloņu analīze un ieviesti attiecīgie pasākumi. Inspekcijas KDD vecākie inspektori analizē izmeklēšanas rezultātu pārskatus, lai izvērtētu vai attiecīgie novērojumi tiek izvērtēti un korektīvās darbības pieņemtas. Ir iespējams veikt organizācijas brieduma novērtējumu, pamatojoties uz novērojumiem.

## 4.1. Informācijas saņemšana un izbraukšana uz negadījuma vietu

Inspekcija informāciju par dzelzceļa satiksmes negadījumu saņem no publiskās lietošanas dzelzceļa infrastruktūras pārvaldītāja dežurējošiem darbiniekiem, tieši no dzelzceļa satiksmes negadījumā iesaistītām personām (piemēram, privātās lietošanas dzelzceļa infrastruktūras pārvaldītāja, pārvadātāja u.c.), negadījuma lieciniekiem vai masu informācijas līdzekļiem.

Attiecīgais KDD vecākais inspektors izvērtē saņemto informāciju un informē Inspekcijas vadību. Vadība pieņem lēmumu, vai KDD vecākajiem inspektoriem ir nepieciešamība doties uz negadījuma vietu.

Izbraucot uz negadījuma vietu, KDD vecākais inspektors ņem līdzi nepieciešamo ekipējumu un aizsargapģērbu atbilstoši gadalaikam un negadījuma apstākļiem. Uz negadījumu, kas noticis ar bīstamām kravām, nodarbinātais obligāti nodrošinās ar personīgās aizsardzības ekipējumu – aizsargmasku ar filtriem, aizsargapģērbu un aizsargapaviem.

## 4.2. Negadījuma vieta

KDD vecākais inspektors uz vietas noskaidro, kādas infrastruktūras pārvaldītāja un pārvadātāja personas atrodas negadījuma vietā, un saņem no tām sākotnējo informāciju par negadījumu, tā sekām, seku bīstamību apkārtējai videi vai cilvēka dzīvībai un kādi seku novēršanas darbi jau veikti un kura persona vada novēršanas darbus.

Ja pastāv būtisks apdraudējums apkārtējai videi vai cilvēka dzīvībai, KDD vecākais inspektors, lietojot personīgās aizsardzības līdzekļus, seko, kā tiek nodrošināti visi nepieciešamie pasākumi, lai mazinātu apdraudējumu apkārtējai videi vai cilvēka dzīvībai.

Kad apstākļi ļauj tuvoties negadījuma vietai, Inspekcija dokumentē drošības stāvokli un kāda varētu būt saistība ar negadījuma iespējamo cēloni, un, ja nepieciešams, veic foto vai video fiksāciju.

Notikuma vietā tiek sagatavots brīvas formas akts, kurā norāda:

* negadījuma datumu;
* negadījuma laiku;
* negadījuma vietu;
* ja nepieciešams, iesaistītos nodarbinātos (amats, vārds, uzvārds);
* negadījumā iesaistīto ritošo sastāvu;
* negadījuma aprakstu;
* citus datus, kuriem var būt nozīme novērtēšanai.

## 4.3. COR lietošana un dzelzceļa satiksmes negadījumu izmeklēšana

Lai nodrošinātu dzelzceļa satiksmes negadījuma izmeklēšanu, dzelzceļa infrastruktūras pārvaldītājs un pārvadātājs iespējami īsā laikā pēc negadījuma sagatavo un iesniedz informāciju vienotā dzelzceļa satiksmes negadījumu uzskaites sistēmā (turpmāk- COR)[[8]](#footnote-8), kuru līdz izmeklēšanas pārskata apstiprināšanai atjaunina un papildina, tiklīdz kļūst pieejama jebkāda trūkstošā informācija.

Inspekcija, izmantojot COR, uzrauga, vai izmeklēšana ir veikta pilnībā, izmeklēšanas pārskati ir atbilstoši sagatavoti un apstiprināti, izvērtēti visi cēloņi un apstākļi, sagatavoti secinājumi un ieteikumi dzelzceļa satiksmes drošības uzlabošanai, dzelzceļa satiksmes negadījumi ir atbilstoši klasificēti.

Pēc iesaistīto pušu izmeklēšanas pabeigšanas, attiecīgais KDD vecākais inspektors pieņem lēmumu par negadījuma izmeklēšanas rezultātiem, jo īpaši izvērtējot negadījumu cēloņu analīzi un korektīvās darbības.

Ja Inspekcija piekrīt izmeklēšanas pārskatā norādītajai informācijai, piecu darba dienu laikā tā, izmantojot COR, pieņem lēmumu par izmeklēšanas pabeigšanu. Ja Inspekcija nepiekrīt izmeklēšanas pārskatā norādītajai informācijai, piecu darba dienu laikā tā, izmantojot COR, informē par to organizācijas. Ja organizācija nepiekrīt Inspekcijas secinājumiem, Inspekcija piecu darbadienu laikā, izmantojot COR, pārsūta visus izmeklēšanas materiālus neatkarīgas izmeklēšanas veikšanai Transporta nelaimes gadījumu un incidentu izmeklēšanas birojam.

Veicot negadījumu uzraudzību, KDD vecākais inspektors identificē neatbilstības DPS daļā un to COR atzīmē.

Inspekcija, balstoties uz datiem, izvērtē drošības līmeni un piemēro pasākumus riska pakāpes samazināšanai, ja tādi ir nepieciešami. Riska pakāpi novērtē visai sistēmai kopumā un cietušajiem attiecīgajās kategorijās.

# 5. Administratīvie lēmumi

Inspekcija var izdot administratīvu lēmumu (tas var būt gan audita ziņojums, gan pārbaudes protokols, gan lēmums) attiecībā uz sistēmu, lai atjaunotu tās darbības drošību, kad pierādījumi norāda uz to, ka ir nepieciešama tūlītēja rīcība un atjaunotu vai uzturētu pieņemamu drošības līmeni.

Tādi var būt, ja:

* tiek apdraudēta cilvēku dzīvība vai veselība;
* satiksmes drošības būtiska pasliktināšanās;
* kaitējums apkārtējais videi;
* cilvēkfaktora ietekme, kuram ir augsta iespējamība radīt nopietnu un smagu ietekmi uz dzelzceļa drošību.

Ja drošība tiek apdraudēta, Inspekcija var:

* pārtraukt vilcienu satiksmi;
* apturēt sertifikātu, atļauju vai apliecību darbību;
* samazināt kustības ātrumu;
* aizliegt tehnisko līdzekļu un ritošā sastāva ekspluatāciju.

Lēmumā norāda:

* apdraudošās situācijas identificējošo aprakstu;
* sistēmas vai tās daļas identifikāciju;
* nepieciešamās darbības un to pamatojumu;
* laika ierobežojumu pieprasītajām darbībām;
* lēmuma pieņemšanas datumu.

Inspekcija uzrauga pieņemtā lēmuma virzību un nepieciešamības gadījumā var veikt pēcpārbaudi. Veicot uzraudzības pasākumus, Inspekcijai ir jāgūst pārliecība, ka apdraudošā situācija vairs nepastāv un pieņem lēmumu par darbības vai ekspluatācijas atjaunošanu.

Inspekcija administratīvo procesu veic Administratīvā procesa likumā noteiktajā kārtībā.

# 6. Kompetences

Inspekcija uzraudzības procesā nodarbinātajiem piemēro kompetenču pārvaldības sistēmu. Papildus tam, lai nodrošinātu KDD nodarbināto kvalifikācijas uzturēšanu, KDD nodarbinātajiem divu gadu periodā ir jāpiedalās vismaz vienā auditā un vienā pārbaudē.

