Turība University

DROŠĪBAS RISKU VADĪBA

Labās prakses piemēri un praktiskie uzdevumi

Funded by the European Union

iSecureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

Turība University

DROŠĪBAS RISKU VADĪBA

Labās prakses piemēri un praktiskie uzdevumi

Funded by the European Union

iSecureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

Autoru kolektīvs
DROŠĪBAS RISKU VADĪBA. Labās prakses piemēri un praktiskie uzdevumi

REDAKTORI

Ivita Kīsnica, Tiesību zinātņu katedras vadītāja, Biznesa augstskola *Turība*, Latvija
Kristīne Neimane, Projektu daļas vadītāja, Biznesa augstskola *Turība*, Latvija
Kārlis Apalups, Maģistra studiju programmas "Organizācijas drošības vadība" direktors, Biznesa augstskola *Turība*, Latvija
Uģis Začs, lektors, SECUEU projekta eksperts, Biznesa augstskola *Turība*, Latvija

KOREKTORE

Ludmila Viļumova

AUTORI

AVANS LIETIŠĶO ZINĀTŅU UNIVERSITĀTE, Nīderlande:
Lambert Bambach, vecākais lektors

BARSELONAS AUTONOMĀS UNIVERSITĀTES FONDS, Spānija:
Javier Dorado, pētnieks, Integrētā drošība un prevencija
Elisabet Garcia Rull, pētniece, Integrētā drošība un prevencija

BIZNESA AUGSTSKOLA *TURĪBA*, Latvija:
Kārlis Apalups, Maģistra studiju programmas "Organizācijas drošības vadība" direktors, lektors
Kristīne Neimane, Projektu daļas vadītāja, lektore
Uģis Začs, lektors

KAZIMIERAS SIMONAVICIUS UNIVERSITĀTE, Lietuva:
Raimundas Kalesnykas, profesors Tiesību un tehnoloģiju institūtā
Rita Lankauskiene, profesore

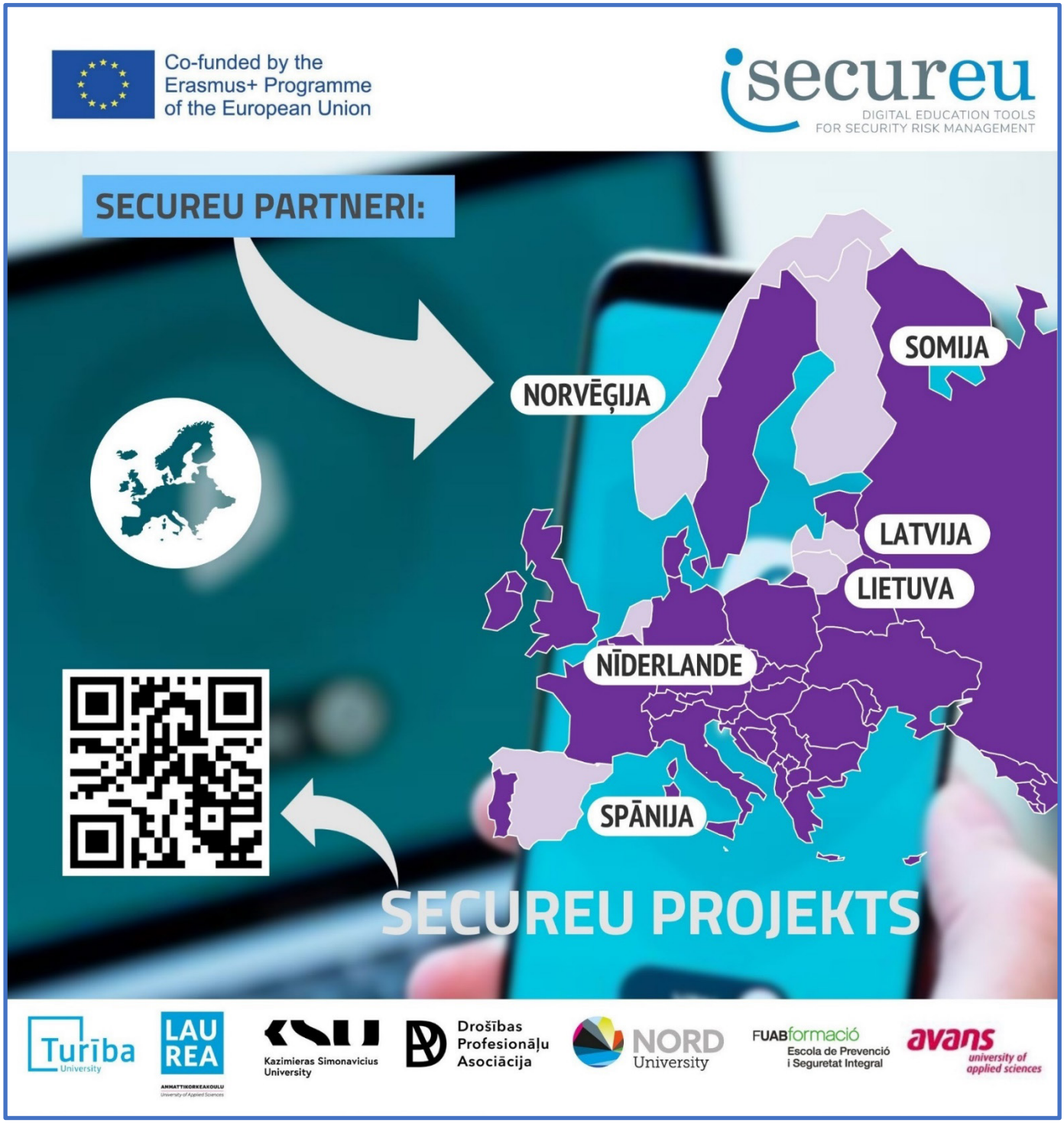
LAUREA LIETIŠĶO ZINĀTŅU UNIVERSITĀTE, Somija:
Anja Aatsinki, vecākā lektore
Hanna Iisakkila Rojas, vecākā lektore
Jyri Rajamäki, vecākais lektors
Kaci Bourdache, vecākais lektors
Oskari Lahtinen, vecākais lektors

NORD UNIVERSITĀTE, Norvēģija:
Natalia Andreassen, profesore, Nord Universitātes Biznesa skola, Krīzes vadības un sadarbības centrs
Rune Elvegard, vecākais zinātniskais padomnieks, Nord Universitātes Biznesa skola, Krīzes vadības un sadarbības centrs
Ensieh Roud, asociētā profesore, Nord Universitātes Biznesa skola, Krīzes vadības un sadarbības centrs

ISBN 978-9934-543-53-1

Makets IK "DR dizains"

Iespiests SIA "Drukātava"



Šī grāmata ir publicēta ERASMUS+ sadarbības projekta "Digitālie mācību rīki drošības risku vadībā" ietvaros, ko finansē Eiropas Savienība, projekta numurs 2021-1-LV01-KA220-HED-000023056.

SATURS

IEVADS

Drošība arvien izteiktāk kļūst globāla. Lai varētu runāt par drošību, ir jāņem vērā virkne starptautisku aspektu un notikumu, ir jāsadarbojas un jāspēj "runāt vienā valodā". Tieši šī "spēja runāt vienā valodā" drošības speciālistu vidū tika atzīta kā viena no centrālajām problēmām. Ne tikai vienotu terminu izpratne sabiedrības un speciālistu vidū par drošības jēdzieniem ir svarīga, bet arī vienota izpratne par procesu norisi. Piemēram, par drošības risku vadību, lai nākotnē sadarbība dažādu risku novēršanā būtu vēl vienotāka. Līdz ar to, apvienojoties vairākiem partneriem no dažādām Eiropas valstīm, kuri sagatavo drošības speciālistus, tika uzsākta sadarbība, lai pilnveidotu studiju programmas un papildinātu mācību materiālus. Materiāli tika sagatavoti, koncentrējoties uz procesu izpratni un metodēm, kā drošības jautājumi tiek plānoti un ieviesti dažādās valstīs un dažādās organizācijās.

Šādas vienotas pieejas un jautājumu izpratnes nodrošināšanai bieži vien talkā nāk starptautiski standarti, kā, piemēram, ISO standarti.

ISO 31000:2018 ir globāls standarts, kas sniedz vadlīnijas risku pārvaldībai dažādās jomās. Standarts gan nav izstrādāts specifiski drošības jomai, tomēr tas ir veiksmīgi pielietojams arī drošības jomā.

Šajā grāmatā varēsiet iepazīties ar ISO 31000:2018 standartu un tā pielietojumu drošības jomā. Grāmatā atradīsiet labās prakses piemērus – gadījumu analīzi, kuros ir pielietots ISO 31000 standarts, lai mazinātu drošības riskus, apdraudējumu vai ieviestu šo principu pielietošanu reālās organizācijās un uzņēmumos.

Grāmatas otrajā daļā atradīsiet praktiskus uzdevumus, ko pasniedzēji var pielietot savās lekcijās un praktiskajās nodarbībās, runājot par drošības risku vadību. Uzdevumus var lietot arī pašmācības nolūkiem, izpildot uzdevumus individuāli.

Grāmatas mērķgrupa ir studenti, kas apgūst drošības studiju programmas, kā arī citu jomu studenti, piemēram, vadībzinātņu studenti, kuriem interesē drošības jautājumu nodrošināšana savās organizācijās.

Tāpat grāmata būs noderīga pasniedzējiem, kuri atradīs praktiskus piemērus, ar kuru palīdzību demonstrēt ISO standarta pielietojumu saviem studentiem. Pasniedzēji arī novērtēs praktiskos uzdevumus, kurus varēs izspēlēt savās nodarbībās.

Grāmata būs interesanta arī drošības jomas speciālistiem, lai dziļāk izpētītu ISO 31000:2018 standarta pielietojumu un iepazītos ar dažādiem labās prakses piemēriem.

PAR PROJEKTU

Septiņas partnerorganizācijas no Latvijas (Biznesa augstskola *Turība* un Drošības profesionāļu asociācija), Lietuvas (Kazimiras Simonavičius Universitāte), Somijas (Laurea Lietišķo zinātņu Universitāte), Nīderlandes (AVANS Lietišķo zinātņu Universitāte), Norvēģijas (Nord Universitāte) un Spānijas (Barselonas autonomās universitātes fonds) apvienoja savas zināšanas un pieredzi, lai izstrādātu ERASMUS+ sadarbības partnerības projektu, kura mērķis bija attīstīt dažādus mācību materiālus par drošības risku vadību.

Šī projekta rezultātā ir izveidots Eiropas līmeņa drošības speciālistu tīkls, nostiprināta sadarbība starp dažādām augstskolām, kas sagatavo drošības speciālistus. Projekta laikā partneri izstrādāja

rekomendācijas augstākās izglītības iestādēm par drošības speciālistu apmācību un izglītības programmu veidošanu šajā jomā. Tāpat tika izstrādāti visaptveroši un aktuāli digitālie mācību materiāli un rīki, kas apkopoti vienotā tīmekļa platformā. Šeit atradīsiet gan dažādus izglītojošus lasāmos materiālus, gan mācību video, gan praktiskos uzdevumus, ierakstus un materiālus no konferencēm un pasākumiem.

Informāciju atradīsiet projekta mājaslapā: https://security.turiba.lv

KAS IR ISO?

Mūsdienās ik uz soļa mēs dzirdam, ka tiek runāts par riskiem un risku vadību – risks ir nenoteiktības ietekme uz mērķiem. Mēs dzīvojam pastāvīgi mainīgā pasaulē, kur mēs esam spiesti tikt galā ar nenoteiktību katru dienu. Visas organizācijas neatkarīgi no tā, vai tās ir publiskas vai privātas, peļņas vai bezpeļņas, savā darbībā sastopas ar dažādām nenoteiktībām.

Apgūstot vadības un menedžmenta programmas un kursus, studentiem noteikti nākas saskarties ar ISO standartiem. ISO standarti palīdz kvalitātes vadībā, ļauj organizācijām un uzņēmumiem sakārtot dažādus vadības procesus un ražot kvalitatīvas preces vai piedāvāt augstas kvalitātes pakalpojumus.

ISO ir Starptautiskā Standartizācijas organizācija (angļu valodā: *International Organization for Standardization*, ISO), kas ir nacionālo standartizācijas organizāciju federācija, nevalstiska organizācija. ISO apvieno 164 valstu pārstāvētās standartizācijas organizācijas. ISO izstrādā standartus dažādās jomās, kopumā pastāv vairāk nekā 17 000 ISO standarti, katru gadu tiek publicēti aptuveni 1000 jauni standarti.

ISO ir globāls standarts, kas ļauj mums atpazīt uzticamas preces un pakalpojumus. Standarti nosaka vienotus un konsekventus etalonus gan uzņēmumiem, gan patērētājiem — nodrošinot uzticamību un vienkāršojot izvēli. Starptautiskie standarti nodrošina to, ka produkti un pakalpojumi, ko izmantojat ikdienā, ir droši, uzticami un augstas kvalitātes. Tie arī palīdz uzņēmumiem ieviest un realizēt ilgtspējīgu un ētisku praksi, palīdzot radīt nākotni, kurā jūsu iegādātās preces ir augstas kvalitātes, kā arī tās ir ražotas saudzīgi pret mūsu planētas resursiem.

ISO 31000:2018[1] ir starptautisks standarts, ko izstrādājusi jau iepriekš minētā Starptautiskā Standartizācijas organizācija, kas nodrošina principus, vadlīnijas risku pārvaldības sistēmai. Šis standarts pirmo reizi tika publicēts 2009. gadā, un kopš tā laika tas ir pārskatīts 2018. un 2023. gadā.

Šis dokuments ir paredzēts speciālistiem, kuri rada un aizsargā vērtību organizācijās, pārvaldot riskus, pieņemot lēmumus, nosakot un sasniedzot mērķus un uzlabojot sniegumu. Visu veidu un lielumu organizācijas saskaras ar ārējiem un iekšējiem faktoriem un ietekmēm, kas rada riskus un apdraud organizāciju mērķu sasniegšanu.

Riska pārvaldība ir iteratīva un palīdz organizācijām noteikt stratēģiju, sasniegt mērķus un pieņemt apzinātus lēmumus. Riska pārvaldība ir daļa no pārvaldības un vadības, un tā ir būtiska organizācijas pārvaldībai visos līmeņos. Pārdomāta risku pārvaldība veicina vadības sistēmu uzlabošanu. Riska pārvaldība ir daļa no visām darbībām, kas saistītas ar organizāciju, un tā ietver mijiedarbību ar visām ieinteresētajām pusēm. Riska pārvaldībā tiek ņemts vērā organizācijas ārējais un iekšējais konteksts, tostarp cilvēka uzvedība un kultūras faktori.

Izmantojot ISO, organizācija var veidot "kopīgu valodu" un pieeju risku pārvaldībai, ļaujot uzlabot lēmumu pieņemšanu, palielināt noturību un aizsargāt savus mērķus no iespējamiem draudiem un nenoteiktības. Īpaši būtiski tas ir gadījumos, kad organizācijā vai uzņēmumā ar risku pārvaldību

[1] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

jāstrādā starptautiskā līmenī. Tad vēl jo būtiskāk ir tas, ka visi drošības speciālisti neatkarīgi no valsts, valodas vai darba kultūras spēj sarunāties "vienā valodā".

Ir svarīgi mācīt šos standartus drošības speciālistiem, lai tiem būtu instrumenti un pārbaudītas sistēmas, uz kuru pamata organizācija var veidot iekšējās drošības sistēmu un strādāt ar drošības riskiem, lai tādējādi izvairītos no lielām krīzēm ar smagām sekām.

ISO 31000:2018 STANDARTS

ISO 31000:2018 standarts nodrošina riska pārvaldības sistēmu. Izveidojot un ieviešot riska pārvaldības sistēmu saskaņā ar ISO 31000:2018 principiem, organizācijas var sistemātiski identificēt un novērst riskus, pieņemt apzinātus lēmumus un uzlabot spēju sasniegt savus mērķus, neskatoties uz nenoteiktību un izaicinājumiem.

Risku pārvaldības ietvars

Zemāk attēlā ir vizualizēta ISO 31000:2018 risku pārvaldības sistēma un tās galvenie komponenti.

1. attēls. **Risku pārvaldības ietvars saskaņā ar ISO 31000:2018**[2]

Līderība un apņemšanās ir visa centrā. Tā uzsver, ka efektīva riska pārvaldība sākas ar organizācijas vadību. Bez spēcīgas vadības risku pārvaldības stratēģijas netiks pilnībā integrētas organizācijas kultūrā. Jāatceras arī tas, ka bez apņemšanās ir nepieciešami arī resursi, līdz ar to augstākās vadības līmenī risku pārvaldībai tie ir jāpiešķir.

[2] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Vēl ietvars nosaka un apskata piecus citus komponentus – integrācija, dizains, īstenošana, novērtēšana un uzlabošana.

Integrācija. Šis elements uzsver, ka riska pārvaldībai nevajadzētu būt atsevišķai funkcijai, bet tā ir jāintegrē visos organizācijas procesos.

Dizains. Dizaina posms ietver pielāgotas riska pārvaldības sistēmas izveidi, pamatojoties uz organizācijas kontekstu, vajadzībām un mērķiem. Šeit ir būtiski, ka risku pārvaldības sistēma tiek veidota, piemērojot to organizācijas lielumam, struktūrai un apdraudējumiem.

Šis posms ietver:

- risku vadības politikas izstrādi;
- skaidru mērķu un kritēriju definēšanu risku novērtēšanai;
- atbildīgo nominēšanu.

Īstenošana. Kad risku pārvaldības sistēma ir izstrādāta, tā ir jāievieš visā organizācijā. Šis posms ietver:

- risku pārvaldības stratēģiju ieviešanu praksē;
- darbinieku apmācību;
- risku pārvaldības iekļaušanu lēmumu pieņemšanas un operatīvajās darbībās.

Novērtēšana. Pēc ieviešanas sistēma ir regulāri jānovērtē, lai nodrošinātu, ka tā darbojas efektīvi. Tas ietver:

- ietvara veiktspējas uzraudzību;
- trūkumu vai uzlabošanas jomu noteikšanu;
- organizācijas risku novēršanas pasākumu piemērotības pārskatīšanu.

Uzlabošana. Risku pārvaldība ir dinamisks process, un organizācijai ir nepārtraukti jācenšas to uzlabot. Tas ietver risku pārvaldības sistēmas atjaunināšanu un pilnveidošanu, kad parādās jauni riski vai mainās organizatoriskais konteksts. Pastāvīgi uzlabojumi nodrošina, ka riska pārvaldības sistēma joprojām ir atbilstoša un efektīva.

Katrs no šiem komponentiem ir daļa no **cikliska procesa**, kas nozīmē, ka tie nedarbojas atsevišķi. Vadība un tās apņēmība virza visu sistēmu, nodrošinot, ka risku pārvaldība ir prioritāra un integrēta. Integrācija nodrošina, ka risku pārvaldība kļūst par ikdienas organizatorisku darbību sastāvdaļu. Dizains pielāgo risku pārvaldības sistēmu organizācijas vajadzībām, savukārt īstenošana ievieš dizainu darbībā. Novērtēšana ļauj organizācijai novērtēt sistēmas efektivitāti, un uzlabojumi nodrošina, ka sistēma attīstās līdz ar organizācijas mainīgo risku vidi.

Šis cikls turpinās, veicinot nepārtrauktu izaugsmi un pielāgošanos mainīgajiem riskiem un pastāvošai nenoteiktībai. Izpratne par šo savstarpēji saistīto procesu ir ļoti svarīga drošības speciālistiem, jo viņi gatavojas pārvaldīt drošības riskus dažādās nozarēs.

Risku pārvaldības principi

ISO 31000:2018 standarts nosaka arī efektīvas risku pārvaldības principus. Šie principi attēloti zemāk vizualizācijā.

2. attēls. **Risku pārvaldības principi saskaņā ar ISO 31000:2018**[3]

Galvenais risku vadības mērķis un arī centrālais risku pārvaldības princips ir radīt un aizsargāt organizāciju un tās vērtības. Tas var ietvert finanšu līdzekļu, reputācijas, informācijas vai cilvēkresursu aizsardzību.

Drošības speciālista loma ir nodrošināt to, ka drošības pasākumi ne tikai novērš draudus, bet arī atbalsta organizācijas vispārējos mērķus un pievieno vērtību.

Integratīvi: riska vadība ir jāintegrē visos organizācijas aspektos un līmeņos, tostarp stratēģiskajā plānošanā, lēmumu pieņemšanā un darbības procesos.

Strukturēti un visaptveroši: organizācijām ir jāievieš sistemātisks un strukturēts process, lai identificētu, novērtētu un pārvaldītu riskus visos organizācijas līmeņos.

Pielāgoti: riska pārvaldības process ir jāpielāgo organizācijas īpašajām vajadzībām, kontekstam, vērtībām un mērķiem.

Iekļaujoši: riska pārvaldības procesā jāiesaista visas ieinteresētās puses – gan iekšējās, gan ārējās, lai nodrošinātu visaptverošu izpratni par riskiem un iespējamo ietekmi.

Dinamiski: riska pārvaldībai ir jābūt nepārtrauktam procesam, kas pielāgojas izmaiņām iekšējā un ārējā vidē, ļaujot pastāvīgi uzlaboties.

[3] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Labākā pieejamā informācija: efektīva saziņa par riskiem, to iespējamām sekām un riska pārvaldības stratēģijām ir būtiska apzinātu lēmumu pieņemšanai.

Cilvēku un kultūras faktori: efektīvi pārvaldot riskus, jāņem vērā cilvēka uzvedība, kultūra un organizācijas vērtības.

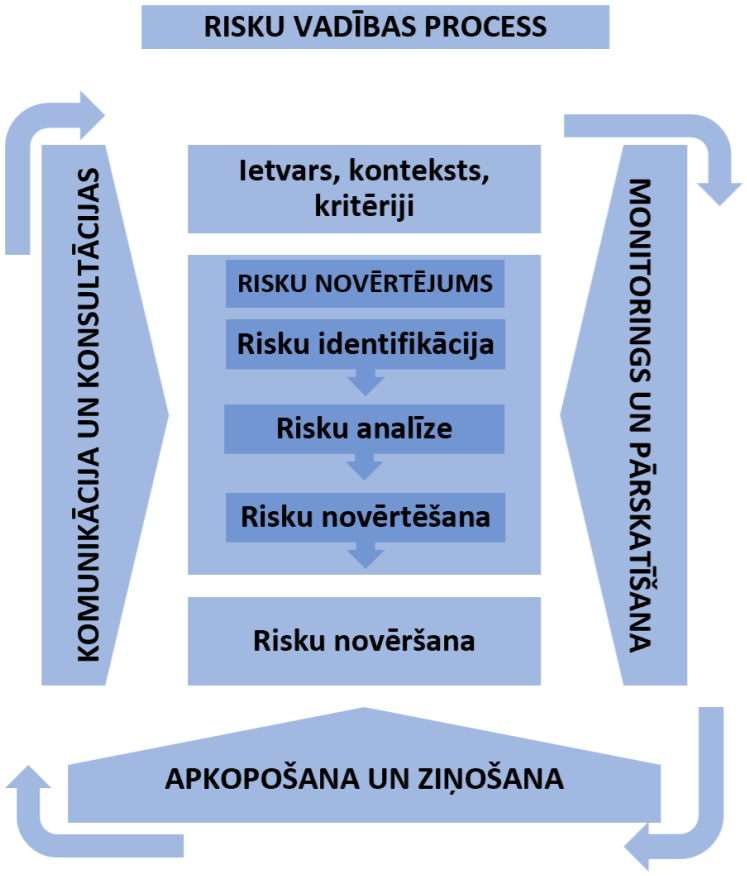
Nepārtraukta uzlabošana: organizācijai regulāri jāpārskata un jāuzlabo sava riska pārvaldības sistēma, lai nodrošinātu tās efektivitāti un atbilstību mainīgai situācijai.

Ievērojot šos principus, organizācijas var izveidot stabilu un proaktīvu pieeju risku pārvaldībai, tādējādi uzlabojot lēmumu pieņemšanu un nodrošinot mērķus.

Vairāk par galvenajiem risku pārvaldības principiem efektīvai vadībai var lasīt INCLUS izstrādātajā rokasgrāmatā: https://inclus.com/en/iso-31000-risk-management-principles/

Risku pārvaldības process

ISO 31000:2018 standarts piedāvā arī strukturētu pārvaldības procesa modeli, kas palīdz organizācijām konsekventi un sistemātiski strādāt ar riskiem. Tas nodrošina, ka riski tiek ne tikai pārvaldīti, bet arī lēmumi par riskiem ir saskaņoti ar organizācijas mērķiem.



3. attēls. **Risku vadības process saskaņā ar ISO 31000:2018**[4]

Risku pārvaldības process sastāv no vairākiem savstarpēji saistītiem posmiem.

[4] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Ietvars, konteksts, kritēriji: izprotiet organizācijas mērķus, ieinteresētās personas un ārējos un iekšējos faktorus, kas var ietekmēt risku pārvaldības procesu.

Risku novērtējums: sastāv no trīs posmiem: risku identifikācijas, risku analīzes un risku novērtēšanas.

Risku identifikācija: identificējiet riskus, kas varētu ietekmēt organizācijas mērķu sasniegšanu.

Risku analīze: analizējiet identificētos riskus, izpētiet to rašanās iespējamību, iespējamo ietekmi un visus esošos kontroles mehānismus. Šis solis palīdz izprast katra riska būtību un īpašības.

Risku novērtēšana: novērtējiet riskus pēc iepriekš noteiktiem kritērijiem, lai noteiktu to nozīmīgumu. Šis process ietver risku salīdzināšanu, lai noteiktu to prioritāti turpmākai rīcībai.

Risku novēršana: izstrādājiet un īstenojiet risku novēršanas plānu. Šis solis ietver atbilstošu risku reaģēšanas iespēju izvēli un ieviešanu, piemēram, izvairīšanos no riskiem vai rīcību to ietekmes mazināšanai, ja risks ir iestājies.

Apkopošana un ziņošana: dokumentējiet visu risku pārvaldības procesu. Veiciet datu reģistrēšanu un ziņošanu, tas palīdzēs veidot "caurspīdīgu" sistēmu un veicinās atbildību.

Monitorings un uzraudzība: pastāvīgi uzraugiet un pārskatiet risku pārvaldības procesa efektivitāti. Tas ietver risku novēršanas darbību rezultātu uzraudzību, risku ainavas pārskatīšanu un nepieciešamo korekciju veikšanu.

Komunikācija un konsultācijas: laba komunikācija un informācijas aprite jebkurā organizācijā vai uzņēmumā ir viens no veiksmes stūrakmeņiem. Tikpat būtiska komunikācija ir arī risku pārvaldības procesā. Sistēma nekad nedarbosies, ja to veidos viens cilvēks, neieklausoties kolēģos, ieinteresētajās pusēs un speciālistos. Līdz ar to ir svarīgi nodrošināt iespēju iesaistītajām pusēm izteikties, uzklausīt to viedokli. Viens no efektīviem veidiem, kā to sasniegt, ir pielietot "prāta vētras" metodi. Konsultācijas jeb apspriešanās ar ieinteresētajām personām un informācijas apmaiņa nodrošina, ka visi darbojas vienoti.

ISO 31000 standarts uzsver iteratīva un pastāvīga riska pārvaldības procesa nozīmi, kas ir iestrādāta organizācijas lēmumu pieņemšanas un plānošanas procesos. Tā veicina sistemātisku un proaktīvu pieeju risku identificēšanai, novērtēšanai un pārvaldībai, galu galā palīdzot organizācijām pieņemt apzinātus lēmumus un uzlabot to noturību.

ISO 31000 var integrēt ar esošajām drošības pārvaldības sistēmām, piemēram, ISO 27001 (Informācijas drošības pārvaldības sistēma) vai nozarei specifiskiem drošības standartiem, lai uzlabotu organizācijas vispārējo drošības riska pārvaldības praksi.

ISO 31000:2018 UN DROŠĪBAS JOMA

Drošības jomas speciālistiem jāatceras, ka ISO 31000:2018 ir globāls standarts, kas sniedz vadlīnijas risku pārvaldībai dažādās jomās, tas nav izstrādāts specifiski drošības jomai. Tomēr tas ir veiksmīgi pielietojams, tostarp arī drošības jomā. Tas, ka šo standartu lieto arī citās jomās, ir nozīmīgs pozitīvs aspekts. Tas nozīmē, ka arī kolēģi no ražošanas, administrācijas un citiem departamentiem izpratīs šo standartu un tajā noteiktos procesus. Tas savukārt organizācijas iekšienē drošības speciālistam var dot iespēju labāk izskaidrot drošības vadības procesus saviem kolēģiem.

Riska pārvaldība ir risku identificēšanas, novērtēšanas un prioritāšu noteikšanas process, kam seko koordinēta resursu izmantošana, lai samazinātu, kontrolētu un uzraudzītu nevēlamo notikumu iespējamību vai ietekmi. Tā ir kritiska disciplīna dažādās jomās, tostarp finansēs, veselības aprūpē, inženierzinātnēs un uzņēmējdarbībā, jo tā palīdz organizācijām pārvarēt neskaidrības un aizsargāt savus aktīvus, reputāciju un ilgtermiņa dzīvotspēju. Efektīva riska pārvaldība ļauj organizācijām pieņemt pārdomātus lēmumus, efektīvi sadalīt resursus un uzlabot noturību pret iespējamiem draudiem. Proaktīvi risinot riskus, organizācijas var izvairīties no zaudējumiem vai tos mazināt, izmantot iespējas un sasniegt stratēģiskos mērķus, tādējādi nodrošinot noturīgu izaugsmi un stabilitāti pastāvīgi mainīgā vidē.

Mūsdienās drošības dienesta darbinieki vairs neatbild tikai par fizisko drošību organizācijā, bet ir iesaistīti dažādos procesos. Dažādos procesos un organizācijas darbības laukos pastāv dažādi riski, izpratne par šiem dažādajiem risku veidiem ļauj organizācijām īstenot mērķtiecīgas stratēģijas, lai mazinātu to ietekmi, un drošības dienesta darbinieki ir neatņemami šī procesa dalībnieki. Riskus iedala vairākās grupās.

Finanšu riski – saistīti ar finanšu aktīvu un saistību pārvaldību, un tie var ietekmēt organizācija finansiālo stabilitāti un rentabilitāti. Galvenie finanšu risku veidi ir:

- tirgus risks: finansiālu zaudējumu risks tirgus cenu vai likmju, piemēram, akciju cenu, procentu likmju, preču cenu un ārvalstu valūtas kursu, nelabvēlīgu izmaiņu dēļ;
- kredītrisks: zaudējumu risks, kas izriet no aizņēmēja vai darījuma partnera nespējas pildīt savas finansiālās saistības, kā rezultātā tiek nepildīts vai nemaksāts;
- likviditātes risks: risks, ka organizācija var nespēt izpildīt savas īstermiņa finansiālās saistības nepietiekamu likvīdo aktīvu vai nespējas piekļūt finansējuma avotiem dēļ.

Operacionālie riski – zaudējumu risks, kas izriet no neadekvātiem vai neveiksmīgiem iekšējiem procesiem, sistēmām, cilvēkiem vai ārējiem notikumiem. Tas ietver riskus, kas saistīti ar tehnoloģiju kļūmēm, krāpšanu, cilvēka kļūdām un uzņēmējdarbības traucējumiem. Operacionālie riski rodas no ikdienas darbībām un procesiem organizācijā. Tie var ietekmēt efektivitāti, produktivitāti un spēju piegādāt produktus vai pakalpojumus.

Tehnoloģiju riski – riski, kas saistīti ar IT sistēmām, kiberdrošības draudiem, datu pārkāpumiem un tehnoloģiskām kļūmēm.

Piegādes ķēdes riski – riski, kas saistīti ar pārtraukumiem vai kļūmēm piegādes ķēdē, tostarp ar piegādātājiem saistītas problēmas, loģistikas problēmas un atkarība no galvenajiem piegādātājiem.

Procesa riski – riski, kas rodas no neatbilstošiem vai neefektīviem biznesa procesiem, kas izraisa kļūdas, aizkavēšanos vai darbības kļūmes.

Cilvēkresursu riski – riski, kas saistīti ar cilvēka faktoriem, piemēram, darbinieku pārkāpumiem, nolaidību vai neatbilstošu apmācību.

Stratēģiskie riski – riski, kas ietekmē organizācijas spēju sasniegt savus stratēģiskos mērķus un ilgtermiņa mērķus. Šie riski rodas no ārējiem faktoriem, tirgus dinamikas, konkurences spiediena un stratēģiskiem lēmumiem. Stratēģiskie riski ietver:

- tirgus konkurences riski – riski, kas saistīti ar izmaiņām tirgus apstākļos, konkurences vidē un patērētāju preferenču maiņu;
- biznesa modeļa riski – riski, kas saistīti ar organizācijas biznesa modeļa dzīvotspēju un ilgtspējību, reaģējot uz nozares tendencēm un traucējumiem;
- inovācijas riski – riski, kas izriet no tehnoloģiju sasniegumiem, jaunu produktu izstrādes un inovācijas stratēģijām, kas var dot vai nedot gaidītos rezultātus.

Atbilstības riski – riski rodas, neievērojot likumus, noteikumus, standartus vai iekšējās politikas un procedūras. Par noteikumu neievērošanu var tikt piemērotas juridiskas sankcijas, naudas sodi, kaitējums reputācijai un uzņēmējdarbības iespēju zaudēšana.

Reputācijas riski – riski ietver iespējamu kaitējumu organizācijas reputācijai vai zīmola tēlam. Šos riskus var izraisīt negatīva sabiedrības uztvere, skandāli, ētikas pārkāpumi, klientu neapmierinātība vai negatīvs atspoguļojums plašsaziņas līdzekļos. Reputācijas riski var būtiski ietekmēt ieinteresēto pušu uzticību, investoru uzticību un biznesa attiecības, izraisot finansiālus zaudējumus un ilgtermiņa kaitējumu organizācijas vērtībai un uzticamībai.

Drošībnieku fundamentālā nozīme organizācijā galvenokārt ir risku samazināšana, kas ir vērsta uz pasākumu un kontroles pasākumu ieviešanu, lai mazinātu tādu risku iespējamību vai smagumu, no kuriem nevar pilnībā izvairīties vai kurus nevar pilnībā pārnest. Šīs stratēģijas mērķis ir samazināt ievainojamības un uzlabot organizācijas spēju efektīvi reaģēt uz iespējamiem draudiem. Lai to nodrošinātu, drošībniekiem ir savā darbā jāpielieto dažādas riska samazināšanas metodes, kas sevī ietver:

- **drošības pasākumus** – drošības koncepcijas, drošības protokolu, procedūru un kontroles pasākumu ieviešana, lai mazinātu riskus, kas saistīti ar nelaimes gadījumiem darba vietā, vides apdraudējumiem un ar veselību saistītiem incidentiem;
- **kontroles ieviešanu** – fiziskās, tehnoloģiskās vai darbības kontroles ieviešana, lai samazinātu risku rašanās iespējamību. Kā piemērus var minēt drošības sistēmu uzstādīšanu, kiberdrošības pasākumu ieviešanu un iekšējās kontroles ieviešanu, lai novērstu krāpšanu, u.c.;
- **diversifikāciju** – ieguldījumu, aktīvu vai operāciju izplatīšana dažādās jomās vai tirgos, lai samazinātu koncentrācijas risku un mazinātu nelabvēlīgu notikumu ietekmi uz kopējo sniegumu. Sadalīt pakalpojumus starp vairākiem piegādātājiem. Kā piemēru var minēt divu elektrības avotu izveidi, lai situācijā, ja viens elektrības avots nefunkcionē, funkcionētu otrs un organizācijā nodrošinātu drošības tehnisko līdzekļu nepārtrauktu darbību, u.c.;
- **procesu uzlabošanu** – darbības procesu, darbplūsmu un procedūru uzlabošana, lai racionalizētu darbības, uzlabotu efektivitāti un samazinātu kļūdas vai traucējumus, kas varētu radīt potenciālus riskus, kā arī palielinātu kontroli un procesu, darbinieku drošību un caurspīdīgumu.

Iesaistot drošībniekus organizācijas visaptverošos riska samazināšanas pasākumos, izmantojot iepriekš aprakstītās metodes, kā arī izmantojot riska nodošanas, izvairīšanās un samazināšanas stratēģiju kombināciju, organizācijas var izstrādāt visaptverošu riska pārvaldības sistēmu, kas aizsargā pret nenoteiktību, saglabā darbības nepārtrauktību un atbalsta ilgtspējīgu izaugsmi.

Lai neapjuktu daudzajās definīcijās un terminos risku vadības jomā, aicinām ieskatīties **drošības terminu skaidrojošajā vārdnīcā**, kurā atradīsiet gan galveno drošības un risku vadības terminu definīcijas (galvenokārt saskaņā ar ISO 31000 standartu), gan tulkojumus angļu un vairākās citās valodās. Tur arī atradīsiet interaktīvo rīku *Quizlet*, kas palīdzēs apgūt šos terminus angļu valodā.

Tālākajās grāmatas nodaļās jums būs iespēja iepazīties ar dažādiem labās prakses piemēriem – gadījumu analīzi, kuros ir pielietots ISO 31000 standarts, lai mazinātu drošības riskus, apdraudējumu vai ieviestu šo principu pielietošanu reālās organizācijās un uzņēmumos.

Grāmatas otrajā daļā atradīsiet praktiskus uzdevumus, ko pasniedzēji var pielietot savās lekcijās un praktiskajās nodarbībās, runājot par drošības risku vadību. Uzdevumus var lietot arī pašmācības nolūkiem, izpildot uzdevumus individuāli.

Lai papildinātu savas zināšanas drošības risku vadības jomā un iepazītos arī ar atsevišķiem grāmatā prezentētajiem gadījumiem **video formātā**, aicinām skatīties video lekcijas.

SADARBĪBA PASĀKUMA ORGANIZĒŠANAS DROŠĪBĀ UN DROŠĪBAS RISKU NOVĒRŠANA: RUISROK PIEMĒRS

Anja Aatsinki un Hanna Iisakkila Rojas / Laurea Lietišķo zinātņu Universitāte, Somija / 2023

KOPSAVILKUMS

Šī raksta mērķis ir parādīt sadarbības nozīmīgumu un procesu pasākumu organizēšanas jomā, plānojot pasākumu drošību. Labā prakse parāda modeli, ko izmanto Somijas dienvidrietumu varas iestādes, sadarbojoties ar pasākumu organizatoriem. Process atbilst ISO 31000:2018[5] risku pārvaldības procesam. Šī raksta izstrādē ir notikušas konsultācijas un intervijas ar Somijas policiju un Dienvidrietumu Somijas glābšanas iestādes pārstāvjiem.