# pielikums

**Kritēriji vispārīgā līmeņa noteikšanai:**

|  |  |
| --- | --- |
| **4** | **Kritiska neatbilstība jeb nepietiekamas rīcības DPS uzturēšanā**. **Inspekcijai ir jāpieņem nepieciešamie pasākumi, lai pārtrauktu tiesību aktiem neatbilstošas rīcības.** **Inspekcija piemēro pagaidu drošības pasākumus, tostarp nekavējoties ierobežo vai aptur attiecīgās darbības.**Ir DPS, taču ir būtiski trūkumi, kuru dēļ rādītāju līmenis ir zemāks par tiesību aktos noteikto minimumu. Pastāv procedūras un norādījumi, lai pārvaldītu drošības pasākumus, bet uzraudzības laikā ir skaidrs, ka pastāv kopumā nopietnas problēmas. Atsevišķi riski tiek kontrolēti, tomēr vispārīgais process, kas to pārvalda, ir vājš. Organizācija praksē darbojas tādā veidā, ka, šķiet, pastāv būtiskas neatbilstības tam, kas aprakstīts DPS vai vispār nedarbojas.  |
| **3** | **Nopietna neatbilstība jeb DPS procesi nav atbilstoši un nav gūta pārliecība, ka riski tiek apzināti, kontrolēti un vadīti. Šī neatbilstība rada kritiskas neatbilstības iestāšanās risku.**DPS ir pietiekama, lai novērtējuma posmā tiktu piešķirts vienotais drošības sertifikāts vai drošības apliecība. Rakstveida DPS pastāv un tiek izmantota, lai kontrolētu drošības riskus, tomēr trūkst struktūras un saskaņotības. Sistēma kopumā ir saskaņota, tomēr dažādās jomās pastāv trūkumi, pieejas nesaskaņotība un nekonsekvence. Pamatā organizācija ar grūtībām tiek galā ar saviem pienākumiem drošības jomā. Pastāv liela varbūtība, ka rodas kritiska neatbilstība, 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 DPS izmantošanu. Ārkārtas risinājumu pieeja riska pārvaldībai ir ierasta parādība, kas rosina reaģēt uz negadījumiem vai starpgadījumiem, nevis proaktīvi veikt pasākumus to profilaksei. |
| **2** | **Pamata darbība**. **Neatbilstība, kur konstatēti trūkumi atsevišķos procesos**, taču ir vērojama konsekvence. DPS ir izstrādāta, lai izveidotu sistemātisku un konsekventu pieeju riska pārvaldībai. Visas daļas ir vietā un darbojas, un tiek ņemti vērā visi drošības aspekti. Uzmanība tiek pievērsta drošības kultūras uzlabošanai organizācijā, izstrādājot drošības kultūras uzlabošanas stratēģiju. Kaut arī organizācija ir konsekventa, trūkst risku iepriekšēja prognozēšana, kā arī tajā nav pietiekami attīstīta drošības kultūra riska pārvaldības procesa nodrošināšanai. Ārkārtas pasākumi ir snieguši pamatu pārdomātākai riska pārvaldības pieejai, tomēr pastāv varbūtība, lai organizācija atgrieztos nopietnas neatbilstības režīmā, piemēram, nespēja pārvaldīt galvenos procesus vai procedūras laika gaitā. |
| **1** | **Mērķtiecīgs. Novērojumi atbilst prasībām**, ir atsevišķas nepilnības dokumentos un/vai pierakstos. Šajā līmenī tiek prognozētas problēmas, identificēti riski.Tas ir tāds pats kā 2. līmenis, un papildus tam DPS pastāvīgi pārvalda riskus proaktīvi. Šeit organizācija uzrauga riska cēloņus un pēc iespējas rīkojas, lai nepieļautu nopietnus negadījumus. Organizācija ir apņēmusies attīstīt drošības kultūru, darbinieki ir iesaistīti darbībā, pārvaldot drošību attīstītā veidā. Šajā līmenī pastāv organizācijas augstākā līmeņa vadības izteikta līderība drošības nodrošināšanā, kam darbinieki uzticas un atbalsta.Tiek pievērsta uzmanība regulārai rādītāju pārskatīšanai un centieniem izprast tos riskus, ar kuriem organizācija saskaras, to raksturu un iespējamai rīcībai šajā jomā. |
| **0** | **Izcila. Procesi tiek kontrolēti un pastāvīgi pilnveidoti, riski apzināti un vadīti**. Izcila DPS darbība.Tāds pats kā 1. līmenis, un papildus tam DPS 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. Pastāv pierādījumi, ka organizācija apzinās pastāvošās un iespējamās problēmas, un aktīvi cenšas tās risināt, izmantojot DPS. Šajā līmenī organizācija ir pārliecināta par tās spēju pārvaldīt riskus, ar kuriem tā saskaras, un papildus cenšas arī ietekmēt tos, ar kuriem tai mijiedarbība. Organizācija tiecas mācīties no citu jomu pieredzes, ko var iekļaut savā darbībā. Drošība ir organizācijas darbības prioritāte. |

# pielikums

**Kritēriji DPS daļu vērtējumiem pa līmeņiem**:

## Organizācijas konteksts (O)

|  |  |
| --- | --- |
| **Mērķis:** | Organizācija definē darbības veidu, apjomu un jomu, jāparāda, kā tā nosaka nopietnus riskus, ar kuriem saskaras, jāidentificē “iesaistītās puses”, jānorāda, kā tā pilda juridiskos drošības pienākumus un kādi tie ir, kā arī jāpaskaidro DPS 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 DPS, tiek atspoguļotas reālajā ikdienas darbībā. |
| **Apraksts:** | Ir ļoti svarīgi, ka organizācija spēj paziņot uzraudzības iestādei savas darbības pareizo veidu, apjomu un jomu. Tas ir saistīts ar darbības robežu noteikšanu, kas jāatspoguļo organizācijas DPS. 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 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. |
| **O - Organizācijas konteksts** |
| **4** | Pastāv pamata apraksti, tomēr praksē ir novērojamas atšķirības starp DPS aprakstiem un realitāti. Pastāv pamatotas šaubas, vai organizācija efektīvi ievēro visas tiesību normas, kā tā apgalvo. Šķiet, ka ne visas iesaistītās puses ir pienācīgi atspoguļotas DPS pasākumos. |
| **3** | Pastāv visi apraksti, tomēr ir pamatotas bažas, ka darbības joma un apjoms nav pienācīgi aprakstīti. Ir apzinātas tiesiskās un citas prasības, kas ietekmē iesaistītās puses, tomēr šajā jomā ir konstatētas problēmas. Ir konstatētas dažas iesaistītās puses, kas nav iekļautas sākotnēji iesniegtajā DPS, vai pastāv pierādījumi, ka dažkārt nopietni riski netiek pienācīgi kontrolēti, kas attiecīgi ietekmē DPS efektivitāti. |
| **2** | Papildus 3.līmenim darbības apraksts, DPS apraksts un risku apraksts atbilst praksē redzamajam. Organizācija skaidri apzinās, ko dara, un zina mērķus uz kuriem virzās. Pastāv skaidrs priekšstats par to, kuri tiesību akti ir piemērojami, un ir apzinātas iesaistītās puses. |
| **1** | Papildus 2.līmenim, organizācija cenšas attīstīties un labāk sevi pierādīt iesaistītajām pusēm drošības jomā, kā arī sadarboties ar tām, lai izstrādātu drošākas procedūras un procesus DPS ietvaros. Organizācija aktīvi cenšas sadarboties ar attiecīgajām valsts iestādēm, lai izstrādātu stratēģijas tiesisko prasību ievērošanai. Robežas ar citām biznesa daļām ir skaidri saprastas un tiek pārvaldītas. |
| **0** | Papildus 1.līmenim, 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. |

## Līderība (L)

|  |  |
| --- | --- |
| **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. Par efektīvu uzskata tādu līderību, kura nosaka virzienu, paņēmienu, resursus un spēju ieviest atbilstošu kultūru uzņēmējdarbībā vēlamo mērķu sasniegšanai. Vadībai ir efektīvi jāvada organizācijas darbība tā, lai savā starpā 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 saistītās aktivitātes ir atbilstošas, pielietotas un efektīvas. Pārliecināties, ka vadības komunikācija ir konsekventa, skaidra un veidota tā, lai radītu labāko vidi drošības pārvaldībai. |
| **Apraksts:** | Vāja līderība izraisa ievērojamas drošības kļūdas. Organizācijas pieeja drošībai bieži vien atspoguļo to darbinieku attieksmi, kuri pieņem ar biznesu 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 drošības politikā ietverto komunikāciju (vīziju). Dzelzceļa drošības pasākumi ir integrēti biznesā. |
| **L1- Līderība un apņemšanās**Līderība un apņemšanās attiecas uz organizācijas augstāko vadību, kas nosaka virzienu un pozitīvu, uz attīstību vērstu ikdienas rīcību saviem darbiniekiem risku pārvaldībai visos biznesa procesos. Augstākā vadība nosaka toni un kultūru uzvedībai gan organizācijas iekšienē, gan tiem, kas sadarbojas ar šo organizāciju. Tiem darbiniekiem, kuri ieņem vadošus amatus, ir vislielākā ietekme uz organizācijas kultūru, organizācijas struktūru un tās efektīvu vadību. Tāpēc ir svarīgi, kā viņi pauž savus uzskatus visiem, kas strādā organizācijas labā. Ja iespējams, ir jāizvērtē, vai starp drošības pārvaldību un citiem biznesa procesiem nav pretrunīgu prioritāšu. |
| **4** | Procedūras un drošības mērķi ir novecojuši vai nav noteikti organizācijā, un trūkst 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.Trūkst pierādījumu organizācijas vadības interesei par drošības jautājumiem, jo ikdienas bizness ir svarīgāks. Ir grūti atrast resursus riska pārvaldības jautājumu risināšanai, jo organizācija nenovērtē, cik svarīgi ir tos izmantot šim nolūkam.Pa zemu ir atzīta tā svarīgā loma, kāda tā ir tiem cilvēkiem, kuri nodrošina drošus, efektīvus un kvalitatīvus pārvadājumus.Trūkst vadības apņemšanās īstenot drošības kultūru, un organizācijā trūkst 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 komunikācija par to notiek tik ierobežoti, ka organizācijā par to neviens nezina. Drošību uzskata par slogu, nevis par labumu organizācijai. Pozitīvas drošības kultūras īstenošanā organizācijas augstākā vadība neuzņemas virsvadību. Attiecībā uz starpgadījumiem un negadījumiem dominē fatālistiska kultūra (lai ko nedarītu, negadījumi vienalga 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.Drošības rādītāji ir sliktāki, nekā to prasa tiesību akti, un tāpēc Inspekcijai ir jāapsver, kā panākt, lai organizācija uzlabo savus rādītājus.  |
| **3** | Nepastāv saikne starp drošības un biznesa nodrošināšanas 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 atspoguļojumā DPS ir pretrunas un neskaidrības.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 no augstākā līmeņa vadības līdz zemākajam līmenim ir reaktīva (iesaistās tikai reaģējot uz problēmu). Vadības ieguldījums ir negatīvs, reaģējot tikai tad, 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 uzskata, ka ir svarīgi pārvaldīt cilvēkfaktoru un organizatoriskos faktorus, lai uzturētu un pilnveidotu organizācijas darbības rādītājus. Tāpēc resursi un cits atbalsts, kas vajadzīgi, lai īstenotu stratēģiju, faktiski nav pieejami.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis. Papildus tam darbiniekus aktīvi iesaista drošības politikas un drošības mērķu pārskatīšanā un pārstrādāšanā, kā arī to piemērošanā.Novērojamas pozitīvas drošības kultūras attīstības pazīmes. 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 vairāk dod priekšroku proaktīvai drošības nodrošināšanai, 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 drošības kampaņas (pasākumi) un uzraudzības kontrole, galvenokārt no augstākā līmeņa vadības lejup, tomēr ar darbinieku iesaistīšanu.Drošības pārvaldības sistēma ir konsekventa, kontrolējot lielāko daļu risku, kuri attiecas uz organizāciju. |
| **1** | Tas pats kā 2. līmenis. Papildus tam drošības mērķus atbalsta ikviena darbinieka rīcība, kurš ir vadības ķēdē.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:* pārskatīta un pārstrādāta, lai panāktu uzlabojumus paredzamā veidā; un
* vienādi interpretēta visās organizācijas daļās, kas to piemēro.