Atsauce uz ISO 31000

Šajā rakstā sadarbības modelis ir parādīts, izmantojot atsauci uz ISO 31000:2018 riska pārvaldības sistēmu (4. attēls).

4. attēls. **Risku vadības process** (pielāgots no ISO 31000:2018[6])

[5] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

[6] Turpat

IEVADS

Pasākuma organizators ir atbildīgs par risku novēršanu, risku pārvaldību un sadarbību ar dažādām iesaistītajām pusēm un iestādēm. Somijā pasākumu drošība un apsardze ir stingri reglamentēta, un šī iemesla dēļ ir svarīgi savlaicīgi plānot pasākuma drošību. Būtiskākie Somijas tiesību akti ietver *Pulcēšanās likumu*, *Glābšanas likumu* un *Zemes izmantošanas un būvniecības likumu*. Katrā pasākumā organizatoram ir jānovērš un jāpārvalda konkrētā pasākuma riski. Lielums un riska profils ietekmē prasības, taču būtībā visos gadījumos, kad riski tiek uzskatīti par lielākiem, ārkārtas situāciju plāns ir obligāts.

Šajā rakstā uzmanība pievērsta riska novēršanai pasākuma ietvaros, *Ruisrok* (*Ruisrock*) vasaras festivālā, kas norisinās Somijā.

5. attēls. ***Ruisrok* festivāls**

Ruisrok ir viens no vecākajiem festivāliem Somijā. Tas notiek Ruissalo salā, kas ir daļa no Turku pilsētas.[7] Ruissalo ir unikāla pasākumu vieta, jo tās daba ir ļoti aizsargāta un atrašanās vieta salā rada savus izaicinājumus riska pārvaldībai. Sala ir savienota ar cietzemi ar vienu tiltu. *Ruisrok* ir trīs dienu festivāls, un nedēļas nogalē pasākumu apmeklē aptuveni 100 000 cilvēku.[8] Šajā rakstā ir parādīts sadarbības modelis starp organizatoru un dažādām iestādēm. Risku pārvaldības process tiek veidots atbilstoši ISO 31000:2018 standartam.

GADĪJUMA IZPĒTE

Ikgadējo lielo pasākumu, piemēram, *Ruisrok*, plānošana parasti ir nepārtraukts process, un nākamā gada pasākumu plānošana sākas tūlīt pēc iepriekšējā pasākuma beigām. Somijas *Pulcēšanās likums* (530/1999)[9] nosaka, ka pasākuma organizatoram ir jābrīdina policija vismaz piecas dienas pirms pasākuma, bet lielāku pasākumu gadījumā sadarbība, plānošana un konsultācijas ir praktiski nemainīgas visu gadu. Somijas *Glābšanas likums* (379/2011)[10] nosaka, ka visiem publiskajiem

7 Ruisrock festival (2022). Iegūts no https://ruisrock.fi/en/info/
8 Ruisrock (2022). Iegūts no https://ruisrock.fi/en/sold-out-ruisrock-makes-a-stellarcomeback-attracting-a-total-of-105-000-visitors/
9 Finnish Assembly Act (530/1999). Iegūts no 530/1999 English – Translations of Finnish acts and decrees – FINLEX ®
10 Rescue Act (379/2011). Iegūts no http://nwfp-policies.efi.int/wiki/Rescue_Act,_2011_(Finland)

pasākumiem, kuros vienlaikus piedalās 200 vai vairāk cilvēku, ir jāizstrādā ārkārtas rīcības plāns. Visa atbildība gulstas uz organizatoru.

Pasākuma organizēšana prasa arī sadarbību ar dažādām ieinteresētajām pusēm, piemēram, izpildītājmāksliniekiem un viņu pārstāvētājām organizācijām, dažādiem uzņēmumiem, kas piedāvā pakalpojumus pasākumā. Plānošana notiek ciešā sadarbībā ar pasākuma apsardzes nodrošinātāju, policiju, glābšanas dienestiem un veselības pakalpojumu sniedzēju. Šajā rakstā kā labā prakse ir aprakstīts sadarbības modelis ar Somijas dienvidrietumu varas iestādēm.[11]

LABĀ PRAKSE

Komunikācija un konsultācijas

Drošam pasākumam būtiska ir cieša un tūlītēja daudzu institūciju sadarbība, kā arī nepārtraukta mijiedarbība ar pasākuma organizatoru. Ja tiek nodrošināta sadarbība ar dažādām iestādēm, tad ir pieejama plaša ekspertīze drošības jomā, kas tiek apvienota ar aktuālo informāciju ar organizatoru. Drošības plānošanu pietiekami laicīgi uzsāk pasākuma organizators. Tieši organizators arī pieprasa no citiem un nodrošina, lai dažādi pasākuma elementi tiktu plānoti un veikti savlaicīgi. Lielos pasākumos pasākuma organizatoram parasti ir jākonsultējas ar drošības ekspertiem, nevis jādara viss pašam. Ir svarīgi spēt atpazīt jomas, kurās ar pašu pieredzi nepietiek. Varas iestādes konsultēs par pamatlietām, bet atbildība gulstas uz organizatoru. Papildus uzraudzībai iestādes sniedz arī informāciju un norādījumus. Tomēr jāatceras, ka neatkarīgi no sadarbības juridiskā atbildība gulstas tieši uz pasākuma organizatoru. Tādēļ organizators notikuma glābšanas plānu iesniedz reģionālajām glābšanas iestādēm ne vēlāk kā 14 dienas pirms notikuma sākuma.[12]

Funkcionālā drošība un drošības mērījumi ir būtisks pasākums veiksmīgam pasākumam, tāpēc ir ļoti svarīgi, lai organizators būtu motivēts ievērot drošības kultūru un labo praksi, lai gan arī tas nozīmētu vairāk naudas vai resursu ieguldījumu.

Ietvars, konteksts, kritēriji

Veidojot *Ruisrok* festivāla risku vadības grupu, lai aptvertu pietiekamu pieredzi, konkrētos riskus un iezīmes, tika ņemti vērā šādi aspekti:

- teritorijas specifiskās īpašības (ūdens, atrašanās vieta uz salas, intensīva satiksme, augstuma atšķirības, pilsētvide, sabiedriskais transports utt.);
- cilvēku skaits, kas piedalās pasākumā (vides uzturēšana, apsardze, vadība, pakalpojumi, izejas utt.);
- pasākuma būtība (vai pasākumā ir priekšnesumi vai izpildītāji, kas "uzkurina" pūli, cilvēki ar invaliditāti, bērni, seniori);
- vai pasākumā ir īpašas programmas vai aprīkojums, kam nepieciešama īpaša drošības plānošana un zināšanas, organizatora/valsts iestāžu resursu pieejamība.

[11] Varsinais-Suomen pelastuslaitos (2019). Iegūts no https://www.vspelastus.fi/uutinen/2019-10-02_valtakunnallinen-turvallisuuspalkinto-varsinaissuomee

[12] Rescue Act (379/2011). Iegūts no http://nwfp-policies.efi.int/wiki/Rescue_Act,_2011_(Finland)

Saskaņā ar Somijas *Glābšanas likumu* (379/2011)[13] ar notikumu saistītie apdraudējumi un riski ir jāprecizē un jānovērtē. Visiem pasākumiem ārkārtas situācijās ir jābūt balstītiem uz šo risku novērtējumu. Pasākuma organizatoram ir jārūpējas, lai tiktu ņemts vērā viss nepieciešamais tiesiskais regulējums.

Risku novērtējums

Vispirms riska novērtēšanas procesā tiek izveidots kopējais situācijas apskats. Tas ietver struktūras, programmu, vides pārvaldību un izvietojumu, cilvēkresursus un visus citus būtiskos faktorus. Risku identificēšana balstās uz notikuma specifiskajām iezīmēm un iepriekšējos gados gūtajām atziņām. Risku analīze tiek veikta, apzinot katra riska cēloņus un sekas. Pēc tam analīzi izmanto, lai novērtētu risku lielumu. Visām galvenajām iestādēm, kas ietekmē pasākumu drošību, ir jāpiedalās riska novērtēšanas kopīgās sanāksmēs. Organizators iepazīstina iestādes ar faktoriem, kas var ietekmēt situāciju, un kopā tiek izvērtēts risku nozīmīgums un sagatavotības līmenis tiem. Organizators sastāda provizorisku ārkārtas situāciju plānu, ko var apspriest ar iestādēm.

Identificētie cēloņi un sekas tiek izmantoti, lai plānotu specifiskus risku novēršanas pasākumus. Pasākuma organizatoram ir jāidentificē uzticami kritēriji un jāpierāda, ka viņu riska pārvaldības pasākumi ir orientēti uz risku novēršanu un atbilst tiesību aktiem. Varas iestādes izvērtē, vai glābšanas plānā minētie pasākumi ir pietiekami, un nepieciešamības gadījumā var lūgt pasākuma organizatoram uzlabot pasākuma drošības un apsardzes plānu.

Turklāt attiecībā uz kopējo sabiedrības drošību varas iestādēm pēc tam jāveic pasākuma radīto risku izvērtējums. Iestādēm ir jāsagatavojas tiem identificētajiem riskiem, kas nav tiešā pasākuma organizatora atbildībā. Šī sagatavotība var ietvert iestāžu resursu palielināšanu, papildu telpu rezervēšanu, iekšējās informācijas plūsmas nodrošināšanu, informācijas sniegšanu utt. Papildus liela mēroga pasākumam ir plašāka ietekme uz sabiedrību, un par tās ietekmes radīto riska novērtējumu ir atbildīgas varas iestādes.

Risku novēršana

Risku novēršana ir strukturālu, tehnisku un operatīvu pasākumu kombinācija, kuras pamatā ir risku novērtējums. Noziegumu un citu apzinātu kaitīgu darbību novēršanu lielā mērā nosaka likums. Likumi regulē dažādu dalībnieku (apsardzes darbinieku, policijas) pilnvaras. Piemēram, drošības pārbaudes un personu pārmeklēšanu, apmeklētāju izraidīšanu no teritorijas un aizturēšanu regulē likums. Lielākos pasākumos, piemēram, *Ruisrok*, papildus glābšanas plānam ir jāsastāda vairāki citi plāni, kas ir daļa no risku novēršanas procesa.

Monitorings un uzraudzība

Uzraudzība festivālā *Ruisrok* tiek veikta ar oficiālu pārbaudi tieši pirms pasākuma sākuma. Pasākuma laikā tiek veikta klātienes uzraudzība, to veic gan dažādas iestādes, gan drošības pakalpojumu sniedzējs. Apsardzes dienesta un veselības pakalpojumu sniedzēju pienākums ir arī izveidot un pildīt dienesta pasākumu žurnālu, kas palīdz organizatoram izstrādāt un plānot pasākumu nākotnē. Pēc pasākuma notiek pārrunas ar organizatoru, informācija tiek iegūta arī no medijiem un citiem publiskiem avotiem. Visa šī informācija un avoti palīdz pārskatīt un attīstīt *Ruisrok* festivālu.

[13] Rescue Act (379/2011). Iegūts no http://nwfp-policies.efi.int/wiki/Rescue_Act,_2011_(Finland)

Nozīmīgākos notikumus varas iestādes pēc tam vienmēr izvērtē kopā, nereti pārrunas tiek veiktas arī kopā ar organizatoru. Ja ir jāveic kriminālizmeklēšanas pasākumi, tad to mērķis ir saukt atbildīgās personas pie krimināltatbildības par viņu nolaidību.

Apkopošana un ziņošana

Visos posmos iestādes veic piezīmes, lai pēc gada konstatētās nepilnības tiktu ņemtas vērā nākamā pasākuma plānošanā. Procesa laikā ir jāsagatavo vairāki obligātie dokumenti. Tie, piemēram, ir:

- ugunsdrošības pārbaudes protokoli;
- notikumu žurnāli;
- sapulču protokoli.

Dinamisks un nepārtraukti pilnveidojams ārkārtas situāciju plāns kalpo arī kā rīks, kas apkopo zināšanas un gūto pieredzi, un mācības.

Izmantotie avoti

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Ruisrock festival (2022). Iegūts no https://ruisrock.fi/en/info/

Ruisrock (2022). Iegūts no https://ruisrock.fi/en/sold-out-ruisrock-makes-a-stellarcomeback-attracting-a-total-of-105-000-visitors/

Finnish Assembly Act (530/1999). Iegūts no 530/1999 English - Translations of Finnish acts and decrees - FINLEX ®

Rescue Act (379/2011). Iegūts no http://nwfp-policies.efi.int/wiki/Rescue_Act,_2011_(Finland)

Varsinais-Suomen pelastuslaitos (2019). Iegūts no https://www.vspelastus.fi/uutinen/2019-10-02_valtakunnallinen-turvallisuuspalkinto-varsinaissuomee

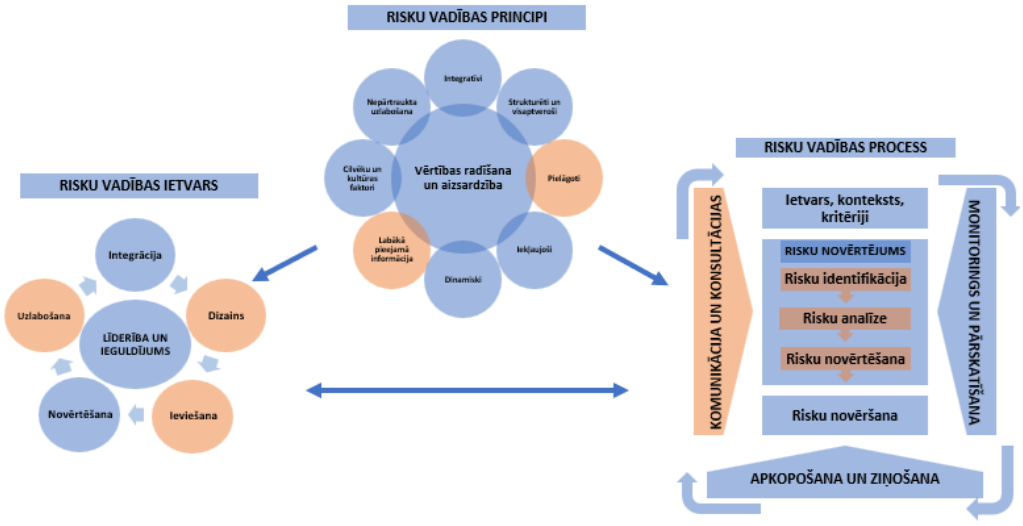
DROŠĪBAS RISKU PĀRVALDĪBAS ĪSTENOŠANA ORGANIZĀCIJĀ, KAS DARBOJAS KĀ ELEKTROTĪKLA PĀRVALDNIEKS KRITISKAJĀ INFRASTRUKTŪRĀ

Lambert Bambach / Avans Lietišķo zinātņu Universitāte, Nīderlande / 2023

KOPSAVILKUMS

Draudi nacionālajai drošībai un organizētās noziedzības draudi maina kritiskās infrastruktūras apdraudējumu ainavu, kurā darbojas organizācijas, kas pārvalda elektrotīklus. Apdraudējumu piemēri ir uzlaušana, zādzības, manipulācijas ar elektrotīklu, to bojāšana un iznīcināšana. Lai cīnītos pret šiem draudiem, ir svarīgi izstrādāt un regulāri atjaunot aktīvu jeb vērtību aizsardzības programmu. Tas tiek panākts, kartējot dažādus aizsargājamos īpašumus atbilstoši organizācijas mērķiem, veicot draudu un risku analīzi sadarbībā ar ierēdņiem un dažādu iestāžu pārstāvjiem Eiropas un valsts līmenī, konkurējošiem citiem elektrotīkla operatoriem valsts līmenī un vairākiem departamentiem pašā organizācijā.

Atsauce uz ISO 31000



6. attēls. **Risku vadības ietvars, principi un process** (pielāgots no ISO 31000:2018[14])

Risku vadības principi: vērtību radīšana un aizsardzība – labākā pieejamā informācija, cilvēki un kultūras faktori, nepārtraukta uzlabošana, integrativitāte, dinamika.

Risku vadības ietvars: līderība un ieguldījums – uzlabošana, integrācija, dizains, ieviešana, novērtēšana; risku vadības process: komunikācija un konsultācijas, monitorings un uzraudzība, risku identifikācija, risku izvērtējums, risku novērtēšana, apkopošana un izzināšana.

[14] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Jaunākajam apsardzes darbiniekam elektrotīkla pārvaldnieka aktīvu aizsardzības nodaļā tika lūgts sniegt ieskatu par aktīvu un vērtību aizsardzības programmas atjaunošanas metodēm 40 000 decentralizētiem aktīviem, sākot no zemsprieguma, vidējā sprieguma telpām, augstsprieguma kabeļiem un beidzot ar diviem centrālajiem objektiem, kur atrodas lieli datu centri.

Organizācijai ir ļoti nozīmīgi, lai aktīvu aizsardzības programma būtu izveidota sadarbībā ar iekšējām un ārējām ieinteresētajām pusēm, lai tādējādi nodrošinātu aizsardzību pret draudiem aktīviem informācijas drošības, tehnoloģiju darbības un fiziskās aizsardzības jomās.

Līdz ar atjaunoto aktīvu aizsardzības programmu ir jāīsteno drošības līmenis, kas, sadarbojoties ar dažādiem dalībniekiem, būs spējīgs tikt galā ar mainīgo draudu ainavu, kurā nacionālo valstu dalībnieki, organizētā noziedzība un zagļi arvien vairāk apdraud mērķu īstenošanu. Tas apdraud arī organizācijas galveno mērķi: "vienmēr nodrošināt un sadalīt enerģiju pa visiem tīkliem katru dienu".

Organizācija vēlas noskaidrot, kā varētu īstenot šo aktīvu aizsardzības programmu.

GADĪJUMA IZPĒTE

Organizācija darbojas kā elektroenerģijas tīkla pārvaldnieks, kas ir atbildīgs par pareizu enerģijas sadali visos savos tīklos ik dienu. Izmantojot kabeļus, vairāk nekā trīs miljoni Nīderlandes mājsaimniecību un uzņēmumu tiek apgādāti ar elektrību. Šim nolūkam tiek izmantoti 40 000 decentralizēti aktīvi, sākot no zemsprieguma, vidējā sprieguma telpām, augstsprieguma kabeļiem un diviem centrāliem objektiem, kur atrodas lieli datu centri. Organizācija vēlas, lai tās tīkls arī turpmāk būtu viens no pasaulē uzticamākajiem un saglabātu tīkla uzticamību un pieejamību saviem klientiem.

Drošības risku vadītājs skaidro, ka aktīvu aizsardzības programmai jāspēj tikt galā ar mainīgo apdraudējumu ainavu, lai varētu turpināt īstenot organizācijas mērķus. Šajā mainīgajā terorisma draudu vidē palielinās iespēja, ka nacionālo valstu dalībnieki var uzlauzt operētājsistēmas un organizētā noziedzība un zagļi var nozagt vērtīgus materiālus.

Apsardzes vadītājs arī apzinās, ka aizsargājamo īpašumu skaits ir ne tikai plašs, bet arī daudzveidīgs. Tas attiecas gan uz aktīviem, kas ir saistīti ar darbības nodrošinājuma tehnoloģijām, gan Informācijas tehnoloģijām. To darot, viņam ir jāsadarbojas ar vairākām ieinteresētajām pusēm, kuras spēlē nozīmīgu lomu draudu novēršanā un ar kurām ir svarīga sadarbība. Šiem dalībniekiem ne vienmēr ir tādas pašas intereses kā organizācijai. Pagaidām arī nav skaidrs, kā vislabāk var izpildīt dažādas prasības, ko nosaka likums un regulējums.

Visu šo iemeslu dēļ labās prakses izpētē tika lūgts sniegt ieskatu iespējamās aktīvu aizsardzības programmas realizācijas metodēs. To darot, ir svarīgi ņemt vērā: a) organizācijas mērķi; b) draudu un risku analīzi; c) dažādās ieinteresētās puses.

LABĀ PRAKSE

Organizācijas mērķis

Organizācijas galvenais mērķis ir spēt nepārtraukti un ik dienu sadalīt un nogādāt enerģiju pa visiem saviem tīkliem, lai šis tīkls būtu viens no uzticamākajiem pasaulē.

Dažādi aktīvu veidi

Organizācijai ir decentralizēti un centralizēti aktīvi. Decentralizētajā jomā organizācijai ir jānodarbojas ar tādiem aktīviem kā vadības skapji un transformatori. Operacionālās jeb Darbību nodrošinošās tehnoloģijas (OT[15]) spēlē svarīgu lomu šajos aktīvos. Operacionālās tehnoloģijas raksturo fakts, ka to galvenais mērķis ir: darboties pēc iespējas ilgāk un ar pēc iespējas mazāku dīkstāvi. Šīs iekārtas kalpo ilgu laiku, un tās parasti neatbilst mūsdienu standartiem, jo tās savulaik tika būvētas atbilstoši standartiem, kas tika pieņemti pirms 30 gadiem. Turklāt OT īpašums nevar sevi aizsargāt digitāli.

Centralizēti organizācija nodarbojas ar tādiem aktīviem kā biroju ēkas un datu centri, kas ir vairāk saistīti ar informācijas tehnoloģijām (IT). IT vidē tiek pieņemts, ka informācijas resursam ir jāspēj sevi aizsargāt pašam. Tiek uzskatīts, ka darbā ar informāciju tehnoloģijām ir nepieciešama liela elastība, jūs galvenokārt strādājat pie to funkcionalitātes. IT tehnoloģijām ir jāatbalsta biznesa mērķi, tās ir ātras, elastīgas, un tām ir īss kalpošanas laiks.

Tas nozīmē, ka ir nepieciešama atšķirīga pieeja Operacionālajiem jeb darbību nodrošinošajiem tehnoloģiju aktīviem un Informācijas tehnoloģiju aktīviem. Parasti Operacionālās tehnoloģijas var uzskatīt par īpašumu, kas nevar sevi aizsargāt pats. Tas nozīmē, ka ir jāizveido pasākumi, lai aizsargātu šādu īpašumu.

Runājot par Informācijas tehnoloģijām, ir jāatceras trīs informācijas drošības pamatprincipi: integritāte, konfidencialitāte un pieejamība, kā arī fakts, ka šīm tehnoloģijām ir pieņemama periodiska dīkstāve. Savukārt Operacionālajām tehnoloģijām pamatprincipi ir atšķirīgi, proti: pieejamība, integritāte un tikai tad konfidencialitāte, kā arī dīkstāves laiks nav pieņemams.[16]

Draudu un risku analīze

- **Risku identifikācija un analīze**

Galvenie draudi ir nacionālās valsts dalībnieki, organizētā noziedzība un zagļi, kas var apdraudēt organizācijas galveno mērķi, veicot uzlaušanu, zādzību, iznīcināšanu un manipulāciju ar elektroenerģijas tīklu.

- **Risku novērtējums**

Nacionālās valsts dalībnieku[17] gadījumā ir grūti šos draudus mazināt, jo šiem cilvēkiem bieži vien ir neierobežoti resursi. Tas ir uzskatāms par pieņemamu risku. Taču kritiskā infrastruktūra nedrīkst tikt apdraudēta, un tai ir jābūt pieejamai nepārtraukti, jo no tās ir atkarīgi daudzi citi sabiedriskie pakalpojumi un organizācijas. Piemēram, policija sagaida, ka tās sakaru sistēmas vienmēr tiks uzturētas darba kārtībā un tās darbosies. Ja policija krīzes laikā vairs nespēj sazināties, tad šī ir nopietna problēma organizācijai, kas sniedz šo pakalpojumu. Tas rada nacionālās drošības apdraudējumu, un organizācija nesasniedz savu primāro mērķi – pakalpojuma piegādes drošību. Tas nozīmē, ka organizācijai ir būtiski nepārtraukti nodrošināt un novadīt enerģiju pa visiem tīkliem.

Organizētās noziedzības gadījumā organizācijai ir jāveic vēl citi drošības pasākumi. Īpaši attiecībā uz operacionālajiem tehnoloģiju aktīviem, jo šie līdzekļi nevar paši sevi aizsargāt. Tas nozīmē, ka ir

[15] Operational Technology (OT). Iegūts no https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

[16] How Do OT and IT Differ? Iegūts no How Is OT Different From IT? OT vs. IT - Cisco

[17] Cybersecurity And Nation-State Threats: What Businesses Need To Know. (2021). Iegūts no Cybersecurity And Nation-State Threats: What Businesses Need To Know (forbes.com)

jāizstrādā pasākumu plāns, lai aizsargātu šos īpašumus, piemēram, ar kameru sistēmu, žogu un pastiprinātas piekļuves kontroles palīdzību. Lai nodrošinātu šo tehnoloģiju aizsardzību, organizācijai ir nepārtraukti jāattīstās un katru gadu jāpārskata drošības pasākumi un pamatprincipi – jāizvērtē, vai tie ir pietiekami, vai arī tie ir jākoriģē. Zādzību novēršanai bieži vien pietiek ar standarta pasākumiem šo draudu mazināšanai. Zagļus raksturo tas, ka iespēja, ka tiks veikta zādzība, palielinās, ja nav nodrošināta objekta aizsardzība. Tātad, ja iespēja ir ierobežota, pastāv liela varbūtība, ka zaglis neturpinās savas darbības.

Tiesību akti un regulējums

Šīs organizācijas gadījumā viena no svarīgākajām ieinteresētajām pusēm ir likumdevējs. Organizāciju uzrauga Ekonomikas un klimata ministrijas Nacionālā digitālās infrastruktūras inspekcija, jo organizācija tiek regulēta saskaņā ar NIS 1 un tuvākajā nākotnē tiks regulēta saskaņā ar NIS 2, jo organizācija ir daļa no vitāli svarīgās infrastruktūras. NIS ir direktīva par tīklu un informācijas sistēmu drošību (NIS direktīva[18]), ko pārrauga Eiropas Savienības Kiberdrošības aģentūra (ENISA)[19].

Turklāt organizācija ir sertificēta saskaņā ar ISO 27001[20] un ISO 27019[21] standartiem.

ISO standartizācija ir palīdzējusi fiziskās un informācijas drošības nodaļai objektīvi konsultēt un novērtēt darbību, standartizācija palīdz arī organizācijas iekšienē "runāt vienā universālā valodā", piemēram, ar vadību. Tas palīdz arī veidot kopīgu izpratni ar ārējiem spēlētājiem, piemēram, regulatoru un palīdz nepārtraukti meklēt uzlabojumus organizācijā.

Ieinteresētās puses jeb mērķgrupas

Dažādas ieinteresētās puses veido avotus, uz kuriem organizācija var paļauties, lai iezīmētu savu draudu ainavu un riska apetīti un pārbaudītu, vai tās ir uz pareizā ceļa. Organizācijai ir svarīgi gūt ieskatu par draudiem no dažādām perspektīvām un strādāt kopā, lai mazinātu draudus.

Iekšējā mērķgrupa

- **Vadība**

Tieši organizācijas vadība ir tā, kas izdara izvēli, vai pasākumi patiešām tiks īstenoti. Tā pieņem lēmumus, pamatojoties uz draudu ainavu, ko tai ieteikusi Fiziskās un informācijas drošības nodaļa. Šim nolūkam ir izveidota Informācijas drošības vadības sistēma (*information security management system* (*ISMS*)[22]), kas ir tieši pakļauta Direktoru padomei. Tā ir augstākā institūcija, kurā tiek pieņemti visi organizācijas galīgie lēmumi. Brīdī, kad organizācija saskaras ar risku, Fiziskās un informācijas drošības nodaļa var ziņot par to Direktoru padomei. Tā savukārt nekavējoties var novirzīt resursus problēmas risināšanai.

Apsveramie jautājumi ir: vai mēs patiešām īstenosim visus pasākumus draudu novēršanai un kādā laika periodā mēs šo pasākumus ieviesīsim? Vai varbūt mēs organizācijā nenosakām pietiekamus

[18] Supporting the implementation of Union policy and law regarding cybersecurity. (2023). NIS Directive. Iegūts no NIS Directive — ENISA (europa.eu)
[19] The European Union Agency for Cybersecurity. Iegūts no ENISA (europa.eu)
[20] Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Edition 3. Iegūts no https://www.iso.org/standard/27001
[21] Information technology — Security techniques — Information security controls for the energy utility industry. Iegūts no https://www.iso.org/standard/68091.html
[22] Information security management system (ISMS). Iegūts no What is Information Security Management System (ISMS)? (techtarget.com)

drošības pasākumus, kas nākotnē vājinās mūsu spējas novērst apdraudējumu? Kādus vēl papildu pasākumus mēs varam veikt draudu novēršanai?

- **Fiziskās un informācijas drošības nodaļa**

Fiziskās un informācijas drošības nodaļas strādā kopā. Organizācijā nodaļas ir tieši pakļautas Direktoru padomei. Konkrētajā organizācijā ir divi departamenti, kas strādā ar drošības jautājumiem, tomēr katrs no departamentiem veic savu neatkarīgo lomu. No vienas puses, drošība ir zināmu prasību izpilde, no otras puses, kontrolēšana, bet tai nekad nepiemīt izpildvaras funkcijas. Ļoti bieži var redzēt, ka drošības joma organizācijās tiek ievietota izpildinstitūcijā. Tomēr tādā gadījumā drošības departamenti nekad nevar būt neatkarīgi savos spriedumos un sniegtajos padomos.

Lai varētu noteikt konkrētas prasības, organizācijai ir jāapskata trīs jautājumi: 1) Ko mēs patiesībā aizsargāsim? 2) Ko mēs šobrīd aizsargājam? 3) Kas ir mūsu "kroņa dārgakmeņi"[23]?

Šeit svarīgs uzdevums ir palīdzēt darbiniekiem apzināties, ka draudu ainava faktiski ir mainījusies un ka tas noved pie jauniem pasākumiem. Svarīgi ir pašus darbiniekus iesaistīt pārmaiņās, kas attiecas uz drošības nodrošināšanu. Mūsu darbā ienāk jauni informācijas tehnoloģiju līdzekļi: ko tas nozīmē darbam, kā mainās drošības pasākumi saistībā ar šiem jaunajiem līdzekļiem? Tas nenozīmē, ka darbiniekiem ir tikai jābūt tehniski apmācītiem, bet arī to, ka ir jāievieš citi pārvaldības pasākumi un jāinformē darbinieki, kāpēc šie jauninājumi nepieciešami. Šeit ļoti svarīga ir drošības izpratnes veicināšana darbinieku vidū.

Ārējās mērķgrupas

- **Eiropa**

Eiropas elektroenerģijas transporta sistēmu operatoru tīkls (ENTSO-E[24]) ir partnerība, kurā ir pārstāvēti visi Eiropas tīklu operatori, kas darbojas Eiropas sinhronizētajā tīklā. Organizācija ir ENTSO-E dalībniece, lai apmainītos ar zināšanām par mainīgo draudu ainavu.

- **Nacionālā valdība**

Lai iegūtu informāciju draudu un risku analīzei, organizācija sadarbojas ar Tieslietu un drošības ministrijas Nacionālo kiberdrošības centru, Tieslietu un drošības ministrijas Nacionālo pretterorisma un drošības koordinatoru un Iekšlietu ministrijas Vispārējās izlūkošanas un drošības dienestu. Organizāciju arī uzrauga Ekonomikas un klimata politikas ministrijas Nacionālās digitālās infrastruktūras inspekcija.

[23] Identify Your "Crown Jewels". Iegūts no https://staysafeonline.org/cybersecurity-for-business/identify-your-crown-jewels/#:~:text=Crown%20jewels%20are%20the%20data,high%2Dvalue%20target%20for%20cybercriminals

[24] European Network of Transmission System Operators for Electricity. Iegūts no Home (entsoe.eu)

Citi konkurējošie elektrotīkla operatori

Organizācija strādā kopā ar trīs citiem tīkla operatoriem. Tiem visiem ir vienādas intereses – aizsargāt svarīgo infrastruktūru, taču tās vienlaikus ir arī konkurējošas organizācijas. Viņi strādā kopā, lai noteiktu minimālo drošības bāzes līniju, kas periodiski jāpārskata, lai tā atbilstu jaunākajai draudu ainavai. Organizācijām ir svarīgi pārliecināties, vai šie noteikumi ir ieviesti pašu organizācijā un arī pārējās konkurējošās organizācijās. No komerciālā viedokļa ir svarīgi tas, cik daudz organizācija ir ieguldījusi drošības pasākumos. Ir izdevīgi, ja drošības pasākumi ir labāki nekā konkurentiem, jo noziedznieks tomēr skatās uz vājāko posmu.

Izmantotie avoti

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Operational Technology (OT). Iegūts no https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

How Do OT and IT Differ? Iegūts no How Is OT Different From IT? OT vs. IT – Cisco

Cybersecurity And Nation-State Threats: What Businesses Need To Know. (2021). Iegūts no Cybersecurity and Nation-State Threats: What Businesses Need to Know (forbes.com)

Supporting the implementation of Union policy and law regarding cybersecurity. (2023). NIS Directive. Iegūts no NIS Directive – ENISA (europa.eu)

The European Union Agency for Cybersecurity. Iegūts no ENISA (europa.eu)

Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Edition 3. Iegūts no https://www.iso.org/standard/27001

Information technology — Security techniques — Information security controls for the energy utility industry. Iegūts no https://www.iso.org/standard/68091.html

information security management system (ISMS). Iegūts no What is Information Security Management System (ISMS)? (techtarget.com)

Identify Your “Crown Jewels”. Iegūts no https://staysafeonline.org/cybersecurity-for-business/identify-your-crown-jewels/#:~:text=Crown%20jewels%20are%20the%20data,high%2Dvalue%20target%20for%20cybercriminals

European Network of Transmission System Operators for Electricity. Iegūts no Home (entsoe.eu)

KIBERDROŠĪBAS TEHNOLOĢIJU IZVĒLE, BALSTOTIES UZ RISKA VADĪBAS PROCESU

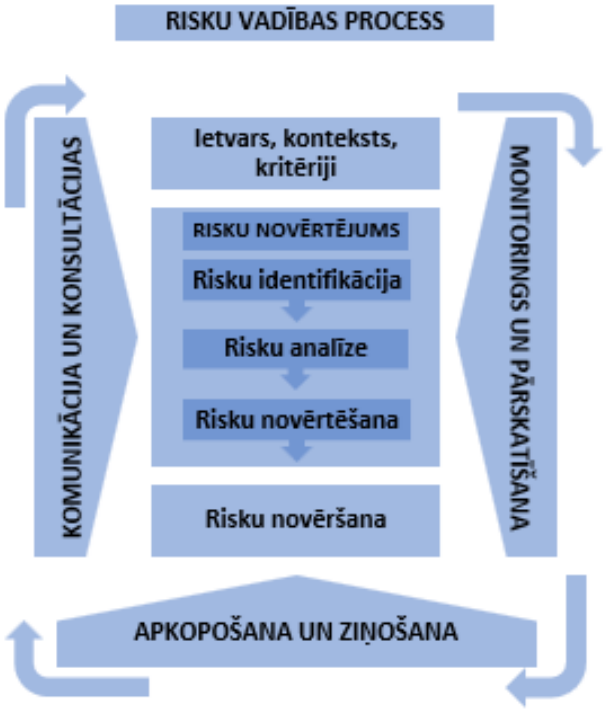
Jyri Rajamäki / Laurea Lietišķo zinātņu universitāte, Somija / 2023

KOPSAVILKUMS

Ievērojot ISO 31000:2018 standarta principus, organizācijas var pieņemt pārdomātus lēmumus par kiberdrošības tehnoloģiju izvēli, ieviešanu un pastāvīgu pārvaldību, lai efektīvi mazinātu riskus un aizsargātu savus informācijas līdzekļus. Balstoties uz programmas *DIMECC Cyber Trust*[25] rezultātiem, šajā rakstā ir sniegta strukturēta pieeja nepieciešamo drošības tehnoloģiju izvēlei, pamatojoties uz riska pārvaldības procesiem, kas ir izšķiroši svarīgi nepārtraukti mainīgajos kiberdrošības apdraudējumos.

Atsauce uz ISO 31000

ISO 31000 risku vadības process: risku novērtējums, risku novēršana, monitorings un uzraudzība, apkopošana un ziņošana, komunikācija un konsultācijas.

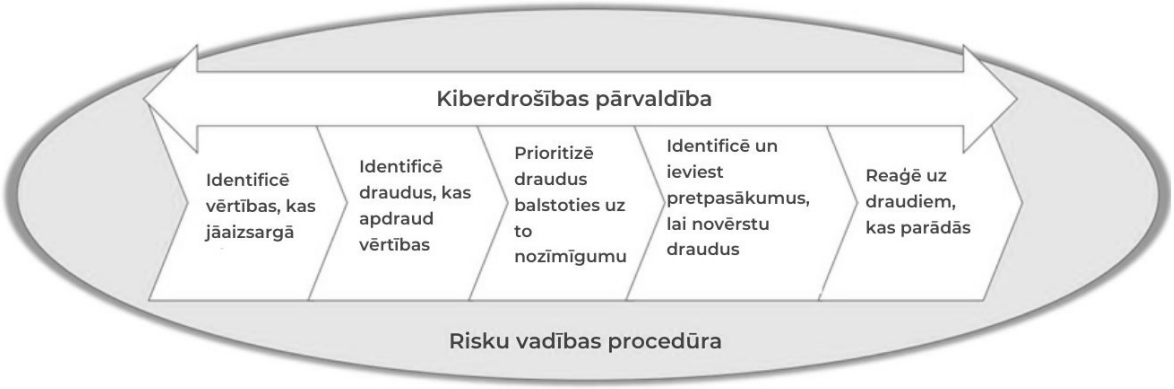


7. attēls. **Risku vadības process** (pielāgots no ISO 31000:2018[26])

[25] Cyber Trust program. Iegūts no https://cybertrust.dimecc.com/
[26] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Risku vadība ir būtiska sastāvdaļa stratēģijas noteikšanai, mērķu sasniegšanai un lēmumu pieņemšanai dažādos organizācijas līmeņos. ISO 31000:2018 nodrošina vadlīnijas un principus efektīvai risku pārvaldībai jebkurā organizācijā. Risku vadībai ir ļoti svarīga loma jebkurā vadības sistēmā. Piemēram, kā redzams attēlā zemāk, praksē kiberdrošības pārvaldība ir risku pārvaldības procedūra.