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 biznesa 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 koncentrējas uz veicinošiem un kavējošiem rādītājiem, izmantojot visus pieejamos datus.Ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītie jautājumi ir integrēti visās organizācijas darbībās, un augstākā vadība to atbalsta. |
| **0** | Tas pats kā 1. līmenis. 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 citās nozarēs.Tiek atzīts, ka drošības risku pārvaldība nav atsevišķa funkcija, bet produktīvas, konkurētspējīgas un rentablas organizācijas neatņemama sastāvdaļa.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 biznesa rādītājiem. Vadības ieguldījums drošībā ir liels, un organizācija dara visu, 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 organizācijā, gan arī plašāk nozarē. |
| **L2 – Drošības politika**Ar efektīvu drošības politiku nosaka skaidru virzienu, kas organizācijai jāievēro. Tā palīdz visiem biznesa aspektiem pastāvīgi uzlaboties. Drošības politika ir svarīgs dokuments, kas parāda, kā organizācija pārvalda savus pienākumus drošības jomā, kā arī līderību un ieguldījumu pienācīgā drošības pārvaldībā. |
| **4** | Politikas izklāsts ir novecojis vai nav zināms organizācijā. Nav pierādījumu, ka notiek apspriešanās ar darbiniekiem.Netiek pienācīgi atzīta cilvēku loma drošības un efektīvas darbības nodrošināšanā. Drošības politikā nav apņemšanās ievērot normatīvo regulējumu.Drošības rādītāju līmenis ir sliktāks par minimālo. |
| **3** | Drošības politika ir atjaunināta un ir zināma organizācijā, tomēr tās virziens vai interpretācija zemākā līmeņa vadītājiem un iekšējā uzraudzības procesā iesaistītajiem atšķiras. Tādējādi organizācijā drošības politiku piemēro atšķirīgi.Drošības politiku neuzskata par būtisku drošības uzturēšanai.Zināmā mērā atzīst to vērtību, ka cilvēka lomas izpratnes uzlabošana var veicināt biznesu, tomēr tas nenotiek konsekventi.Drošības politikā ir apņemšanās ievērot tiesību aktu prasības.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Papildus 3. līmenim, drošības politiku un citas saistītās politikas vadītāji izmanto kā paraugu, kas rezultējas tajā, ka 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. |
| **1** | Tas pats, kā 2.līmenis.Drošības politika ir atbilstoša ikviena vadības ķēdē esoša darbinieka vajadzībām.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 un pielāgo atbilstoši organizācijas briedumam un sarežģītībai, orientējoties uz uzlabojumiem laika gaitā.Drošības politika un saistītās politikas ir:* savstarpēji saskaņotas;
* pārskatītas un pārstrādātas, lai panāktu uzlabojumus paredzamā veidā; un
* vienādi interpretētas visās organizācijas daļās, kas tās piemēro.
 |
| **0** | Tas pats, kā 1.līmenis.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 biznesa rādītāju risku.Cilvēka lomu 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. |
| **L3 - Funkcijas, pienākumi un pilnvaras**Šīs prasības mērķis ir demonstrēt, ka organizācija ir strukturēta un tajā tiek sadalīti pienākumi, lai sasniegtu organizācijas vispārīgus mērķus un īstenotu drošības politiku. Var pastāvēt darba hierarhija, kura to atbalsta, raugoties no politikas un stratēģiskās perspektīvas.Riska uzraudzībai ir jābūt pārdomāti iekļautai pārvaldības struktūrās tā, lai būtu skaidra atbildības sadale. Pārvaldības struktūrām ir jāievēro un efektīvi jānovērš riski, ko rada mijiedarbība ar apakšuzņēmējiem, partneriem un piegādātājiem.Funkcijas, pienākumi un pilnvaras ir svarīgākie elementi, kas ļauj saprast, cik labi organizācijas drošības pārvaldības sistēma kontrolē risku. Organizācija parāda, 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 parāda, kā organizatoriskā struktūra un indivīda funkcijas un pienākumi nodrošina līdzsvaru starp atbilstību un drošības kultūru. Tas nozīmē domāšanas kultūru, nevis vienīgi drošības prasību ievērošanu tikai atbilstības dēļ. |
| **4** | 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 pienākumus.Funkciju un pienākumu sadalījums organizācijā netiek koordinēts un nav saistīts ar organizācijas darbības mērķiem.Darbības rādītāju līmenis ir sliktāks par līmeni, kas ir noteikts vienota drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | 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.Trūkst saskaņotības starp atsevišķām struktūrvienībām vai ar organizācijas biznesa plašāko mērķu uzdevumiem.Trūkst saskaņotības organizatoriskajās struktūrās un pienākumu sadalē, kas nepieciešams pienākumu efektīvai īstenošanai.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis.Papildus tam organizatoriskā struktūra atbilst pienākumiem, kuri ir skaidri sadalīti starp struktūrvienībām.Vispārējā politika un procedūras attiecībā uz funkcijām un pienākumiem atbilst attiecīgo struktūrvienību politikai un procedūrām.Pastāv kritēriji pienākumu un uzdevumu deleģēšanai un sadalei tādām funkcijām, kurām nepieciešama noteiktā 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 deleģēšanai ir sistēmiska pieeja. Deleģētie 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. |
| **1** | Tas pats kā iepriekš norādītajā 2. līmenī, tomēr ar skaidru saikni starp organizatoriskās struktūras daļām no organizācijas augšējā līdz zemākajam līmenim, bet nevis tikai darba uzdevumos.Vispārējā politika un procedūras ir izstrādātas tā, lai tās viena otru papildina organizācijas stratēģisko mērķu īstenošanas veicināšanai attiecībā uz visām struktūrvienībām.Atbildību par sniegumu no darbiniekiem, kuri atbild par drošību, prasa godīgi un konsekventi. Organizācijas kultūra ļauj par drošību atbildīgajiem darbiniekiem ietekmēt uzdevumu izpildi un veikt uzlabojumus.Pamatojoties uz izpratni par darba faktisko veikšanu, ir panākta individuālo un kolektīvo centienu atbilstība darbības rādītāju mērķiem. |
| **0** | Tas pats kā 1. līmenis.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 mainīgā organizācijā, stratēģijā un vidē. Organizācija savā sistēmā konsekventi uzskata indivīdu par pārskatīšanas procesa neatņemamu daļu. |
| **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, kāda ir drošības kultūra organizācijā un cik aktīvi tā iesaista attiecīgās trešās puses drošības pārvaldībā tajās jomās, kuri riski ir kopīgi. |
| **4** | Apspriešanās notiek reti vai nenotiek nemaz.Nodarbinātie nesaprot, kā viņi veicina savu un savu kolēģu drošību. Organizācija neatbilst minimālajām normatīvajām prasībām. |
| **3** | Darbinieki saprot, ka viņi ir atbildīgi par savu un kolēģu drošību, tomēr organizācijā tas nenotiek konsekventi.Notiek apspriešanās par drošības un veselības jautājumiem, tomēr, nav pierādījumu, ka tas notiek sistemātiski un aptver visus darbiniekus.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis.Papildus tam organizācijā ir izveidotas 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 noteiktās prasības piemēro vienādi. |
| **1** | Tas pats kā 2.līmenis.Organizācijai ir politika, kuras mērķis ir iesaistīt darbiniekus visos organizācijas līmeņos, un pastāv skaidra tās paziņošanas metode. Notiek apspriešanās ar darbiniekiem, kad tiek pieņemti lēmumi par riska kontroles pasākumiem.Organizācija regulāri apspriežas ar darbiniekiem dažādos veidos, piemēram, veicot aptaujas, rīkojot seminārus, sanāksmes ar vadītājiem un drošības paraugdemonstrējumus.Darbinieki ir motivēti sasniegt darbības mērķus un demonstrē konsekventu izpratni par to, kā tos sasniedz. Darbinieki spēj pieņemt lēmumus mērķu sasniegšanas ietvaros.Darbinieki ar līdzīgām funkcijām organizācijā prasības piemēro konsekventi.Personāls saprot pārmaiņu nepieciešamību un ir pierādījumi, ka ar viņiem konsultējas par pārmaiņu ieviešanu. |
| **0** | Tas pats, kā 1.līmenis.Organizācija pilnībā izmanto darbinieku un citu ieinteresēto pušu potenciālu un aktīvi iesaista viņus, lai izveidotu kopīgas vērtības, uzticēšanos, atklātību un pilnvarošanas kultūru.Organizācija izmanto darbinieku iesaistīšanos, lai apkopotu idejas uzlabojumiem un īstenotu tās praksē.Darbinieki demonstrē, 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. |