8. attēls. **Kiberdrošības pārvaldība**

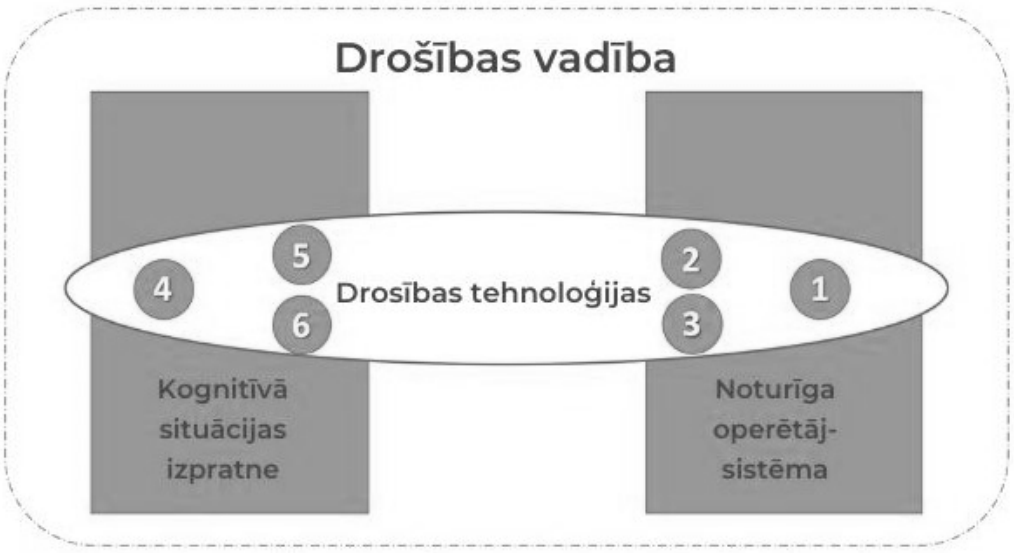
Drošības tehnoloģijas sevī ietver tehniskos līdzekļus kiberdrošības nodrošināšanai, tostarp drošas sistēmu arhitektūras, protokolus un rīkus. Tās nodrošina infrastruktūru, platformu, ierīču, pakalpojumu un datu aizsardzību. Galvenie aspekti šeit ietver lietotāja identifikāciju, autorizāciju un piekļuves tiesības. Kopējie drošības tehnoloģiju standarti tīkla drošībai ir noteikti ISO/IEC 27033[27] standartā, savukārt lietojumprogrammu drošībai – ISO/IEC 27034[28] standartā. Lai gan ISO 31000 īpaši neattiecas uz kiberdrošības tehnoloģijām, tā principus un sistēmu var piemērot kiberdrošības tehnoloģiju atlasei un ieviešanai organizācijā.

GADĪJUMA IZPĒTE

DIMECC Cyber Trust programma[29] radīja pamatu Somijas pētniecībai un rūpniecībai, lai risinātu kiberdrošības vajadzības. *DIMECC Cyber Trust* programmas galvenais pētniecības mērķis bija uzlabot privātumu, uzticēšanos un lēmumu pieņemšanu digitālajā infrastruktūrā. Konsorcijas sastāvā bija 19 uzņēmumi un astoņi pētniecības institūti un universitātes. Programma publicēja vairāk nekā 130 zinātniskos rakstus par kiberdrošību un privātuma aizsardzību.

Kiberdrošība kalpo kā galvenais faktors uzticamības veicināšanai digitālajā pasaulē, lai nodrošinātu visu operētājsistēmu un infrastruktūru noturību. *DIMECC* iezīmē četras galvenās kiberdrošības tēmas, proti, drošības pārvaldība, situācijas izpratne, drošības tehnoloģijas un operētājsistēmu noturība.

[27] Information technology — Security techniques — Network security. ISO/IEC 27033-1:2015. Iegūts no https://www.iso.org/standard/63461.html
[28] Information technology — Security techniques — Application security. ISO/IEC 27034-1:2011. Iegūts no https://www.iso.org/standard/44378.html
[29] Cyber Trust program. Iegūts no https://cybertrust.dimecc.com/



9. attēls. **Drošības vadība un drošības tehnoloģijas**

Drošības tehnoloģijas var iedalīt sešās dažādās kategorijās pēc to mērķa:

1) tehnoloģijas operētājsistēmas drošības uzlabošanai, piemēram, sistēmu arhitektūras, protokoli, izstrādes rīki un izstrādes platformas;
2) aizsardzības tehnoloģijas, piemēram, lietotāju identifikācija un autorizācija, ugunsmūri, pretvīrusu programmas, ielaušanās aizsardzības sistēmas (IPS) un drošības informācijas un notikumu pārvaldības sistēmas (SIEM);
3) tehnoloģijas drošības datu iegūšanai, piemēram, sensori (ugunsmūra žurnāli, sistēmas notikumu žurnāli, pretvīrusu uztveršana), tīkla trafika analizatori, ielaušanās atklāšanas sistēmas (IDS) un atvērtā pirmkoda izlūkošanas (OSINT) tehnoloģijas;
4) drošības datu analīzes tehnoloģijas. Šīs tehnoloģijas var iedalīt trīs līmeņos:
   1. līmenis – vēsture: kriminālistika;
   2. līmenis – pašreizējās situācijas izpratne (datu saplūšana, SIEM);
   3. līmenis – nākotnes statusa prognozēšana;
5) situācijas attēla vizualizācijas tehnoloģijas, tostarp cilvēka un mašīnas saskarnes tehnoloģijas;
6) tehnoloģijas kiberdraudu izlūkošanas informācijas apmaiņai starp organizācijām, piemēram, agrīnās brīdināšanas sistēmas, ļaunprātīgas programmatūras informācijas koplietošanas platforma (MISP), *Cortex* un *TheHieve*.

Tajā pašā laikā vairākas tehnoloģijas var piederēt vairāk nekā vienai kategorijai.

LABĀ PRAKSE

Apvienojot minētās informācijas drošības tehnoloģijas ar ISO 31000 procesiem, var izveidot visaptverošu kiberdrošības ietvaru. Apskatīsim šīs integrētās pieejas galvenos aspektus.

Risku identifikācija, novērtēšana, novēršana

- **Risku identifikācija (ISO 31000 – 5. punkts)**
  - Izmantojiet tehnoloģijas drošības datu iegūšanai (sensori, tīkla trafika analizatori, IDS, OSINT), lai identificētu iespējamos draudus un ievainojamības.
  - Izmantojiet atvērtā pirmkoda izlūkošanas tehnoloģijas, lai izprastu kiberdrošības vidi.[30]
- **Risku izvērtējums (ISO 31000 – 6. punkts)**
  - Apvienojiet tehnoloģijas drošības datu analīzei (kriminālistika, datu saplūšana, SIEM), lai novērtētu identificēto risku iespējamību un ietekmi.
  - Izmantojiet tehnoloģijas situācijas attēla vizualizēšanai, lai izprastu pašreizējo kiberdrošības situāciju.[31]
- **Risku novēršana (ISO 31000 – 7. punkts)**
  - Izvēlieties un ieviesiet aizsardzības tehnoloģijas (ugunsmūri, antivīruss, IPS, SIEM), pamatojoties uz novērtētajiem kiberdrošības riskiem.
  - Izmantojiet tehnoloģijas kiberdraudu izlūkošanas informācijas kopīgošanai (agrīnās brīdināšanas sistēmas, MISP, *Cortex*), lai būtu informēti par draudiem, kas attīstās.[32]

Monitorings un pārskatīšana

- **Monitorings un pārskatīšana (ISO 31000 – 8. punkts)**
  - Izmantojiet tehnoloģijas nepārtrauktai drošības infrastruktūras uzraudzībai (sensori, IDS).
  - Analizējiet drošības žurnālus, izmantojot tehnoloģijas drošības datu (SIEM) analīzei, lai identificētu anomālijas.
  - Regulāri pārskatiet un atjauniniet kiberdrošības pasākumus, pamatojoties uz mainīgo draudu ainavu.[33]

Komunikācija un konsultācijas

- **Komunikācija un konsultācijas (ISO 31000 – 2. un 3. punkts):**
  - Izveidojiet cilvēka un mašīnas savstarpējo sadarbību, izmantojot tehnoloģijas situācijas attēla vizualizēšanai, lai atvieglotu saziņu.
  - Izmantojiet tehnoloģijas kiberdraudu izlūkošanas informācijas apmaiņai ar citām organizācijām, lai paziņotu par draudiem un mazināšanas stratēģijām.[34]

Integrācija ar vispārējo vadību

- **Integrācija ar vispārējo vadību (ISO 31000 – 4. punkts):**
  - Integrējiet kiberdrošības risku pārvaldību kopējā pārvaldībā, izmantojot tehnoloģijas operētājsistēmas drošības uzlabošanai.
  - Saskaņojiet kiberdrošības aspektus ar uzņēmējdarbības mērķiem, izmantojot aizsardzības tehnoloģijas un riska novēršanas iespējas.[35]

---

30 ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html, 5. p.
31 Ibid, 6. p.
32 Ibid, 7. p.
33 Ibid, 8. p.
34 ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html, 2., 3. p.
35 Ibid, 4. p.

Šāda integrēta pieeja nodrošina visaptverošu kiberdrošības stratēģiju, kas apvieno dažādu drošības tehnoloģiju stiprās puses un saskaņo pārvaldību ar ISO 31000 risku pārvaldības procesiem. Regulāri atjauninājumi un komunikācijas kanāli palīdz pielāgoties kiberdrošības draudu dinamiskajam raksturam.

Izmantotie avoti

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Information technology – Security techniques – Network security. ISO/IEC 27033-1:2015. Iegūts no https://www.iso.org/standard/63461.html

Information technology – Security techniques – Application security. ISO/IEC 27034-1:2011. Iegūts no https://www.iso.org/standard/44378.html

Cyber Trust program. Iegūts no https://cybertrust.dimecc.com/

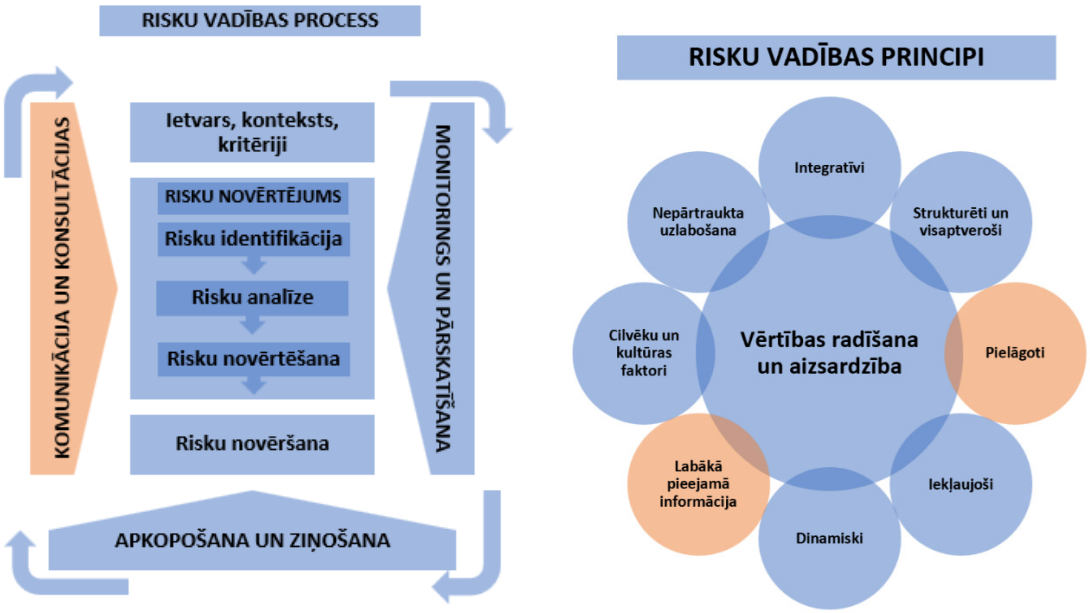
Ensieh Roud / Nord Universitāte, Norvēģija / 2023

KOPSAVILKUMS

Šajā rakstā ir apskatīti veiksmīgas sadarbības elementi ārkārtas reaģēšanas laikā Gjerdrumā, Norvēģijā, kad notika zemes nogruvums. Šis piemērs skaidri izgaismo saziņas un zināšanu apmaiņas galveno lomu iesaistīto organizāciju sadarbībā. Būtiska ir plānošana, nevis improvizācija un oficiāli noteikti un saskaņoti saziņas kanāli un procedūras. Šī incidenta novēršanā veiksmīgi tika organizēti efektīvi sadarbības tīkli, kam raksturīga vienota darbošanās, līdzdalība lēmumu pieņemšanā un kopīga vadība.

Atsauce uz ISO 31000

Šajā rakstā uzsvērta komunikācijas un sadarbības nozīme, parādot ISO 31000:2018 riska vadības principa – Labākā pieejamā informācija un pielāgotība nozīmīgumu. Tāpat raksts parāda komunikācijas un konsultāciju nozīmi risku vadības procesā ISO 31000:2018 standartā.



10. attēls. **Risku vadības process un principi** (pielāgots no ISO 31000:2018[36])

[36] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Valstīm un kopienām ir jāizstrādā pielāgošanās risinājumi un jāīsteno pasākumi, lai reaģētu uz jau notiekošo klimata pārmaiņu ietekmi, kā arī jāsagatavojas nākotnes draudiem. To uzsver ANO Klimata pārmaiņu sekretariāts[37], apspriežot pielāgošanos klimata pārmaiņām. Tomēr dabas katastrofas nav atsevišķi notikumi, jo tās bieži vien ir sarežģītas sociālās un vides mijiedarbības rezultāts.[38] Lai risinātu šo daudzpusīgo problēmu, šajā rakstā tiks apskatīti ISO 31000 principi un atsauce uz *ASIS International* sertifikācijas rokasgrāmatas[39] septīto domēnu (*Domain Seven*).

Sadarbība pāri vairākām ģeogrāfiskām un organizatoriskām robežām ir viena no galvenajām riska pārvaldības un noturības uzlabošanas sastāvdaļām, kas nodrošina efektīvas reaģēšanas un atjaunošanas darbības dabas katastrofas gadījumā.[40] Novērtējuma ziņojumi par vairākām katastrofām, piemēram, viesuļvētru "Katrīna", Kalifornijas meža ugunsgrēkiem un plūdiem Vācijā 2021. gadā, liecina, ka organizētāka starporganizāciju sadarbība būtu samazinājusi šo notikumu postošās sekas. Strauji mainīgā situācija dabas katastrofu gadījumā un reaģēšana uz sarežģītiem notikumiem bieži vien liek glābšanas dienestiem novirzīties no izveidotajām organizatoriskajām struktūrām, lai darbotos jaunā kontekstā un risinātu jaunus uzdevumus.[41] Reaģējot uz dabas katastrofām, organizācijām ir jāsadarbojas, jo viena organizācija var nebūt spējīga patstāvīgi risināt situāciju strauju vides izmaiņu, pieredzes trūkuma, uzdevuma apjoma un nepietiekamu resursu dēļ.[42] Šo starporganizāciju sadarbību var nodrošināt, sistemātiski daloties ar katras organizācijas rīcībā esošo informāciju un apvienojot savus mērķus.[43] Tāpēc šādā sadarbībā ārkārtas situācijās vajadzētu tikt iesaistītām vairākām organizācijām, piemēram, policijas departamentiem, medicīniskās palīdzības dienestiem un glābšanas dienestiem. Turklāt atkarībā no ārkārtas situācijas mēroga var tikt iesaistītas arī vietējās varas iestādes, valdības departamenti, militārie spēki un dažādi uzņēmumi no dažādām valstīm.

Tāpēc efektivitātes uzlabošanai dabas katastrofas gadījumā ir nepieciešams izstrādāt integrētu apdraudējuma mazināšanas un noturības plānu, kas ietver starporganizāciju sadarbību starp savstarpēji atkarīgām organizācijām.[44]

Šajā rakstā ir sniegti daži paraugprakses piemēri starporganizāciju attiecībām zemes nogruvuma laikā mazajā Askas pilsētā, kas atrodas Gjerdurmas pašvaldībā Norvēģijā. Pateicoties tās krasta līnijai un plašām kalnu grēdām, Norvēģija ir ļoti pakļauta mainīgiem laikapstākļiem. Norvēģijas Klimata pakalpojumu centra[45] sniegtajā ziņojumā "Klimats Norvēģijā 2100" norādīts, ka pakāpeniski pieaugošā temperatūra, palielināts nokrišņu daudzums, kā arī pieaugošie plūdi nākotnes klimatā

[37] United nations climate change annual report (2021). Iegūts no https://unfccc.int/sites/default/files/resource/UNFCCC_Annual_Report_2021.pdf

[38] Boin, A., Ekengren, M. & Rhinard, M. (2020). Hiding in plain sight: Conceptualizing the creeping crisis. Risk, Hazards & Crisis in Public Policy, 11 (2), 116–138.

[39] ASIS International Board Certification Handbook. Iegūts no https://www.asisonline.org/globalassets/certification/documents/certification-handbook_final.pdf

[40] Therrien, M. C., Beauregard, S. & Valiquette-L'Heureux, A. (2015). Iterative factors favoring collaboration for interorganizational resilience: The case of the greater Montréal transportation infrastructure. International Journal of Disaster Risk Science, 6, 75–86.

[41] Andreassen, N., Borch, O. J., & Sydnes, A. K. (2020). Information sharing and emergency response coordination. Safety Science, 130, 104895.

[42] Kapucu, N., & Garayev, V. (2011). Collaborative decision-making in emergency and disaster management. International Journal of Public Administration, 34 (6), 366–375.

[43] Therrien, M. C., Beauregard, S. & Valiquette-L'Heureux, A. (2015). Iterative factors favoring collaboration for interorganizational resilience: The case of the greater Montréal transportation infrastructure. International Journal of Disaster Risk Science, 6, 75–86.

[44] Godschalk, D. R. (2003). Urban hazard mitigation: Creating resilient cities. Natural hazards review, 4 (3), 136.–143.

[45] Climate in Norway 2100 (2017). Iegūts no https://www.miljodirektoratet.no/globalassets/publikasjoner/M741/M741.pdf

var izraisīt ātrāku mālu noslīdēšanu atsevišķās Norvēģijas vietās. Šajā ziņojumā ir arī apskatīti daži plūdu un zemes nogruvumu gadījumi, lai uzlabotu risku un krīžu pārvaldību saistībā ar dabas apdraudējumiem.

GADĪJUMA IZPĒTE

2020. gada Gjerdrumas zemes nogruvums notika Norvēģijā, Askas pilsētā, Gjerdrumas administratīvajā centrā. Šis ātrais māla nogruvums aptvēra 300 x 700 metru lielu platību un izraisīja gružu plūsmu, kas ietekmēja papildu 9 hektārus. Kamēr daži cilvēki tika izglābti, bet citi evakuējās paši, dzīvību zaudēja 10 cilvēki, un tika iznīcinātas vairākas ēkas, kā rezultātā ekonomiskās izmaksas pārsniedza 100 miljonus ASV dolāru.[46] Apvienotā glābšanas koordinācijas centra (JRCC) ziņojumā teikts, ka Gjerdrumas zemes nogruvuma agrīnajā fāzē galvenais izaicinājums bija iegūt visaptverošu izpratni par tā apmēru un pieprasīt atbilstošus resursus.[47] Ārkārtas situācijas bieži raksturo nenoteiktība un ierobežota informācija, un incidenti, kas notiek naktī vai nelabvēlīgos laikapstākļos, piemēram, Gjerdrumas zemes nogruvums naktī Ziemassvētku periodā, saasina izaicinājumu iegūt informāciju. Negadījuma dēļ bija jāveic pamatīga meklēšanas un glābšanas operācija, jo bija ievērojams skaits cilvēku, kuriem bija nepieciešama tūlītēja palīdzība. Tam sekojošie infrastruktūras, piemēram, ūdensvada, kanalizācijas, ceļu un elektrības, darbības traucējumi apgabalā vēl vairāk sarežģīja situāciju.[48]

LABĀ PRAKSE

Reaģēšana uz Gjerdrumas zemes nogruvumu tiek uzskatīta par diezgan veiksmīgu. Šī situācija varēja beigties kā daudz lielāka traģēdija. Pārskatot novērtējuma ziņojumus un intervējot iesaistītos dalībniekus, atklājās daži lieliskas sadarbības elementi. Norvēģijā pēc 2011. gada terorakta ir notikušas vairākas reformas un krīzes vadības principiem tika pievienota sadarbība. Kopš tā laika dažādas organizācijas kopā ir piedalījušās virknē mācību, lai uzlabotu starporganizāciju sadarbību. Gjerdrumas pašvaldība plānoja mācības, pamatojoties uz zemes nogruvuma scenāriju, taču Covid uzliesmojuma dēļ tās diemžēl nevarēja realizēt. Ja šīs mācības tiktu realizētas, starporganizāciju sadarbības izaicinājumi, ar kuriem viņi saskārās nogruvuma laikā, noteikti būtu mazāki. Šī situācija parādīja kopīgu mācību un reālu situāciju izspēļu nozīmi un to, kā tas var pozitīvi ietekmēt **informācijas izplatīšanu, komunikāciju, lomu skaidrību, vienotu darbības nosacījumu noteikšanu un resursu sadali**.

Incidenta laikā ugunsdzēsēju brigādes uz savām sanāksmēm aicināja Norvēģijas civilās aizsardzības direktorātu (CAD), kas ir augstākā līmeņa vadība. Šī bija pirmā reize, kad tika organizētas šādas kopīgas sanāksmes. Šī pieredze tika identificēta kā efektīvs veids, kā nodot informāciju augstāka līmeņa lēmumu pieņēmējiem, neradot neskaidrības. Tomēr CAD uzskata, ka šādai iniciatīvai vajadzētu nākt no zemākā līmeņa, nevis būt augstākās vadības pieprasījumam. Šis piemērs izceļ elastības un uzticēšanās nozīmi iesaistīto organizāciju un līmeņu starpā.

---

[46] Nikel, D. (2021). Norway Landslide Insurance Bill Tops $100 Million [Press release]. Retrieved from https://www.forbes.com/sites/davidnikel/2021/01/08/norway-landslide-insurance-bill-tops-100-million/

[47] JRCC (2021). Evaluation report of the rescue operation and the emergency management under quick clay landslide at Gjerdrum. Iegūts no https://www.regjeringen.no/contentassets/52d43dc95b5b44fd80293c2b3515713b/rapport-gjerdrum-hovedredningssentralen-03-06-2021-digital-1.pdf

[48] Ibid

Turklāt persona, kurai ir lēmumu pieņemšanas pilnvaras, tika identificēta kā sadarbības koordinators ārkārtas reaģēšanā. Tas var ietaupīt daudz laika krīzes laikā.

Norvēģijas krīzes vadības struktūra zemes nogruvuma laikā darbojās ļoti labi, jo operāciju vadīja policija un gandrīz nebija nekādu konfliktu attiecībā uz lēmumu pieņemšanu un lomu skaidrību. Glābšanas operācijas dienās bija divi operāciju centri – abi atradās blakus, un viens no tiem turpināja darbību divus mēnešus pēc pirmā centra slēgšanas. Viens operāciju centrs bija vērsts uz glābšanas operācijām, otrs uz visiem pārējiem uzdevumiem, kas neietilpa tiešā glābšanas operācijā. Uzdevumi, kas tika risināti ar otrā operāciju centra palīdzību, arī bija ļoti svarīgi, tie ietekmēja iedzīvotāju dzīvību un veselību. Evakuētajā zonā bija, piemēram, saimniecības ar vairākiem simtiem dzīvnieku. Bija nepieciešami pasākumi, lai uzlabotu infrastruktūru, piemēram, ūdens apgādi un ceļus. Bija nepieciešams izvest svarīgus priekšmetus un vērtības no evakuētajām ēkām. Šī ir identificēta kā novatoriska pieeja krīzes pārvarēšanai un informācijas pārslodzes novēršanai vienā centrā. Uzdevumu klasificēšana glābšanas darbību laikā atviegloja sadarbību.

Šis gadījums atklāja, cik kritiska ir personiska un neformāla saskarsme krīzes laikā. Piemēram, pašvaldība skaidroja, ka visi ceļi pēc nogruvuma bija izpostīti, tāpēc radās problēmas ar cilvēku nogādāšanu drošā vietā. Sakārtot sabiedrisko transportu bija gandrīz neiespējami. Tāpēc atbildīgā persona sazinājās ar privātu transporta uzņēmumu un lūdza tam palīdzību.

Visi iepriekš minētie piemēri apliecina ERASMUS+ SECUREU projekta ietvaros organizēto ekspertu diskusiju secinājumus, kas uzsver, cik nozīmīgas ir starpdisciplinārās prasmes, piemēram, komunikācija, nepārtraukta mijiedarbība, sadarbība un inovatīvu lēmumu pieņemšana.

Izmantotie avoti

ASIS International Board Certification Handbook. Iegūts no https://www.asisonline.org/globalassets/certification/documents/certification-handbook_final.pdf

Andreassen, N., Borch, O. J. & Sydnes, A. K. (2020). Information sharing and emergency response coordination. *Safety Science*, 130, 104895.

Boin, A., Ekengren, M. & Rhinard, M. (2020). Hiding in plain sight: Conceptualizing the creeping crisis. *Risk, Hazards & Crisis in Public Policy*, 11 (2), 116.–138.

Climate in Norway 2100 (2017). Iegūts no https://www.miljodirektoratet.no/globalassets/publikasjoner/M741/M741.pdf

Godschalk, D. R. (2003). Urban hazard mitigation: Creating resilient cities. *Natural hazards review*, 4 (3), 136.–143.

JRCC (2021). Evaluation report of the rescue operation and the emergency management under quick clay landslide at Gjerdrum. Iegūts no

https://www.regjeringen.no/contentassets/52d43dc95b5b44fd80293c2b3515713b/rapport-gjerdrum-hovedredningssentralen-03-06-2021-digital-1.pdf

Kapucu, N. & Garayev, V. (2011). Collaborative decision-making in emergency and disaster management. *International Journal of Public Administration*, 34 (6), 366.–375.

Nikel, D. (2021). Norway Landslide Insurance Bill Tops $100 Million [Press release]. Iegūts no https://www.forbes.com/sites/davidnikel/2021/01/08/norway-landslide-insurance-bill-tops-100-million/

Therrien, M. C., Beauregard, S. & Valiquette-L'Heureux, A. (2015). Iterative factors favoring collaboration for interorganizational resilience: The case of the greater Montréal transportation infrastructure. *International Journal of Disaster Risk Science*, 6, 75.–86.

United nations climate change annual report (2021). Iegūts no https://unfccc.int/sites/default/files/resource/UNFCCC_Annual_Report_2021.pdf

MĀKSLĪGAIS INTELEKTS UN BIOMETRISKĀ SEJAS IDENTIFIKĀCIJA DROŠĪBAS JOMĀ

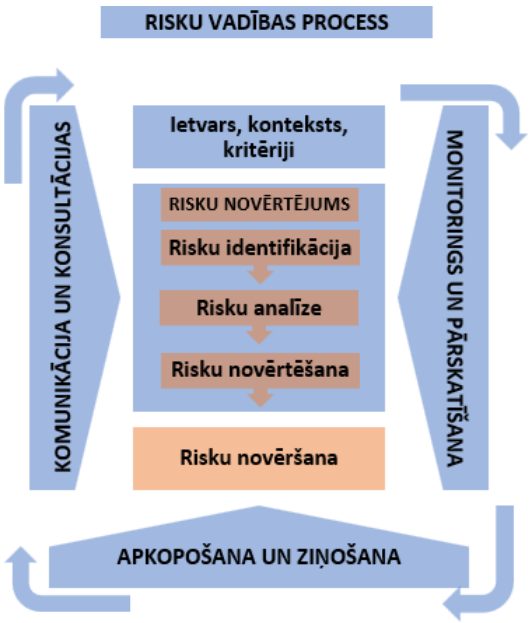
Javier Dorado / Aizsardzības un integrētās drošības skola, Spānija / 2023

KOPSAVILKUMS

Biometrisko sejas identifikācijas tehnoloģiju izmantošana valsts un privātajās iestādēs drošības nolūkos ir mūsdienu realitāte. Šī tehnoloģija palīdz noziedzīgu nodarījumu atklāšanā un novēršanā, piekļuves kontrolē, aizdomās turēto personu meklēšanā, personu identificēšanā. Tomēr šo tehnoloģiju, kas darbojas ar mākslīgo intelektu un automatizētiem lēmumiem, izmantošana rada vairākas problēmas ne tikai no likumiskās leģitimitātes un pamattiesību aizsardzības viedokļa, bet arī no darbību regulējuma viedokļa. Biometriskās identifikācijas gadījumā ir jāizvērtē gan tehniski-operatīvā, gan juridiski regulējošā dimensija, jo abas dimensijas var radīt riskus organizācijai un indivīdu fiziskajai integritātei.

Atsauce uz ISO 31000

Šajā rakstā ISO 31000 standarts risku vadības procesa ietvaros apskatītas sadaļas: Risku novērtējums; risku novēršana.



11. attēls. **Risku vadības process** (pielāgots no ISO 31000:2018[49]), rakstā apskatītās risku vadības procesa sadaļas

[49] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Uzņēmums savās telpās vēlas biometriskās identifikācijas kameras piekļuves kontroles vajadzībām. Lai šo projektu realizētu, sākumā ir nepieciešams veikt risku analīzi, kas saistīta ar biometriskās identifikācijas kameru izmantošanu. Šo uzņēmumu uztrauc iespējamās kļūmes, ko šīs tehnoloģijas varētu radīt, tādējādi apdraudot personu privātumu un drošību. Tāpat uzņēmumu uztrauc administratīvās sankcijas, kas varētu sekot datu aizsardzības pārkāpšanas gadījumos.

Kā viena no identificētajām prioritātēm ir nepieciešamība atklāt vairākas personas, kas iepriekš sodītas par zādzībām vai ielaušanos. Uzņēmuma rīcībā ir šo personu biometriskie sejas identifikācijas dati. Tomēr uzņēmumam ir bažas par kļūmju iespējamību (viltus pozitīvu vai viltus negatīvu rezultātu), kas var rasties, lietojot šīs tehnoloģijas.

Runājot par regulējumu, uzņēmumam nav skaidrs, cik lielā mērā un ar kādiem nosacījumiem tas var izmantot šo tehnoloģiju, neizraisot datu aizsardzības pārkāpumu.

GADĪJUMA IZPĒTE

Šajā gadījumā apskatītais uzņēmums ir juvelierizstrādājumu veikals, un, kā minēts iepriekš, tam ir datu bāze ar to personu sejas biometriskajiem datiem (kopā 15 personas), kuras pēdējo trīs gadu laikā ir notiesātas tieši par zādzībām vai ielaušanos juvelierizstrādājumu veikalos.

Juvelierizstrādājumu veikala vadītājs skaidro, ka biometriskās identifikācijas kamera, ja tā tiks uzstādīta, informēs tiesībsargājošās iestādes, lai tās varētu reaģēt un arestēt identificētās personas. Šīm personām ir noteikts aizliegums apmeklēt šo un līdzīgus veikalus.

Tomēr vadītājs zina, ka šāda veida tehnoloģijas dažkārt sniedz kļūdaini pozitīvu (kļūdainu identifikāciju) vai viltus negatīvu (nespēja atklāt konkrēto personu datu bāzē) rezultātu. Pirmajā gadījumā uzņēmums nevēlas radīt problēmas ar saviem klientiem, jo viltus pozitīvs rezultāts var radīt sarežģītu situāciju, kurā sistēma brīdina policiju, un tā ierodas aizturēt personu. Otrajā gadījumā, gluži pretēji, ja identifikācija neizdodas, var tikt apdraudēta darbinieku drošība un/vai uzņēmuma īpašums.

Turklāt uzņēmumam nav skaidrs, vai tas var legāli izmantot šāda veida tehnoloģijas, vai pastāv sodu un sankciju riski, kas uzņēmumam var radīt finansiālas problēmas.

Visu šo iemeslu dēļ uzņēmums vēlas veikt analīzi un lūgt ekspertam sagatavot ziņojumu gan par tehniskajiem ekspluatācijas darbības riskiem un priekšrocībām, izmantojot biometriskās identifikācijas kameras piekļuves kontroles nodrošināšanai, gan par normatīvo regulējumu un nosacījumiem, kādos šo tehnoloģiju var izmantot, nepārkāpjot datu aizsardzības noteikumus.

LABĀ PRAKSE

Tehniskās ekspluatācijas riski: a) kļūdaini pozitīvs; b) viltus negatīvs

- **Riska identificēšana**

Galvenie ekspluatācijas riski, kuri uzņēmumam ir šajā gadījumā, ir kļūdaini pozitīvi vai viltus negatīvi identifikācijas rezultāti.

- **Riska novēršana**

Uzņēmumam ir ļoti būtiski, lai attiecīgās tehnoloģijas piegādātājs informētu to par visām šādām tehniskās ekspluatācijas iespējamajām kļūmēm un programmatūras vājībām. Kad visa nepieciešamā informācija par iespējamām kļūmēm ir saņemta, ir jāievieš divpakāpju protokols, kas nodrošina to, ka netiek apturēta neviena persona, kura neatbilst pilnīgi visām pazīmēm. Šeit ir ieteicams izveidot sistēmu, kas izfiltrē aizdomīgus pozitīvus rezultātus, t.i., tos, par kuru identitāti ir šaubas.

Lietojot automatizētas biometriskās identifikācijas sistēmas, tomēr ir nepieciešama cilvēka klātbūtne un iesaiste. Ja mākslīgais intelekts nespēj atsevišķos gadījumos veikt personas identificēšanu un pieņemt atbilstoši lēmumu, cilvēka intelekts to spēj izdarīt. Šeit ir svarīgi iesaistīt darbinieku, kas ir speciāli apmācīts, lai identificētu gadījumus, kad ir jāvēršas tiesībsargājošās iestādēs reālu draudu gadījumos.

Tiesiskā regulējuma riski: Vispārīgās datu aizsardzības regulas (GDPR) sankcijas

- **Riska identificēšana**

Tiesiskā regulējuma līmenī uzņēmuma uzdevums rada vēl lielākus izaicinājumus. Pirmkārt, ir jāuzsver, ka uz uzņēmumu attiecas GDPR 9. pants, kas nosaka aizliegumu "biometrisko datu, kas paredzēti fiziskas personas unikālai identifikācijai"[50] izmantošanai. Šo aizliegumu papildina virkne izņēmumu, kas leģitimizē personas datu izmantošanu, izmantojot šīs konkrētās tehnoloģijas. Šie izņēmumi ietver: a) nepārprotamu piekrišanu; b) datu subjekta vai citas fiziskas personas būtiskas intereses; c) juridisku darbību veikšanu; d) būtiskas sabiedrības intereses.

- **Riska novēršana**

Attiecībā uz konkrēto uzņēmumu nav iespējas piemērot "nepārprotamas piekrišanas" principu. [51] Uzņēmums nevar pieprasīt katram klientam, kas ienāk veikalā, nepārprotamu, konkrētu piekrišanu datu apstrādes nolūkos. Šajā gadījumā ir arī jāizslēdz princips par būtiskajām sabiedrības interesēm, jo šajā gadījumā uzņēmums ir privātu interešu subjekts.

Savukārt pārējie divi principi (būtiskas intereses un tiesiska darbība) varētu atcelt aizliegumu apstrādāt biometriskos datus piekļuves kontroles nolūkos.

Tomēr, ņemot vērā miljoniem eiro lielos administratīvos sodus, kas varētu tikt piemēroti šādu datu nelikumīgas izmantošanas gadījumā (GDPR 83. panta 5. punkts[52]: administratīvie naudas sodi līdz EUR 20 000 000 vai uzņēmuma gadījumā summa līdz 4 % no iepriekšējā finanšu gada kopējā gada globālā apgrozījuma), vispirms ir ieteicams konsultēties ar nacionālo datu aizsardzības aģentūru vai centru. Pirms šādām konsultācijām uzņēmumam nav ieteicams izmantot šīs tehnoloģijas, jo pamatojums, kas var attaisnot šo tehnoloģiju izmantošanu, var nebūt pietiekams un juridiski pamatots.

---

[50] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1.–88. lpp.). Iegūts no https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32016R0679&from=LV, 9. pants

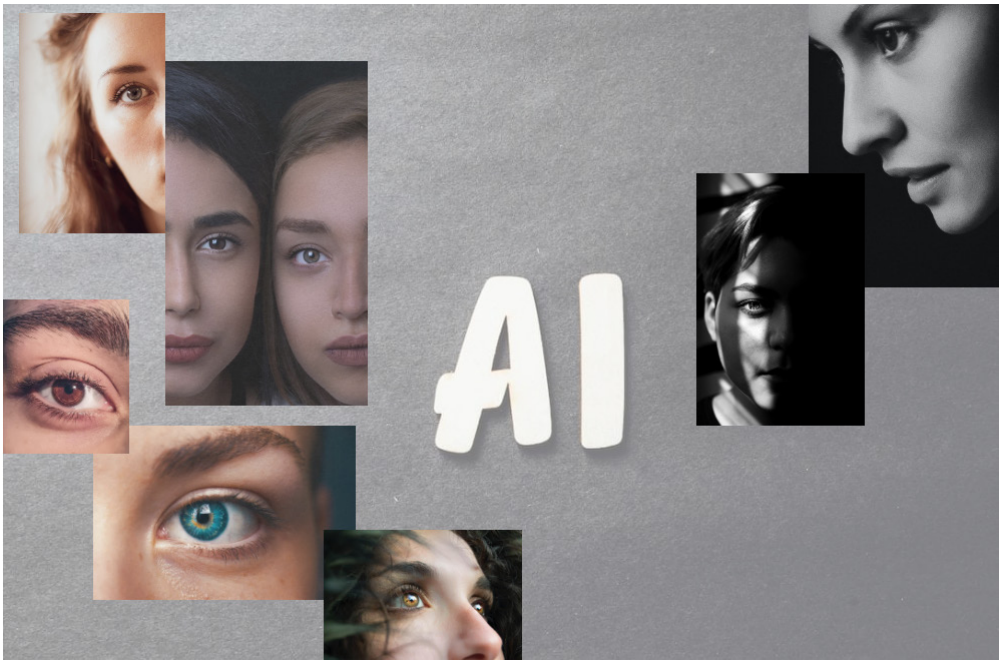
[51] Turpat, 7. pants

[52] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1.–88. lpp.). Iegūts no https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32016R0679&from=LV

Izmantotie avoti

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1.–88. lpp.). Iegūts no https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32016R0679&from=LV



PAŠNĀVĪBU NOVĒRŠANA UZ DZELZCEĻA

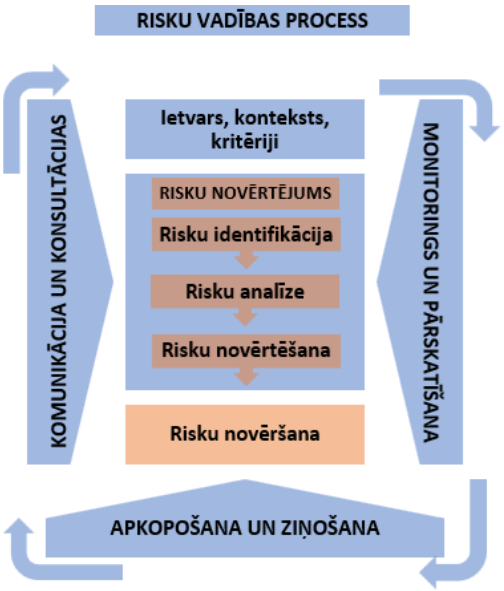
Elisabet Garcia Rull / Aizsardzības un integrētās drošības skola, Spānija / 2024

KOPSAVILKUMS

Pašnāvība ir definēta kā nāve, ko izraisa kaitējums sev ar nolūku mirt. Saskaņā ar Pasaules Veselības organizācijas (PVO) datiem viens no 100 nāves gadījumiem ir pašnāvība. Pašnāvības tiek atzītas par nopietnu sabiedrības veselības problēmu. Saskaņā ar PVO datiem "vairāk nekā 700 000 cilvēku katru gadu mirst no pašnāvībām. Turklāt katrai pašnāvībai ir vairāk nekā 20 pašnāvības mēģinājumi"[53]. Pašnāvības ir novēršamas. Cilvēki bieži izdara pašnāvības, izmantojot dzelzceļa tīklus visā Eiropā, tādējādi radot arī transporta problēmas un apdraudējumu pasažieriem. Tāpēc ļoti būtiski ir novērst visus iespējamos riskus un iespējas, lai pašnāvību izdarīšana, izmantojot dzelzceļu, nebūtu iespējama. Tas prasa visu iesaistīto privāto un sabiedrisko organizāciju un institūciju sadarbību. Šajā rakstā mēs, izmantojot PVO un ekspertu vadlīnijas un ISO 31000 standartu, izveidosim vispārīgu profilakses rokasgrāmatu kā pamatu drošības riska pārvaldībai šajā jomā.