## Plānošana (PL)

|  |  |
| --- | --- |
| **Mērķis:** | Pārliecināties, ka organizācija spēj definēt un īstenot riska kontroli, kas ļauj organizācijai darboties droši. Pārliecināties, ka organizācija plāno drošas darbības un pienācīgi ņem vērā savu darbinieku un pārējo, kurus ietekmē tās darbības, labklājību. |
| **Apraksts:** | Laba plānošana ir sākuma punkts riska pārvaldīšanai. Organizācijai ir jāizstrādā attiecīgas procedūras, lai organizācija var izpildīt savus juridiskos pienākumus un darboties kā organizācijai, 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. |
| **PL1 – Riska novērtējums**Šis elements attiecas uz DPS būtību, un tā mērķis ir ļaut organizācijai parādīt, kā organizācijas sistēmas identificē un kontrolē riskus, ar kuriem tā saskaras. Uzraudzībā organizācijai ir jādemonstrē, kā organizācija praksē izmanto riska novērtējuma rezultātus, lai uzlabotu riska kontroli, kā arī kā šis process tiek uzturēts. Ir svarīgi atcerēties, ka šis elements tieši neattiecas uz pārmaiņu risku pārvaldību (kas ir vēl viens elements), bet ir saistīts ar to. Jānorāda, ka ir īpaša prasība ar risku novērtēšanas procesu 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 attiecīgajam normatīvajam regulējumam un ļauj organizācijai produktīvi un efektīvi sasniegt savus mērķus. |
| **4** | Organizācijai 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 novērtējumi nav pabeigti vai pārskatīti 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.Nav pierādījumu, ka riska novērtēšanā tiek ņemti vērā riski, kas saistīti ar cilvēkfaktora jautājumiem. Organizācijai nav apņēmības risināt šos jautājumus.Organizācijas darbības rādītāju līmenis ir sliktāks par līmeni, kas ir noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam.Riska novērtēšanas procesā nav pierādījumu, ka, pārvaldot pārmaiņas, pienācīgi ņem vērā drošības riskus, tostarp tos, kas saistīti ar cilvēkfaktoru un organizatoriskajiem faktoriem. |
| **3** | Riska novērtējums tiek veikts, bet par vispārējo koordināciju rodas šaubas.Darbības kontroles pasākumos 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 nepiemēro identificētos kontroles pasākumus.Apmācība par riska novērtējumu ir nodrošināta visiem attiecīgajiem darbiniekiem nepieciešamajā līmenī.Pastāv pierādījumi par riska kontroles pasākumu piemērošanu 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 DPS.Pastāv tikai daži pierādījumi, ka pārmaiņu pārvaldības procesā ņem vērā drošības riskus, tostarp ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītos jautājumus.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis.Papildus tam organizācijai ir skaidra politika attiecībā uz riska novērtējumu piemērošanu un to, kādi riski ir pieļaujami un kāpēc tas ir pieņemams.Riska pārvaldību konsekventi izmanto dažādās organizācijas daļās, tostarp pārmaiņu pārvaldības procesā. Vadītāji izprot savu funkciju šajā procesā.Tiek efektīvi izmantota risku kontrole un risku cēloņu novēršana. Vērtējumu koordinācija 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 riska novērtēšanas procesā identificētu riskus, kas saistīti ar cilvēkfaktoru un organizatoriskajiem faktoriem. Ja nepieciešams, organizācija var izmantot piesaistītu ekspertu zināšanas. |
| **1** | Tas pats kā 2. līmenis.Papildus tam riska novērtējumi ir iekļauti citos darbības aspektos, lai nodrošinātu sistēmisku pieeju riska kontrolei.Visu līmeņu darbinieki un ārējās organizācijas var sniegt savu ieguldījumu riska novērtēšanā.Riska novērtējums, ieskaitot riska cēloņu novēršanu, ir pārmaiņu procesa un organizācijas kultūras sastāvdaļa.Pārskatīšana ir riska novērtējuma procesa sastāvdaļa.Riska pārvaldības principus saprātīgi piemēro visos līmeņos.Pastāv kompleksa sistēma, lai pārbaudītu efektivitāti risku kontroles pasākumiem, kas ieviesti regulāras risku novērtēšanas rezultātā .Cilvēkfaktora un organizatorisko faktoru jautājumi ir pilnībā integrēti DPS riska novērtēšanas un pārmaiņu pārvaldības procesos. Tiem, kuri atbild par riska novērtēšanu, tiek sniegta atgriezeniskā saite par viņu sniegumu. |
| **0** | Tas pats kā 1. līmenis.Papildus tam riska novērtējums tiek izmantots, lai veicinātu nepārtrauktu organizācijas riska profila uzlabošanu.Riska pārvaldības pieeja ir ieviesta, un to konsekventi piemēro visā organizācijā. Riskus rūpīgi novērtē un apsver savlaicīgi pirms jebkādām pārmaiņām.Riska cēloņu novēršana ir konsekventas pieejas daļa un ir atspoguļota organizācijas politikā.Ir izveidotas proaktīvas procedūras riska kontroles pasākumu izstrādei sadarbībā ar citām organizācijām, kas ir atbildīgas par riska kontroli, ja pastāv starpnozaru jautājumi.Cilvēkfaktora un organizatorisko faktoru informāciju no riska novērtēšanas izmanto visā organizācijā, lai veicinātu nepārtrauktu drošības uzlabošanu. Novērtējumu rezultātus attiecīgos gadījumos kopīgo ar apakšuzņēmējiem, partneriem un piegādātājiem, lai uzlabotu šo organizāciju darbību efektivitāti. |
| **PL2 – Drošības mērķi un plānošana**Lai panāktu organizācijas atbilstību normatīvajām 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” *(Specific, Measurable, Achievable, Realistic and to a Suitable Timescale – SMART)*. Līdztekus plašākiem biznesa mērķiem ir jānosaka gan īstermiņa, gan ilgtermiņa drošības mērķi, kā arī jādefinē to prioritāte. Konfliktējošas prioritātes jāpārvalda tā, lai netiktu apdraudēti drošības mērķi salīdzinājumā ar citām biznesa vajadzībām. Dažādu līmeņu vai dažādu organizācijas daļu mērķiem jābūt pielāgotiem tā, lai tie atbalstītu organizācijas drošības politikas vispārējos mērķus. Ar atsevišķām personām var vienoties par personīgiem mērķiem, lai būtu pārliecība par organizācijas mērķu sasniegšanu. |
| **4** | Drošības mērķi (objectives) nav noteikti.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 neatbilst organizācijas vispārējās drošības politikas mērķiem.Organizācijas darbības rādītāju līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | 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 iespējams pretrunīgi, un tādējādi ne vienmēr atbalsta organizācijas drošības politikas vispārējos mērķus.Personīgie mērķi pārsvarā atbilst organizācijas vispārējās drošības politikas mērķiem. Tiek veiktas drošības pārbaudes, lai sasniegtu drošības mērķus.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis. Papildus tam ir noteikti drošības mērķi un pastāv drošības plāns, kas parāda, kā organizācija sasniegs tās mērķus.Noteiktajos drošības mērķos ievēro piemērojamās normatīvas un citas prasības.Ir mēģināts noteikt SMART mērķus un izvirzīt prioritātes mērķiem un uzdevumiem, kā arī savstarpēji saskaņot tos.Pastāv sistēma, lai sekotu mērķu sasniegšanai.Mērķu sasniegšana nav pienācīgi saskaņota ar pārskatīšanas procesu, t. i., pārskatīšanā neņem vērā izvirzītos mērķus.Darbinieki saprot savas darbības sasaisti un nozīmi, kā arī veidu, kā viņi palīdz sasniegt drošības mērķus un plāno pārvaldīt drošības riskus. |
| **1** | Tas pats kā 2. līmenis.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. |
| **0** | Tas pats kā 1. līmenis, un papildus organizācija salīdzina savus veiktspējas rādītājus ar citiem rādītājiem dzelzceļa nozarē un ārpus tās, lai pārliecinātos par mērķu atbilstību izcilībai. |

## Atbalsts (A)

|  |  |
| --- | --- |
| **Mērķis:** | Šīs prasības mērķis ir nodrošināt, lai organizācija piešķirtu pietiekamus resursus, tostarp kompetentu personālu, lai tie DPS var kontrolēt risku atbilstoši tās mērķiem.Noteikt 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. |
| **Apraksts:** | 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.Lai pārvaldītu drošību savā organizācijā ir ļoti svarīgi drošības pārvaldības sistēmā ietvert un ievērot visaptverošu kompetences pārvaldības sistēmu, kā arī ieviest attiecīgus informācijas apmaiņas pasākumus no vadības personālam un otrādi, kā arī citiem, kuri ir atkarīgi no komunikācijas no organizācijas puses. Šīs DPS daļa ir svarīgas tāpēc, ka tās atbalsta DPS produktivitāti un efektivitāti. Kompetenta darbinieka esamība amatā, kurš veic viņam uzticētos pienākumus, samazina tāda kļūdaina lēmuma pieņemšanas risku, kas sagrauj DPS darbību. Tajā pašā laikā jāpārliecinās, ka informācijas apmaiņas sistēma gan no augšas lejup, gan no apakšas augšup organizācijā nodrošina, ka atbildīgie darbinieki saņem svarīgāko informāciju savlaicīgi. |
| **A1 – 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. |
| **4** | 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 sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | 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.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis, un papildus tam organizācija var pierādīt, ka resursi ir pietiekami un to sadalījums ir konsekvents visās darbības jomās. Atsevišķu darbinieku prombūtne nav nozīmīgs jautājums, jo to risina DPS procesos. Organizācija sāk domāt par resursu efektīvāku izmantošanu. |
| **1** | Tas pats kā 2. līmenis, bet šeit organizācija prognozē savas nākotnes vajadzības, lai tā būtu jau iepriekš gatava gaidāmajām pārmaiņām un tai būtu nodrošināti resursi to pārvaldībai. |
| **0** | Tas pats kā 1. līmenis, un papildus tam organizācija resursu pārvaldību veic ļoti aktīvi, elastīgi izmantojot tos visā organizācijā lielākas drošības un efektivitātes sasniegšanai. |
| **A2 – Kompetence**Par drošību atbildīga personāla vadībai ir svarīgi, lai laika gaitā organizācija ieviestu 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. |
| **4** | 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 konsekvents process kompetences identificēšanai nepastāv.Apmācības nepieciešamība netiek pārvaldīta sistēmiski, un tūlītējas vajadzības ir svarīgākas pār ilgtermiņa attīstību.Organizācijas darbības rādītāju līmenis ir sliktāks, nekā noteikts vienotā 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. |
| **3** | 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.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. 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 zināmās kompetences.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, psihofizioloģiskie 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 ārkārtas 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. |
| **1** | Tas pats kā 2. līmenis, un papildus tam politikai attiecībā uz pieņemšanu darbā, 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 izmantoti mentori, 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. |
| **0** | Tas pats kā 1. 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. |
| **A3 – Komunikācija**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. |
| **4** | 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 sliktāks, nekā noteikts tā atbilstībai tiesību aktiem. |
| **3** | Šajā līmenī darbiniekiem sniedz vairāk informācijas, taču nav pierādījumu, ka tās formāts ir konsekvents un sniegtie ziņojumi visā organizācijā ir skaidri. Organizācija cenšas nodrošināt darbinieku sapratni par viņu nozīmi drošības veicināšanā drošības pārvaldības sistēmas ietvaros.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai.Savāktā informācija liecina, ka organizācijas drošības kultūra ir vāja un tās līmenis dažādās organizācijas daļās ievērojami atšķiras. |
| **2** | Tas pats kā 3. 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 DPS efektīvas darbības nodrošināšanā.Organizācijas drošības kultūra šķiet konsekventa, bet joprojām pastāv daži trūkumi, un tā netiek pilnveidota. |
| **1** | Tas pats kā 2. 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 DPS gūst vajadzīgos rezultātus. |
| **0** | Tāds pats kā 1. 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 organizāciju ceļā uz tās mērķiem. |
| **A4 – Informācija un komunikācija**Lai pieradītu atbilstību šajā elementā ir nepieciešams, lai organizācija savā DPS dokumentācijā sniegtu pietiekamus pierādījumus, ka tai ir attiecīgi līdzekļi, lai dažādos līmeņos identificētu ar drošību saistītu informāciju un paziņotu to īstajā laikā un īstiem darbiniekiem. Ir paredzēts pētīt nākotnes iespējas, lai pašreizējā riska kontrole joprojām būtu atbilstoša un aktuāla, lai varētu noteikt jaunus draudus un iespējas, ko rada ārējā ietekme (politiskā, sociālā, vides, tehnoloģiskā, ekonomiskā un juridiskā ietekme). Lai organizācija 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 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 ziņas; kā arī
* norādījumi un ziņojumi.
 |
| **4** | Trūkst pierādījumu par organizācijas mēģinājumiem sniegt attiecīgu drošības informāciju. Ja procedūras ir ieviestas, darbinieki pieņem lēmumus, pamatojoties uz savu spriedumu.Informācija par drošību tiek vākta vai izplatīta nepietiekošajā līmenī.Vadītāji nerunā ar “nevadošiem” darbiniekiem, 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 sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | Personāla rīcībā ir procedūras un kārtības 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 ir ievērojams konsekvences trūkums.Zināmā mērā tiek atzīta drošībai būtiskas komunikācijas nozīme, lai nodrošinātu drošu darba izpildi. Pastāv pierādījumi, ka tiek izstrādāti drošības komunikācijas nodrošināšanas plāni.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis, un papildus tam darbības rakstveida mērķu, kārtību 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 atbalsta procedūras drošības mērķu sasniegšanai. Darbinieki ziņo par savu sniegumu un pieredzi, jo organizācija veicina un atbalsta 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 nodefinēta. Komunikācijas uzraudzība un novērtēšana notiek regulāri |
| **1** | Tas pats kā 2. 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. |
| **0** | Tas pats kā 1. 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 organizācijai ir mijiedarbība, kā arī ar apakšuzņēmējiem.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. |
| **A5 –Dokumentēšana**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. |
| **4** | DPS dokumentācija ir sagatavota. Tā neietver visas organizācijas darbības, un to regulāri neatjaunina pēc jebkura veida pārmaiņām, kas to prasītu. Dokumentācija netiek pareizi izplatīta vai kopīgota. Organizācija neizmanto DPS kā “darba instrukcijas”, darbības prakse ir atšķirīga un bieži vien ir saistīta ar personāla un darbinieku personīgo atmiņu un vēsturisko praksi, neņemot vērā pagājušo laiku un pārmaiņas, kuru dēļ tās var būt nepieciešamas.Dokumentāciju izmanto tikai sertificēšanas/atļaujas saņemšanas mērķiem.Dokumentu kontroles sistēmas ir vājas, tāpēc dažādas organizācijas daļas izmanto dažādas dokumentu versijas.Organizācijas darbības rādītāju līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | Organizācija parasti strādā saskaņā ar procedūrām un instrukcijām, kas izveidotas DPS. Ir iespējamas dažas novirzes. Ir reģistrēta zināma informācija par svarīgiem riska kontroles pasākumiem, tomēr ieraksti ir nekonsekventi.Ikgadējais drošības pārskats, ko iesniedz valsts drošības iestādei, iekļauj organizatorisko struktūru, drošības mērķus nākamajam gadam un to izvēles iemeslus. Tajā iekļauj arī informāciju par iekšēju negadījumu un starpgadījumu izmeklēšanu, detalizētu informāciju par izvēlētajiem drošības rādītājiem, lai pārraudzītu savu sniegumu salīdzinājumā ar izvirzītiem mērķiem, kā arī informāciju par aktuāliem valsts izmeklēšanas iestādes ieteikumiem.Dokumentu kontroles sistēma parasti ir uzticama, taču pastāv problēmas ar versiju numerāciju un dokumentu sistemātisku atjaunināšanu.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis, un papildus tam ir reģistrēta galveno risku procesu un kārtību informācija. Svarīgu informāciju un lēmumus, kas varētu būt vērtīgi nākotnē, reģistrē.Pastāv darbību apraksts attiecībā uz drošības pārvaldības procesiem un šo procesu mijiedarbību DPS ietvaros. Personāls konsekventi īsteno drošības pārvaldības procesus.Ir izpratne par darba izpildes procesiem un citiem darbības līgumiem, ieskaitot detalizēto informāciju par drošības risku kontroli. Pastāv apakšuzņēmēju, partneru un piegādātāju aktuāls saraksts ar sniegtā pakalpojuma veida un apjoma aprakstu, ko atjaunina ikreiz, kad ir izmaiņas uzdevumos.Dokumentu pārvaldības sistēma ir uzticama un spēj nodrošināt, ka apritē atrodas tikai dokumenta jaunākā versija. |
| **1** | Tas pats kā 2. līmenis, un papildus tam lietotājiem un lēmumu pieņēmējiem ir pieejami visaptveroši dati par procesiem saistībā ar drošību, ar tiem saistītajiem riskiem un kārtībām, lēmumiem un informāciju.Dokumentu kontrole ir pietiekami attīstīta, lai signalizētu, kad dokumenti ir jāatjaunina un kurš par to ir atbildīgs. |
| **0** | Tas pats kā 1. līmenis, un papildus tam plašāk izmanto procesu, lai veicinātu pārvaldības sistēmas produktivitāti un efektivitāti. DPS atspoguļo pārvadātāja/ infrastruktūras pārvaldītāja faktisko darbības praksi. DPS ir dokuments, kas nepārtraukti mainās un attīstās, lai uzlabotu drošību, nevis administratīvs slogs.Dokumentu kontroles sistēmas darbojas, lai uzlabotu un attīstītu DPS, un tās tiek uzskatītas par noderīgu līdzekli DPS mērķa konsekvences nodrošināšanai. |
| **A6 – Cilvēkfaktora un organizatorisko faktoru integrēšana**  |
| **4** | Pastāv cilvēkfaktora un organizatorisko faktoru (turpmāk-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, darba vietas, darba sistēmu un rīku veidošanā maz tiek ņemtas vērā lietotāju vajadzības. Paļaujas uz komerciāli pieejamām ražotāju procedūrām, tās maz pielāgojot vai nemaz nepielāgojot organizācijas konkrētajām vajadzībām, un procedūras, neiesaistot lietotājus, izstrādā citas personas, nevis lietotāji. Par lietotāju vajadzībām darba vidē tiek domāts maz. |
| **3** | Ir atzīts, ka jānosaka riski, kas saistīti ar cilvēku rīcību, bet tie netiek noteikti visā organizācijā konsekventi.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 tiem 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. |
| **2** | Tas pats kā 3. līmenis, un papildus tam tiek atzīts, kādu vērtību var dot speciālās zināšanas par COF.Organizācijā visi izprot COF jēdzienu, un visi saprot, cik svarīgi ir izmantot sistēmisku pieeju COF, lai panāktu efektīvu drošību organizācijā.Visās organizācijas daļās tiek piemērota sistēmiska 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 sistēmiski izmantot COF organizācijas drošības un efektivitātes sasniegšanai. |
| **1** | Tas pats kā 2. 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 organizācijas 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 COF 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 COF saistītā spēja tiek mērīta, pielāgota un ir samērīga ar organizācijas brieduma un sarežģītības pakāpi un vērsta uz uzlabošanos laika gaitā. |
| **0** | Tas pats kā 1. līmenis, un papildus tam veids, kā organizācija sevi prezentē, ir orientieris 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 organizācijas darbība un 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 COF saistītos jautājumus. |