Atsauce uz ISO 31000

Šajā rakstā ISO 31000 standarts risku vadības procesa ietvaros apskatītas sadaļas: Risku novērtējums; risku novēršana, kā arī sniegta atsauce uz standarta risku vadības ietvaru.



12. attēls. **Risku vadības process** (pielāgots no ISO 31000:2018[54]), rakstā apskatītās risku vadības procesa sadaļas

[53] World Health Organization. One in 100 deaths is by suicide. World Health Organization. Guidance to help the world reach the target of reducing suicide rate by 1/3 by 2030. Iegūts no https://www.who.int/news/item/17-06-2021-one-in-100-deaths-is-by-suicide

[54] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

15–29 gadus vecu jauniešu vidū pašnāvības ir bijis ceturtais galvenais nāves cēlonis pēc ceļu satiksmes negadījumiem, tuberkulozes un savstarpējās vardarbības. Katalonijā jauniešiem ir samazinājies vidējais vecums pirmajā pašnāvnieciskās uzvedības epizodē.[55]

Saskaņā ar PVO datiem vīrieši vairāk nekā divas reizes mirst, izdarot pašnāvības, nekā sievietes.[56]

Gadu desmitiem gan dažādas institūcijas, gan mediji ir noklusējuši pašnāvību problēmu. Tomēr mūsdienās pašnāvības tiek atzītas par sabiedrības un pasaules mēroga veselības problēmu. PVO un eksperti atzīst, ka šie nāves gadījumi ir novēršami.

Daudzi pašnāvības mēģinājumi un arī izdarītie pašnāvību gadījumi notiek tieši uz dzelzceļiem visā Eiropā un pasaulē.[57]

Neskatoties uz to, trūkst datu par pašnāvības mēģinājumiem Spānijas dzelzceļā, statistikas par šiem gadījumiem nav vispār.

GADĪJUMA IZPĒTE

Pašnāvību cēloņi ir dažādi un bieži saistīti ar garīgās veselības problēmām, taču tie joprojām ir neskaidri. Riska faktori tiek klasificēti sistēmiskajos un sociālajos, kopienas, attiecību faktoros un indivīdos.

Riska faktori ir garīgi traucējumi, īpaši depresija; personības traucējumi; atkarību izraisoša uzvedība; vardarbība ģimenē, tostarp fiziska vai seksuāla vardarbība; sociāla dislokācija vai vientulība; nesena atbrīvošana no cietuma vai ieslodzījuma; stresu izraisoši dzīves notikumi un hroniskas sāpes; tieša vai netieša pakļaušana citu personu pašnāvnieciskai uzvedībai; iepriekšējie pašnāvības mēģinājumi.

Mūsdienās pašnāvības joprojām ir sociāli stigmatizētas. Pašnāvību skaits uz dzelzceļiem nav skaidrs statistikas trūkuma dēļ, taču tas pastāv.

Sekas ir ļoti dažādas:

- cilvēka dzīvības zaudējums;
- nopietnas traumas pašnāvības mēģinājumā;
- pašnāvība atstāj smagas mentālas sekas un sēras pašnāvnieka tuviniekiem;
- traumēti var tikt aculiecinieki un visi tie, kas tieši vai netieši saistīti ar pašnāvību: no vilciena mašīnista līdz dispečeram un personālam, kas iesaistīts apkopē un uzkopšanā pēc notikuma.

Arī ekonomiski pašnāvības valstij ir negatīvas: mirušais vairs nestrādā; tiek radītas apbedīšanas izmaksas, ko bieži vien jāsedz valstij; iespējamā valsts iestāžu atbildība; pašnāvnieka tuvumā esošajiem var būt nepieciešama medicīniskā palīdzība, tie var kļūt darba nespējīgi; ja cilvēks ir bijis apgādnieks, valstij būs jāpiedāvā ģimenei arī ekonomiska palīdzība, piemēram, bāreņa pensijas;

[55] Health Department of Catalonia. Suicide prevention plan in Catalonia 2021–2025. Iegūts no https://scientiasalut.gencat.cat/handle/11351/6319

[56] World Health Organization. One in 100 deaths is by suicide. World Health Organization. Guidance to help the world reach the target of reducing suicide rate by 1/3 by 2030. Iegūts no https://www.who.int/news/item/17-06-2021-one-in-100-deaths-is-by-suicide

[57] U.S. DOT Volpe Center. Rail Suicide Prevention Resource Page. Last updated: Thursday, March 23, 2023. Iegūts no https://www.volpe.dot.gov/rail-suicide-prevention

iesaistītie darbinieki arī var ciest, un viņiem var būt nepieciešama medicīniskā palīdzība, un tie pat var aiziet no darba.

Ja pašnāvība tiek izdarīta uz dzelzceļa, tā rada nopietnu kavēšanos uz dzelzceļa līnijām. Dažiem darbiniekiem var būt nepieciešams psiholoģisks atbalsts, viņi var pat aiziet no darba pēc šādiem notikumiem.[58]

Tāpēc pašnāvības ir jānovērš, lai aizsargātu cilvēku dzīvību un veselību, kā arī ekonomisku iemeslu dēļ.

LABĀ PRAKSE

PVO uzsver, ka pašnāvību prevencijā svarīga ir situācijas analīze, daudznozaru sadarbība, izpratnes veidošana, reaģēšanas spēju stiprināšana, finansēšana, arī uzraudzība un novērtēšana.[59]

Risku novērtēšana

Risku novērtējuma grupas saraksts:

- organizācijas vadītājs;
- atbildīgais organizācijā par pašnāvību novēršanu;
- par organizāciju atbildīgie mediji;
- vilciena vadītāju pārstāvis;
- vilcienu dispečeru pārstāvis;
- pieredzes bagāts darbinieks (dzīves pieredze);
- psihologs;
- psihiatrs[60];

Izstrādājot profilakses plānu, ir jāuzklausa un jānovērtē to cilvēku viedokļi, kuriem ir plaša pieredze ar pašnāvību gadījumiem. Šos cilvēkus arī mēdz dēvēt par izdzīvojušajiem vai tuvinieku zaudējušajiem pašnāvībā.

Jo mazāk būs atstātas iespējas uz dzelzceļa, kur pašnāvību mēģinājumi var tikt veikti, jo mazāks būs pašnāvību risks.

Risku identifikācija

Risku novērtēšana sākas ar risku identifikāciju. Identifikāciju jāveic, analizējot gan psihosociālos aspektus, gan tehniskos aspektus.

No psihosociālā aspekta:

- Kur personai ir lielāka iespēja izdarīt pašnāvību?
- Kuram ir lielāka iespēja izdarīt pašnāvību? Vai tie ir vīrieši vai sievietes?
- Vai pastāv kaut kādas vecuma robežas vai izteikts vecuma nogrieznis?
- Vai pašnāvnieciskā persona ir bijusi narkotiku reibumā?
- Vai ir bijuši iepriekšējie pašnāvības mēģinājumi?

---

58 U.S. DOT Volpe Center. Rail Suicide Prevention Resource Page. Last updated: Thursday, March 23, 2023. Iegūts no https://www.volpe.dot.gov/rail-suicide-prevention

59 World Health Organization. One in 100 deaths is by suicide. World Health Organization. Guidance to help the world reach the target of reducing suicide rate by 1/3 by 2030. Iegūts no https://www.who.int/news/item/17-06-2021-one-in-100-deaths-is-by-suicide

60 Cristino Sanchez, I. (2023). Psychosocial risk factors and their impact on reliability. Psychosociological study of the train dispatcher position. Unpublished final Degree Thesis, School of Prevention and Integral Safety and Security

- Kad tas visticamāk notiks? Vai ir noteikti mēneši/datumi gadā, kad ir vairāk pašnāvību?
- Kāda ir cilvēku, kuri gatavojas izdarīt pašnāvību, tipiskā uzvedība? Novērojumu izdarīšana par divām grupām: tie, kuri dodas tieši uz pašnāvības izdarīšanas vietu, un tie, kuri pavada laiku un vilcinās pirms mēģinājuma.[61]

No tehniskā aspekta:

- Kur notiek pašnāvības un pašnāvības mēģinājumi: jānosaka, kur ir notikušas pašnāvības un pašnāvības mēģinājumi un kur pastāv liela iespējamība, ka tie notiks. Te ir jāapzinās, ka dzelzceļam ir sava specifiska. Piemēram, gadījumi metro būs pilnīgi savādāki nekā dzelzceļā. Riska kontrole ir noteikt, kuri ir melnie punkti, piemēram, stacijas pie slimnīcām, citas vietas, kur cilvēks var izdarīt pašnāvību.
- Vietu identifikācija novērošanai, kur cilvēks var izdarīt pašnāvību. Tehnoloģiju identifikācija (jaunas tehnoloģijas, piemēram, droni).[62]

Organizācija apkopo visu nepieciešamo informāciju, ievācot to no visiem novērtējuma grupas dalībniekiem, no datu ierakstiem un videonovērošanas, sadarbojoties ar valsts iestādēm. Noteikti ir jāievieš sistēma, kas garantē pašnāvību izdarījušo cilvēku anonīmo identitāti.

Pašnāvības parasti notiek krīzes vai saasinājuma laikā. Ja persona, kura gatavojas izdarīt pašnāvību, uzskatīs, ka tas nav iespējams vai ir grūti, tad ir daudz lielāka iespēja, ka pašnāvības mēģinājums notiks izdarīts saasinājuma vai krīzes laikā. Bieži vien cilvēks atrodas narkotiku un/vai alkohola ietekmē, tāpēc saasinājums vai krīze, iespējams, beigsies pēc apreibinošo vielu iedarbības izbeigšanās.[63]

Pašnāvību novēršana uz dzelzceļa

Atturēšana no mēģinājuma:

- visās stacijās jābūt atbilstošam apgaismojumam, labiekārtotām telpām ar mūziku un sociālajām aktivitātēm;
- apgaismojums dzelzceļa līnijās, lai atturētu no iebraukšanas pašnāvību mēģinājumiem;
- attīrītas līnijas un apkārtne, lai nepieļautu nepārredzamas vietas un slēptuves, kas vilcienu vadītājiem dotu iespēju pārredzēt apkārtni no liela attāluma, un viņi varētu samazināt ātrumu vai apstāties.

Pašnāvību ietekmes novēršana

Līdzekļi, lai novērstu piekļuvi sliedēm.

Fiziskais šķērslis: organizācijai ir jāizvērtē, vai pastāv fiziski šķēršļi, kas neļautu personai mēģināt izdarīt pašnāvību, kā arī jāizsver metodes risku mazināšanai. Ja ir fiziskas barjeras, vai tās ir efektīvas? Ja nē, vai šīs vietas ir viegli pieejamas iedzīvotājiem? Vai ir iespējams pievienot/uzlabot fiziskās barjeras? Ja tas nav iespējams (piemēram, ja platība ir pārāk liela), organizācijai ir jānovērš piekļuve ar citiem līdzekļiem, piemēram:

- visās dzelzceļa līniju stacijās, kurām garām brauc ātrvilcieni, ir jāuzstāda vismaz daļējas fiziskas barjeras;

[61] Cristino Sanchez, I. (2023). Psychosocial risk factors and their impact on reliability. Psychosociological study of the train dispatcher position. Unpublished final Degree Thesis, School of Prevention and Integral Safety and Security

[62] National Institute of Mental Health. NIH Publication No. 23-MH-6389. (2023). Frequently Asked Questions About Suicide. Iegūts no https://www.nimh.nih.gov/health/publications/suicide-faq

[63] Hallewell, M.J., Ryan, B., Hughes, N., Coad, N. (2023). Conceptualising innovative lighting interventions for suicide, trespass and risky behaviour on the railway. *Lighting Res. Technol*. 2023; 55: 79–99

- veģetācija;
- cilvēku detektori;
- zonu pārkāpšanas uzraudzība.

Pašnāvību traumu novēršana

Jaunajās dzelzceļa stacijās ierīkojot pret-pašnāvību bedres un atbilstoši budžeta līdzekļiem ierīkot tās esošajās stacijās, kur notiek vairāk pašnāvību un nelaimes gadījumu.[64]

Psiholoģiskās pieejas profilakse risku novēršanā

Mērķēta profilakse attiecībā uz cilvēku, kas vēlas izdarīt pašnāvību

Šāda veida profilaksi veic sabiedrības veselības sistēma, ievērojot PVO vadlīnijas. Tomēr arī dzelzceļš var veikt virkni profilaktisko darbību:

- nodrošināt informatīvās zīmes ar informāciju par palīdzību cilvēkiem, kam ir krīzes situācijas vai pašnāvnieciskas tieksmes, saskaņojot to ar reģionālo veselības departamentu;
- mēnešos/datumos, kuros ir visaugstākais pašnāvību skaits, veikt aktīvas informēšanas kampaņas;
- iepriekš izdarīts pašnāvības mēģinājums liecina par to, ka pastāv ļoti augsts riska faktors, ka cilvēks mēģinās to veikt vēlreiz. Tādēļ veselības dienestiem jāveic atbilstošu pašnāvības mēģinājumu veicēju veselības uzraudzību piecu gadu laikā pēc pašnāvības mēģinājuma.

Trešo personu profilakse

- **Darbinieki**

Organizācijai ir jāapmāca viss personāls, kas saskaras ar pasažieriem, lai atpazītu cilvēkus, kam ir dzīves krīze. Darbiniekiem ir svarīgi atpazīt šādas personas un sazināties ar neatliekamās palīdzības dienestiem, ja viņi atpazīst personu, kas atrodas briesmās un, iespējams, domā par pašnāvību.

Organizācijai jāapmāca un jānodrošinās ar personālu, kas specializējas dzīves krīžu atpazīšanā un komforta nodrošināšanā līdz neatliekamās palīdzības dienesta ierašanās brīdim. Apmācībās noteikti ir jāiekļauj cilvēki ar lielu dzīves pieredzi.

- **Radinieki un draugi**

Organizācijai ir jāatver tālruņa numuru vai jāizveido e-pastu, lai radinieki un draugi varētu sazināties un ziņot par iespējamiem gadījumiem un personām, kas varētu mēģināt izdarīt pašnāvību uz dzelzceļa.

- **Pasažieri un citi sabiedrības locekļi**

Gan pasažieri, gan citi cilvēki var palīdzēt novērst pašnāvību. Pašnāvību un krīžu dzīves līnija (Spānijā numurs 024, līnija izveidota 2022. gadā) būs noderīga arī ikvienam, lai informētu par personu, kas grasās izdarīt pašnāvību un saņemtu tūlītēju un ātru palīdzību. Cilvēki var arī informēt jebkuru dzelzceļa darbinieku, kurš:

- nekavējoties sazināsies ar neatliekamās palīdzības dienestu;
- nekavējoties sazināsies ar iekšējo pašnāvību novēršanas uzticības tālruni;
- ja nepieciešams, lai aizsargātu personu, aizkavēs to, tādējādi nodrošinot tās drošību.

[64] Health Department of Catalonia. Suicide prevention plan in Catalonia 2021–2025. Iegūts no https://scientiasalut.gencat.cat/handle/11351/6319

Organizācijai jānodrošina arī drošības poga, lai apturētu vilcienu, ja kāds jau atrodas uz sliežu ceļa. Pogu var nospiest ikviens.

Mediju komunikācija

Veselības ministrija un Satiksmes ministrija ik gadu publiskā ziņojumā koordinēti informē sabiedrību par notikušo pašnāvību un pašnāvību mēģinājumu skaitu, tādējādi uzsverot to kā sabiedrības veselības problēmu. Koordinētajā ziņojumā ir jāiekļauj informācija par noderīgiem resursiem un vēstījums par iespējām uz atveseļošanos.

Par katru pašnāvības gadījumu komunikācija ir jāveic saskaņā ar atbilstošajām vadlīnijām, kas paredz, kā korekti ziņot par šādiem gadījumiem.

Finansējums: profilakses plānam ir jābūt labi finansētam, iespējams, no dažādiem budžetiem.

Katrā vilciena/metro stacijā būtu jāatrodas pašnāvību novēršanas darbiniekam, kurš ir īpaši apmācīts un atbild par protokola ieviešanu un uzraudzību.

Riska pārvaldības procesa efektivitātei nepieciešama pilnīga koordinācija starp veselības un transporta departamentiem / ministrijām.

Visbeidzot, riska pārvaldības procesa efektivitāte ir nepārtraukti jāuzrauga un profilakses plāns ir regulāri jāpārskata. To uzsver arī ISO31000 standartā definētais risku vadības ietvars.

13. attēls. **Risku vadības ietvars** (no ISO 31000:2018[65]).

[65] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Izmantotie avoti

World Health Organization. One in 100 deaths is by suicide. World Health Organization. Guidance to help the world reach the target of reducing suicide rate by 1/3 by 2030. Iegūts no https://www.who.int/news/item/17-06-2021-one-in-100-deaths-is-by-suicide

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Health Department of Catalonia. Suicide prevention plan in Catalonia 2021–2025. Iegūts no https://scientiasalut.gencat.cat/handle/11351/6319

U.S. DOT Volpe Center. Rail Suicide Prevention Resource Page. Last updated: Thursday, March 23, 2023. Iegūts no https://www.volpe.dot.gov/rail-suicide-prevention

Cristino Sanchez, I. (2023). Psychosocial risk factors and their impact on reliability. Psychosociological study of the train dispatcher position. Unpublished final Degree Thesis, School of Prevention and Integral Safety and Security

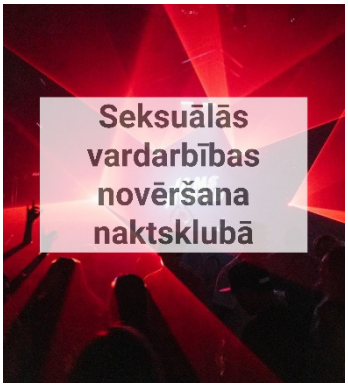
National Institute of Mental Health. NIH Publication No. 23-MH-6389. (2023). Frequently Asked Questions About Suicide. Iegūts no https://www.nimh.nih.gov/health/publications/suicide-faq

Hallewell, M.J., Ryan, B., Hughes, N., Coad, N. (2023). Conceptualising innovative lighting interventions for suicide, trespass and risky behaviour on the railway. *Lighting Res. Technol*. 2023; 55: 79.–99.

SEKSUĀLĀS VARDARBĪBAS NOVĒRŠANA NAKTSKLUBĀ

Elisabet Garcia Rull / Aizsardzības un integrētās drošības skola, Spānija / 2023

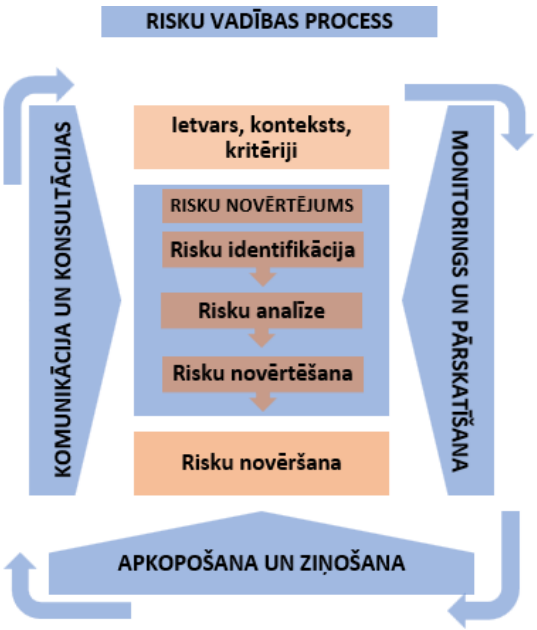
KOPSAVILKUMS



Risku novērtējums saistībā ar aizliegtām seksuāla rakstura darbībām, piemēram, seksuālu uzmākšanos, seksuālu agresiju un izvarošanu lielos pasākumos, piemēram, naktsklubos vai mūzikas festivālos, ietver ne tikai privāto drošību, bet arī sabiedrisko drošību. Šajā rakstā ir aplūkota paraugprakse drošības uzlabošanai un seksuālās vardarbības mazināšanai naktsklubā. Ir svarīgi pielāgot riska novērtējumu atbilstoši ISO 31000 standartu konkrētajam attiecīgajā jomā atbilstošajam likumam. Raksta pamatā ir Katalonijas valdības protokoli sasaistē ar akciju "MĒS NEKLUSĒSIM"[66] un "Drošības protokols pret seksuālu vardarbību atpūtas vietās"[67].

Atsauce uz ISO 31000

Šajā rakstā ISO 31000 standarts risku vadības procesa ietvaros apskatītas sadaļas: ietvars, konteksts, kritēriji; risku novērtējums; risku novēršana.



14. attēls. **Risku vadības process** (pielāgots no ISO 31000:2018[68]), rakstā apskatītās risku vadības procesa sadaļas

[66] Barcelona Hall Town. Protocol "We won't keep quiet" campaign against sexual assault and harassment in private nighttime leisure venues. Iegūts no https://ajuntament.barcelona.cat/dones/sites/default/files/documents/protocol_oci_nocturn_eng_0.pdf

[67] Government of Catalonia. Department of Interior. Security Protocol against sexual violence in leisure spaces. Iegūts no https://interior.gencat.cat/web/.content/home/030_arees_dactuacio/seguretat/violencia_masclista_i_domestica/Protocol_seguretat_violencies_sexuals/protocol/ES_PSCVSEO-2019.pdf

[68] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Statistika liecina, ka naktsklubi, festivāli un citas lielas pulcēšanās vietas, kur ir izplatīta alkohola un narkotisko vielu lietošana, ir tās vietas, kur notiek aizliegtas seksuālās aktivitātes, piemēram, uzmākšanās, seksuāla agresija un izvarošana. Pēdējos gados ir bijuši arī aizliegtu ķīmisko vielu lietošanas gadījumi. Pasaules Veselības organizācija (PVO) seksuālu vardarbību definē: "Jebkura seksuāla darbība, mēģinājums veikt seksuālu darbību, nevēlami seksuāli komentāri vai darbības, kas vērstas uz cilvēku tirdzniecību vai citādi vērstas pret personas seksualitāti, izmantojot piespiešanu, ko veic jebkura persona neatkarīgi no tās attiecībām ar upuri jebkurā vidē, tostarp, bet ne tikai mājās un darbā."[69]

Lielākajā daļā gadījumu iespējamais upuris ir sieviete un iespējamais vainīgais ir vīrietis. Tāpēc dzimumu līdztiesības perspektīva ir būtiska. Organizācijas tūlītējai, ātrai un efektīvai rīcībai var būt izšķiroša nozīme krimināltiesību procesā, lai ātri atrastu iespējamo vainīgo.

Profilakse ir būtiska, lai aizsargātu personas, izvairītos no reputācijas un ekonomiska kaitējuma uzņēmumam/organizācijai, kā arī izvairītos no krimināltatbildības, administratīvās un civiltiesiskās atbildības uzņēmumam/organizācijai.

Prevencijas protokols attiecas uz visa veida darbībām, kas saistītas ar seksuālu vardarbību, neatkarīgi no tā, vai tās ir vai nav noziedzīgs nodarījums.

GADĪJUMA IZPĒTE

Vietējais naktsklubu uzņēmums, kas atrodas Barselonas provincē, pieprasa vispārēju riska novērtējumu attiecībā uz aizliegtām seksuāla rakstura darbībām, piemēram, uzmākšanos, seksuālu vardarbību, seksuālu agresiju utt. Balstoties viņu pieredzē, šādas aizliegtas darbības pēdējā laikā ir palielinājušās, it īpaši naktskluba tualetēs. Tas naktsklubiem rada sliktu reputāciju plašsaziņas līdzekļos, un tiem draud administratīvā tiesvedība. Šo incidentu rezultātā naktsklubs ir zaudējis savas klientes – sievietes, un tas atstāj negatīvu ekonomisko ietekmi. Sievietēm naktsklubos ir bezmaksas ieejas politika, bet vīriešiem – maksas ieeja. Uzņēmuma klientu vidējais vecums ir no 18 līdz 25 gadiem. Klubs parasti ir atvērts katru piektdienu un sestdienu no 00.00 līdz 6.00.

Naktsklubs lūdz speciālistam veikt kompleksu novērtējumu, kur uzbrucēji ir vīrieši, lai mazinātu aizliegtās darbības tā telpā un uzlabotu sabiedrisko tēlu.

LABĀ PRAKSE

Ietvars, konteksts, kritēriji

Labā prakse ietver profilaksi un efektīvu un iedarbīgu reakciju pret seksuālo noziegumu gadījumiem, kam arī būs izšķiroša nozīme nevēlamu notikumu novēršanā nākotnē.

Profilaksei **konteksts** ir naktsklubs ar gados jauniem klientiem un darbiniekiem, vidēji līdz 25 gadiem. Klienti mēdz būt arī alkohola un narkotisko vielu reibumā.

Tieši aizskartā persona var būt gan indivīds, gan grupa. Noziedzīgie nodarījumi ietekmē personas veselību/dzīvību, emocionālo veselību. No uzņēmuma viedokļa ietekme rodas uz uzņēmuma finansēm un reputāciju. Riska izcelsmi nevar paredzēt, jo pētījumi liecina, ka ir iesaistīti daudzi faktori.

[69] World Health Organization (2021). Sexual violence. Iegūts no https://apps.who.int/violence-info/sexual-violence/

Identificējot riskus, jāapskata dažādi aspekti, tai skaitā iepriekšējo gadījumu saraksts. Uzņēmumam jāsazinās ar tiesībsargājošām iestādēm, lai apkopotu informāciju un pārbaudītu ierakstus. Balstoties uz iegūto informāciju, speciālistam jāmēģina izveidot cietušā un likumpārkāpēja profilu un jāizvērtē, vai narkotiskās vielas un alkohols nepalielina riska iespējamību. Arī dzimumu līdztiesības politikas trūkums var būt aspekts, kas jāņem vērā.

Savākto informāciju var izmantot, lai izpētītu iespējas, īpaši, ja ir noteiktas zonas, kur gadījumu ir vairāk, piemēram, tualetes. Tāpēc aktuāli ir pārbaudīt, vai nav iespējas, ko rada dažādas naktskluba telpas vai "melnie punkti". Speciālists pamanīs, ka tualetēs nav kameru, lai tādējādi ievērotu klientu privātumu, un tas var radīt iespējas uzbrucējiem.

Risku novērtējums un analīze

Riska analīze beidzas ar nevēlamā notikuma varbūtību, seku raksturu un apmēru izvērtējumu. Analīzē arī vērtē, vai pastāv kontroles sistēmas un prakses, vai tās ir efektīvas, kā arī to, kāds ir šo metožu uzticamības un precizitātes līmenis. Riska novērtējuma mērķis ir pēc iespējas samazināt nevēlamos noziegumus naktsklubā.

Tas būs pamats, uz kuru risku pārvaldība darbosies atbilstoši attiecīgā reģiona likumiem un protokoliem, kurā atrodas naktsklubs. Šajā gadījumā galvenokārt jāpiemēro Spānijas konstitūcija[70], Katalonijas autonomijas statūti[71], 6. septembra Pamatlikums 10/2022 par visaptverošu seksuālās brīvības garantiju[72], 4. aprīļa likums Nr. 5/2014 par privāto drošību[73], Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar kuru atceļ Direktīvu nr. 95/46/EK (Vispārīgā datu aizsardzības regula)[74], "Drošības protokols pret seksuālu vardarbību atpūtas telpās"[75].

Piemērojamie tiesību akti mainās katrā valstī, izņemot Vispārīgo datu aizsardzības regulu. Organizācijai ir jāizpēta specifiskie tiesību akti, kas attiecas uz tās konkrēto valsti.

Risku novēršana

Pēc risku novērtējuma veikšanas nākamais solis ir risku novēršana.

Preventīvās darbības

- Lai samazinātu risku, naktsklubam ir **jāveido droša vide:**
    - tualetes ir jāpadara par drošāku vietu, veicot nepieciešamās arhitektoniskās izmaiņas un uzstādot kameras, kas var viegli atpazīt cilvēkus, kas ieiet un iziet no tualetēm;
    - jāizvairās vai jālikvidē zonas (tumšas, paslēptas, nepārredzamas), kurās klienti var tikt pakļauti briesmām. Un, ja nav iespējams pilnībā izskaust šādas zonas, tad tajās jāizmanto videonovērošana.

[70] Spanish Constitution. *State official newsletter*, 311 of 29.12.1978., 29313.–29424. Iegūts no https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229; https://www.boe.es/eli/es/l/2014/04/04/5/con

[71] Organic Law 6/2006, of the 19th of July, Autonomy Statute of Catalonia. *State official newsletter*, 172 of 20.07.2006., 27269 a 27310. Iegūts no https://www.boe.es/eli/es/lo/2006/07/19/6/con

[72] Organic Law 10/2022, of the 6th of September, on the comprehensive guarantee of sexual freedom. *State official newsletter*, 215, of 7.9.2022., 124199 to 124269. Iegūts no https://www.boe.es/eli/es/lo/2022/09/06/10/con

[73] Law 5/2014, of the 4th of Abril, of Private Security. *State official newsletter*, 83 of 5.4.2014., 28975 to 29024

[74] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

[75] Government of Catalonia. Department of Interior. Security Protocol against sexual violence in leisure spaces. Iegūts no https://interior.gencat.cat/web/.content/home/030_arees_dactuacio/seguretat/violencia_masclista_i_domestica/Protocol_seguretat_violencies_sexuals/protocol/ES_PSCVSEO-2019.pdf

Par videonovērošanu kā preventīvu metodi, ievērojot likumus, ir skaidri jāinformē klienti, izmantojot informatīvos plakātus un plāksnes.

- Lai veidotu drošāku vidi, naktsklubam ir jāizveido un jāievēro **dzimumu līdztiesības politika.**

Pret lietotājiem:

- ieejas noteikumi, kas paredz iekasēt vienādu ieejas maksu vīriešiem un sievietēm;
- nediskriminējošu attieksmi pret klientu apģērbu vai izskatu;
- ierobežojumus iekļūt klubā tiem, kas izsaka nepiedienīgas piezīmes vai seksuāli uzmācas, piemēram, gaidot ieeju naktsklubā;
- tādu darbību aizliegšana, kas veicina diskrimināciju dzimuma vai seksuālās daudzveidības dēļ.

Pret darbiniekiem:

- cienīgs un nediskriminējošs ģērbšanās kods darbiniekiem.

- **Kontaktpunkta izveide klubā,** kur ziņot par jebkuru seksuālas vardarbības aktu, *WhatsApp* tālruņa numura un e-pasta adreses izveide, ko lietotāji var izmantot, lai ziņotu par seksuālas vardarbības situācijām. Ieteicams izvietot plakātus ar šo informāciju.
- Katru vakaru naktsklubā vajadzētu atrasties personai, kas tiek nozīmēta kā **atbildīgā kontaktpersona,** kura ir atbildīga par seksuālās vardarbības novēršanu, atklāšanu un reaģēšanu uz šādām situācijām. Taču tas neizslēdz faktu, ka šādu gadījumu novēršana ir arī visa personāla vispārējā atbildība.
- Ļoti nozīmīga ir arī **alkohola un narkotisko vielu kontrole klubā.** Naktsklubs var atteikties pārdot alkoholiskos dzērienus klientam, kuram ir augsts alkohola vai narkotisko vielu līmenis.
- Jāveic arī atbilstoša **īpaša apmācība** naktsklubu darbiniekiem, jo īpaši drošības darbiniekiem, lai nodrošinātu viņus ar prasmēm novērst, atklāt un reaģēt uz jebkādu seksuālas vardarbības gadījumu, kā arī saskaņot darbību ar policiju.
- Uz sienas ir jāizvieto **informācija,** kas izskaidro kluba noteikumus. Var izveidot īpašo, tā dēvēto "purpurkrāsas punktu", kur uzstādītās kameras un kas kalpo kā demonstratīva zona pilnīgai jebkāda veida seksuālās vardarbības noliegšanai naktsklubā.

Reaktīvie un iejaukšanās pasākumi

Profilakse ir saistīta ar pareizu atklāšanu un reaģēšanu incidenta gadījumā, jo naktsklubs tādējādi demonstrē savu politiku nepieņemt aizliegtas darbības savās telpās un rada preventīvu efektu, kas pozitīvi ietekmē tā tēlu. Laba reakcijas un iejaukšanās prakse ir būtiska, lai izvairītos no sekundāras viktimizācijas.

Darbiniekiem incidentu gadījumos ir operatīvi jāmeklē iespējamie liecinieki un jāfiksē konkrētais laika periods, lai pārbaudītu novērošanas kameru fiksētos attēlus.

Naktsklubam ir jāveido divas atsevišķas apsargātas zonas – iespējamajam upurim un aizdomās turētajai personai vai personām.

1. Darbības saistībā ar iespējamo upuri:

- darbinieks tiekas ar iespējamo upuri, piedāvā viņam drošu gaidīšanas vietu un jautā, vai iespējamajam upurim ir kāda droša kontaktpersona, kas viņu var pavadīt;
- par lietu atbildīgais darbinieks sniedz iespējamajam cietušajam rakstisku informāciju par viņa tiesībām, nododot viņam jau sagatavotu informatīvo bukletu;
- darbinieks apkopo visu informāciju saistībā ar lietas faktiem, ko cietušais var izteikt mutiski;

- darbinieks sazinās ar policiju un medicīniskajiem dienestiem, respektējot cietušā vēlmi ziņot vai neziņot par notikušo. Ja persona nevar skaidri izteikt savu vēlmi, obligāti ir jāvēršas policijā un medicīniskajā dienestā. Iespējamajam upurim ir svarīgi pēc iespējas ātrāk doties uz medicīnas iestādi, lai saņemtu emocionālu atbalstu par jebkuru uzbrukumā radīto kaitējumu un reģistrētu visus pierādījumus.

2. Darbības saistībā ar aizdomās turēto personu:
   - ja ir aizdomas par noziedzīgu nodarījumu, naktskluba apsargi identificē aizdomās turamo(-s), apkopo informāciju un aiztur viņu drošā zonā līdz policijas ierašanās brīdim. Tomēr būtiski ir veikt darbības, ievērojot nevainīguma prezumpciju. Ja ir vairāk nekā viena persona, apsargiem tie ir jānošķir;
   - apsargiem ir jānodrošina, lai iespējamais upuris un aizdomās turamais nesatiktos, kamēr neierodas policija;
   - sīkāka informācija par upuriem un iespējamajiem vainīgajiem naktskluba darbiniekiem ir konfidenciāla;
   - izmeklējot incidentu jāorganizē regulāras koordinācijas sanāksmes starp naktskluba vadītāju, iestādēm un vietējo policiju.

Vismaz reizi gadā ir jāanalizē statistika, lai uzlabotu un pielāgotu protokolu.

Risku vadības procesa efektivitāte ir nepārtraukti jāuzrauga un jāpapildina, balstoties uz jauniem, precīziem datiem, un profilakses protokols ir jāpārskata vismaz reizi gadā.

Izmantotie avoti

Barcelona Hall Town. Protocol "We won't keep quiet" campaign against sexual assault and harassment in private night-time leisure venues. Iegūts no https://ajuntament.barcelona.cat/dones/sites/default/files/documents/protocol_oci_nocturn_eng_0.pdf

Government of Catalonia. Department of Interior. Security Protocol against sexual violence in leisure spaces. Iegūts no https://interior.gencat.cat/web/.content/home/030_arees_dactuacio/seguretat/violencia_masclista_i_domestica/Protocol_seguretat_violencies_sexuals/protocol/ES_PSCVSEO-2019.pdf

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

World Health Organization (2021). Sexual violence. Iegūts no https://apps.who.int/violence-info/sexual-violence/

Spanish Constitution. *State official newsletter*, 311 of 29.12.1978., 29313.–29424. Iegūts no https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229; https://www.boe.es/eli/es/l/2014/04/04/5/con

Organic Law 6/2006, of the 19th of July, Autonomy Statute of Catalonia. *State official newsletter*, 172 of 20.07.2006., 27269 a 27310. Iegūts no https://www.boe.es/eli/es/lo/2006/07/19/6/con

Organic Law 10/2022, of the 6th of September, on the comprehensive guarantee of sexual freedom. *State official newsletter*, 215, of 7.9.2022., 124199 to 124269. Iegūts no https://www.boe.es/eli/es/lo/2022/09/06/10/con

Law 5/2014, of the 4th of Abril, of Private Security. *State official newsletter*, 83 of 5.4.2014., 28975 to 29024

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

Government of Catalonia. Department of Interior. Security Protocol against sexual violence in leisure spaces. Iegūts no https://interior.gencat.cat/web/.content/home/030_arees_dactuacio/seguretat/violencia_masclista_i_domestica/Protocol_seguretat_violencies_sexuals/protocol/ES_PSCVSEO-2019.pdf

KĀ IZSTRĀDĀT UN IEVIEST DROŠĪBAS KULTŪRU SAVĀ ORGANIZĀCIJĀ

Kārlis Apalups / Biznesa augstskola *Turība*, Latvija / 2023

KOPSAVILKUMS

Drošības kultūras attīstība organizācijā var būt izaicinājums, taču ir daži panākumu soļi, kas jāņem vērā, kad tiek pieņemts lēmums attīstīt drošības kultūru. Šādam lēmumam būtu jānāk no augstākās vadības, jo bez šādas iniciatīvas nevar notikt būtiska organizatoriskās kultūras attīstība. Tāpat ir svarīgi izveidot skaidras un konsekventas drošības politikas, lai tās tiktu ievērotas kā standarts visā organizācijā. Kad vadības atbalsts ir iegūts un politikas ir ieviestas, nākamajam solim vajadzētu būt organizācijas apmācībai par drošības politikām un paraugpraksi. Lai tā būtu mūsdienīga kultūra, ir jāveic arī drošības kultūras uzraudzība un mērīšana, un to var panākt arī, ieviešot īpašus rādītājus, lai izmērītu drošības kultūras panākumus un efektivitāti.