## Ekspluatācija (E)

|  |  |
| --- | --- |
| **Mērķis:** | Pareiza operatīvo darbību, saskarsmju 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. |
| **Apraksts:** | Šajā sadaļā ir ietvertas tās DPS daļas, kas attiecas uz mijiedarbību (piemēram, ar apakšuzņēmējiem, piegādātājiem un avārijas dienestiem), aktīvu pārvaldību laika gaitā un pārmaiņu pārvaldību. Jebkurai organizācijai ir izšķiroši svarīgi konstruktīvi un efektīvi pārvaldīt šīs jomas visa biznesa interesēs. Tā ir DPS daļa, kas nodarbojas ar pārvadātāja vai infrastruktūras pārvaldītāja darbības praktiskajiem aspektiem. Šajā sadaļā ir skaidra sasaiste ar vispārējo DPS 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 (turpmāk- SITS OPE), kas nosaka operatīvās pamatprocedūras, kas jāievēro visās funkcionālajās darbības jomās. Tā kā valsts drošības iestādēm ir jāapstiprina atbilstība SITS OPE, šie daļas ir jāpārbauda uzraudzības laikā. |
| **E1- Darbības plānošana un kontrole**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. |
| **4** | 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 nesistēmiski.Riska novērtēšanas procesi netiek pareizi piemēroti operatīvajām darbībām. Ir nepietiekošas vai vispār neeksistē operatīvas kontroles procedūras, kuras atspoguļotu darba faktisko situāciju, nevis idealizētu versiju, kas liecina par to, ka ar cilvēkfaktoru un organizatoriskajiem faktoriem saistītie jautājumi faktiski nav ņemti vērā operatīvo darbību īstenošanā.Organizācijas darbības līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam.Atbilstība SITS OPE noteiktajiem darbības pamatprincipiem ir ierobežota vai netiek ievērota. |
| **3** | Organizācija ņem vērā atbilstošās savstarpējas izmantojamības tehniskās specifikācijas un attiecīgā gadījumā valsts noteikumus, tomēr tas nenotiek sistēmiski un papildu pasākumi nav skaidri pamatoti ar riska novērtējuma rezultātiem.Darbinieki zina savus pienākumus 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 sistēmiski, tātad daži cilvēkfaktori un organizatoriskie faktori tiek ņemti vērā, bet nepietiekoši.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai.SITS OPE tiek ievērotas, bet tikai minimālajā pieņemamajā līmenī. |
| **2** | Tas pats kā 3. 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. |
| **1** | Tāds pats kā 2. 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 apakšuzņēmēju 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. |
| **0** | Tas pats kā 1. 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 līdzīgām organizācijām kā labo praksi. |
| **E2- 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. |
| **4** | 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.Ir nepietiekoši vai vispār nepastāv jauna aprīkojuma plānošanas un izveides kritēriji.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 ir novecojusi (nav aktuāla).Lietošanas ierobežojumu reģistrēšanai nav sistēmas, un sistēma objektu izņemšanai un atgriešanai atpakaļ pakalpojumā ir nepilnīga.Aktīvu veidošana koncentrējas uz komerciālo pieejamību, nevis atspoguļo lietotāja vajadzības.Organizācijas darbības līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | 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 stāvokli. Informācija tiek kopīgota, tomēr nesniedz pilnīgu priekšstatu par aktīvu pēc tā izveides. Informācija par to, kā un kad pielietot 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.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. 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 izmantošanas plāni ar skaidru norādi par pārvaldītu izslēgšanu no aktīvu bāzes.Tiek izmantoti pieejamie projektēšanas standarti, ar kuriem ņem vērā cilvēkfaktora principus, un paraugpraksi. Ir izveidots testa režīms aktīva izmantošanā, ietverot cilvēkfaktora jautājumus. Galalietotāji sniedz ieguldījumu prasību definēšanā un testēšanas procesā. Pārmaiņu procesu pārvaldība (skat. E4 “Pārmaiņu pārvaldība”) ietver cilvēkfaktora jautājumus kā projekta izskatīšanas daļu. |
| **1** | Tas pats kā 2. 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 izmantošanu. Ir skaidrs mehānisms, kā aktīvu pārvaldīšanas procesā iekļaut informāciju par aktīvu stāvokļa pārmaiņām un pārvaldīt 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. |
| **0** | Tas pats kā 1. 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. |
| **E3- Apakšuzņēmēji, partneri un piegādātāji**Organizācijām ir efektīvi jāuzlabo savu apakšuzņēmēju, 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 apakšuzņēmēju pārvaldību un to nodevumu pārbaudi saskaņā ar noteiktajām specifikācijām ir pārvadātājs/infrastruktūras pārvaldītājs. Apakšuzņēmēju, partneru un piegādātāju izmantošana nenozīmē, ka pārvadātājs/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 apakšuzņēmēju un citu piegādātāju kompetenci un novērtētu to drošības rādītājus kā daļu no iepirkuma procesa.Galvenās apakšuzņēmēja kontroles daļas ir šādas:* skaidri definēti līguma nosacījumi;
* skaidri noteikta darba specifikācija;
* apakšuzņēmēja izvēle;
* apakšuzņēmēja iepazīstināšana ar objektu (ja nepieciešams);
* produktu drošības un kvalitātes kontrole;
* atļauja strādāt (ja nepieciešams);
* darba nodošana un pieņemšana tā beigās;
* veiktspējas uzraudzība un pārskatīšana.

Kāda vai visu iepriekš minēto elementu trūkums vai nepilnīgums būs svarīgs rādītājs lēmumu pieņemšanā organizācijas brieduma līmenī. |
| **4** | Apakšuzņēmēja izmantošanas potenciālā ietekme uz organizācijas drošības rādītājiem netiek novērtēta, un izrietošās organizatoriskās pārmaiņas netiek pienācīgi pārvaldītas. Organizācija īpaši necenšas identificēt vai sadarboties ar citām organizācijām attiecībā uz kopīgu risku kontroli. Apakšuzņēmuma līgumi, ja tādi pastāv, neņem vērā drošības ierobežojumus, un apakšuzņēmējs neapzinās savu atbildību par drošību. Procedūras, kā to panākt, ir vājas vai arī to vispār nav. Kultūras ziņā pastāv tendence nedalīties informācijā attiecībā uz risku kontroli.Drošības informācija netiek vākta vai nodota citai pusei, un līguma noteikumi to neprasa.Apakšuzņēmējus nozīmē, kad nepieciešams. Tomēr, izvēloties apakšuzņēmējus, ir tikai ar izmaksām saistīti apsvērumi. Piemēram, līgumslēdzēja agrākie drošības rādītāji nav starp atlases kritērijiem iepirkuma procesā. Nepietiekoša uzmanība ir veltīta darbu plānošanai un risku kontroles pienākumiem, lemjot par darba izpildes veidu.Nepietiekoša uzmanība ir pievērsta apakšuzņēmēju uzraudzībai vai izpildīta līguma kontrolei. Īstas cilvēkfaktora un organizatorisko faktoru stratēģijas nav, bet tas, kas ir, uz apakšuzņēmējiem, partneriem un piegādātājiem neattiecas.Organizācijas darbības līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | Ar procedūrām faktiski nosaka mijiedarbības starp struktūrvienībām darba līmenī. Sadarbība ar pārējām organizācijām ir saistīta ar īstenojamām procedūrām un kārtībām, taču tā nav sistēmiska. Darbinieki to izmanto dažām kopīgām risku pārbaudēm, kas šajā līmenī ir identificētas.Daži risku kontroles pasākumi ir paredzēti apakšuzņēmēja kontrolei, taču nepastāv sistēmisks process no to atlases līdz kontrolei pēc līguma.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai.Cilvēkfaktora un organizatorisko faktoru stratēģija pienācīgi neaptver apakšuzņēmējus, partnerus un piegādātājus. |
| **2** | Tas pats kā 3. līmenis, un papildus sistēmiski tiek identificēta organizatoriskā mijiedarbība ar apakšuzņēmējiem, partneriem un piegādātājiem.Ir ieviestas procedūras un kārtības, lai kontrolētu kopīgus riskus, ar skaidri identificēto atbildīgo pusi.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 kārtību veidā), faktiskie dati un ziņas, kā arī instrukcijas un ziņojumi.Tiek atzīta apakšuzņēmēju kontroles nozīme, un tas ir atspoguļots organizācijas attiecīgajā politikā. Apakšuzņēmējus izvēlas atbilstoši viņu spējai veikt darbu droši un apmierinošā līmenī.Līguma izpildes laikā tiek uzraudzīts apakšuzņēmēja sniegums, un, lai tam sekotu, tiek efektīvi izmantoti attiecīgi izpildes rādītāji.Cilvēkfaktora un organizatorisko faktoru stratēģija aptver attiecīgus jautājumus, kas saistīti ar apakšuzņēmējiem, partneriem un piegādātājiem, tāpēc ir skaidrs, kādas ir viņu funkcijas un pienākumi savu darbinieku pārvaldībā. |
| **1** | Lēmumi un pasākumi atbilst visai informācijai, kas sniegta 2. līmenī.Visā organizācijā ir pasākumi informācijas apmaiņai, lai veicinātu efektīvu pārskatīšanu un pastāvīgu uzlabošanu.Pastāv sistēmiska pieeja apakšuzņēmēju kontrolei.Efektīva atbilstības prasību sistēma izmanto līdzsvarotu pieeju, tostarp ņemot vērā potenciālo apakšuzņēmēju drošības rādītājus.Visos līguma darbības posmos ir skaidra atbildības izpratne. Labas darba attiecības starp pasūtītāju un visiem apakšuzņēmējiem tiek nodrošinātas, izmantojot efektīvus mijiedarbības pasākumus, tostarp cilvēkfaktora un organizatorisko faktoru stratēģiju, caur kuras prizmu aplūko organizācijas attiecības ar tās apakšuzņēmējiem, 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. |
| **0** | Tāds pats kā 1. līmenis, un papildus tam organizācija pievērš uzmanību citiem sektoriem un valstīm sistēmas drošības problēmu un sasniegumu identificēšanai, lai vajadzības gadījumā iekļautu tos savu apakšuzņēmēju, partneru un piegādātāju pārvaldības pasākumos.Lai labāk sasniegtu kopīgos mērķus, tiek izmantots organizācijas un tā apakšuzņēmēju, partneru un piegādātāju komandas darbs.Labu praksi kopīgo ar citām organizācijām, tostarp apakšuzņēmējiem, partneriem un piegādātājiem. Līgumslēdzēja piegādes ķēde nevainojami nodrošina visus organizācijas mērķus.Apakšuzņēmēja un organizācijas galvenie un drošības pasākumi ir saskanīgi.Apakšuzņēmēja darbinieku un organizācijas 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. |
| **E4- 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. |
| **4** | 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 sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | 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.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. 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. |
| **1** | Tas pats kā 2. 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. |
| **0** | Tas pats kā 1. 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. |
| **E5- 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 daļas ietver:* paredzamu ārkārtas situāciju identificēšanu;
* pasākumu izstrādāšanu rīcībai šādās ārkārtas situācijās;
* atbilstošas apmācības nodrošināšanu un pārliecību, ka ir pieejami nepieciešamie resursi;
* plānu pārbaudi, ja nepieciešams, ar citiem cilvēkiem un organizācijām.
 |
| **4** | Organizācija nav identificējusi 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 negadījumu.Organizācijas darbības līmenis ir sliktāks, nekā noteikts konkrētajam vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | Organizācija ievēro noteikumus un praksi, ko pieprasa ārējas struktūrvienības/organizācijas, piemēram, infrastruktūras pārvaldītājs vai citi pārvadātāji, 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.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. 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 dalītos informācijā 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. |
| **1** | Tas pats kā 2. 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. |
| **0** | Tas pats kā 1. 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. |