Atsauce uz ISO 31000

Šajā rakstā apskatīti ISO 31000:2018 Risku pārvaldības principi: Cilvēka un kultūras faktori.

15. attēls. **Risku pārvaldības principi** (pielāgots no ISO 31000:2018[76]), rakstā apskatītās cilvēka un kultūras faktori

[76] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Drošības kultūra ir ideju, paražu un sociālās uzvedības kopums, kas ietekmē organizācijas drošību. Tas ir vissvarīgākais elements organizācijas drošības stratēģijā, jo tas ietekmē to, kā darbinieki uztver drošības draudus un incidentus un reaģē uz tiem. Spēcīga drošības kultūra var samazināt risku un ietaupīt naudu, novēršot datu aizsardzības pārkāpumus, ievērojot noteikumus un aizsargājot organizācijas reputāciju.

Tomēr drošības kultūras izveide un ieviešana nav vienkāršs uzdevums. Tam nepieciešama stratēģiska ilgtermiņa pieeja, kas ietver augstākās vadības atbalstu, skaidru un konsekventu drošības politiku, efektīvas izpratnes veidošanas un apmācības programmas, kā arī nepārtrauktu novērtēšanu un uzlabošanu.[77] Šajā rakstā apskatīsim dažas labās prakses drošības kultūras izveidei un uzturēšanai jūsu organizācijā. Rakstā arī pētīsim gadījumu ar Akciju Sabiedrību "Latvijas Finieris", kas darbojas starptautiskā vidē un kurā viena no pamatvērtībām ir drošība.

GADĪJUMA IZPĒTE

AS "Latvijas Finieris" ir vadošais saplākšņa un tā produktu ražotājs Baltijas valstīs un Somijā. Uzņēmums nodarbojas arī ar mežu apsaimniekošanu, mežizstrādi un sintētisko sveķu un fenola plēvju ražošanu.[78]

2014. gadā AS "Latvijas Finieris" piedzīvoja milzīgu ugunsgrēku vienā no Rīgā bāzētajām rūpnīcām.[79] Pēc šī notikuma akciju sabiedrība nolēma ieviest drošības kultūru un attīstīt to. Kā daļa no tās centieniem tika izveidots Drošības pārvaldības dienests (DPD), kas pārvaldīja drošības riskus tādās jomās kā ugunsdrošība, arodveselība un darba drošība, vides aizsardzība un fiziskā drošība. Pirms ugunsgrēkiem bija liels ar darbu saistītu nelaimes gadījumu skaits, kā rezultātā tika zaudēta darbspēja, apdrošināšanas izmaksas un samazinājās darbinieku drošības sajūta.

DPD centieni ļāva attīstīt tādu drošības kultūru, kas krasi samazināja ar darbu saistītos incidentus, palielināja ietaupījumus no drošības un drošības ieguldījumiem un uzlaboja vispārējo organizācijas kultūru.

LABĀ PRAKSE

Saņemt augstākās vadības atbalstu. Augstāko vadītāju atbalsta iegūšana ir pirmais solis drošības kultūras veidošanā. Ir svarīgi, lai viņi informētu visus darbiniekus par drošības un drošuma nozīmi un vērtību, piešķirtu pietiekamus resursus un budžetu drošības iniciatīvām un sauktu sevi un citus pie atbildības par drošības veiktspēju. Šis atbalsts var arī palīdzēt radīt pozitīvu toni vadībā, kur drošība tiek uzskatīta par stratēģisku prioritāti un kopīgu atbildību, nevis tikai par vēl vienu budžeta izdevumu pozīciju.

Izveidot skaidru un konsekventu drošības politiku. Drošības politika ir kā organizācijas standarts. Tās ir normas, kas nosaka darbinieku paredzamo uzvedību un rīcību attiecībā uz drošību.

[77] Building a Culture of Security – ISACA. Iegūts no https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security
[78] Latvijas Finieris. Iegūts no https://www.finieris.com/lv/par-koncernu/
[79] Latvijas Finiera rūpnīcā liels ugunsgrēks (2014). Iegūts no https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks

Politikai būtu jāaptver tādas tēmas kā piekļuves kontrole, paroļu pārvaldība, datu aizsardzība, reaģēšana uz incidentiem un atbilstības prasības. Drošības politikai jābūt saskaņotai ar organizācijas mērķiem un vērtībām, kā arī ar attiecīgajiem likumiem un noteikumiem. Tie ir arī jāraksta vienkāršā un saprotamā valodā, jāpaziņo visiem darbiniekiem un konsekventi jāizpilda.

Nodrošināt izpratni un apmācību. Izpratnes veidošanas un apmācības programmas ir būtiskas, lai izglītotu darbiniekus par drošības riskiem, ar kuriem viņi saskaras, par politiku, kas viņiem jāievēro, un par labāko praksi, kas viņiem jāpieņem. Tie būtu jāpielāgo dažādu darbinieku grupu, piemēram, IT darbinieku, vadītāju vai galalietotāju, īpašajām vajadzībām un lomām. Izpratnes veidošanas un apmācības programmas būtu regulāri jānodrošina un bieži jāatjaunina, lai neatpaliktu no mainīgās draudu vides.

Izmērīt un uzlabot drošības kultūru. Drošības kultūra nav statisks stāvoklis, bet gan dinamisks process, kas laika gaitā ir jāuzrauga un jānovērtē (tāpat kā riska pārvaldība). Ir dažādi rīki un metodes, ko var izmantot, lai novērtētu drošības kultūru, piemēram, anketas, aptaujas, intervijas vai auditi. Tie var palīdzēt novērtēt pašreizējo drošības kultūras stāvokli, noteikt stiprās un vājās puses un izsekot progresam un izmaiņām. Pamatojoties uz šo mērījumu rezultātiem, drošības kultūru var uzlabot, novēršot nepilnības, pastiprinot pozitīvu uzvedību, atalgojot labu sniegumu vai labojot sliktus ieradumus.

Iegūt drošības kultūras investīciju atdevi. Drošības kultūra ir ne tikai izmaksu centrs, bet arī organizācijas vērtību virzītājspēks. Izstrādājot un ieviešot drošības kultūru, organizācija var sasniegt dažādas priekšrocības, piemēram:

- drošības incidentu iespējamības un ietekmes samazināšana;
- klientu uzticības un lojalitātes veicināšana;
- darbinieku iesaistes un noturēšanas uzlabošana;
- darbības efektivitātes un produktivitātes paaugstināšana;
- juridisko un reglamentējošo pienākumu izpilde;
- konkurences priekšrocību iegūšana tirgū.

Lai kvantificētu šīs priekšrocības, organizācija var izmantot šādus rādītājus:

- novērsto vai atklāto drošības incidentu skaits;
- naudas summa, kas ietaupīta vai atgūta no drošības incidentiem;
- klientu apmierinātības vai noturēšanas līmenis;
- darbinieku apmierinātības vai mainības līmenis;
- laiks vai resursi, kas ietaupīti vai optimizēti ar drošības pasākumiem;
- atbilstības statuss vai audita rezultāti;
- tirgus daļa jeb ieņēmumu pieaugums.

Izmērot šos rādītājus pirms un pēc drošības kultūras programmas ieviešanas, organizācija var aprēķināt savu drošības kultūras centienu ieguldījumu atdevi (IA).

Ievērojot šo paraugpraksi, organizācija var izveidot un uzturēt spēcīgu drošības kultūru.

Izmantotie avoti

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Building a Culture of Security – ISACA. Iegūts no https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security

Developing a cyber security culture: Current practices and future directions - ScienceDirect. Iegūts no https://www.sciencedirect.com/science/article/pii/S016740482100211X

Latvijas Finieris. Iegūts no https://www.finieris.com/lv/par-koncernu/

Latvijas Finiera rūpnīcā liels ugunsgrēks (2014). Iegūts no https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks

The Importance Of A Strong Security Culture And How To Build One – Forbes Iegūts no https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/

DROŠĪBAS APMĀCĪBAS UNIVERSĀLAI DROŠĪBAS RISKU GATAVĪBAI

Kārlis Apalups / Biznesa augstskola *Turība*, Latvija / 2024

KOPSAVILKUMS

Drošības apmācības izstrāde vispārējai gatavībai pret riskiem ir būtiska jebkurai organizācijai. Process sākas ar augstākās vadības apņemšanos, atzīstot, ka bez viņu atbalsta nav iespējams panākt būtisku progresu apmācību izstrādē. Ir ļoti svarīgi izveidot skaidru un konsekventu drošības politiku, jo tā kalpos par pamatu mācību saturam. Kad šīs politikas ir izveidotas, organizācijai ir jākoncentrējas uz savu kolēģu izglītošanu par šīm politikām un labāko praksi drošības risku mazināšanai. Lai nodrošinātu, ka apmācība joprojām ir aktuāla, ir nepieciešama pastāvīga uzraudzība un novērtēšana. To var panākt, ieviešot īpašus rādītājus, lai novērtētu drošības apmācības efektivitāti un novērtētu ieguldījumu atdevi. Veicot šīs darbības, organizācija var izveidot spēcīgu drošības apmācības programmu, kas sagatavo tās dalībniekus efektīvai drošības risku novēršanai.

Atsauce uz ISO 31000

Šajā rakstā apskatīti ISO 31000:2018 Risku pārvaldības principi: Cilvēka un kultūras faktori.

16. attēls. **Risku pārvaldības principi** (pielāgots no ISO 31000:2018[80]), rakstā apskatītās cilvēka un kultūras faktori

[80] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Drošības apmācība ietver virkni prakšu, kuru mērķis ir uzlabot zināšanas un prasmes, kas vajadzīgas, lai aizsargātu sensitīvu informāciju un fiziskos aktīvus.

Drošības apmācības programmu izstrāde ir kritisks aspekts, kas nodrošina, ka apmācība ir efektīva un atbilstoša organizācijas vajadzībām. Tas ietver mācību programmas izstrādi, kas aptver būtiskas tēmas, piemēram, datu un ierakstu pārvaldību, paroļu drošību, ugunsdrošību, evakuāciju un citas krīzes procedūras. Drošības apmācības dizains ietver arī pārvaldības modeļa izveidi, lai veicinātu atbildību izstrādes laikā un pēc programmas ieviešanas, nodrošinot, ka apmācības mērķi atbilst organizācijas drošības politikām un normatīvajām prasībām.[81]

Turklāt runa nav tikai par saturu, bet arī par apmācību metodēm, kas var būt, sākot no semināriem, krīzes scenārijiem un lomu spēlēm līdz tiešsaistes kursiem un mācību efektivitātes novērtēšanai, izmantojot novērtējumus un atgriezeniskās saites mehānismus. Efektīvas drošības apmācības dizains ir proaktīva pieeja organizācijas aizsardzībai, uzsverot nepārtrauktas mācīšanās un pielāgošanās nozīmi mainīgo draudu apstākļos. Tas ir stratēģisks ieguldījums drošības risku pārvaldības cilvēciskajā elementā, nodrošinot indivīdus ar instrumentiem un izpratni, kas nepieciešama, lai darbotos kā pirmā aizsardzības līnija pret iespējamiem pārkāpumiem un incidentiem.

GADĪJUMA IZPĒTE

AS "Latvijas Finieris" ir vadošais saplākšņa un tā produktu ražotājs Baltijas valstīs un Somijā. Uzņēmums nodarbojas arī ar mežu apsaimniekošanu, mežizstrādi un sintētisko sveķu un fenola plēvju ražošanu.[82]

2014. gadā "Latvijas Finieris" piedzīvoja milzīgu ugunsgrēku vienā no Rīgā bāzētajām rūpnīcām.[83] Pēc šī notikuma akciju sabiedrība nolēma ieviest drošības kultūru un attīstīt to. Kā daļa no tās centieniem tika izveidots Drošības pārvaldības dienests (DPD), kas pārvaldīja drošības riskus tādās jomās kā ugunsdrošība, arodveselība un darba drošība, vides aizsardzība un fiziskā drošība. Pirms ugunsgrēkiem bija liels ar darbu saistītu nelaimes gadījumu skaits, kā rezultātā tika zaudēta darbspēja, apdrošināšanas izmaksas un samazinājās darbinieku drošības sajūta.

DPD apmācību centieni ļāva centralizēt apmācību procesu tā, lai uzņēmējdarbības procesi neciestu no pārliekas birokrātijas vai pārāk ilgas darbinieka iekļaušanas uzņēmumā. Savukārt apmācību procesa rezultātā tika iegūta pārliecība, ka darbinieks ir informēts par drošības prasībām un spēj uzņemties atbildību par savu darbu. Tas iekļāva gan digitālas apmācību platformas, gan apmācību video, gan motivācijas sistēmas veidošanu droša darba praksei.

---

[81] Designing a Successful Security Awareness Training Program. Iegūts no https://www.infosecinstitute.com/resources/security-awareness/designing-security-awareness-training-program/

[82] Latvijas Finieris. Iegūts no https://www.finieris.com/lv/par-koncernu/

[83] Latvijas Finiera rūpnīcā liels ugunsgrēks (2014). Iegūts no https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks

LABĀ PRAKSE

Labs drošības apmācības dizains balstās uz trīs pamata pīlāriem – 1) panika (paškontrole); 2) sagatavotība nezināmajam; 3) baiļu pārvarēšana. Lai to panāktu, drošības apmācības izveide vispārējai drošības risku gatavībai ietver vairākus galvenos soļus.

Aizsardzības risku novērtēšana. Sāciet ar iespējamo drošības draudu un ievainojamības identificēšanu un novērtēšanu organizācijā vai vidē. Tas ietver pagātnes incidentu, pašreizējo drošības pasākumu un iespējamo nākotnes risku analīzi. Labs drošības apmācības dizains balstās uz atbilstošu drošības riska analīzi.

Mācību mērķu definēšana. Skaidri izklāstiet, ko drošības apmācības programma vēlas sasniegt. Mērķos var ietvert informētības uzlabošanu, reaģēšanas stratēģiju uzlabošanu un atbilstības nodrošināšanu drošības politikai.

Mācību programmas izstrāde. Izstrādājiet visaptverošu mācību programmu, kas aptver visas nepieciešamās tēmas, piemēram, risku identificēšanu, novēršanas stratēģijas, reaģēšanu ārkārtas situācijās un atkopšanās plānus. Mācību programmā jāizveido vai jāizvirza arī scenārijs.

Dažādu mācību metožu iekļaušana. Izmantojiet mācību metožu kombināciju, tostarp lekcijas, interaktīvus seminārus, simulācijas un e-mācību moduļus, lai pielāgotos dažādiem mācību stiliem un nodrošinātu labāku informācijas saglabāšanu. Lai iegūtu vislabāko praktisko apmācību, ieteicams izmantot viena un tā paša riska diversificētu scenāriju simulācijas – cilvēkiem nevajadzētu pierast pie gaidītā, bet gan jātrenējas, lai sagatavotos neparedzamajam.

Pielāgošana dažādām lomām. Pielāgojiet apmācības moduļus dažādām lomām organizācijā, nodrošinot, ka katrs darbinieks saņem atbilstošu informāciju atbilstoši saviem pienākumiem un informācijas piekļuves (atbildības) līmenim. Atcerieties par īpašām apmācībām būtiskiem darbiniekiem.

Regulāri atjauninājumi un pārskatīšana. Regulāri atjauniniet mācību materiālus, ņemot vērā jaunākās drošības tendences, tehnoloģijas un praksi. Regulāri pārskatiet un pārstrādājiet saturu, lai saglabātu tā atbilstību un efektivitāti.

Novērtēšana un atgriezeniskā saite. Izveidojiet metriku, lai novērtētu apmācību programmas efektivitāti. Apkopojiet dalībnieku atsauksmes, lai noteiktu jomas, kurās nepieciešami uzlabojumi, un attiecīgi pielāgojiet apmācības. Ir labi iekļaut fokusa grupas darbiniekiem augsta riska vidē un runāt par viņu bailēm un izaicinājumiem darba vietā.

Izmantotie avoti

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Latvijas Finieris. Iegūts no https://www.finieris.com/lv/par-koncernu/

Latvijas Finiera rūpnīcā liels ugunsgrēks (2014). Iegūts no https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks

Designing a Successful Security Awareness Training Program. Iegūts no https://www.infosecinstitute.com/resources/security-awareness/designing-security-awareness-training-program/

HIBRĪDDRAUDI UN DROŠĪBAS RISKU VADĪBA

Prof., dr. Raimundas Kalesnykas / Kazimieras Simonavičius Universitāte, Lietuva / 2023

KOPSAVILKUMS

Hibrīddraudi ir viens no sarežģītākajiem izaicinājumiem drošības pārvaldības sistēmās, ar ko saskaras Eiropas Savienība (ES) un tās dalībvalstis, valsts sektora organizācijas un uzņēmumi. Valstis un to organizācijas meklē inovatīvus drošības risinājumus, lai ātri reaģētu un būtu noturīgas pret tādiem draudiem kā kiberuzbrukumi, nelegālā migrācija, pārrobežu noziedzība un dezinformācija.

Šajā rakstā ir aprakstīta Baltkrievijas varas iestāžu organizētā migrantu instrumentalizācija pie ES austrumu robežām. Tas parāda, ka organizācijām (valsts robežsardzei, privātiem uzņēmumiem, kas ievieš drošības risinājumus) ir jāizveido drošības risku pārvaldības sistēma, kuras pamatā ir reaģēšanas mehānisms uz hibrīddraudiem.

Risku vadības process prasa izpratni par ārējiem un iekšējiem faktoriem, lai novērtētu riskus robežsardzes jomā. Risku pārvaldība, kas apdraud robežu drošību, ietver risku identificēšanu, analīzi un novērtēšanu.

Atsauce uz ISO 31000

Šajā rakstā sadarbības modelis ir parādīts, izmantojot atsauci uz ISO 31000:2018 risku pārvaldības sistēmu – kontekstu noteikšana, ārējo un iekšējo parametru noteikšana risku pārvaldībai, risku novērtējums, juridiskās un normatīvās prasības.

17. attēls. **Risku vadības process** (pielāgots no ISO 31000:2018[84])

[84] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Pēdējos gados hibrīddraudu tēma ir dominējusi ES nacionālās drošības ainavā. Valsts un institūcijas, kas rūpējas par tās drošību, meklē jaunus drošības rīkus un tehnoloģijas, lai novērstu ievainojamību vairākos domēnos. Hibrīddraudu jēdziens pēdējā laikā arvien vairāk no militārā konteksta tiek pārnests arī uz sabiedriskās drošības jomu.

Termins "hibrīddraudi" attiecas uz darbību, ko veic valsts vai nevalstiski dalībnieki, kuru mērķis ir apdraudēt vai kaitēt kādam objektam, ietekmējot tā lēmumu pieņemšanu vietējā, reģionālā, valsts vai institucionālā līmenī. Hibrīddraudus raksturo šādi: a) koordinēta un sinhronizēta darbība, kas apzināti vērsta pret demokrātisku valstu un iestāžu sistēmiskām ievainojamībām, izmantojot plašu līdzekļu klāstu (piemēram, hibrīduzbrukumi, izmantojot cilvēkus, tehnoloģijas, nepatiesu informāciju), b) darbības, kuru realizācijai izmanto dažādas metodes, kā arī dažādus mijiedarbības punktus.[85] Tas nozīmē, ka hibrīddraudi izmanto taktiku, kas apgrūtina to identificēšanu un reaģēšanu uz tiem, bieži vien darbojas dažādās vietās, organizācijās vai cilvēku grupās (piemēram, iekšējās un/vai ārējās drošības iestādēs, vietējās un/vai valsts drošības iestādēs, valsts drošības kontekstā) un/vai starptautiskā drošības jomā. Piemēram, iedomājieties scenāriju, kurā valsts izmanto kiberuzbrukumus, lai izjauktu citas valsts kritisko infrastruktūru, piemēram, elektrotīklus. Tajā pašā laikā viņi sociālajos medijos izplata dezinformāciju, lai radītu iedzīvotāju apjukumu un paniku. Šī kiberkara un psiholoģisko manipulāciju kombinācija apgrūtina mērķa valstij iespējas efektīvi reaģēt, jo tā saskaras gan ar fiziskiem traucējumiem, gan ar dezinformāciju. Tas parāda, kā hibrīddraudi var darboties dažādos domēnos, apgrūtinot atklāšanas un reaģēšanas centienus.

Cīņa pret hibrīddraudiem ir saistīta ar valsts drošību un likuma un kārtības uzturēšanu. Centieni reaģēt uz hibrīddraudiem ir jāpamato ar spēju atklāt agrīnas ļaunprātīgas hibrīddarbības, iekšējos un ārējos faktorus un izprast iespējamās saiknes starp bieži vien šķietami nesaistītiem notikumiem.

Pirmo reizi tas mainījās līdz ar Baltkrievijas hibrīdo agresiju 2021. gada vidū, izveidojot mākslīgu migrācijas ceļu uz ES austrumu valstīm (Latviju, Lietuvu, Poliju), kas atveda tūkstošiem bēgļu pie ES sliekšņa un radīja ES / nacionālo drošību un robežu pārvaldības izaicinājumus turpmākajiem gadiem. Tie var ietvert cilvēku, īpaši sieviešu un bērnu, tirdzniecības pieaugumu, ieroču un citu nelegālu preču kontrabandas pieaugumu, kā arī terorismu un radikalizāciju.

Pārvaldot drošības riskus, kas izriet no hibrīddraudiem, organizācijām (valstiskām vai nevalstiskām) ir jāizveido ārējā un iekšējā vide, kurā organizācija cenšas sasniegt savus drošības mērķus.[86] Šajā kontekstā ir svarīgi izprast un noteikt ārējos un iekšējos parametrus, kas jāņem vērā, pārvaldot risku: (a) sociālā un kultūras, politiskā, juridiskā, regulējošā, finanšu, tehnoloģiskā un ekonomiskā vide, neatkarīgi no tā, vai tā ir starptautiska, nacionālā, reģionāla vai vietējā līmeņa; b) galvenie virzītāji un tendences, kas ietekmē organizācijas drošības mērķus; c) attiecības ar ieinteresētajām personām; d) pārvaldība, organizatoriskā struktūra, lomas un atbildība; e) politikas un stratēģijas, kas ir ieviestas drošības mērķu sasniegšanai; f) iespējas un zināšanas (piemēram, budžets, cilvēki, procesi, informācijas sistēmas un tehnoloģijas)[87] utt.

[85] Hybrid Threats as a Concept. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Iegūts no https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

[86] Ibid

[87] Giannopoulos, G. et al. (2021). The Landscape of Hybrid Threats: A conceptual model. Publications Office of the European Union, Luxembourg

GADĪJUMA IZPĒTE

No 2021. gada jūnija krasi pieaudzis to migrantu skaits, kas no Baltkrievijas vēlas nelegālā veidā šķērsot kaimiņvalstu Latvijas, Lietuvas un Polijas robežu. Baltkrievijas varas iestādes sniedza savu ieguldījumu, organizējot bēgļu un imigrantu pārvietošanu no Irākas, Afganistānas un citām Tuvo Austrumu un Āfrikas valstīm pāri Baltkrievijas–Lietuvas un Baltkrievijas–Polijas–Latvijas robežai.

Saskaņā ar statistiku 2021. gada augustā neatļautu iebraukšanas mēģinājumu skaits Polijā bija 3500, septembrī – 7700 un oktobrī – 17 300. Polijas robežsardze ik mēnesi reģistrēja aptuveni 2 tūkstošus mēģinājumu nelegāli šķērsot Polijas un Baltkrievijas robežu.[88]

2021. gadā Lietuvas un Baltkrievijas robežu šķērsojošo cilvēku skaits, salīdzinot ar iepriekšējo gadu, pieaudzis vairāk nekā trīsdesmit reizes. Laikā no 2021. gada 1. janvāra līdz 2022. gada 31. janvārim Lietuvā *de facto* tika aizturēti 4150 nelegālie migranti (tostarp 2891 persona tikai 2021. gada jūlijā) (Statistikas dati, 2023). Saskaņā ar Lietuvas Robežsardzes datiem laikā no 2021. gada 3. augusta līdz 2023. gada 1. jūlijam Lietuvā liegta ieceļošana 20 679 migrantiem.[89]

Latvijā par nelikumīgu robežas šķērsošanu aizturēto personu skaits 2021. gadā bija gandrīz 15 reizes lielāks (446 mēģinājumi), salīdzinot ar 2020. gadu (30 mēģinājumi), no 2021. gada līdz 2023. gada 20. jūlijam reģistrēti 10 394 robežšķērsošanas atturēšanas (t.i., atgrūšanas) gadījumi.[90]

Lielākā daļa migrantu bija Tuvo Austrumu un Āfrikas valstu pilsoņi (Irākas (kurdi, Irākas arābi), Sīrijas, Irānas, Afganistānas, Kongo, Kamerūnas, Šrilankas pilsoņi).

Baltkrievijas–Eiropas Savienības robežkrīze tika atzīta par "hibrīduzbrukumiem", kuru rezultātā uz Baltkrievijas robežas ar Latviju, Lietuvu un Poliju tika palielināts spiediens saistībā ar migrāciju un patvēruma meklētājiem.[91] Migrantu krīzi izraisīja Baltkrievijas un ES attiecību nopietna pasliktināšanās pēc 2020. gada Baltkrievijas prezidenta vēlēšanām, 2020.–2021. gada Baltkrievijas protestiem, Ryanair lidojuma 4978 incidenta un tai sekojošām sankcijām pret Baltkrieviju. "Hibrīduzbrukumi" sākās ap 2021. gada 7. jūliju, kad Baltkrievijas prezidents draudēja "pārpludināt" ES ar "narkotikām un migrantiem".[92] Pēc tam Baltkrievijā iebraukušajiem migrantiem tika dotas instrukcijas, kā un kur pārkāpt ES robežu, un ko teikt robežsargiem robežas otrā pusē.

Polija, Lietuva un Latvija migrantu krīzi raksturojušas kā "hibrīduzbrukumu", izmantojot migrantus kā ieročus un nosaucot migrantu krīzi par migrantu cilvēktirdzniecības incidentu, ko Baltkrievija ir veikusi pret ES. ES dienaskārtībā šī parādība tika nosaukta par "migrācijas instrumentalizāciju" – spēju kontrolēt nelegālās migrācijas plūsmas,[93] un 3 ES austrumu valstis ierosināja reaģēšanas mehānismu, lai izveidotu risku pārvaldības sistēmu ārējai situācijai un robežu drošībai. Migrācija arvien vairāk tiek formulēta kā drošības problēma, jo tiek pieņemts, ka imigranti rada terorisma,

88 Statista. Number of attempts to illegally cross the Polish-Belarusian border in Poland from August 2021 to June 2023. Iegūts no https://www.statista.com/statistics/1271292/poland-attempts-of-illegal-crossing-of-the-polish-belarusian-border/

89 Lithuanian State Data Management IS. Monitoring of illegal migration (from 01.01.2011) & Registered illegal migrants, Iegūts no https://ls-ospsdg.maps.arcgis.com/apps/dashboards/9b0a008b1fff41a88c5efcc61a876be2

90 Latvia State Border Guard. Statistics at the state border and within the country (from 1 August 2021 to 1 July 2023), Iegūts no https://www.rs.gov.lv/en

91 Parliamentary Assembly of the Council of the Europe Resolution 2404 (2021) "Instrumentalised migration pressure on the borders of Latvia, Lithuania and Poland with Belarus". Iegūts no https://pace.coe.int/en/files/29537/html

92 Evans, J. (2021). "Belarus dictator threatens to 'flood EU with drugs and migrants'". *The Week*, 28 May, 2021. Iegūts no https://www.theweek.co.uk/news/world-news/europe/952979/belarus-dictator-threatens-flood-eu-with-drugs-migrants-avoid-sanctions

93 Rashe, L. (2022). The instrumentalization of migration – how should the EU respond? Jacques Delors Centre, Hertie School, Germany. Iegūts no https://www.delorscentre.eu/en/publications/the-instrumentalisation-of-migration

cilvēku tirdzniecības, pārrobežu noziedzības un nelegālās imigrācijas riskus.[94] Šī situācija norāda uz to, ka mūsdienu drošības izaicinājumi ir ļoti sarežģīti un savstarpēji saistīti, tādēļ visos risku pārvaldības posmos gan ES, gan dalībvalstu līmenī ir nepieciešama plašāka starpnozaru, starpdisciplināra un starpvalstu sadarbība.

LABĀ PRAKSE

Labā prakse ES ārējo austrumu robežu drošības vadība

Risku analīze un kontrole

Ārējo robežu drošību ietekmē tādas parādības kā ģeopolitika, migrācija, pārrobežu noziedzība, terorisms un hibrīddraudi, kas ir mainīgi un daudzdimensionāli, tāpēc to izpratnei, analīzei un pārvaldībai nepieciešama elastīga pieeja.

Robežu drošības aģentūras ES dalībvalstīs izmanto kopējo integrēto riska analīzes modeli (CIRAM)[95], kas koncentrējas uz drošības apdraudējuma dimensiju. Dažādu riska kategoriju analīze sniedz visaptverošu priekšstatu par izaicinājumiem un draudiem, kas apdraud ES ārējo robežu drošību un darbību. Riski ir iedalīti trīs plašās kategorijās: nelegālā migrācija (nelegālā ieceļošana, dokumentu izkrāpšana); sekundārā pārvietošanās pāri robežai un atgriešanās un pārrobežu noziedzība (nelegālo narkotiku kontrabanda, šaujamieroču kontrabanda, zagtu transportlīdzekļu un transportlīdzekļu daļu tirdzniecība, tabakas kontrabanda, cilvēktirdzniecība).

Drošības risku pārvaldība ir nepārtraukts šo robežu drošības risku identificēšanas un to novēršanas plānu īstenošanas process. Risku analīze attiecas uz risku komponentu sistemātisku pārbaudi, lai nodrošinātu informētu lēmumu pieņemšanu. Ārējo robežu drošības pārvaldībā risks tiek definēts kā apdraudējuma apmērs un varbūtība, kas rodas uz ārējām robežām, ņemot vērā uz valsts robežām un ES iekšienē notiekošos pasākumus, kas ietekmēs ES iekšējo drošību, valsts drošību un dalībvalstu drošību kopumā.[96]

Riskus ārējo robežu drošības pārvaldības kontekstā var aplūkot kā trīs komponentus: (1) apdraudējumu, kas tiks novērtēts pēc apjoma un varbūtības; (2) neaizsargātība pret draudiem –, citiem vārdiem sakot, reakcijas uz apdraudējumu līmeni un efektivitāte; (3) ietekme – ja īstenosies apdraudējums ES iekšējai un/vai dalībvalstu nacionālajai drošībai vai ārējo robežu drošībai, kā arī ietekme uz efektīvu *bona fide* (atbilstošu regulējumam, godprātīgu) robežšķērsošanas pārvaldību. Drošības risku pārvaldības praksē apjoms attiecas uz apdraudējuma lielumu vai smagumu (piemēram, liela mēroga kiberuzbrukumam var būt liela ietekme), un ietekme ir šī apdraudējuma sekas, ja apdraudējums notiek (piemēram, liela mēroga kiberuzbrukums). Apmēra draudi parasti rada būtiskāku ietekmi, piemēram, finansiālus zaudējumus vai dzīvības zaudēšanu. Būtībā, jo lielāks ir apdraudējums, jo būtiskāka ir tā iespējamā ietekme uz drošību efektīvi novērtēt riskus.

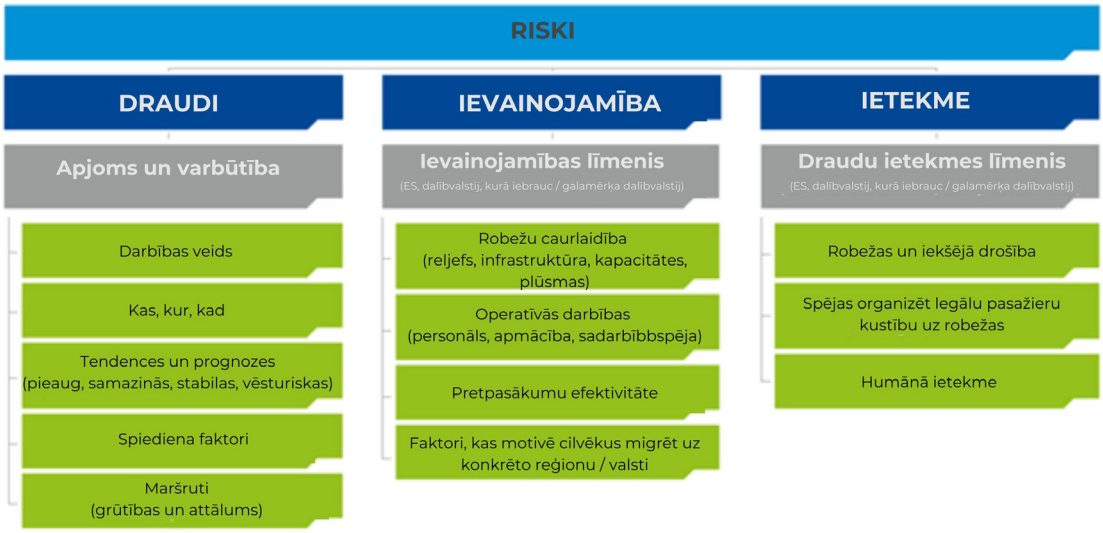
Riski tiek identificēti un novērtēti, ņemot vērā to apdraudējuma līmeni, neaizsargātību un ietekmi, un pēc tam paziņoti lēmumu pieņēmējiem. Lai gan analītiķi ir atbildīgi par draudu identificēšanu

[94] Dekker R., et al. (2016). The use of online media in migration networks. *Population, Space and Place*, 22, 539.–551.

[95] Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.1 (2021), FRONTEX - European Border and Coast Guard Agency. Iegūts no https://prd.frontex.europa.eu/document/common-integrated-risk-analysis-model-2-1/

[96] Joint Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Responding to state-sponsored instrumentalization of migrants at the EU external border (JOIN(2021) 32 final), Iegūts no https://commission.europa.eu/document/4d0c173e-709f-4832-b12f-31792cd10bff_lt

un novērtēšanu, lēmumu pieņēmēji savu lēmumu pieņemšanas spēju ietvaros ir atbildīgi par risku pārvaldību. Risku analīze ietver atsauces periodu – dienu, nedēļu, mēnesi vai gadu, kas atbilst lēmumu pieņemšanas līmenim, par kuru tas ir paredzēts.



18. attēls. **Risku analīzes shēma, izmantojot CIRAM modeli**[97]

Kontroles piemērs

Valsts robežu drošības aģentūru risku analītiķi informē vadību par riskiem, lai tā varētu pieņemt pārdomātus lēmumus par gada budžeta sadali attiecībā uz dažādiem riskiem. Risku analītiķi robežšķērsošanas punktu (RKP) līmenī informē RKP vadītāju par darbības riskiem, lai viņš vai viņa varētu pieņemt pārdomātus lēmumus, piešķirot personālu kontrolei un uzraudzībai. Risku analītiķiem jāziņo, ka, ņemot vērā pagātnes pierādījumus un pašlaik pieejamos izlūkdatus, nelegālas robežas šķērsošanas draudi starp RKP X un RKP Y ir ļoti iespējami, savukārt starp RKP Y un RKP Z tas ir maz ticams. Šī informācija ļauj lēmumu pieņēmējiem piešķirt resursus, kā arī apgabalam starp RKP X un RKP Y uzstādīt kā prioritāti.

Valstu integrētajām robežu uzraudzības sistēmām, kuru darbības pamatā ir risku analīze, jābūt stabilai (organizatoriski, administratīvi un tehniski) kapacitātei un nepārtrauktai darbībai arī trauksmes stāvoklī. Tas ir nepieciešams, lai novērstu un atklātu neatļautu robežšķērsošanu, aizturētu personas, kas robežu šķērsojušas nelikumīgi, un nodrošinātu, ka uz šīm personām attiecas saskaņotas un visaptverošas nosūtīšanas procedūras (t.i., pārbaudes procedūras), kas ievēro viņu pamattiesības, lai pārtvertu transporta līdzekļus, piemēram, kuģus, ko izmanto nelegālai robežšķērsošanai, lai cīnītos pret pārrobežu noziedzību, piemēram, kontrabandu, cilvēku tirdzniecību un terorismu, kā arī lai reaģētu uz hibrīdiem draudiem.

Atbilde uz hibrīddraudiem

- **ES aģentūru operacionālais atbalsts**

Nelegālās migrācijas pieplūduma kulminācijas laikā (2021. gada jūlijā) Lietuvas valdība lūdza atbalstu specializētajām ES aģentūrām – FRONTEX (Eiropas Robežu un krasta apsardzes aģentūra)

[97] Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.0 (2013), FRONTEX - European Border and Coast Guard Agency. Iegūts no https://frontex.europa.eu/what-we-do/monitoring-and-risk-analysis/ciram/

un EUAA (ES Patvēruma aģentūra). FRONTEX[98] un EUAA, risinot ar nelegālajiem migrantiem saistītās problēmas, ir vērstas uz to, lai novērstu nelegālo migrantu plūsmu caur Lietuvu uz Rietumu ES valstīm.

FRONTEX ātri uzsāka ātrās reaģēšanas robežapsardzes pasākumus, lai sniegtu tūlītēju palīdzību ES dalībvalstij, kas ir pakļauta steidzamam un ārkārtējam spiedienam uz tās ārējās robežas, jo īpaši saistībā ar lielu skaitu trešo valstu valstspiederīgo, kas cenšas nelegāli iekļūt tās teritorijā. Ātrās reaģēšanas robežapsardzes darbību laikā FRONTEX piešķīra aptuveni 120 virsniekus, 36 patruļmašīnas un divus helikopterus Lietuvas Valsts robežsardzes dienesta (LVRS) atbalstam, lai veiktu robežu novērošanas un kontroles pasākumus. FRONTEX darbinieki arī palīdzēja vākt datus par nelikumīgiem robežšķērsošanas gadījumiem un apmainīties ar operatīvo informāciju.[99]

EUAA ir sniegusi operatīvo atbalstu un piešķīrusi 73 darbiniekus, kas strādā patvēruma pieteikumu reģistrācijas un apstrādes jomā, tostarp veicot intervijas un izstrādājot atzinumus, kā arī uzlabo spēju pārvaldīt pieteikuma iesniedzēju uzņemšanu. Tāpat Lietuvas Valsts robežsardzes dienests ir saņēmis atbalstu pirmās līnijas uzņemšanas vadības pilnveidošanai, īpaši klātienes vadībai, komunikācijai, informācijas sniegšanai, kā arī palīdzību uzņemšanas kapacitātes paplašināšanā.

- **Fiziskās barjeras**

Īstenojot Likumu par fizisko barjeru uzstādīšanu (2021), Lietuvas valdība apstiprināja fiziskas barjeras uzstādīšanu 2021. gada augusta beigās pēc tam, kad Baltkrievijas režīms sāka hibrīduzbrukumu pret Lietuvu, kā rezultātā notika nelegālo migrantu pieplūdums valstī. Fiziskā barjera tiek ierīkota atbilstoši Valsts robežsardzes dienesta prasībām – uz valsts robežas uzstādīts žogs, un tam blakus tika izbūvēti žoga segmenti, kas papildināti ar spirālveida spoli. Kopējais žoga augstums ir aptuveni 4 metri virs zemes. Fiziskās barjeras izbūves laikā tika uzstādīti 530 kilometri jaunu žoga segmentu un izbūvēti kopā 357 kilometri žoga. Lietuvas robežas ar Baltkrieviju kopējais garums ir 679 kilometri. Vairāk nekā 100 kilometru valsts robeža iet gar upju un ezeru krastiem, kur nav plānots uzstādīt fiziskas barjeras.[100]

- **Automatizētās robežas novērošanas sistēmas**

Lai maksimāli palielinātu valsts robežas aizsardzību, būtiski ir nodrošināt, ka viss Baltkrievijas robežas posms tiek uzraudzīts, izmantojot jaunākās tehnoloģijas. Lietuva ir uzstādījusi automatizēto valsts robežas uzraudzības sistēmu, kas aprīkota ar videonovērošanas kamerām un kustību detektoriem 640 kilometru garumā un uzraudzīs 100 % valsts robežas ar Baltkrieviju. Tāpat Lietuvas Valsts robežsardzes dienests nelegālās migrācijas izsekošanai izmanto bezpilota lidaparātus, izlūkošanas lidmašīnas, ārzonas sensorus un satelītu attālināto izpēti.

---

98 FRONTEX – European Border and Coast Guard Agency: Risk Analysis for 2022/2023 (2022). Iegūts no https://frontex.europa.eu/publications/risk-analysis-for-2022-2023-RfJIVQ

99 Blažytė, G., et al. (2022). Comparative report on the influx of irregular migrants across the Belarus border: the response by the Governments of Lithuania and Latvia. Diversity Development Group and PROVIDUS Center for Public Policy. Iegūts no https://ec.europa.eu/migrant-integration/library-document/niem-comparative-report-influx-irregular-migrants-across-belarus-border_en

100 Law on Installation of a Physical Barrier in the territory of the Republic of Lithuania near the External Border of the European Union with the Republic of Belarus, adopted by the Parliament of the Republic of Lithuania, 10 August 2021, No. XIV-513, Iegūts no https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/4763ca32fa7211ebb4af84e751d2e0c9?positionInSearchResults=1&searchModelUUID=e617cf00-5855-4e3f-afc8-d9021687a307

Iekļūšanas atteikums

2021. gada jūlija sākumā Lietuvas parlaments paziņoja, ka valstī ir valsts līmeņa ārkārtas situācija masveida migrantu pieplūduma dēļ. Lietuvas parlaments pieņēma grozījumus likumā par valsts robežu un aizsardzību (2023. gada 25. aprīlī), legalizējot nelegālo migrantu izraidīšanu uz robežas valsti ekstrēmās situācijās vai ārkārtas stāvokļa apstākļos.

Grozījumi *Valsts robežas un aizsardzības likumā* (2023) ievieš iespēju atteikt ieceļošanu Lietuvā valsts līmeņa ārkārtējas situācijas laikā un ārzemnieku pieplūduma dēļ; arī tiem ārzemniekiem, kuri plāno vai ir šķērsojuši valsts robežu šim nolūkam neparedzētās vai šim nolūkam paredzētās vietās, bet pārkāpušas valsts robežas šķērsošanas kārtību. Lietuvas Valsts robežsardzes dienesta darbiniekiem ir tiesības nelegālos migrantus atraidīt tikai gar robežu – līdz 5 km iekšzemē.

Noteikums par migrantu izraidīšanu attiecas uz katru ārzemnieku individuāli un atsevišķos gadījumos var tikt neattiecināts, lai nodrošinātu ieceļošanu vai humānās palīdzības piekļuvi Lietuvas teritorijā ārzemniekiem, kuri bēg no militāras agresijas vai vajāšanas. Ārzemniekiem, kuriem nebija atļauts ieceļot, tika veikts palīdzības nepieciešamības izvērtējums. Ja migrantiem tiktu konstatēta nepieciešamība, viņiem būtu jāsniedz nepieciešamā neatliekamā medicīniskā vai cita palīdzība.

Grozījumi *Valsts robežas un aizsardzības likumā* (2023) skaidri nošķir dabisko migrāciju no Baltkrievijas režīma veicinātās instrumentalizētās migrācijas.[101]

Robežu drošības risku pārvaldības tiesiskais regulējums

2021. gada oktobrī Eiropas Padome aicināja Komisiju ierosināt nepieciešamās izmaiņas ES tiesiskajā regulējumā, lai reaģētu uz valsts sponsorētu cilvēku instrumentalizāciju pie ES ārējās robežas ar Baltkrieviju. Līguma par Eiropas Savienības darbību 78. panta 3. punkts paredz pagaidu pasākumu pieņemšanu ārkārtas migrācijas situācijās pie ES ārējām robežām. Priekšlikuma mērķis bija atbalstīt Latviju, Lietuvu un Poliju, nodrošinot pasākumus un operatīvo atbalstu, kas nepieciešams, lai cilvēcīgi, sakārtoti un cienīgi, pilnībā ievērojot pamattiesības, pārvaldītu personu ierašanos, ko instrumentalizē Baltkrievija.

Ārkārtas migrācijas un patvēruma pārvaldības procedūras galvenās iezīmes uz ES ārējām robežām (Lietuva, Latvija un Polija) ir:

- iespēja attiecīgajām dalībvalstīm reģistrēt patvēruma pieteikumu un piedāvāt iespēju to efektīvi iesniegt tikai īpašos reģistrācijas punktos, kas atrodas robežas tuvumā, tostarp šim nolūkam paredzētajos robežšķērsošanas punktos;
- starptautiskās aizsardzības pieteikumu reģistrācijas termiņš pagarināts līdz četrām nedēļām;
- iespēja visiem pieteikumiem piemērot paātrināto procedūru uz robežas, tādējādi ierobežojot Baltkrievijas iespēju instrumentalizācijai vērsties pret trešo valstu valstspiederīgajiem, kuriem nevar piemērot robežprocedūru;
- atgriešanas procedūra uz ārējām robežām;
- uzņemšanas materiālie nosacījumi – tikai pamatvajadzību segšanai. Latvijai, Lietuvai un Polijai ir jānodrošina, lai visās darbībās tiktu ievērotas humānās pamatgarantijas, piemēram, trešo valstu valstspiederīgo nodrošināšana to teritorijā ar pārtiku, ūdeni, apģērbu, atbilstošu medicīnisko aprūpi, palīdzību neaizsargātām personām un pagaidu pajumti.[102]

[101] Sari, A. (2023). Instrumentalized migration and the Belarus crisis: Strategies of legal coercion. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

[102] The European Commission's proposal for a Council Decision on Provisional emergency measures for the benefit of Latvia, Lithuania and Poland (COM/2021/752 final). Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A752%3AFIN&qid=1638547296962

Eiropas Komisijas priekšlikums ir veidots saskaņā ar visaptverošo pieeju, kas noteikta jaunajā migrācijas un patvēruma aktā.[103] Šī akta mērķis ir izveidot kopēju pieeju migrācijai un patvērumam, kuras pamatā ir solidaritāte, atbildība un cilvēktiesību ievērošana. Akts ir devis dažādus rezultātus, piemēram, noteica ES mehānismu ar migrāciju saistītu krīžu gatavībai un pārvarēšanai, izstrādāja agrīnās brīdināšanas un prognozēšanas sistēmu, kas ļauj operatīvi identificēt migrācijas situācijas, ļauj efektīvi sagatavoties un reaģēt. Tas arī risināja krīzes un nepārvaramas varas situācijas migrācijas un patvēruma jomā, izveidoja ES integrētās robežu pārvaldības sistēmu – koordinētu sistēmu, sākot no robežuzraudzības līdz kontrabandas apkarošanai un migrantu atgriešanai.

Eiropas Komisijas gaidāmie priekšlikumi Šengenas robežu kodeksa reformai ietvers ES tiesiskā regulējuma stiprināšanu, lai sniegtu dalībvalstīm labākus instrumentus ārējo robežu aizsardzībai migrantu instrumentalizācijas situācijās, vienlaikus nodrošinot pilnīgu pamattiesību ievērošanu. Tajos būs ietverti arī pasākumi, kas palīdzēs tām dalībvalstīm, kuras saskata neatļautu migrantu pārvietošanos, tostarp instrumentalizācijas sekas tālu prom no ārējās robežas.

Eiropas Komisijas priekšlikums ir jaunākais no vairākām saskaņotām ES darbībām, kas ietver: mērķtiecīgus pasākumus pārvadātājiem, kas veicina kontrabandu vai iesaistās tajā; diplomātisko un ārējo darbību; humānās palīdzības un atbalsta palielināšanu robežu drošībai un migrācijas pārvaldībai.

Izmantotie avoti

Amendments to the Law on the State Border and Protection, adopted by the Parliament of the Republic of Lithuania, 25 April 2023, No. XIV-1891. Iegūts no https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ff701250e35a11eda305cb3bdf2af4d8?jfwid=fwi8z9chx

Blažytė, G., et al. (2022). Comparative report on the influx of irregular migrants across the Belarus border: the response by the Governments of Lithuania and Latvia. Diversity Development Group and PROVIDUS Center for Public Policy. Iegūts no https://ec.europa.eu/migrant-integration/library-document/niem-comparative-report-influx-irregular-migrants-across-belarus-border_en

Building walls, restricting rights: Lithuania's response to the EU-Belarus border 'crisis', Statewatch, 1 February 2022. Iegūts no https://www.statewatch.org/analyses/2022/building-walls-restricting-rights-lithuania-s-response-to-the-eu-belarus-border-crisis/

Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.1 (2021), FRONTEX - European Border and Coast Guard Agency. Iegūts no https://prd.frontex.europa.eu/document/common-integrated-risk-analysis-model-2-1/

Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.0 (2013), FRONTEX - European Border and Coast Guard Agency. Iegūts no https://frontex.europa.eu/what-we-do/monitoring-and-risk-analysis/ciram/

Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum (COM/2020/609 final). Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0609

Communication from the European Commission to the European Parliament the Council on Establishing the multiannual strategic policy for European integrated border management (COM (2023) 146 final). Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0146

Dekker R., et al. (2016). The use of online media in migration networks. Population, Space and Place, 22, 539–551.

Evans, J. (2021). "Belarus dictator threatens to 'flood EU with drugs and migrants'". The Week, 28 May 2021. Iegūts no https://www.theweek.co.uk/news/world-news/europe/952979/belarus-dictator-threatens-flood-eu-with-drugs-migrants-avoid-sanctions

FRONTEX - European Border and Coast Guard Agency: Risk Analysis for 2022/2023 (2022). Iegūts no https://frontex.europa.eu/publications/risk-analysis-for-2022-2023-RfJIVQ

[103] Communication from the European Commission to the European Parliament the Council on Establishing the multiannual strategic policy for European integrated border management (COM(2023) 146 final). Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0146

Giannopoulos, G. et al. (2021). The Landscape of Hybrid Threats: A conceptual model. Publications Office of the European Union, Luxembourg.

Hybrid Threats as a Concept. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Iegūts no https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Joint Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Responding to state-sponsored instrumentalization of migrants at the EU external border (JOIN (2021) 32 final), Iegūts no https://commission.europa.eu/document/4d0c173e-709f-4832-b12f-31792cd10bff_lt

Joint Communication from the European Commission to the European Parliament and the Council on Joint Framework on countering hybrid threats - a European Union response (JOIN/2016/018 final), Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

Latvia State Border Guard. Statistics at the state border and within the country (from 1 August 2021 to 1 July 2023), Iegūts no https://www.rs.gov.lv/en

Law on Installation of a Physical Barrier in the territory of the Republic of Lithuania near the External Border of the European Union with the Republic of Belarus, adopted by the Parliament of the Republic of Lithuania, 10 August 2021, No. XIV-513, Iegūts no https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/4763ca32fa7211ebb4af84e751d2e0c9?positionInSearchResults=1&searchModelUUID=e617cf00-5855-4e3f-afc8-d9021687a307

Lithuanian State Data Management IS. Monitoring of illegal migration (from 01.01.2011) & Registered illegal migrants, Iegūts no https://ls-ospsdg.maps.arcgis.com/apps/dashboards/9b0a008b1fff41a88c5efcc61a876be2

Parliamentary Assembly of the Council of the Europe Resolution 2404 (2021) "Instrumentalised migration pressure on the borders of Latvia, Lithuania and Poland with Belarus". Iegūts no https://pace.coe.int/en/files/29537/html

Rashe, L. (2022). The instrumentalization of migration – how should the EU respond? Jacques Delors Centre, Hertie School, Germany. Iegūts no https://www.delorscentre.eu/en/publications/the-instrumentalisation-of-migration

Sari, A. (2023). Instrumentalized migration and the Belarus crisis: Strategies of legal coercion. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

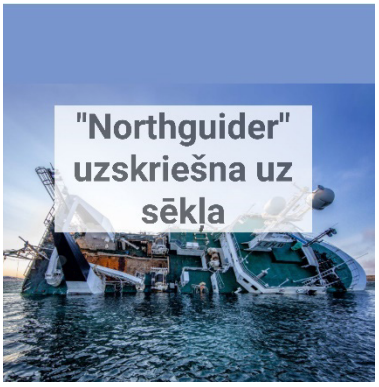
Statista. Number of attempts to illegally cross the Polish-Belarusian border in Poland from August 2021 to June 2023, Iegūts no https://www.statista.com/statistics/1271292/poland-attempts-of-illegal-crossing-of-the-polish-belarusian-border/

The European Commission's proposal for a Council Decision on Provisional emergency measures for the benefit of Latvia, Lithuania and Poland (COM/2021/752 final), Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A752%3AFIN&qid=1638547296962

MĀCĪBAS NO KUĢA "NORTHGUIDER" UZSKRIEŠANAS UZ SĒKĻA

Natalia Andreassen & Rune Elvegård / Nord Universitāte, Norvēģija /2024

KOPSAVILKUMS



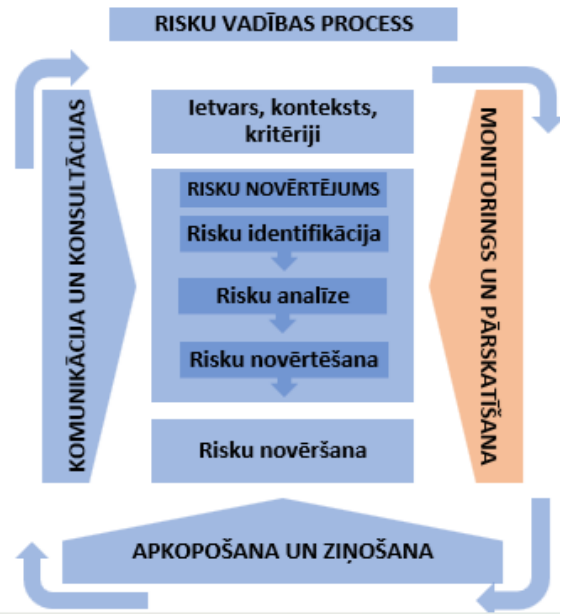
Šajā rakstā ir sniegts piemērs, ko var mācīties no kuģa "Northguider" avārijas pieredzes un kā var ieviest uzlabojumus avārijas gatavības sistēmās. Raksts sniedz ieskatu situācijā un krīzes pārvarēšanas operācijā. Pēc tam tiek prezentēts avārijas gatavības mācību gadījums, kas tika balstīts uz šī incidenta scenāriju.

Saistībā ar ISO 31000 standartu tiek minēts pilnveidošanas princips, kā arī tiek ieteikts izstrādāt mācības par sagatavotību ārkārtas situācijām, lai nepārtraukti mācītos un pilnveidotos.

Atsauce uz ISO 31000

ISO 31000 standarts nosaka risku pārvaldības principu vadlīnijas. ISO 31000 ir svarīgs un noderīgs rīks drošības speciālistiem risku pārvaldības stratēģiju izstrādei. Kā norāda Starptautiskā standartizācijas organizācija, organizācijas panākumi ilgtermiņā ir atkarīgi no daudzām lietām, sākot no nepārtrauktas piedāvājuma novērtēšanas un atjaunināšanas līdz procesu optimizēšanai. It kā tas nebūtu pietiekams izaicinājums, viņiem ir jāņem vērā arī neparedzētie risku pārvaldīšanas gadījumi.

Tomēr drošības speciālistiem ir jāveido un jāintegrē viņu organizācijām visatbilstošākās vadlīnijas un jāuzlabo risku pārvaldības process un veiktspēja atbilstoši savai pieredzei.



19. attēls. **Risku vadības process** (pielāgots no ISO 31000:2018[104])

[104] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Pēdējais ISO 31000 princips ir nepārtraukta uzlabošana. Šis princips apstiprina, ka risku pārvaldības pasākumiem ir jānodrošina nepārtraukti uzlabojumi. Risku pārvaldība tiek nepārtraukti uzlabota, mācoties un iegūstot pieredzi.

20. attēls. **Risku pārvaldības principi saskaņā ar ISO 31000:2018**[105]

ISO 31000 ietvars apraksta, ka organizācijām ir jāizvērtē sava prakse un esošie risku pārvaldības procesi. Pēdējā ietvara sastāvdaļa ir uzlabošana, kas ietver risku pārvaldības vērtību, ietvara pielāgošanu un risku pārvaldības aktivitāšu integrāciju atbilstoši organizācijas vajadzībām.

21. attēls. **Risku vadības ietvars saskaņā ar ISO 31000:2018**[106]

Organizācijai ir nepārtraukti jāuzlabo un jāstiprina tā risku pārvaldības sistēma, mācoties un pārskatot pieredzi.

[105] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html
[106] Ibid

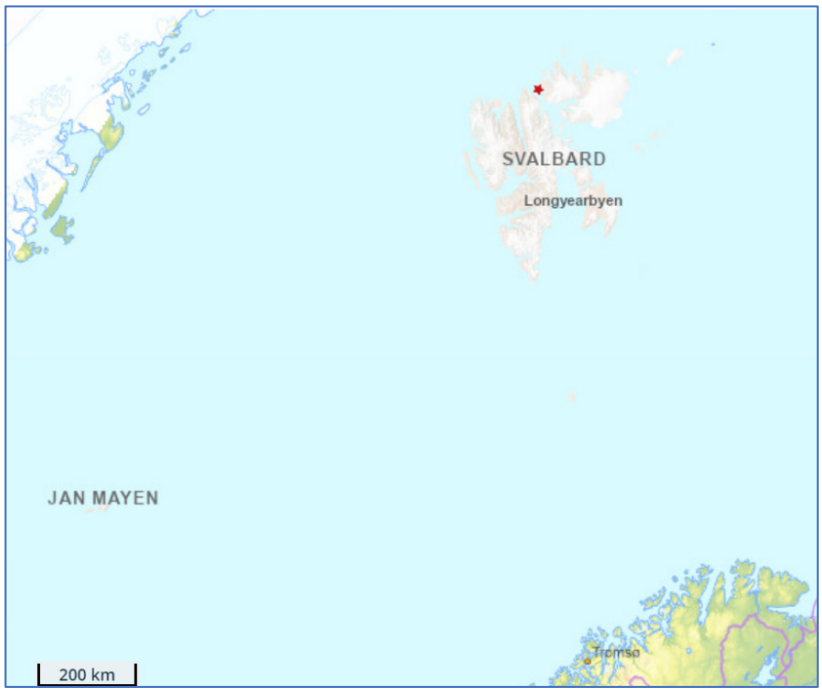
IEVADS

Šajā rakstā aprakstīts kuģa "Northguider" uzskriešanas uz sēkļa gadījums, kas bija ļoti sarežģīta meklēšanas un glābšanas, un jūras vides reaģēšanas operācija. Scenārijs vēlāk tika izmantots ārkārtas gatavības mācībās, lai uzlabotu risku un krīžu vadības sistēmas Arktikā. Viens no šādiem vingrinājumiem šajā gadījuma izpētē ir parādīts kā labās prakses piemērs, lai mācītos no pašu un citu ārkārtas situāciju pieredzes.

GADĪJUMA IZPĒTE

Ziemassvētku laikā, 2018. gada 28. decembrī, Norvēģijas traleris "Northguider" ar 14 cilvēku apkalpi Svalbāras arhipelāgā zvejoja garneles. Apm. 13:00 tas uzskrēja uz sēkļa Hinlopenas šauruma šaurajā ziemeļu daļā. Citu kuģu apkārtnē nebija. "Northguider" sūtīja sacienu pēc palīdzības, izmantojot savu avārijas bāku un MF/HF radio. "Northguider" nesaņēma nekādu atbildi uz briesmu signālu, bet ziņojumu pārtvēra Norvēģijas krasta apsardzes kuģis “Barentshav”, kas atradās netālu no *Bjørnøya* salas. "Barentshav" devās uz Hinlopenu, taču ledus apstākļu dēļ nācās pagriezties atpakaļ.

Pēc vairākām stundām visa apkalpe tika izglābta ar diviem helikopteriem no Svalbāras ļoti grūtā glābšanas operācijā sliktos laikapstākļos. Pacelšanās arktiskajos apstākļos ir izaicinājums pats par sevi, taču šī operācija tika veikta -20 grādu pēc Celsija temperatūrā, tumsā un stiprā vējā.



22. attēls. **“Northguider” gābšanas lokācijas karte**[107]

Pēc operācijas pabeigšanas atbildību par reaģēšanu pārņēma Norvēģijas piekrastes pārvalde. Ledus apstākļu dēļ tika nolemts, ka Norvēģijas krasta apsardzes kuģis "Svalbard" varētu izvērtēt situāciju turpmākajam darbam. Šis kuģis bija ledlauzis, kas spēj pārvietoties cauri vairākus gadus uzkrātam

[107] Neimane, K., Začs, U., Apalups, K., Andreassen, N., Elvegård, R., Kibsgaard, D., Bambach, B., Goffin, B., Bergman, J., Dorado, X., Garcia, E., Aatsinki, A., Rojas, H. I., Kalesnykas, R. (2024). Recommendations for Higher Education Institutions Teaching Security. Focus on Security Risk Management., SECUREU report, EU Erasmus+, Iegūts no https://security.turiba.lv/recommendations/

ledum. 2019. gada 9. janvārī tika uzsākta degvielas avārijas izkraušana, lai samazinātu milzīgās sekas uz vidi gadījumā, ja tralerim sāksies noplūde.

2019. gada februārī no "Northguider" tika iztukšota visa degviela un videi bīstamās vielas. No 2019. gada augusta līdz oktobrim profesionāli glābēji, ar kuriem bija noslēgts līgums, nesekmīgi mēģināja pacelt un vilkt kuģi. Ledus situācijas, skarbā klimata un attālā stāvokļa dēļ glābējiem glābšanas operācija bija jāatliek uz 2020. gada vasaras sezonu. Galu galā līdz 2020. gada septembrim kuģis tika sagriezts metāllūžņos uz vietas un aizvests.

23. attēls. **"Northguider" traleris,** foto: *Håkon Kjøllmoen*

Attālums, ierobežota infrastruktūra un skarbie klimatiskie apstākļi ir izaicinājums jūrniecības aktivitātēm Arktikā.[108] Ārkārtas reaģēšanas pārvaldības operācijās bieži ir iesaistīts plašs dalībnieku loks ar specializētiem uzdevumiem un lomām, kas saistītas ar informācijas apmaiņu, lēmumu pieņemšanu un vadības personāla rīkojumiem.[109] Reaģēšanas operāciju vadība ir atkarīga no tās vadītājiem un sistēmām, uz ko balstās lēmumu pieņēmēji, piemēram, procedūrām, protokoliem, formālām struktūrām utt. Nepastāvīgās un sarežģītās vidēs koordinācija ir mazāk atkarīga no iepriekš izplānotā plāna nekā no pašreizējām prasmēm, risinot jaunus uzdevumus un izaicinājumus.[110]

Šis gadījums parādīja, ka ir svarīgi iepriekš plānot lomas un pienākumus gan glābšanas operācijām, gan jūras vides reaģēšanas incidentiem. Tas nodrošina vietējo, reģionālo un valsts iestāžu galveno kontaktpersonu labu sadarbību incidenta laikā. Turklāt sākotnējais novērtējums ir vitāli svarīgs, nepieciešamie pasākumi jāveic jau glābšanas operācijas plānošanas fāzes laikā.

2021. gada novembrī Arktikas un Ziemeļatlantijas drošības un krīzes gatavības tīkla (*Arctic and North Atlantic Security and Emergency Preparedness Network, ARCSAR*) paspārnē notika galda

[108] Kruke, B.I. & Austad, A. C. (2021). Emergency preparedness and rescue in Arctic waters. *Safety Science*, Volume 136, 105163, https://doi.org/10.1016/j.ssci.2021.105163

[109] Bigley, G. A., & Roberts, K. H. (2001). The incident command system: High reliability organizing for complex and volatile task environments., *Academy of Management Journal*, 44 (6), 1281.–1299.

[110] Andreassen, N., Borch, O. J. & Sydnes, A. K. (2020). Information sharing and emergency response coordination. *Safety Science*, Volume 130, 104895, https://doi.org/10.1016/j.ssci.2020.104895

mācības “Oil in Ice”, kas bija liels ES finansēts inovāciju projekts. Mācības uzraudzīja Nord Universitātes NORDLAB ārkārtas gatavības vadības laboratorija.[111] Mācību "Oil in Ice 2021" galvenais mērķis bija pārrunāt, kā tiek organizēta gatavība naftas noplūdei, un reaģēt uz tām liela mēroga operācijas gadījumā Svalbāras reģionā, kā arī apzināt mācības no citām vietām un aģentūrām Arktikā un Ziemeļatlantijas reģionos.

24. attēls. **ARCSAR mācības “Oil in Ice”,**
foto: Krīzes vadības un sadarbības centrs – Nordlab[112]

Šo mācību scenārijs tika balstīts uz "Northguider" uz sēkļa uzskriešanas gadījumu ar to atšķirību, ka noplūde patiešām notika. Situācija Svalbāras apgabalā ir diezgan sarežģīta, jo ir vairāki dalībnieki no glābšanas operācijas un jūras vides reaģēšanas sektora, kuriem ir jāsadarbojas, lai risinātu starpgadījumu. Tas ietver reaģēšanu lai pasargātu jūras vidi, glābšanas operāciju un kuģa un vides aizsardzību.

Lai izpētītu un apspriestu potenciāli nepieciešamos uzlabojumus, apmācību mērķauditorija tika sadalīta trīs grupās: galvenā apmācību mērķgrupa – tie, kas būtu iesaistīti naftas noplūdes gadījumā; sekundārā apmācību mērķgrupa – paralēlās organizācijas citās Arktikas valstīs un novērotāji – visas pārējās ieinteresētās puses. Mācības veicināja dziļāku izpratni par prasmēm, novērtēšanas sistēmām un kompetencēm, lai risinātu Arktikas jūras vides negadījumus.

LABĀ PRAKSE

Ir izveidota rakstiska procedūra, kas nosaka informācijas un uzdevumu nodošanu starp Apvienoto glābšanas koordinācijas centru un Norvēģijas Piekrastes pārvaldi. Tomēr ir svarīgi saprast, kā izmantot procedūru un nepārtraukti uzlabot sistēmas. Šīs mācības bija nozīmīgs ieguldījums zināšanu un pieredzes apmaiņā par to, kā Arktikā var tikt galā ar nopietnu starpgadījumu un tam

[111] ARCSAR (2022) Tabletop Exercise ARCSAR TTX 2021 “OIL IN ICE”. Exercise Report. WP3 T3.2, Iegūts no https://arcsar.eu/wpcontent/uploads/2018/11/ARCSAR-TTX-2021-OIL-IN-ICE.pdf
[112] Ibid

sekojošu naftas piesārņojumu ekstremālos apstākļos.[113] Mācības veicināja uzlabojumus, attiecīgo procedūru izpratni un jaunu risku un jaunu kompetenču novērtēšanu, kas vajadzīgas, lai risinātu šādus starpgadījumus Arktikā.

Scenārijs tika balstīts uz reālu gadījumu, tāpēc šāda mācību izspēle, izmantojot reālu situāciju, sniedza iespējas demonstrēt riskus un izaicinājumus dažādām ieinteresēto personu grupām. Šādām mācību izspēlēm ir nepieciešama laba pedagoģiskā plānošana, koncentrējoties uz dažādu dalībnieku atšķirīgo pieredzi un vajadzībām. Vissvarīgākais ir atvieglot katra iesaistītā indivīda un organizācijas mācīšanos un ideju apmaiņu par to, kā risināt sarežģītu notikumu sarežģītos apstākļos.[114]

ISO 31000 standarts paredz, ka krīzes vai riska pārvaldība tiek nepārtraukti uzlabota, mācoties un pieredzot dažādas situācijas. Gan ietvara sastāvdaļa, gan viens no principiem ir vērsti uz nepārtrauktu sistēmu uzlabošanu, mācīšanos, rutīnas un kompetences atjaunināšanu. Ārkārtas situācijām sagatavotības vingrinājumi kalpo kā īpaši efektīva mācību metode uzlaboto zināšanu novērtēšanai, mācību atvieglošanai un zināšanu ieviešanai organizācijās.[115] Mācības veicina drošības risku pārvaldības spēju uzlabošanu, uzticības veidošanu un sadarbību starp iesaistītajām ieinteresētajām pusēm.[116] Izveidojot telpu un vietu pieredzes apmaiņai, komandas locekļi var pārdomāt savu kolektīvo pieredzi un apspriest iespējamās atbildes darbības.

Izmantotie avoti

Andreassen, N., Borch, O. J. & Sydnes, A. K. (2020). Information sharing and emergency response coordination. *Safety Science*, Volume 130, 104895, https://doi.org/10.1016/j.ssci.2020.104895

Andreassen, N., Elvegård, R., Villanger, R. & Johnsen, B. H. (2024). Enhancing cognitive motivation: an evaluation model for emergency preparedness exercises, The Learning Organization, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/TLO-06-2023-0100

ARCSAR (2022). Tabletop Exercise ARCSAR TTX 2021 "OIL IN ICE". Exercise Report. WP3 T3.2, Iegūts no https://arcsar.eu/wpcontent/uploads/2018/11/ARCSAR-TTX-2021-OIL-IN-ICE.pdf

Bigley, G. A., & Roberts, K. H. (2001). The incident command system: High reliability organizing for complex and volatile task environments. *Academy of Management* Journal, 44 (6), 1281.–1299.

Elvegård, R. & Andreassen, N. (2022). Internasjonalt samarbeid med fokus på oljevern i Arktis, High North News, Iegūts no https://www.highnorthnews.com/nb/internasjonalt-samarbeid-med-fokus-pa-oljevern-i-arktis?fbclid=IwAR020Lb75C6x9q6yfRzRuw7u4JrLZCveQPU2BqB9_4De37Lmp5kTTkixUl0

Elvegård, R., Andreassen, N. & Badu, J. (2024). Building collaboration and trust in emergency preparedness: a model for planning collaboration exercises. Safety in Extreme Environments, Iegūts no https://doi.org/10.1007/s42797-024-00107-w

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

Kruke, B. I. & Austad, A. C. (2021). Emergency preparedness and rescue in Arctic waters. *Safety Science*, Volume 136, 105163, https://doi.org/10.1016/j.ssci.2021.105163

[113] Kystverket [Norwegian Coastal Administration] (2021). Ledet og deltok på øvelse med fokus på nordområdene, Kystverkets Nyhetsarkiv, 11.01.2021, Iegūts no https://kystverket.no/nyheter/2020/ledet-og-deltok-pa-ovelse-med-fokus-pa-nordomradene2/

[114] Elvegård, R. & Andreassen, N. (2022). Internasjonalt samarbeid med fokus på oljevern i Arktis, High North News, Iegūts no https://www.highnorthnews.com/nb/internasjonalt-samarbeid-med-fokus-pa-oljevern-i-arktis?fbclid=IwAR020Lb75C6x9q6yfRzRuw7u4JrLZCveQPU2BqB9_4De37Lmp5kTTkixUl0

[115] Andreassen, N., Elvegård, R., Villanger, R. & Johnsen, B. H. (2024). Enhancing cognitive motivation: an evaluation model for emergency preparedness exercises, The Learning Organization, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/TLO-06-2023-0100

[116] Elvegård, R., Andreassen, N. & Badu, J. (2024). Building collaboration and trust in emergency preparedness: a model for planning collaboration exercises. Safety in Extreme Environments, Iegūts no https://doi.org/10.1007/s42797-024-00107-w

Kystverket [Norwegian Coastal Administration] (2021). Ledet og deltok på øvelse med fokus på nordområdene, Kystverkets Nyhetsarkiv, 11.01.2021, Iegūts no https://kystverket.no/nyheter/2020/ledet-og-deltok-pa-ovelse-med-fokus-pa-nordomradene2/

Neimane, K., Začs, U., Apalups, K., Andreassen, N., Elvegård, R., Kibsgaard, D., Bambach, B., Goffin, B., Bergman, J., Dorado, X., Garcia, E., Aatsinki, A., Rojas, H. I., Kalesnykas, R. (2024). Recommendations for Higher Education Institutions Teaching Security. Focus on Security Risk Management., SECUREU report, EU Erasmus+, Iegūts no https://security.turiba.lv/recommendations/

KĀ DROŠĪBAS RISKU PĀRVALDĪBA VAR VEICINĀT ORGANIZĀCIJAS NOTURĪBU

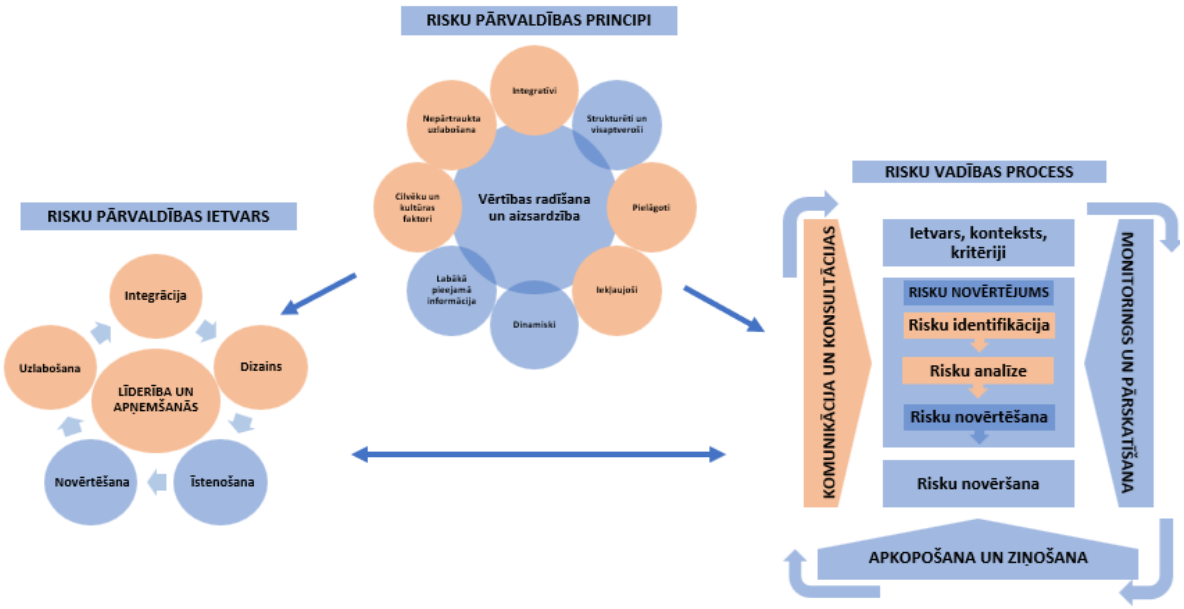
Lambert Bambach / Avans Lietišķo zinātņu universitāte, Nīderlande / 2024

KOPSAVILKUMS

Jūrniecības uzņēmuma vadība apzinās, ka organizācijas noturība, kas ietver darbības nepārtrauktības pārvaldību, prasa vairāk nekā paļaušanos uz procedūrām, lai atgūtu aktīvus. Ko darīt, ja tos nevar atgūt saprātīgā termiņā vai tie nav atgūstami vispār? Vadība vēlas gūt ieskatu soļos, kas nepieciešami, lai nodrošinātu organizācijas noturību. Veiktspējas, pielāgošanās, mācīšanās un reģenerācijas spēju veidošana, kas nodrošinās to, ka organizācija spēs tikt galā ar sarežģītām situācijām (piemēram, pandēmija, klimata pārmaiņas vai kiberuzbrukumi) ir nākotnes atslēga.

Atsauce uz ISO 31000

Uzlabošana, integrācija, līderība un apņemšanās, dizains, cilvēku un kultūras faktori, nepārtraukta uzlabošana, pielāgota, integratīva, iekļaujoša komunikācija un konsultācijas, risku identificēšana un risku analīze.