## Darbības rādītāju novērtējums (N)

|  |  |
| --- | --- |
| **Mērķis:** | Novērtējuma mērķis ir pārliecināties, ka riska kontroles pasākumi ir izveidoti un darbojas pareizi, sasniedzot organizācijas mērķus. |
| **Apraksts:** | 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.Iekšējā 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.Pārraudzība, revīzija un pārskatīšana veido atgriezeniskās saites cilpu vispārējā drošības pārvaldības sistēmā un ir būtiskas pastāvīgas uzlabošanas un izcilības sasniegšanas programmu daļa. |
| **N1- Pārraudzība**Organizācijai jāspēj pierādīt, ka tā ir izveidojusi drošības pārvaldības sistēmas piemērošanas un efektivitātes pārraudzības 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 DPSdarbības traucējumus. |
| **4** | 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 biznesa nepieciešamība pārvaldīt un novērtēt cilvēkfaktora un organizatorisko faktoru jautājumus. Ja tos ņem vērā, tad pēc ātras nepieciešamības (ad hoc) principa.Organizācijas darbības līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam.Nav atzīta vajadzība pārraudzīt organizācijas drošības kultūru. |
| **3** | Pārraudzība tiek īstenota, bet tas bieži notiek haotiski: daži procesi tiek pārraudzīti un dažas iekārtas tiek pārbaudītas, tādējādi pieeja datu vākšanai ir nekonsekventa.Dokumentācija ir nodalīta un netiek analizēta organizācijas līmenī. Tā sekas ir rīcības plāni, kuri nav skaidri definēti un nav saskaņoti organizācijas līmenī.Nav skaidras saiknes starp drošības politiku, organizācijas drošības mērķiem un uzlabošanas rīcības plāniem.Vadība neatzīst vajadzību pārraudzīt riska kontroli, un tas ir atsevišķu nodaļu vai vienību atbildībā izlemt, kādu informāciju apkopot.Ir atzīts, ka cilvēkfaktoram un organizatoriskajiem faktoriem ir nozīme uzņēmējdarbībā, tomēr to piemērošana nav konsekventa.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai.Organizācijas drošības kultūra tiek uzraudzīta ierobežotā apmērā. |
| **2** | Tas pats kā 3. līmenis, un papildus organizācija mēģina izmantot attiecīgo kopīgās drošības metodi, lai pārbaudītu drošības pārvaldības sistēmas pareizu piemērošanu un visus tajā ietvertos procesus un procedūras, kā arī īsteno visas korektīvās darbības, kas nepieciešamas identificēto neatbilstību dēļ.Pārraudzība ir process, tomēr tajā nav noteiktas prioritātes pārraudzīt būtiski svarīgās un neaizsargātās sistēmas. Rādītāju izvērtēšana notiek vērtēšanas pēc, nevis ar skaidri noteiktu mērķi.Saikne ar riska novērtējumu aprobežojas ar riska kontroles pasākumu identificēšanu, kurus pēc tam pārrauga vesela saprata līmenī.Pārraudzības 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 pārraudzībai nav noteiktas prioritātes saskaņā ar riska novērtējuma rezultātiem.Darbības rādītāju novērtēšanā ir apstiprināts process, lai pārbaudītu cilvēkfaktora un organizatorisko faktoru jautājumu ietekmi DPS darbībā. Tā novērtēšanai vajadzības gadījumā ir pieejamas speciālistu īpašās zināšanas.Ir ieviests konsekvents drošības kultūras pārraudzības process. |
| **1** | Tas pats kā 2. līmenis, un papildus tam ir izpratne par būtisko un viegli ievainojamo sistēmu pārraudzību.Attiecīgās kopīgās drošības metodes (turpmāk-CSM (Common Safety Methods)) tiek pilnībā piemērotas, un pārraudzība ir pilnībā balstīta uz risku. Būtiski nozīmīgiem procesiem ir noteikta prioritāte resursu piešķiršanā.Vadītāji un pārraudzības veicēji ir labi apmācīti, un tiem ir nepieciešamie resursi, kā arī pastāv pierādījumi par pašreizējo darba sistēmu pārbaudēm trūkumu noteikšanai.Vidējā un augstākā līmeņa vadītāji pārrauga rezultātus, pamatojoties uz riska apsvērumiem, un rīcības plānus koordinē un apspriež organizācijas līmenī. Pārraudzības mērķis ir nepieļaut drošības rādītāju pasliktināšanos un meklēt uzlabojamās jomas, nevis tikai novērtēt DPS rezultātus.Ir specifiski rādītāji, kas ļauj novērtēt cilvēkfaktora un organizatorisko faktoru ietekmi uz DPS piemērošanu un izsekot kontroles procesu.Drošības kultūras pārraudzības process tiek veikts regulāri, un tā rezultāti tiek izmantoti drošības kultūras stratēģijas uzlabošanā, lai nodrošinātu pastāvīgu uzlabošanos. |
| **0** | Tas pats kā 1. līmenis, un papildus tam tiek izmantoti uzlaboti pārraudzības 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 pārraudzība ir iekļauta visaptverošā pārraudzības procesā, ietverot visas struktūrvienības un nodaļas. Organizācijai ir visaptveroša datu pārvaldības sistēma, lai izsekotu tās aktīvu datubāzi un izmantošanas nosacījumus.Organizācija apzinās, cik svarīgi ir izmantot riska modeļus un dalīties ar datiem 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 organizācijā.Pārraudzības 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 pārraudzību. Iegūto informāciju kopīgo ar partneriem, piegādātājiem un līgumslēdzējiem.Drošības kultūras pārraudzības process ir piemērs tam, kā šādi pasākumi būtu jāveic gan organizācijā, gan ārpus tās. |
| **N2- Iekšējā revīzija**Iekšējā revīzija ir būtiska neatkarīga un sistēmiska riska kontroles un vadības pasākumu pārbaude ar mērķi nodrošināt biznesa mērķu sasniegšanu. Iekšējās revīzijas nepieciešamību nosaka arī CSM attiecībā uz pārraudzību. Revīzijas parasti ir paredzētas, lai mēģinātu ierobežot subjektivitāti, atbalstot uz pierādījumiem balstītu pieeju. Revīziju sistemātiskums DPS kontekstā ir paredzēts, lai sniegtu augstākā līmeņa vadībai skaidrus pierādījumus, uz kuriem balstīt lēmumus drošības rādītāju uzlabošanai. |
| **4** | Trūkst vai vispār nav pierādījumu par revīziju veikšanu.Veiktie auditi nav plānoti vai prioritizēti, un uz to konstatējumiem netiek reaģēts. Auditori netiek konsekventi apmācīti, un saikne ar CSM procesu ir nepilnīga.Audita process nav strukturēts, starp auditiem un pārbaudēm nav reālas atšķirības.Organizācijas darbības līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | Auditi vispār notiek, bet izmantotajās metodēs un aptvertajās jomās neņem vērā konkrētās riska kontroles sistēmas būtību vai nozīmību.Ir auditu plāni, tomēr tie nav saskaņoti.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis, un papildus tam ir pierādījumi par koordinētu, efektīvu un plānotu pieeju auditiem. Auditu darbība ir vērsta uz tiesību aktu ievērošanu un darbības mērķu sasniegšanu.Auditi tiek sistemātiski dokumentēti, un rezultāti tiek reģistrēti. Organizācijas valde apzinās rezultātus un apspriež tos regulāro valdes sanāksmju laikā.Kompetenču pārvaldības sistēmā ir ietverti noteikumi par auditoru apmācību. Tiek uzturēts kompetentu auditoru reģistrs. |
| **1** | Tas pats kā 2. līmenis, un papildus tam plāno audita pasākumus un nosaka to prioritāti, ņemot vērā iepriekšējo auditu un pārraudzības rezultātus.Izmanto attiecīgu audita metožu kombināciju, lai sniegtu informāciju par drošības rādītājiem salīdzinājumā ar biznesa mērķiem.Augstāko vadību informē par audita rezultātiem, lai tā var pārskatīt drošības pārvaldības sistēmu. Šajā līmenī DPS noteiktais nepārtrauktais uzlabojums pats ir pakļauts analīzei, lai pārbaudītu, vai uzlabojumi patiešām sniedz gaidītos ieguvumus, vai arī ir jāmaina, lai uzlabotu rezultātus. |
| **0** | Tas pats kā 1. līmenis ar papildinājumu, ka darbības mērķi, ar ko salīdzina veikto auditu rezultātus, ir daudz grūtāk sasniedzami, un tādēļ tos salīdzina ar labāko praksi.Ir iekļauti līdzīgu organizāciju auditu mērķi. |
| **N3- Pārvaldības pārskatīšana**Lai organizācijas drošības pārvaldības sistēma darbotos konstruktīvi un efektīvi, kā arī turpinātu attīstīties laika gaitā, ir nepieciešama vadības spēcīga drošības līderība. Organizācijai ir jāparāda, ka vadība aktīvi iesaistās drošības pārvaldības sistēmas darbības pārskatīšanā un tās izstrādē nākotnei. Vadības līmeņa pārskatīšanu var uzskatīt par daļu no pārraudzības, ko organizācija veic, lai nodrošinātu, ka ar tās procesiem un procedūrām sasniedz paredzēto rezultātu. |
| **4** | Augstākā vadība maz nodarbojas ar pārraudzības un audita konstatējumu analīzi. Tas tiek vairāk darīts struktūrvienības/nodaļas līmenī.Biznesa un drošības mērķi netiek regulāri pārskatīti.Organizācijas darbības līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | Veiktās pārskatīšanas nav iekļautas sistēmiskās uzlabošanas pieejā. Tās bieži ir stihiskas un reti tiek plānotas kā pārvaldības cikla daļa.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai. |
| **2** | Tas pats kā 3. līmenis, un papildus tam vadība automātiski izmanto pārraudzības un auditu konstatējumus, lai pārskatītu organizācijas rādītājus un vajadzības gadījumā veiktu izmaiņas.Pārskatīšanas ieteikumi ir skaidri sadalīti, izsekojami un parāda, ka ir ņemtas vērā plašākas sekas. |
| **1** | Tas pats kā 2. 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. |
| **0** | Tāds pats kā 1. 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. |