25. attēls. **Risku pārvaldības ietvars, Risku pārvaldības principi, Risku vadības process saskaņā ar ISO 31000:2018**[117]

[117] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Nīderlandes jūrniecības uzņēmums, kas specializējas bagarēšanas, meliorācijas darbos un mākslīgo salu būvniecībā, ir pieredzējis, ka ar reaktīvu stratēģiju vien nepietiek, lai tiktu galā ar iespējamām pārmaiņām un to pieaugošo tempu, ko rada pēkšņi satricinājumi un nākotnes izaicinājumi. Vadība apzinās, ka organizācijas noturība, kas ietver darbības nepārtrauktības pārvaldību, prasa vairāk nekā paļaušanos uz procedūrām, lai atgūtu aktīvus. Un ko darīt, ja tos nevar atgūt saprātīgā termiņā vai nevar atgūt vispār?

GADĪJUMA IZPĒTE

Uzņēmuma vadība sagaida, ka nākamā krīze varētu ļoti atšķirties no COVID-19 pandēmijas un visdrīzāk nākamajās krīzēs uzņēmumiem varētu nebūt pieejams atbalsts no valsts vai arī tas varētu stipri samazināties. Tāpēc uzņēmumiem ir jāuzņemas lielāka atbildība par savu noturību un jāiegulda nākotnes noturībā.

Uzņēmuma vadība lūdz darbiniekus izpētīt pasākumus, kas ir nepieciešami, lai progresīvā veidā nodrošinātu organizācijas noturību.[118] Piemērotākais nākotnes attīstības modelis varēs balstīties uz veiktspējas, pielāgošanās, mācīšanās un reģenerācijas spēju veidošanu, lai tādējādi nodrošinātu, ka organizācija spēs tikt galā ar sarežģītākiem un smagākiem notikumiem (piemēram, pandēmija, klimata pārmaiņas vai kiberuzbrukumi).

LABĀ PRAKSE

Organizācijas mērķis

Organizācija tiecas uz inovācijām jūrniecības jomā ilgtspējīgai un drošai nākotnei.

Risku novērtējums

Organizācija identificē riskus un pārvērš tos efektīvos un praktiskos risinājumos. Organizācija identificē draudus un riskus drošības risku pārvaldības jomā, kas tieši ietekmē tās primāros procesus. Tāpat tiek analizētas arī tendences draudiem, kas izriet no ģeopolitiskas spriedzes, piemēram, klimata pārmaiņām, kas var netieši ietekmēt organizācijas primāros procesus. Organizācija nepārtraukti uzrauga izvērtējumu, vai organizācijas drošības bāze joprojām ir pietiekama un vai tā ir jākoriģē. Ir svarīgi izstrādāt drošības pasākumu kopumu, lai stiprinātu organizācijas izturību.

Soļi, lai stiprinātu organizācijas noturību

Lai pakāpeniski veicinātu organizācijas noturību, turpmākajā drošības pasākumu izstrādē būtu jāņem vērā šādi soļi.

- **Apspriediet iespējamās nākotnes neveiksmes**

Noturīgas organizācijas atzīst un pieņem, ka to plāni, dizaini un darbības var būt kļūdainas. Šīs organizācijas, vērtējot nākotni un riskus, uzdod sev jautājumu: kā būtu, ja? Kas notis, ja?

[118] Hoge, N. (2024). Why Organizations Need to Measure Resilience. Iegūts no https://www.rmmagazine.com/articles/article/2024/07/09/why-organizations-need-to-measure-resilience

Šīs organizācijas arī neizdara pašapmierinātus pieņēmumus par nākotnes problēmām. Tās vaicā – kas tālāk?

Ar šādu skatījumu uz lietām var ļaut izteikt viedokli darbiniekiem, kurus pretējā gadījumā varētu uzskatīt par negatīviem vai pesimistiem. Tas palīdz mazināt pārmērīgo optimismu par organizācijas drošību. Ja tiek pieņemts, ka incidents jau ir noticis, nevis izliekas, ka tas varētu notikt, cilvēki var spriest daudz reālistiskāk. Turklāt tas palīdz cilvēkiem pārvarēt aklās zonas – liek cilvēkiem redzēt lietas no dažādām perspektīvām, it īpaši, ja kolektīvā ir pietiekama kognitīvā daudzveidība.

- **Izvērtējiet saistītās ietekmes**

Neviena organizācija nav noturīga, ja vien sistēma nav elastīga. Piecu kapitālu modeli[119] var izmantot, lai ļautu organizācijām pārbaudīt piecas saistītās ietekmes katram nopietnam, bet ticamam scenārijam (1. tabula). Modelis var arī palīdzēt organizācijām pārbaudīt to saistīto noturību un apsvērt, kas jādara, lai maksimāli palielinātu piecu kapitālu vērtību, pārvaldītu kompromisus un izvairītos no to novājināšanas. Daudzās organizācijās šīs ietekmes tiek iedalītas sekojoši: cilvēki; reputācija; operacionālās darbības; vide; finanses. Lai gan modelis var palīdzēt pārbaudīt saistīto noturību, ir kļūdaini pieņemt, ka konkrētas problēmas vienā no sadaļām attiecīgi ietekmēs arī citas. Piemēram, ietekme uz reputāciju var būt neparedzama.

1. tabula

Piecu kapitālu modelis[120]

Pieci kapitāli	**"Atslēgas" ietekmes**
Cilvēkkapitāls (piem., prasmes, spējas, pieredze, zināšanas, taktiskās zināšanas)	Ietekme uz cilvēkiem (piem., kaitējums, labklājība, veselības problēmas, prombūtne, darbinieku mainība)
Sociālais kapitāls (piem., sadarbības tīkli, normas, vērtības un izpratne, kas veicina sadarbību un kopienu)	Reputācijas/regulatīvā ietekme (piem., reputācija, uzticība, sūdzības, klientu lojalitāte, regulatīvie sodi, līgumsodi, tirgus integritāte)
Infrastruktūras kapitāls (piem., ēkas, ūdensapgādes sistēmas, ražošanas un pārstrādes rūpnīcas, enerģētika, transports, komunikāciju infrastruktūra, tehnoloģijas)	Operacionālā ietekme (piem., iekārtu dīkstāve, sistēmas traucējumi, jaudas izmantošana, piegāde laikā, ražas zudumi, datu zudumi)
Dabas kapitāls (piem., materiāli, augsne, gaiss, ūdens, augi un dzīvnieki)	Vides ietekme (piem., bioloģiskās daudzveidības zudums, piesārņojums, mežu izciršana)
Finanšu kapitāls (piem., nauda, aktīvi, kredīts un citi līdzekļi, kas veido uzņēmuma finanšu labklājību)	Finansiālā ietekme (piem., rentabilitāte, likviditāte, naudas plūsma, maksātspēja, vērtējums)

- **Izprotiet būtiskos rezultātus (BR)**

Bieži vien noturība tiek uzskatīta par traucējumu neesamību (vai par pieņemamu risku līmeni). Šajā perspektīvā noturība tiek definēta kā stāvoklis, kurā pēc iespējas mazāk lietu "noiet greizi". Būtiski, ka šis uzskats neizskaidro, kāpēc būtiskie rezultāti tiek sasniegti. Alternatīva tradicionālajai pieejai, cenšoties panākt, lai "pēc iespējas mazāk lietu noiet greizi", ir mēģināt panākt, lai "pēc iespējas vairāk lietu tiktu realizētas pareizi".

[119] The Five Capitals - a framework for sustainability. Iegūts no https://www.forumforthefuture.org/the-five-capitals?trk=article-ssr-frontend-pulse_little-text-block

[120] Ibid

Lai gūtu ieskatu organizācijā, kas strādā pēc šāda principa būtisko rezultātu sasniegšanai, var izmantot ceļa kartēšanu (projektēšanu[121]) un noturības plānu[122], iesaistot maksimāli daudzveidīgu komandu. Šādas kartēšanas priekšrocības ir parādītas zemāk 2. tabulā.

2. tabula

Pakalpojumu projektēšanas priekšrocības[123]

Pakalpojumu projektēšanas priekšrocības
Stabilas, kopīgas izpratnes veidošana par būtiskajiem rezultātiem
Veicinošo faktoru apkopošana saskaņotā cēloņsakarības diagrammā
Konkrētu kļūdu / alternatīvu ceļu trūkuma, būtisku saskarņu, kritisko soļu (punktu, no kuriem nav atgriešanās) un darbību risku svarīguma izpēte
Izpētīt, kā faktori ir savstarpēji saistīti
Dažādu pasaules uzskatu un datu no dažādiem avotiem iekļaušana
Iespējas izveidot plašu un vizuāli uzskatāmu skatījumu, ar kuru var dalīties ar kolēģiem
Problēmzonu izcelšana, kas būtu jārisina, lai novērstu incidentu rašanos nākotnē

- **Definējiet noturības slieksni, pamatojoties uz ietekmes tolerances pieeju**

Organizācijas var definēt pašas savus noturības sliekšņus, kas galu galā ietver kvantitatīvu rādītāju noteikšanu izpratnei, kā traucējumi var ietekmēt organizāciju, dažādas klientu grupas un plašāku sektoru un sistēmu. Lai pakāpeniski veicinātu organizācijas noturību, organizācijām ir jāveido ietekmes tolerances pieeja tradicionālās, uz risku balstītās pieejas vietā. Zemāk (3. tabula) ietekmes tolerances pieeja ir salīdzināta ar tradicionālo risku pārvaldības pieeju.

3. tabula

Ietekmes tolerances pieejas salīdzinājums ar tradicionālo risku pārvaldības pieeju

Tradicionālo risku pārvaldības pieeja	**Ietekmes tolerances pieeja**
Pamatā uz iekšieni vērsta perspektīva – ietekme uz organizācijas mērķiem	Pamatā uz āru vērsta perspektīva – ietekme uz ārējām ieinteresētajām personām un plašāku sistēmu
Fokuss uz konkrētiem risku veidiem	Fokuss uz būtiskajiem rezultātiem
Risku klasifikācija: mazs, vidējs, augsts vai smags	Pieļaujamā / pieņemamā sliekšņi
Riska iestāšanās iespējamības vērtēšana	Pieņēmums, ka risks ir iestājies
Definē ietekmi un darbības vai iejaukšanos, kas samazinātu raksturīgo iedarbību	Definē ietekmi un darbības vai iejaukšanos, kas samazinātu raksturīgo iedarbību un atgūšanās faktorus
Bieži lieto tādus vārdus kā "nozīmīgs", "būtisks", "daži", "plašs", "kaitējums", kurus var interpretēt un kurus nevar noteikt kvantitatīvi	Definē skaidrus iznākuma rādītājus

[121] Journey mapping 101: What it is and why it's important. Iegūts no https://www.valtech.com/blog/journey-mapping-101-what-it-is-and-why-its-important/

[122] Gibbon, S. (2017). Service Blueprints: Definition. Iegūts no https://www.nngroup.com/articles/service-blueprints-definition/

[123] Gibbon, S. (2017). Service Blueprints: Definition. Iegūts no https://www.nngroup.com/articles/service-blueprints-definition/

Atjaunināšana un periodiska pārskatīšana (reizi ceturksnī, reizi gadā)	Pastāvīga būtiskā rezultāta uzraudzība un pārskatīšana. Dažās organizācijās tas ietver "tiešsaistes" informācijas ievadīšanu un nemitīgu papildināšanu, lai paredzētu un novērstu traucējumus

- **Balansējiet stratēģiskās izvēles**

Kad būtiskajiem rezultātiem ir noteikti sliekšņi, ir iespējams pārbaudīt katru no šiem rezultātiem un veikt izvēles un izmaiņas, kas var uzlabot noturību. To var darīt, pamatojoties uz četrām noturības intervences izvēlēm un četriem noturības rezultātiem. Četri noturības rezultāti jeb 4R ir: gatavība, reaģētspēja, atveseļošanās un atjaunošanās.

4. tabula

Intervences izvēles un noturības rezultāti

Vadības mehānismi gatavības paaugstināšanai	piem., jauni drošības pasākumi, jauni plāni vai procedūras, jauni rīcības kodeksi, atbilstības nodrošināšana, kļūdu atrašana, uzraudzības palielināšana
Fleksibilitāte reaģētspējas paātrināšanai	piem., palielinātas pilnvaras, daudzveidības radīšana, darbiniekiem dota lielāka elastība, dota iespēja rīkoties, dota rīcības brīvība, komandas darba attīstība un komunikācijas uzlabošana
Optimizācija, lai uzlabotu atveseļošanos	piem., esošo lomu un pienākumu precizēšana, esošo procesu uzlabošana, izmaksu samazināšana, uzraudzības uzlabošana, trūkumu novēršana zināšanās un prasmēs
Inovācijas, lai veicinātu atjaunošanos	piem., drošas telpas eksperimentiem radīšana, neformālu tīklu veidošanās veicināšana, jaunu spēju, resursu un darba veidu attīstīšana, dizaina domāšanas stimulācija

- **Stresa testa sliekšņi**

Organizācijas katru dienu saskaras ar dažādiem mazākiem un lielākiem starpgadījumiem, kas ir jāuztver kā mācību iespējas. Noturīgas organizācijas pārskata savus panākumus un neveiksmes, sistemātiski tās novērtē un piefiksē savu pieredzi formātā, kas ir brīvi pieejams darbiniekiem.[124]

Negadījumi ne tikai rada kaitējumu, pakalpojuma zudumu vai ārkārtas situāciju, bet arī rada pārsteigumu un šoku. Šie incidenti var negatīvi ietekmēt darbinieku un to organizācijas uztveri (piemēram, kas ir drošs, kas ir pieņemams, ētisks, pieļaujams, kāds ir standarts). Tāpēc, lai atgūtos no ekstrēma notikuma, ir nepieciešama "pilnīga kultūras pielāgošana uzskatiem, normām un piesardzības pasākumiem, padarot tos saderīgus ar jauno pasaules izpratni". To var atbalstīt ar adaptīvu vadību[125], izmantojot dizaina domāšanu[126] daudznozaru komandās. Bieži vien starpgadījuma izvērtēšana un mācīšanās no tā beidzas ar pieredzes aprakstīšanu un publicēšanu, ignorējot un neizvērtējot to, kā var šīs gūtās mācības[127] un atziņas reāli pielietot. Neveicot izmaiņas darba veikšanas veidā, pastāv tikai uzlabojumu potenciāls, bet ne reāli uzlabojumi.

[124] Simon, R. (2010). Stress-Test Your Strategy: The 7 Questions to Ask. Iegūts no https://hbr.org/2010/11/stress-test-your-strategy-the-7-questions-to-ask

[125] Michaels, G. (2023). Adaptive leadership: principles and a framework for the future. Iegūts no https://www.atlassian.com/blog/leadership/adaptive-leadership

[126] Linke, R. (2017). Design thinking, explained. Iegūts no https://mitsloan.mit.edu/ideas-made-to-matter/design-thinking-explained

[127] Triple Loop Learning. Iegūts no https://www.thinknpc.org/resource-hub/systems-practice-toolkit/triple-loop-learning/

Standarti

Organizācijas noturības stiprināšanai ir dažādi standarti un normas. Pieci zemāk minētie standarti ir visizplatītākie, ko organizācijas pieņem, lai stiprinātu savu noturību. Ir svarīgi atzīmēt, ka šo standartu ieviešanai jābūt pielāgotai katras organizācijas konkrētajam kontekstam un vajadzībām.

ISO 22301 – starptautiskais darbības nepārtrauktības pārvaldības standarts. Tas nodrošina pamatu dokumentētas sistēmas plānošanai, izveidei, ieviešanai, uzraudzībai, novērtēšanai, uzturēšanai un nepārtrauktai uzlabošanai, lai sagatavotos traucējošiem notikumiem, reaģētu uz tiem un atgūtos no tiem, tiklīdz tie notiek.

ISO 27001 – starptautiskais informācijas drošības pārvaldības standarts. Tas palīdz organizācijām pārvaldīt savu informācijas līdzekļu drošību, piemēram, finanšu informāciju, intelektuālo īpašumu, darbinieku datus vai trešo pušu uzticēto informāciju.[128]

ISO 31000 – starptautiskais risku pārvaldības standarts. Tas nodrošina principus un vadlīnijas efektīvai risku pārvaldībai jebkurā organizācijā neatkarīgi no lieluma, darbības veida vai nozares.[129]

ISO 22316 – organizācijas noturības starptautiskais standarts. Tajā sniegti norādījumi par to, kā uzlabot organizācijas noturību, palielinot tās spēju reaģēt uz izmaiņām un traucējumiem un pielāgoties tām.[130]

ISO 22320 – starptautiskais standarts ārkārtas situāciju pārvaldībai. Tas sniedz norādījumus reaģēšanai uz incidentiem, tostarp incidenta plānošanas, iestatīšanas, vadīšanas, koordinēšanas, izpildes, izbeigšanas un novērtēšanas aspektus.[131]

Drošības risku pārvaldības ieguldījums, lai atbalstītu darbības, kas palīdz nodrošināt noturību organizācijā

Drošības risku pārvaldība var atbalstīt pasākumus, lai nodrošinātu noturību organizācijā. Tā var palīdzēt radīt domāšanu, kura nepieļauj to, ka noturības veidošana ir vienreizējs pasākums.[132] Noturība ir mērķis, kas pastāvīgi mainās, reaģējot uz mainīgajām prasībām saistībā ar organizācijas darbību un mainīgajiem apstākļiem, ar kuriem tā saskaras attiecībā uz tās būtiskajiem rezultātiem. Atbalstot domāšanu par noturību, drošības risku pārvaldība var izmantot tālāk izskaidrotos sešus soļus[133] un ar tiem saistītos jautājumus (5. tabula).

Lai progresētu noturības veicināšanā, organizācijai jāseko tabulā skaidrotajām vadības un menedžmenta darbībām. Šo darbību veikšana var palīdzēt veicināt pielāgošanās, mācīšanās un reģenerācijas spējas, lai nodrošinātu to, ka organizācija spēj tikt galā ar sarežģītākiem notikumiem (piemēram, pandēmija, klimata pārmaiņas vai kiberuzbrukumi)

---

[128] ISO 27001. What is ISO 27001? A detailed and straightforward guide. Iegūts no https://advisera.com/27001academy/what-is-iso-27001/

[129] ISO 31000. Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

[130] ISO 22316. Security and Resilience. Iegūts no https://www.bsigroup.com/en-AE/industries-and-sectors/Government/ISO-22316-Security-and-Resilience/

[131] ISO 22320. Security and resilience — Emergency management — Guidelines for incident management. Iegūts no https://www.iso.org/standard/67851.html

[132] Hoge, N. (2024). Why Organizations Need to Measure Resilience. Iegūts no https://www.rmmagazine.com/articles/article/2024/07/09/why-organizations-need-to-measure-resilience

[133] Resilience Reimagined: A practical guide for organisations. Iegūts no https://www.deloitte.com/uk/en/services/risk-advisory/research/resilience-reimagined-a-practical-guide-for-organisations.html

5. tabula

Soļi, kas palīdz nodrošināt noturību organizācijā

Diskutējiet par neveiksmi, izvairieties no ieslīgšanas "pašapmierinātībā", iedarbiniet organizācijā "nākotnes domāšanu". Vaicājiet "Ja nu...?", "Ko pēc tam?" Mudiniet cilvēkus izteikties.	**Izvērtējiet savstarpējo saistītu** starp "pieciem kapitāliem", lai izprastu traucējumu iespējamo ietekmi uz ieinteresētajām personām, organizāciju un plašāku sabiedrību.	**Saprotiet, kas ir svarīgi** ieinteresētajām personām un sabiedrībai. Kas ir "būtiskie rezultāti", kuri prasa augstu noturības pakāpi.	**Nosakiet ietekmes sliekšņus** "būtiskajiem rezultātiem", lai noteiktu pieļaujamos ierobežojumus, kurus nevajadzētu pārkāpt, ņemot vērā ietekmi uz "pieciem kapitāliem".	**Izdariet stratēģisku izvēli** attiecībā uz noturības intervencēm, līdzsvarojot kontroli, elastību, efektivitāti un inovācijas.	**Veiciet stresa testu,** lai noteiktu, vai spējat ievērot ietekmes sliekšņus neatkarīgi no apdraudējuma.
Kādi ir jūsu darbinieku uzskati par neveiksmēm?	Kādu ieguldījumu organizācijas uzlabotā noturība dos jūsu nozares, kopienas un sabiedrības vispārējai noturībai?	Kā "būtiskie rezultāti" tiek sasniegti?	Kas veidotu nepanesamu ietekmi uz "būtiskajiem rezultātiem"?	Cik progresīvs vai aizsargājošs (konservatīvs) domāšanas veids ir organizācijā?	Kā tiks sasniegti "būtiskie rezultāti" stresa vai traucējumu laikā?
Vai darbinieki atklāti apspriež nākotnes iespējamās neveiksmes, iespējamās problēmas un kļūdas?	Kā organizācijas darbība vai bezdarbība varētu ietekmēt "piecus kapitālus" tagad un nākotnē (daba, cilvēks, sociālais kapitāls, infrastruktūra un finanses)?	Kas varētu kavēt "būtisko rezultātu" sasniegšanu vai atgūšanos, lai tos sasniegtu?	Kā "būtisko rezultātu" darbības traucējumi ietekmētu dažādas klientu grupas, organizāciju un plašāku sektora sistēmu?	Cik elastīgs vai konsekvents ir organizācijas dizains attiecībā uz noturību?	Kādas garantijas jums ir, ka alternatīvi līdzekļi un neparedzēti apstākļi ļaus jums izpildīt "būtiskos rezultātus", ievērojot ietekmes toleranci smagos, bet ticamos scenārijos?
Vai un kā darbiniekiem tiek uzdots pamanīt izaicinājumus, izmaiņas vai potenciālus traucējumus pie apvāršņa?		Vai "būtiskie rezultāti" var tikt sasniegti alternatīvos veidos?		Kā jūs līdzsvarojat spriedzi un izmantojat domāšanas veidu "gan/un"?	Kā jūs pārbaudīsit nākotnes iespējas un izvēles, kuras jums vajadzētu (vai nevajadzētu) izdarīt šodien? Kā šīs izvēles varētu ierobežot jūsu iespējas dažus gadus vēlāk?
Kuras nākotnes tendences organizācijai varētu sniegt jaunas iespējas? Kādas priekšrocības jūs varētu attīstīt?		Vai mums ir pietiekama elastība, lai nodrošinātu "būtisko rezultātu" sasniegšanu pat smagos vai ekstremālos scenārijos?		Kādi papildu ieguldījumi ir nepieciešami, lai "būtiskos rezultātus" uzturētu pieļaujamās pielaides robežās?	

Izmantotie avoti

Gibbon, S. (2017). Service Blueprints: Definition. Iegūts no https://www.nngroup.com/articles/service-blueprints-definition/

Hoge, N. (2024). Why Organizations Need to Measure Resilience. Iegūts no https://www.rmmagazine.com/articles/article/2024/07/09/why-organizations-need-to-measure-resilience

ISO 31000. Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

ISO 22301, Security and resilience — Business continuity management systems — Requirements. Iegūts no https://www.iso.org/standard/75106.html

ISO 22316. Security and Resilience. Iegūts no https://www.bsigroup.com/en-AE/industries-and-sectors/Government/ISO-22316-Security-and-Resilience/

ISO 22320. Security and resilience — Emergency management — Guidelines for incident management. Iegūts no https://www.iso.org/standard/67851.html

ISO 27001. What is ISO 27001? A detailed and straightforward guide. Iegūts no https://advisera.com/27001academy/what-is-iso-27001/

Journey mapping 101: What it is and why it's important. Iegūts no https://www.valtech.com/blog/journey-mapping-101-what-it-is-and-why-its-important/

Linke, R. (2017). Design thinking, explained. Iegūts no https://mitsloan.mit.edu/ideas-made-to-matter/design-thinking-explained

Michaels, G. (2023). Adaptive leadership: principles and a framework for the future. Iegūts no https://www.atlassian.com/blog/leadership/adaptive-leadership

Resilience Reimagined: A practical guide for organisations. Iegūts no https://www.deloitte.com/uk/en/services/risk-advisory/research/resilience-reimagined-a-practical-guide-for-organisations.html

Simon, R. (2010). Stress-Test Your Strategy: The 7 Questions to Ask. Iegūts no https://hbr.org/2010/11/stress-test-your-strategy-the-7-questions-to-ask

The Five Capitals – a framework for sustainability. Iegūts no https://www.forumforthefuture.org/the-five-capitals?trk=article-ssr-frontend-pulse_little-text-block

Triple Loop Learning. Iegūts no https://www.thinknpc.org/resource-hub/systems-practice-toolkit/triple-loop-learning/

MI DROŠĪBAS IZAICINĀJUMS UN RISKU NOVĒRTĒJUMS, IZMANTOJOT ISO 31000: IOTSI VADLĪNIJAS

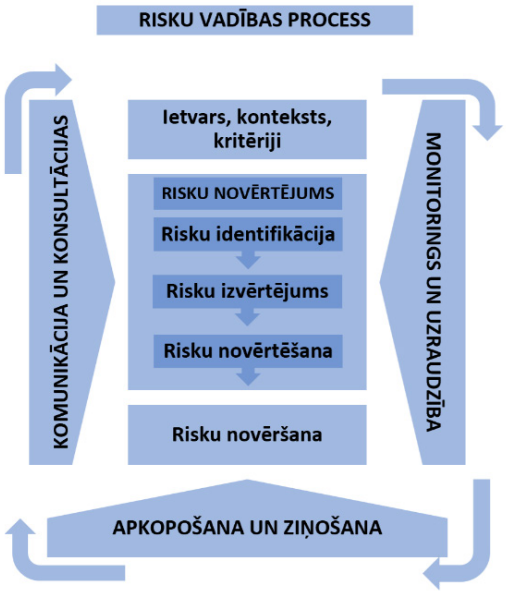
Rita Lankauskiene/ Kazimiras Simonavičius Universitāte, Lietuva /2024

KOPSAVILKUMS

Ģeneratīvā mākslīgā intelekta (MI) tehnoloģiju izmantošana dažādās nozarēs sniedz būtiskas priekšrocības, vienlaikus radot sarežģītas drošības problēmas. Šo risku efektīva pārvaldība ir būtiska, lai saglabātu MI sistēmu integritāti, uzticamību un drošību. ISO 31000 standarts piedāvā sistemātisku metodiku risku pārvaldībai, ko var pielāgot īpašām MI drošības prasībām. Šajā rakstā ir izklāstītas jaunās kiberdrošības problēmas, kuru pamatā ir MI izaicinājumi, kas rodas sakarā ar neprognozējami straujo lietu interneta (IoT) nozares paplašināšanos, ko paātrina digitālā transformācija. Pamatojoties uz Lietu interneta drošības institūta (IoTSI) paraugpraksi, ir sniegts soli pa solim skaidrojums par to, kā MI drošības risku novērtējumā izmantot ISO 31000 standartu, ietverot visaptverošas metodes, tehnisko analīzi un ilustratīvus piemērus.

Atsauce uz ISO 31000

Šajā rakstā ir apskatīta ISO 31000 standarta sistemātiskās metodoloģijas un procesu ietvara pielietošana ģeneratīvā mākslīgā intelekta drošības risku novērtējumam organizācijās.



26. attēls. **Risku pārvaldības ietvars, risku pārvaldības principi, risku vadības process saskaņā ar ISO 31000:2018**[134]

[134] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

IEVADS

Jaunās tehnoloģijas ar ģeneratīvo mākslīgo intelektu (MI) priekšgalā ir plaši atzītas par nozīmīgiem digitālās transformācijas un inovāciju katalizatoriem visā pasaulē.[135] Ir savākti daudzi pierādījumi, kas parāda milzīgos ieguvumus, kas rodas no dažādu MI rīku lietošanas dažādās cilvēku darbības jomās un tehnoloģiju attīstībā (piemēram*, Ghobakhloo, et al.*, 2024[136]; *Kanbach, et al.*, 2024[137]; *Sedkaoui & Benaichouba*, 2024[138]).

Straujā mākslīgā intelekta tehnoloģiju attīstība un plašā radošo MI risinājumu izmantošana izraisa jaunu risku veidu strauju parādīšanos, kas vēl vairāk palielina MI izveidē un ieviešanā jau tā sarežģīto procesu neparedzamību.[139] Pieaugošais incidentu skaits,[140,141] ko izraisa mākslīgā intelekta (ne)lietošana, arvien vairāk apgrūtina plašu ieinteresēto personu loku no visas sabiedrības, organizācijām un valdībām dažādā – valsts, starptautiskā un globālā līmenī.[142]

Lai ierobežotu mākslīgā intelekta negatīvo ietekmi, tiek īstenotas daudzas iniciatīvas starptautiskā, kā arī globālā mērogā, sākot no risku pārvaldības standartiem un normatīvajiem regulējumiem līdz vadlīnijām, kas veicina uzticamu izstrādi un izmantošanu. Viens no aktuālākajiem nesen izdotajiem normatīvajiem regulējumiem Eiropā ir *Eiropas Komisijas Mākslīgā intelekta likums*.[143] Šis likums ir pasaulē pirmais visaptverošais MI tiesiskais regulējums. Noteikumu mērķis ir veicināt uzticamu MI lietošanu Eiropā un ārpus tās, lai garantētu, ka MI sistēmas atbilst pamattiesībām, drošībai un ētikas standartiem, novēršot riskus, kas saistīti ar ārkārtīgi spēcīgiem un nozīmīgiem MI modeļiem.

MI likuma galvenais priekšnoteikums ir tas, ka likums garantē eiropiešiem pārliecību par MI potenciālu. Dažas mākslīgā intelekta sistēmas rada riskus, kas jāpārvalda, lai novērstu nelabvēlīgas sekas, pat ja lielākā daļa MI sistēmu ir ar zemu riska pakāpi vai bez riska un var palīdzēt atrisināt daudzas sociālas problēmas. Piemēram, bieži vien nav iespējams noteikt MI sistēmas lēmuma, prognozes vai darbības pamatojumu. Tāpēc noteikt, vai kāds ir nonācis netaisnīgi nelabvēlīgā situācijā –, piemēram, pieņemot lēmumu par nodarbinātību vai piesakoties sabiedriskā labuma programmai, – var kļūt sarežģīti.

Pat ja pašreizējie likumi piedāvā zināmu aizsardzību, ar tiem nepietiek, lai risinātu unikālas grūtības, ko var radīt MI sistēmas. MI likums ir labi zināms, jo tas regulē mākslīgā intelekta izstrādi un piemērošanu sistēmās uz risku orientētā veidā. Ieviešot riska pārvaldības sistēmu riska noteikšanai, analīzei, novērtēšanai un novēršanai, risku pārvaldības prakse cenšas novērst galvenās nenoteiktības.

---

135 Thorat, S. R., Tingare, B. A., Deshmukh, S. R., Dabhade, V. D., William, P., Rakshe, D. S. & Verma, A. (2024). Analysis Of Generative Ai's Impact On Industry 4.0 And Digital Transformation. *Library Progress International*, 44 (3), 13379.–13390.

136 Ghobakhloo, M., Fathi, M., Iranmanesh, M., Vilkas, M., Grybauskas, A. & Amran, A. (2024). Generative artificial intelligence in manufacturing: opportunities for actualizing Industry 5.0 sustainability goals. *Journal of Manufacturing Technology Management*, 35 (9), 94.–121.

137 Kanbach, D. K., Heiduk, L., Blueher, G., Schreiter, M. & Lahmann, A. (2024). The GenAI is out of the bottle: generative artificial intelligence from a business model innovation perspective. *Review of Managerial Science*, 18 (4), 1189.–1220.

138 Sedkaoui, S. & Benaichouba, R. (2024). Generative AI as a transformative force for innovation: a review of opportunities, applications and challenges. *European Journal of Innovation Management*, Vol. ahead-of-print No. ahead-of-print. Iegūts no https://doi.org/10.1108/EJIM-02-2024-0129

139 Golpayegani, D., Pandit, H. J. & Lewis, D. (2022). Airo: An ontology for representing AI risks based on the proposed EU AI act and ISO Risk management standards. In: *Towards a Knowledge-Aware AI* (pp. 51.-65.). IOS Press

140 AI Incident Database (2024). Iegūts no https://incidentdatabase.ai/

141 AIAAIC – AI, Algorithmic and Automation Incident and Controversy Repository (2024). Iegūts no https://www.aiaaic.org/home

142 Herani, R. & Angela, J. (2024). Navigating ChatGPT: catalyst or challenge for Indonesian youth in digital entrepreneurship?. *Journal of Entrepreneurship in Emerging Economies*. Vol. ahead-of-print No. ahead-of-print. Iegūts no https://doi.org/10.1108/JEEE-05-2024-0181

143 AI Act (2019). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

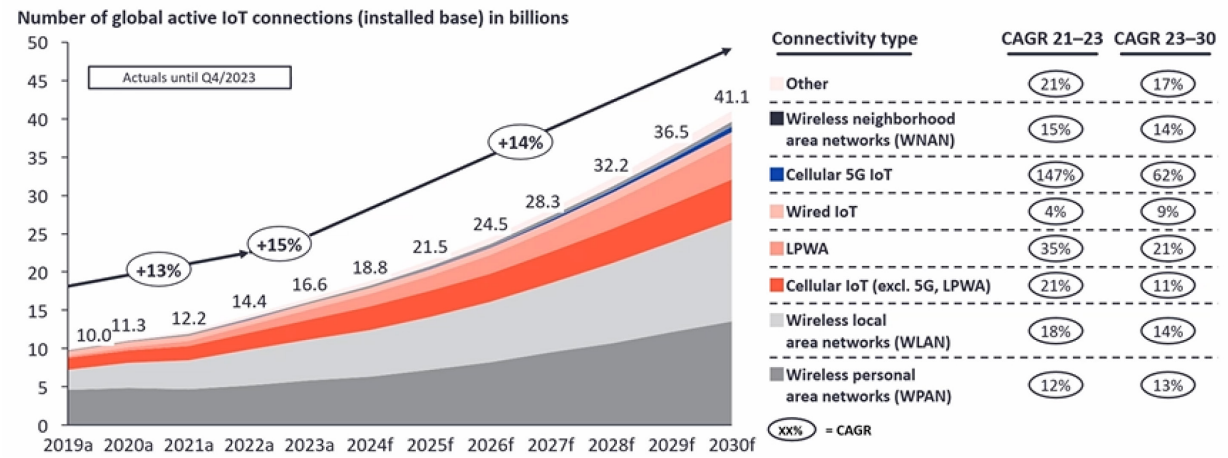
Šajā gadījumā MI sistēmu nenoteiktība un to briesmas ir jārisina, ievērojot ISO risku pārvaldības standartus. Ir apkopoti pierādījumi par to, kā droša un uzticama MI sistēmu izstrāde un izmantošana ir atkarīga no ISO 31000 pareizas ieviešanas jebkura uzņēmuma risku pārvaldības darbībās.

ISO 31000 standarts piedāvā darbības, vadlīnijas un principus, lai palīdzētu organizācijām pārvaldīt riskus. Primārais standarts, kas piedāvā vispārīgas vadlīnijas, ietvaru un procedūras tādu risku pārvaldībai, ar kuriem organizācijas saskaras sava dzīves cikla laikā, ir ISO 31000:2018 Risku pārvaldība – vadlīnijas[144]. Vēl viens būtisks šīs saimes loceklis ir ISO 31073:2022 Riska pārvaldība – vārdnīca[145], kas nodrošina vienotu izpratni dažādās biznesa struktūrvienībās un organizācijās. ISO 31073:2022 piedāvā vispārīgu risku pārvaldības terminu sarakstu kopā ar to nozīmi.

Šajā rakstā ir sniegti Lietu interneta Drošības institūta (IoTSI) izstrādāti norādījumi par paraugpraksi, kā ieviest soli pa solim MI drošības risku novērtēšanas procedūru organizācijā, izmantojot ISO31000 sistēmu.

GADĪJUMA IZPĒTE

Digitālās transformācijas rezultātā strauji un neprognozējami paplašinās Lietu interneta (IoT) nozare. Arvien vairāk ierīču kļūst savienotas un nodrošina jaunas funkcijas un lielākas ērtības gan personiskajā, gan profesionālajā jomā. Saskaņā ar IoT *Analytics*[146] datiem līdz 2023. gada beigām bija pieslēgti 16,6 miljardi IoT ierīču, un tas ir par 15 % vairāk nekā 2022. gadā. Līdz 2024. gada beigām IoT *Analytics* prognozē, ka šie skaitļi pieaugs par 13 % līdz 18,8 miljardiem un arī turpinās pieaugt (skat. 27. attēlu).



27. attēls. **Lietu interneta savienojumi, *pēc IoT Analytics* datiem**[147]

Līdzās pieaugošajam IoT ierīču un sistēmu skaitam pieaug arī to sarežģītība un izsmalcinātība, piedāvājot daudzas priekšrocības dažādām nozarēm, piemēram, ražošanai, veselības aprūpei, viedajām pilsētām, mājas automatizācijai un daudzām citām nozarēm (skat. 28. attēlu).

144 ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html
145 ISO 31073, Risk Management – Vocabulary (2022). Iegūts no https://www.iso.org/obp/ui/en/
146 IoT Analytics. State of IoT, Summer 2024. Market Report. Iegūts no https://iot-analytics.com/product/state-of-iot-summer-2024/
147 Ibid

28. attēls. **Lietu interneta (IoT) lietojumprogrammu jomas – MI drošības izaicinājumi**[148]

Tajā pašā laikā IoT lietojumu jomas un plaši izplatītā MI tehnoloģiju ieviešana daudzās nozarēs sniedz būtiskas priekšrocības, vienlaikus radot sarežģītas drošības problēmas. Saskaņā ar labo praksi šajā jomā iepriekš aprakstītās drošības problēmas ir veiksmīgi pārvaldāmas, ievērojot ISO 31000 standartu saimē iestrādātos principus.

Saistībā ar jautājuma pieaugošo sarežģītību ir izveidota īpaša akadēmiskās un kibernozares domnīca – Lietu interneta drošības institūts.[149] Šī domnīca ir vērsta uz drošības sistēmu, mācību resursu un kiberdrošības kursu izstrādi un pasniegšanu, lai veicinātu paraugpraksi drošības pārvaldībā viedo tehnoloģiju, lietu interneta un Inteliģentā lietu interneta ekosistēmās.

IoTSI iesaka izmantot ISO 31000 standarta sistemātisku risku pārvaldības sistēmu, kas var būt labi pielāgota konkrētām MI drošības prasībām. Tālāk ir detalizēti aprakstīts, kā piemērot uz ISO 31000 balstītu metodoloģiju MI drošības risku novērtēšanai, ietverot visaptverošas metodes, tehnisko analīzi un ilustratīvus piemērus.