## Uzlabošana (U)

|  |  |
| --- | --- |
| **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 DPS pozitīvu attīstību, kad tās notiek. |
| **Apraksts:** | 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 ir gandrīz noticis, kā ieveidojusies šāda situācija un kā varētu izvairīties no līdzīga atgadījuma. Ar izmeklēšanas secinājumiem un to rezultātiem ir pēc iespējas jādalās visā organizācijā un ar citām līdzīgām organizācijām. Organizācijām jābūt aktīvām attiecībā uz iespēju mācīties veikt uzlabojumus, ne tikai mācoties no negadījumiem un starpgadījumiem, bet arī izmantojot jebkuru citu atbilstošu pieejamu informācijas avotu, piemēram, pārraudzību un auditu vai citu cilvēku pieredzi, kas tai varētu palīdzēt veikt uzlabojumus. |
| **U1- 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 (turpmāk- NIB (*National Investigation Bodies*) un citas dalībvalsts NIB, kā arī no starpgadījumu un negadījumu izmeklēšanas rezultātiem visā pasaulē. |
| **4** | Trūkst efektīvas izmeklēšanas pierādījumu, 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.Trūkst vai vispār nepastāv pierādījumu, ka pienācīgi ņem vērā cilvēka lomu negadījumos vai starpgadījumos.Organizācijas darbības līmenis ir sliktāks, nekā noteikts vienotā drošības sertifikāta vai drošības atļaujas turētājam. |
| **3** | Starpgadījumus izmeklē, tomēr nav norādes kā un kas ir jāizmeklē. 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 apmācīti, 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 bieži tiek aizmirsts, kad ziņojumus paraksta vadības līmenī.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai.Lai gan tiek atzīts, ka šiem jautājumiem var būt nozīme negadījumos un starpgadījumos, visbiežāk joprojām tiek vainotas atsevišķas personas, nevis novērsti sistēmiski organizatoriskie trūkumi. |
| **2** | Tas pats kā 3. 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. |
| **1** | Tas pats kā 2. līmenis, un papildus tam izmeklēšanas kvalitāte nodrošina ieteikumus, ko var piemērot gan organizācijā, gan ārpus tās.Izpētīto starpgadījumu sarakstā vajadzības gadījumā ir ietverti darba pārtraukumi 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 DPS ietvaros. Organizācija sevi pozicionē kā taisnīgu organizāciju, un realitātē vainošanas kultūra nepastāv. |
| **0** | Tas pats kā 1. 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. |
| **U2- Pastāvīga uzlabošana**Organizācijai ir jāpierāda, ka tā cenšas visu laiku veikt uzlabojumus, mācoties no notikumiem, komunicējot ar regulatīvajam iestādēm un citā veidā. Uzraudzības laikā sagaida, ka organizācijas parāda, ka tām ir process, lai identificētu un īstenotu pozitīvas pārmaiņas savās DPS, tostarp, izmantojot drošības kultūras pastāvīgas uzlabošanas stratēģiju. Korektīvās darbības ir saistītas ar tādu darbību definēšanu, noteikšanu un izpildi, kas pēc pārraudzības, izmeklēšanas, audita un pārskatīšanas ir noteiktas kā nepieciešamas. |
| **4** | Neraugoties uz DPS procesiem un procedūrām, pārraudzība, auditi 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 sliktāks, nekā noteikts vienotā 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. |
| **3** | Vienkāršie konstatējumi no pārraudzības, izmeklēšanas, audita un pārskatīšanas rada vienkāršas darbības un izmaiņas drošības pārvaldības sistēmas zemākajos līmeņos. Organizācijā notiek atsevišķi mēģinājumi meklēt notikumu pamatā esošās problēmas, sistemātiski pārskatot pārraudzības, izmeklēšanu un audita informāciju.Šajā līmenī organizācija atbilst minimālajām prasībām, kas ir jāizpilda vienotā drošības sertifikāta vai drošības atļaujas piešķiršanai.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 korektīvās darbības 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, nobraukšanu no sliedēm, pabraukšanu garām aizliedzošam signālam (SPAD) u. tml. Organizācijai ir vairāk nopietnu starpgadījumu un negadījumu nekā konkurentiem. |
| **2** | Tas pats kā 3. līmenis, un papildus tam ir izveidots process, lai pārliecinātos, ka tiek īstenotas nepieciešamās darbības, kas noteiktas, veicot pārraudzību, auditu 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.Korektīvo darbību īstenošana 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 sistēmisks secinājumu izdarīšanas process. Ir pastāvīga stratēģija drošības kultūras nepārtrauktai uzlabošanai, kas ir labi izveidota un kuras panākumus var attiecīgi novērtēt. Organizācijā valda taisnīguma kultūra. |
| **1** | Tas pats kā 2. līmenis, un papildus tam ir mehānisms progresa izsekošanai un korektīvo darbību pabeigšanai.Korektīvās darbības ir saistītas ar drošības pārvaldības sistēmā noteiktajiem mērķiem.Drošības mērķu un plānošanas rezultāti, riska novērtējums, personāla un citu personu iesaistīšana, informācija un komunikācija, pārraudzība, autits, 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 sistēmiska pieeja taisnīguma nodrošināšanai. Tiek veicināts veselīgs dzīvesveids un pārraudzīti negadījumi, kas nav saistīti ar darbu. Stratēģijā pastāvīgai drošības kultūras uzlabošanai un taisnīguma kultūras īstenošanai vadās no paraugprakses ar reāliem un izmērāmiem mērķiem. |
| **0** | Tas pats kā 1. līmenis, un papildus tam ir korektīvie darbības, 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. Vienāda ranga 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. |

1. Stājoties spēkā jaunākajai izmaiņai, iepriekšējā izmaiņa zaudē spēku un ir atzīstama par spēku zaudējušu. [↑](#footnote-ref-1)
2. 17.11.2022. Nr.1-1/2-32 Kompetenču pārvaldības sistēma [↑](#footnote-ref-2)
3. 04.11.2022. Nr. 1-1/2-28 Dokumentu pārvaldības kārtība [↑](#footnote-ref-3)
4. KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2018/763 (2018. gada 9. aprīlis), ar ko nosaka praktisku kārtību vienoto drošības sertifikātu izdošanai dzelzceļa pārvadājumu uzņēmumiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/798 un atceļ Komisijas Regulu (EK) Nr. 653/2007 [↑](#footnote-ref-4)
5. Atbilstoši Vispārīgai datu aizsardzības regulai (Regula 2016/679) auditējamais tiek informēts par audio ieraksta veikšanu DPS audita ietvaros. Ierakstu veic Inspekcijas darbinieki, kuri ir audita grupas dalībnieki. Katrs no viņiem ir atbildīgs par ieraksta glabāšanu. Ieraksti tiks lietoti tikai Inspekcijas darbam un netiks publicēti vai jebkādā veidā nodoti trešajām personām. Ieraksti tiks saglabāti līdz audita noslēgšanai. Ieraksta labošana vai grozīšana, kā arī dzēšana pirms audita slēgšanas nav pieļaujama. Auditējamais var iesniegt sūdzību par ieraksta veikšanu Inspekcijas vadītājam. Auditējamais var atteikties sniegt informāciju, bet tas tiek uzskatīts par Inspekcijas nolikuma 10.5. apakšpunkta prasību neievērošanu. [↑](#footnote-ref-5)
6. KOMISIJAS DELEĢĒTĀ REGULA (ES) 2018/762 (2018. gada 8. marts),ar ko saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/798 izveido kopīgas drošības metodes, kas attiecas uz prasībām drošības pārvaldības sistēmām, un atceļ Komisijas Regulas (ES) Nr. 1158/2010 un (ES) Nr. 1169/2010 [↑](#footnote-ref-6)
7. 27.06.2022. Nr.1-1/2-20 Uzraudzības metodes [↑](#footnote-ref-7)
8. 02.06.2020. Ministru kabineta noteikumi Nr. 334 "Dzelzceļa satiksmes negadījumu klasifikācijas, izmeklēšanas un uzskaites kārtība" [↑](#footnote-ref-8)