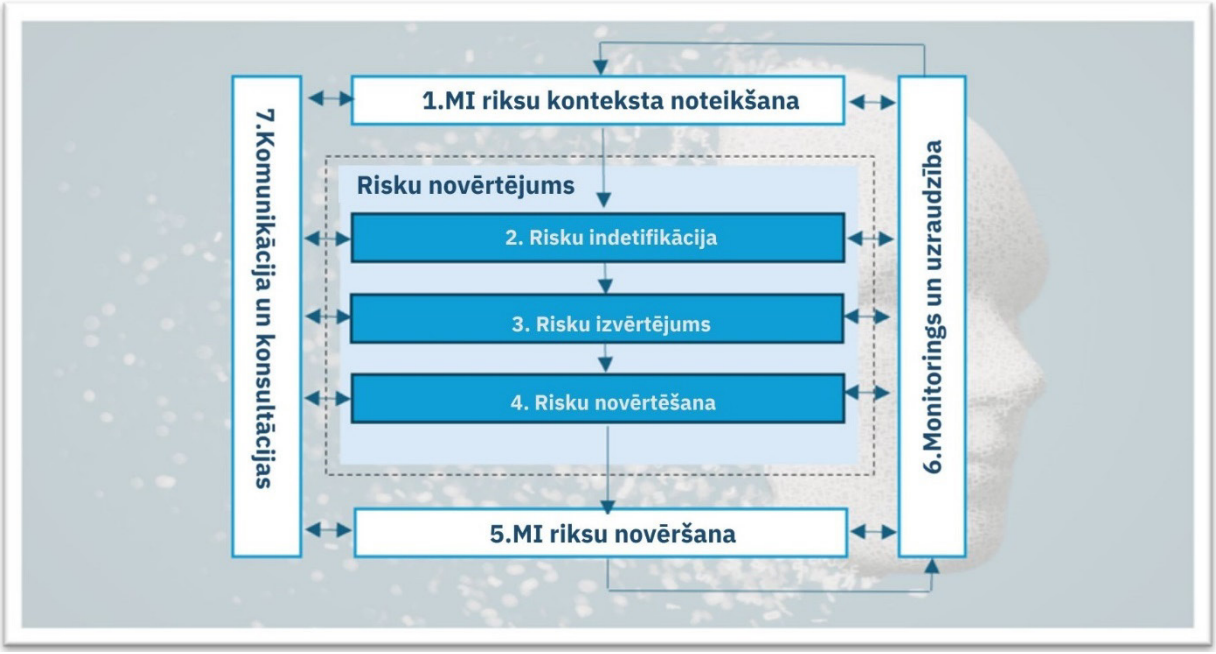
[148] Petrov, Ch. (2024). 26 Insightful Internet of Things Statistics 2024. Techjury.net. Iegūts no https://techjury.net/blog/internet-of-things-statistics/

[149] IoTSI (Internet of Things Security Institute) (2024). Iegūts no https://iotsecurityinstitute.com/iotsec/index.php/about

LABĀ PRAKSE

ISO 31000 ir starptautisks standarts, kas nosaka risku pārvaldības vadlīnijas, lai garantētu, ka riski tiek konsekventi un sistemātiski pārvaldīti visos organizācijas līmeņos.[150] Tas ietver trīs primāros elementus: 1) principus; 2) ietvaru un 3) procesu. Ietvars nodrošina ieviešanas strukturālos elementus, principi nodrošina, ka risku pārvaldība ir lēmumu pieņemšanas sastāvdaļa un rada pievienoto vērtību, un process ietver risku identificēšanas, novērtēšanas un mazināšanas pasākumus.

Saskaņā ar IoTSI norādījumiem MI drošības risku novērtējums, izmantojot ISO 31000, ir pakāpeniska procedūra, kas sastāv no vairākām papildu darbībām (skat. 29. attēlu).



29. attēls. **MI drošības risku novērtējums, izmantojot ISO 31000**[151]

Konteksta noteikšana

ISO 31000 procesa pirmais solis ir konteksta izveide, kas nodrošina nepieciešamo fonu, lai izprastu vidi, kurā darbojas MI sistēma. Ir jāapsver vide no diviem galvenajiem kontekstiem: no ārējā un iekšējā.

Vērtējot iekšējo kontekstu, ir jākoncentrējas uz trīs galvenajām lietām:

1) normatīvā aina – atrodiet noteikumus un likumus, kas attiecas uz datu apstrādi, privātumu un drošību, piemēram, GDPR (Vispārīgā datu aizsardzības regula), CCPA (Kalifornijas Patērētāju Privātuma Likums, attiecas uz ASV) un HIPAA (Veselības apdrošināšanas pārnesamības un atbildības likums, arī ASV teritorijā). Piemēram, GDPR noteikumi ir jāievēro jebkurai MI sistēmai, kas apstrādā personas datus Eiropas Savienībā;
2) tirgus un tehnoloģiju tendences – uzziniet par izmaiņām tirgū un tehnoloģijās, kas var ietekmēt MI sistēmas drošību. Piemēram, ja uzlabojas uzbrukuma metodes, iespējams, būs jāatjaunina aizsardzība;

[150] ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. Iegūts no https://www.iso.org/iso-31000-risk-management.html

[151] Adaptēts no AI security risk assessment using ISO 31000 (2024). IoTSI. Iegūts no https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/155-conducting-an-ai-security-risk-assessment-using-iso-31000

3) draudu ainava – apskatiet pašreizējo bīstamības ainavu. Tajā jāiekļauj uz šo brīdi zināmie kiberdraudi, kas vērsti uz MI sistēmām, piemēram, datu saindēšanās vai modeļu inversijas uzbrukumi.

Ārējais konteksts attiecas uz šādām galvenajām tēmām:

4) organizatoriskā struktūra — noskaidrojiet, kurš par ko ir atbildīgs, kad runa ir par MI sistēmu pārvaldību un aizsardzību. Atrodiet svarīgos cilvēkus, piemēram, IT, juridiskās, drošības un biznesa vienības;
5) risku pārvaldības politikas — pārbaudiet pašreizējās risku pārvaldības politikas, lai redzētu, vai tās atbilst riskiem, kas saistīti ar MI un ISO 31000 noteikumiem;
6) riska apetīte un tolerance – nosakiet uzņēmuma riska apetītes un tolerances līmeņus, īpaši, ja runa ir par sistēmas drošību, datu pārkāpumiem un intelektuālā īpašuma zādzībām.

Kad vides konteksts ir izveidots, ir jādefinē risku kritēriji. Jums vajadzētu izdomāt konkrētus veidus, kā novērtēt riskus. Piemēram, vispirms varat definēt ietekmes rādītājus, piemēram, finansiālus zaudējumus, kaitējumu reputācijai, darbības traucējumus un juridiskās sekas. Pēc tam apsveriet iespējamības rādītājus, tostarp draudu rašanās biežumu, ievainojamības izmantojamību un kontroles efektivitāti. Un visbeidzot – ir nepieciešams noteikt riska kategoriju, t.i., zemu, vidēju un augstu, pamatojoties uz iepriekš minēto, – to ietekmi un iespējamību.

MI risku novērtēšanas procedūra

Nākamais solis ir MI risku novērtējums (skat. 29. attēlu), kas sastāv no vairākām komponentēm. ISO 31000 ir uzskaitīti trīs galvenie risku novērtēšanas soļi: risku identificēšana, risku izvērtējums un risku novērtēšana. Šīs daļas mērķis ir pilnībā izprast visus iespējamos draudus un vājās vietas MI sistēmā.

MI risku indetifikācija

Risku identificēšanas posmā ir jāņem vērā visi iespējamie riska avoti, tostarp datu riski, modeļu riski un darbības riski.

Datu riski sastāv no datu pārkāpumiem, datu sabojāšanas un datu integritātes. Datu pārkāpumi ir saistīti ar nesankcionētu piekļuvi privātiem vai slepeniem datiem, kas var izraisīt naudas sodu un uzticības zaudēšanu. Datu sabojāšana ir datu uzlaušana, lai mainītu MI modeļa darbību. Piemēram, mainīt surogātpasta bloķētāja precizitāti, pievienojot nepatiesus datus tā apmācības komplektam. Datu integritāte ir riski, kas izriet no datu pareizības un pamatīguma, kas var ietekmēt to, cik labi un uzticami darbojas MI modelis.

Modeļa riski ietver dažādus uzbrukumus, modeļu zādzību un modeļu neobjektivitāti. Uzbrukumi izraisa izmaiņas ievades datos, kuru mērķis ir apmānīt MI modeli, piemēram, attēlu maiņa, lai piespiestu attēlu atpazīšanas sistēmu pieņemt nepareizus lēmumus. Modeļu zagšana notiek, ja hakeri bez atļaujas var iekļūt MI modeļa struktūrā vai iestatījumos, kas var izraisīt intelektuālā īpašuma zādzību vai konkurējošu modeļu izveidi. Modeļa novirze kļūst aktuāla, jo MI modeļos var būt neparedzētas novirzes, kas var novest pie negodīgiem rezultātiem. Tas ir īpaši svarīgi tādās jutīgās jomās kā aizdevumi vai pieņemšana darbā.

Operacionālie riski iekļauj sistēmas kļūmes, drošības konfigurāciju un trešo pušu riskus. Sistēmas kļūmes rodas no aparatūras vai programmatūras problēmām, kas var apturēt MI sistēmas darbību. Drošības konfigurācija rada problēmas ar MI sistēmas drošību, piemēram, nepietiekamas piekļuves kontroles vai nepilnības, kas nav novērstas, kas var ielaist uzbrucējus. Savukārt trešo pušu riskus

rada pārdevēji vai trešo pušu pakalpojumi, piemēram, mākoņpakalpojumu sniedzēji, kas var padarīt datus mazāk drošus un sistēmas mazāk pieejamas.

MI risku izvērtējums

Risku izvērtējuma būtība ir rūpīgi aplūkot katru risku, ko esat atradis iepriekšējā posmā, lai uzzinātu, kas tas ir, kā tas var jūs ietekmēt, un cik iespējams, ka tas varētu notikt. Tas nozīmē veikt ietekmes novērtējumu un iespējamības novērtējumu. Labākā IoTSI prakse iesaka novērtēt riskus, izmantojot gan skaitliskās, gan kvalitatīvās metodes.

Ietekmes novērtējuma laikā vispirms apsveriet finansiālo ietekmi, noskaidrojot, cik daudz datu aizsardzības pārkāpumi varētu izmaksāt naudas sodos, tiesas nodevās un problēmu novēršanas ziņā. Pēc tam apsveriet darbības ietekmi, t.i., padomājiet par to, kā sistēmas dīkstāve, lietderības zudums un izmaiņas biznesa procesos var ietekmēt situāciju. Un visbeidzot – analizējiet ietekmi uz reputāciju, apsverot, kā tas ilgtermiņā ietekmēs uzņēmuma reputāciju, klientu uzticību un pozīciju tirgū.

Iespējamības novērtējumā, pirmkārt, apsveriet vēsturiskos datus, aplūkojot pagātnes notikumus un vājās vietas, lai noskaidrotu, cik liela ir iespējamība, ka tie atkārtosies. Pēc tam veiciet ievainojamības analīzi, novērtējot MI sistēmas pakļaušanu identificētiem draudiem, ņemot vērā tādus faktorus kā sistēmas sarežģītība un esošo drošības pasākumu noturība. Tad analizējiet apdraudējuma dalībnieku spējas, t.i., novērtējiet potenciālo uzbrucēju, piemēram, hakeru, ļaunprātīgu iekšējo personu vai konkurentu spējas un motivāciju. Piemēram, lai novērtētu pretinieku uzbrukumu bīstamību sensoru datiem uz mākslīgo intelektu balstītā autonomā automašīnas sistēmā, ņemiet vērā ietekmi uz pasažieru drošību un sistēmas uzticamību.

MI risku novērtēšana

Sekojošā risku novērtēšanas procedūra tiek īstenota, sarindojot riskus un salīdzinot izpētītos ar noteiktajiem risku standartiem. Tas palīdz izlemt, kur likt resursus un kādi riski ir vissvarīgākie.

IoTSI labākā prakse iesaka izmantot risku matricu, lai sašķirotu riskus grupās, pamatojoties uz to rašanās iespējamību un iespējamo risku. Šis vizuālais rīks palīdz sakārtot riskus svarīguma secībā un izdarīt saprātīgu izvēli, kā novērst riskus. Lēmumu pieņemšana būs efektīvāka, iesaistot visus, lai noskaidrotu, kādi riska apmēri ir pieņemami un kā noteikt risku prioritātes. Pieņemot lēmumus, cilvēkiem var nākties izsvērt briesmu samazināšanas izmaksas un ieguvumus.

Risku novēršana

Risku novēršana ir process, kurā tiek izvēlēti un īstenoti veidi, kā mainīt draudošās briesmas. ISO 31000 standarts skaidro, ka tas var nozīmēt izvairīšanos no riskiem, to samazināšanu vai risku uzņemšanos.

Lai vadītu procesu, ir jāizstrādā risku novēršanas plāni. Katram nozīmīgam riskam ir jāizstrādā rūpīgs riska novēršanas pasākums. Izmantojot labāko praksi, katrā plānā ir jādefinē mērķis, darbības un resursi, kā arī jāsadala pienākumi. Mērķim ir skaidri jādefinē, kas ir paredzēts konkrētai darbībai, piemēram, datu noplūdes riska samazināšana vai naidīgu uzbrukumu ietekmes vājināšana. Darbības ir jāprecizē, lai informētu cilvēkus par to, kas viņiem jādara. Piemēram, jāievieš

vairāku faktoru pieteikšanās, jāšifrē dati vai jāveic regulāras drošības pārbaudes. Risku novēršanas pasākumi ir jānodrošina ar saprātīgiem resursiem, personālu un tehnoloģijām, lai tos varētu īstenotu. Katrā plānā ir skaidri jānosaka atbildība par novēršanas plāna izpildi, atbildības un uzraudzības nodrošināšanu.

Riska novēršanas plāna piemērs: lai mazinātu modeļa novirzes risku, novēršanas plāns var ietvert apmācības datu dažādošanu, taisnīguma metrikas piemērošanu un regulāru auditu veikšanu, lai identificētu un labotu novirzes.

Nākamais solis ir risku novēršanas plāna iedzīvināšana un pārliecināšanās, ka šis plāns ir daļa no organizācijas darbības un pārvaldības.

Tehniskās kontroles parasti tiek veiktas, izmantojot augsto tehnoloģiju drošības rīkus, piemēram, šifrēšanu, ugunsmūrus, ielaušanās atklāšanas sistēmas un programmas, kas meklē dīvainas darbības. Procedūru kontrole tiek nodrošināta, izveidojot vai uzlabojot procesus datu pārvaldībai, kontrolējot, kas tos var redzēt, un reaģējot uz incidentiem. Piemēram, iestatot veidu, kā katru dienu pārbaudīt un atjaunināt drošības ielāpus. Organizatoriskās kontroles ir veltītas drošības izpratnes veidošanai, izmantojot apmācības programmas, kampaņas un nodrošinot IT un biznesa vienību sadarbību.

Risku novēršanas plāna īstenošanas piemērs: nulles uzticamības drošības sistēmas izveide mākslīgā intelekta vadītam mākoņpakalpojumam, iekļaujot stingrus piekļuves ierobežojumus, pastāvīgu uzraudzību un auditu.

Monitorings un uzraudzība

Ir nepieciešamas regulāras pārbaudes un pastāvīga uzraudzība, lai nodrošinātu, ka risku pārvaldības metodes turpina darboties, un varētu pielāgoties jauniem riskiem.

Pirmkārt, labā prakse uzsver nepieciešamību izveidot veidu, kā visu laiku sekot līdzi MI sistēmai un tās infrastruktūrai, lai varētu ātri pamanīt un risināt jaunus riskus. Drošības informācijas un notikumu pārvaldības (*Security Information and Event Management,* SIEM) risinājumi tiek izmantoti, lai apkopotu un pētītu datus par drošību, reāllaikā nosūtot brīdinājumus par iespējamiem drošības incidentiem. Vēl viena būtiska daļa ir modeļa uzraudzība, lai nepārtraukti uzraudzītu MI modeļa veiktspēju, lai atrastu "dīvainas" lietas, piemēram, izvades modeļus, kuriem nav jēgas, kas varētu liecināt par uzbrukumu vai modeļa maiņu. Turklāt incidentu pārvaldība tiek izmantota, lai iestatītu incidentu reaģēšanas plānus ar lomām, saziņas kanāliem un atkopšanas darbībām, lai ātri risinātu drošības incidentus.

Nepārtrauktas uzraudzības piemērs: uz MI balstītu uzraudzības rīku izmantošana, lai atrastu “dīvainas” tendences saistībā ar piekļuvi finanšu datiem MI sistēmā, var nozīmēt, ka pastāv draudi no uzņēmuma iekšpuses vai ārpus uzņēmuma.

Lai nodrošinātu labi funkcionējošu uzraudzības sistēmu, ir nepieciešamas periodiskas pārbaudes. Labās prakses pieeja ir bieži pārskatīt risku novēršanas plānus un riska pārvaldības procesu, lai pārliecinātos, ka tie joprojām ir noderīgi un efektīvi. Tam ir paredzēti iekšējie auditi, scenāriju analīze un ieinteresēto pušu iesaistīšana. Ieteicams veikt iekšējos auditus, lai noskaidrotu, vai risku pārvaldības metodes ir adekvātas un darbojas labi. Tas ietver pārbaudi, vai tiek ievēroti uzņēmuma noteikumi un politika. Scenāriju analīze ir noderīga, lai pārbaudītu, cik labi MI sistēma var tikt galā ar izdomātiem draudiem, piemēram, koordinētu kiberuzbrukumu vai lielu datu pārkāpumu. Uzņēmumam ir svarīgi veikt scenāriju analīzi. Ieinteresēto pušu iesaistīšana ir noderīga monitoringā:

sarunas ar ieinteresētajām personām palīdz pārskatīt risku pārvaldības rezultātus, veikt izmaiņas risku faktoros un uzlabot risku novēršanas plānus.

Periodiskas pārskatīšanas piemērs: MI vadīta veselības aprūpes diagnostikas instrumenta risku novērtējuma izvērtēšana un pārskatīšana, ievērojot jaunākās regulatīvās direktīvas par pacientu datu privātumu.

Komunikācija un konsultācijas

Efektīva komunikācija un konsultācijas ir būtiskas ISO 31000 procesa sastāvdaļas, kas garantē pārredzamību un ieinteresēto pušu iesaisti. Labā prakse šajā jomā pieprasa ņemt vērā gan iekšējo, gan ārējo komunikāciju.

Iekšējā komunikācija attiecas uz risku pārvaldības darbībām un rezultātiem, kas regulāri jānokomunicē visām iekšējām ieinteresētajām personām, kurām tas ir jāzina, piemēram, direktoru padomei, vadībai un operatīvajiem darbiniekiem. Ziņošana ir nepieciešama, lai sniegtu rūpīgus ziņojumus par incidentiem, risku novērtējumiem un centieniem samazināt riskus. Labā prakse paredz iekļaut svarīgus rādītājus, piemēram, riska līmeni, kontroles mehānismu darbību un atbilstības stāvokli. Iekšējā komunikācija ir saistīta ar apmācību un informētību. Ir nepieciešams regulāri mācīt personālu par drošības labo praksi, jauniem draudiem un to, kā tie var palīdzēt kontrolēt riskus.

Iekšējās komunikācijas piemērs: sanāksmju rīkošana inženieriem un datu zinātniekiem, lai runātu par drošiem veidiem, kā veidot MI un cik svarīgi ir domāt par datu kvalitāti un ētiku.

Ārējā komunikācija tiek izmantota, lai informētu ārējās grupas, piemēram, klientus, partnerus un regulējošās iestādes par centieniem pārvarēt riskus un ievērot noteikumus. Ir svarīgi ņemt vērā caurspīdīguma principu, t.i., skaidri noteikt MI sistēmas drošības pasākumus, jo īpaši attiecībā uz privātumu un datu aizsardzību. Vēl viena svarīga sastāvdaļa ir ziņošana par incidentiem. Jāizstrādā noteikumi, kā par tiem ziņot regulatoriem un drošības incidentu skartajiem cilvēkiem, pārliecinoties, ka informācija tiek sniegta pareizi un laikā.

Ārējās komunikācijas piemērs: pēc drošības pārkāpuma patērētāju lietotnē, ko vada MI, ir jāsniedz publisks paziņojums, izskaidrojot darbības, kas tika veiktas, lai aizsargātu lietotāja datus un apturētu turpmākos pārkāpumus.

Apkopošana un ziņošana

Lai nodrošinātu atbildību, atvērtību un pastāvīgu izaugsmi, ir svarīgi veikt detalizētu uzskaiti un pārskatus. Dokumentācija ir pirmais svarīgais komponents. Labā prakse iesaka pierakstīt visu, ko darāt risku pārvaldības procesa laikā, piemēram, risku identificēšanu, to analīzi, novēršanas plānu sastādīšanu un novērošanu. Lai izveidotu ierakstu pārvaldību, ir jāiestata ierakstu pārvaldības metode, lai uzglabātu un sakārtotu dokumentus, lai tos būtu viegli atrast un lai ievērotu likumus. Revīzijas pēdas tiek izmantotas, lai saglabātu pilnīgu visu risku pārvaldības darbību uzskaiti, piemēram, izdarītajām izvēlēm, veiktajām darbībām un sasniegtajiem rezultātiem, lai tos varētu viegli pārbaudīt.

Dokumentācijas piemērs: izstrādājiet visaptverošu dokumentāciju par MI sistēmas risku novērtēšanas procedūru, kas ietver datu avotus, risku kritērijus, analītiskās metodes un mazināšanas iespējas.

Atskaites pamatā ir regulāru ziņojumu sagatavošana: periodiskie ziņojumi un atbilstības ziņojumi. Tos izmanto, lai informētu ieinteresētās personas par MI drošības risku pārvaldības statusu. Ieteicams regulāri sagatavot pārskatus, kuros apkopoti svarīgākie riski, kā tie tiek pārvaldīti, un drošības notikumi, tostarp mērījumi un tendences, lai iegūtu pilnīgu priekšstatu par risku. Atbilstības pārskati palīdz nodrošināt to, ka tiek sekots noteikumiem un regulējumam.

Pārskatu sniegšanas piemērs: ikgadēja risku pārvaldības ziņojuma izstrādāšana mākslīgā intelekta vadītai finanšu sistēmai, uzsverot nozīmīgos riskus, kontroles efektivitāti un uzlabošanas iespējas.

Rezumējot – IoTSI piedāvātā labā prakse MI drošības risku novērtēšanai, izmantojot ISO 31000, ir piemērota vairāku iemeslu dēļ. ISO 31000 sistēma piedāvā visaptverošu un metodisku stratēģiju, lai novērstu atsevišķus drošības apdraudējumus, kas saistīti ar MI sistēmām. Organizācijas var samazināt iespējamās briesmas, garantēt atbilstību normatīvajiem aktiem un aizsargāt savus MI aktīvus, ievērojot disciplinētu pieeju, kas ietver konteksta noteikšanu, riska novērtējumu veikšanu, novēršanas plānu izpildi un regulāru uzraudzību un pārskatīšanu. Efektīva komunikācija un visaptveroša dokumentācija uzlabo MI drošības risku pārvaldības caurspīdīgumu, atbildību un pastāvīgus uzlabojumus. Attīstoties MI tehnoloģijām un ar tām saistītajiem riskiem, uzņēmumiem būs obligāti jāievieš visaptveroša risku pārvaldības sistēma, piemēram, ISO 31000, lai efektīvi orientētos sarežģītajā MI drošības vidē.

Izmantotie avoti

AI Act (2019). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Iegūts no https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

AI Incident Database (2024). Iegūts no https://incidentdatabase.ai/

AIAAIC – AI, Algorithmic and Automation Incident and Controversy Repository (2024). Iegūts no https://www.aia-aic.org/home

Conducting an AI security risk assessment using ISO 31000 (2024). IoTSI. Iegūts no https://iotsecurityinsti-tute.com/iotsec/index.php/iot-security-institute-blog/155-conducting-an-ai-security-risk-assessment-using-iso-31000

Ghobakhloo, M., Fathi, M., Iranmanesh, M., Vilkas, M., Grybauskas, A. & Amran, A. (2024). Generative artificial intelligence in manufacturing: opportunities for actualizing Industry 5.0 sustainability goals. *Journal of Manufacturing Technology Manage-ment*, 35 (9), 94.–121.

Golpayegani, D., Pandit, H. J. & Lewis, D. (2022). Airo: An ontology for representing AI risks based on the proposed EU AI act and ISO Risk management standards. In Towards a Knowledge-Aware AI (pp. 51.-65.). IOS Press

Herani, R. & Angela, J. (2024). Navigating ChatGPT: catalyst or challenge for Indonesian youth in digital entrepreneurship? *Journal of Entrepreneurship in Emerging Economies*. Vol. ahead-of-print No. ahead-of-print. Iegūts no https://doi.org/10.1108/JEEE-05-2024-0181

IoT Analytics. State of IoT, Summer 2024. Market Report. Iegūts no https://iot-analytics.com/product/state-of-iot-summer-2024/

IoTSI (Internet of Things Security Institute) (2024). Iegūts no https://iotsecurityinstitute.com/iotsec/index.php/about

ISO 31000:2018. Risk management – Guidelines (2018). Iegūts no https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

ISO 31073:2022 Risk Management – Vocabulary (2022). Iegūts no https://www.iso.org/obp/ui/en/

Kanbach, D. K., Heiduk, L., Blueher, G., Schreiter, M. & Lahmann, A. (2024). The GenAI is out of the bottle: generative artificial intelligence from a business model innovation perspective. *Review of Managerial Science*, 18 (4), 1189.–1220.

Petrov, Ch. (2024). 26 Insightful Internet of Things Statistics 2024. Techjury.net. Iegūts no https://techjury.net/blog/inter-net-of-things-statistics/

Sedkaoui, S. & Benaichouba, R. (2024). Generative AI as a transformative force for innovation: a review of opportunities, applications and challenges. *European Journal of Innovation Management*, Vol. ahead-of-print No. ahead-of-print. Iegūts no https://doi.org/10.1108/EJIM-02-2024-0129

Thorat, S. R., Tingare, B. A., Deshmukh, S. R., Dabhade, V. D., William, P., Rakshe, D. S. & Verma, A. (2024). Analysis Of Generative Ai's Impact On Industry 4.0 And Digital Transformation. *Library Progress International*, 44 (3), 13379.–13390.

PRAKTISKIE UZDEVUMI

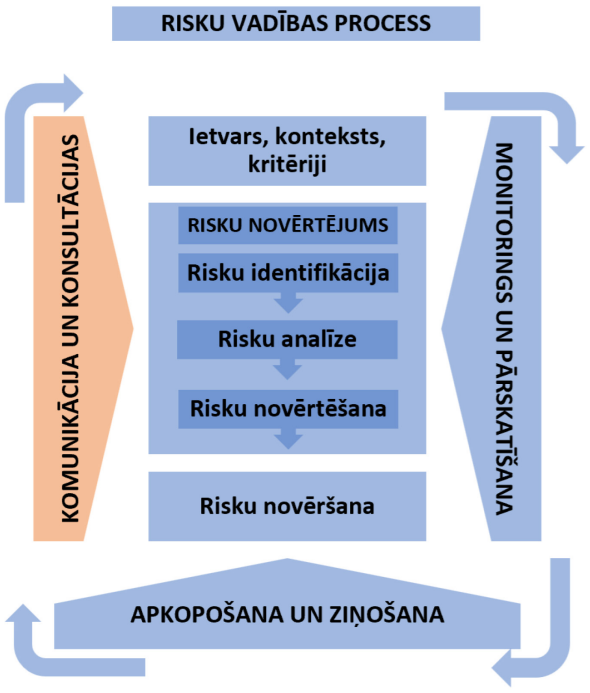
ZINĀŠANU UN IZPRATNES VEICINĀŠANA PAR DROŠĪBAS JAUTĀJUMIEM SABIEDRĪBĀ, ORGANIZĀCIJĀS UN UZŅĒMUMOS

1. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORI: Uģis Začs, Kristīne Neimane, Biznesa augstskola *Turība*, Latvija

Konteksts

Sešu valstu eksperti 2022. gada nogalē veiktajā pētījumā uzsvēra, ka drošības speciālistiem trūkst zināšanu un prasmju informēt un skaidrot drošības jautājumus un drošības risku nozīmi gan saviem kolēģiem, gan sabiedrībai kopumā. Skaidrs, ka bez kolēģu izpratnes un iesaistes drošības nodrošināšana organizācijā vai uzņēmumā kļūst neiespējama. Ja uzņēmuma darbinieki neapzinās drošības nozīmi, būs grūti identificēt un efektīvi pārvaldīt riskus. Tāpēc viens no drošības speciālista uzdevumiem organizācijā vai uzņēmumā ir informēt, izglītot un iesaistīt kolēģus drošības risku identificēšanā un pārvaldībā. Ar pilnu ziņojumu var iepazīties šeit (angļu valodā): https://security.turiba.lv/2022/12/06/what-skills-young-security-specialists-are-missing/

ATSAUCE UZ ISO 31000 STANDARTU Saskaņā ar ISO 31000 standartu komunikācijai ir ārkārtīgi liela nozīme efektīvā risku pārvaldībā. Komunikācijai ir izšķiroša nozīme visos risku pārvaldības procesa posmos, tostarp risku identificēšanā, novērtēšanā, novēršanā un uzraudzībā.	

Uzdevuma mērķis

Sniegt prasmes un iemaņas izstrādāt, formulēt un sagatavot informāciju par drošību un drošības risku pārvaldību organizācijā. Attīstīt prasmes dažāda veida informatīvo materiālu veidošanā kolēģiem, organizācijas vai uzņēmuma darbiniekiem, vai plašākai sabiedrībai.

UZDEVUMS STUDENTIEM

1. Individuāli vai grupās izvēlieties mērķa grupu, kurai tiks veidots informatīvais materiāls par drošības risku pārvaldību. Tas var būt reāls vai izdomāts uzņēmums vai organizācija (mikrouzņēmums, MVU, sabiedriska organizācija, izglītības iestāde u.c.), vai sabiedrības grupa (piemēram, bērni, jaunieši, skolotāji, seniori, kādā jomā nodarbinātie u.c.):
   a) ja izvēlaties uzņēmumu – skaidri definējiet uzņēmuma darbības jomu;
   b) ja izvēlaties konkrētu sabiedrības grupu – definējiet ietvaru (vecums, dzimums, dzīvesvieta);
   c) maksimāli skaidri analizējiet un aprakstiet savu mērķgrupu (tos, ko vēlaties informēt) – definējiet pamata parametrus (vecums, dzimums, dzīvesvieta) un citus mērķgrupu raksturojošos parametrus: kādas ir to intereses, bažas, vajadzības, izmantotie saziņas un informācijas saņemšanas kanāli.
2. Studentu uzdevums ir izstrādāt īsu informatīvu materiālu (1–2 A4 lapas), kas izskaidro izvēlēto drošības vai drošības risku pārvaldības aspektu.
3. Svarīgi veidot informatīvu materiālu, kas ir saprotams, viegli uztverams un vizuāli pievilcīgs. Materiāla izveidei iesakām izmantot vizuālās rediģēšanas rīkus, piemēram, *Canva*, *Infogram* vai *Piktochart*. *Canva* piedāvā arī izveidoto materiālu bezmaksas lejupielādi. *Infogram* bez maksas izveidoto materiālu varēsiet izplatīt digitāli, piemēram, *Facebook* vai *Instagram*. Iesācēju apmācību videoklipus varat atrast vietnē *YouTube*: https://www.youtube.com/playlist?list=PLATYfhN6gQz8GiTG_nUxVar8ycrt9hJxL
4. Prezentējiet savu materiālu un izskaidrojiet tajā ietverto informāciju – kāpēc izvēlēta tieši šī mērķa grupa, kāpēc materiālā iekļautā informācija ir svarīga konkrētai mērķa grupai un kādas zināšanas mērķa grupa iegūs, iepazīstoties ar informatīvo materiālu.

Zemāk pievienots ilustratīvs piemērs. Piemērs izveidots, izmantojot infogram.com.

UZDEVUMS PASNIEDZĒJIEM

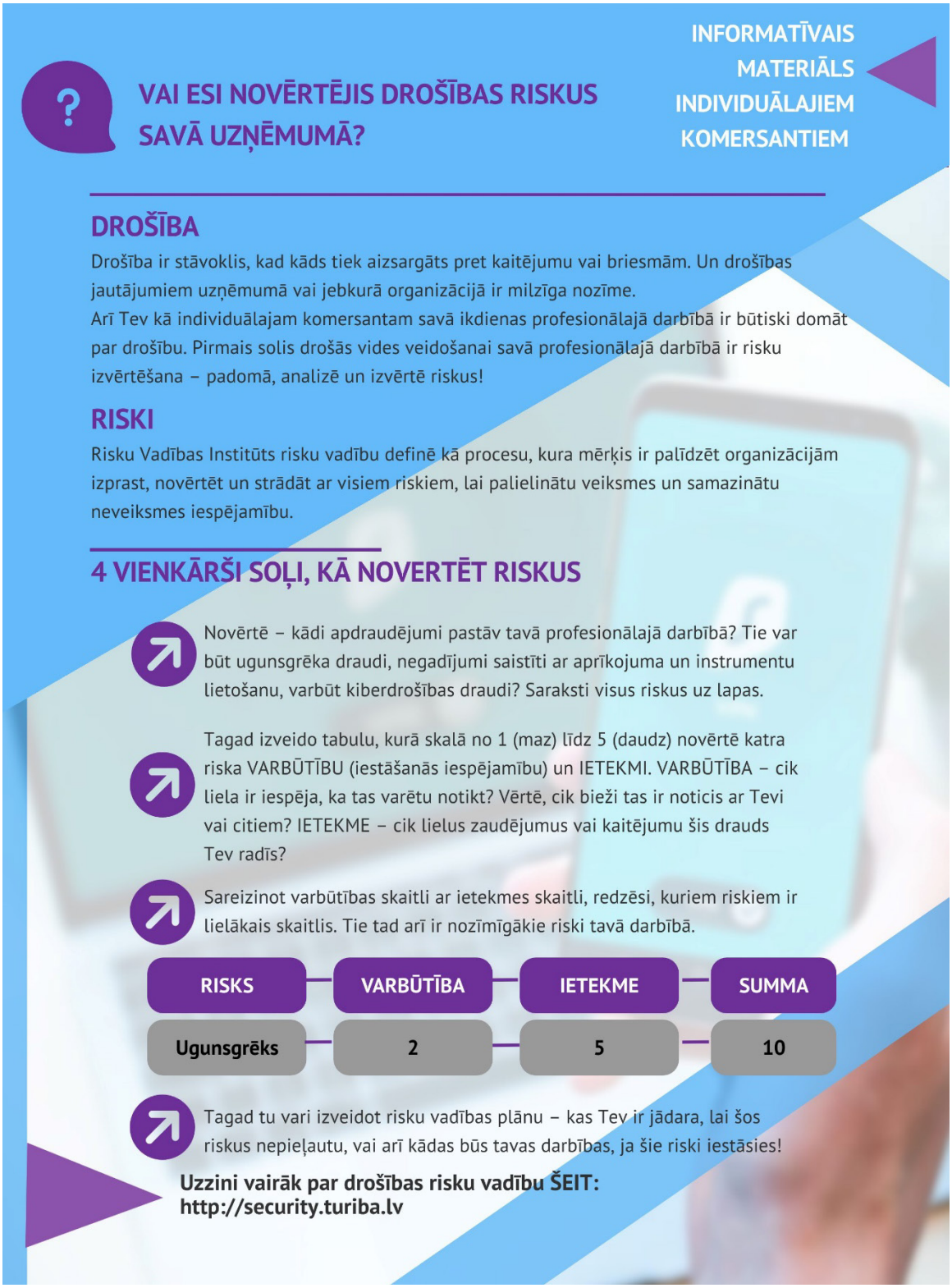
1. Izveidojiet studentu grupas (ieteicams ne vairāk kā četri cilvēki vienā grupā).
2. Izskaidrojiet uzdevumu studentiem, uzsverot, cik svarīgi ir attīstīt prasmes efektīvi nodot drošības informāciju kolēģiem un sabiedrībai. Ieteicams prezentēt pētījumu par jauno drošības speciālistu prasmēm, pētījuma rezultāti pieejami šeit: https://security.turiba.lv/2022/12/06/what-skills-young-security-specialists-are-missing/.
3. Palīdziet studentiem izvēlēties mērķa grupu un informatīvā materiāla fokusu. Ja nepieciešams, sniedziet piemērus un norādījumus.
4. Ja studentiem trūkst pieredzes un prasmju izmantot vizualizācijas rīkus, piemēram, *Canva*, *Infogram* vai *Piktochart*, sniedziet ievadu un pamatapmācību par kādu no šiem vizuālās rediģēšanas rīkiem.

5. Izvērtējiet studentu izstrādātos informatīvos materiālus un pārrunājiet to saturu, sniedzot ieteikumus uzlabojumiem. Īpaši pievērsiet uzmanību, vai studenti ir izpratuši un pietiekami detalizēti analizējuši mērķgrupu un tās vajadzības.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Spēja strādāt komandā; prasmes formulēt informāciju un viedokli, digitālās prasmes (vizuālās rediģēšanas prasmes).

Piemērs



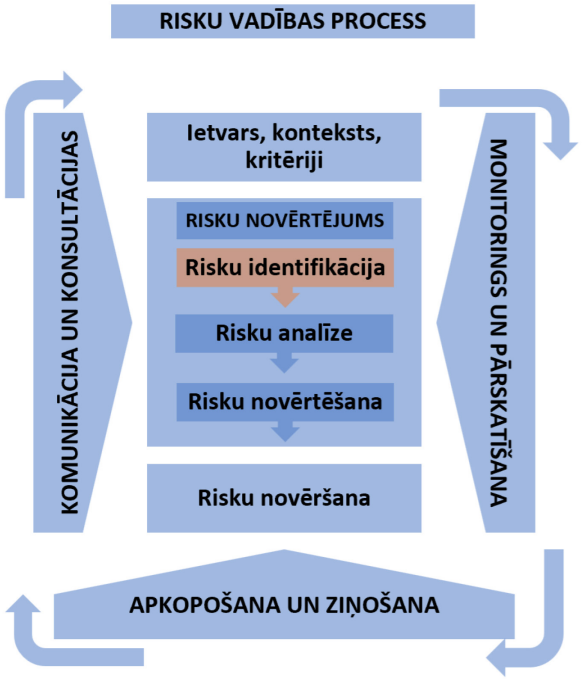
RISKU IDENTIFIKĀCIJAS RĪKI

2. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORI: Kaci Bourdache, Hanna Iisakkila Rojas, Laurea Lietišķo zinātņu universitāte, Somija

Konteksts

Risku vadība prasa rūpīgu risku identificēšanu kā vienu no pirmajiem procesa soļiem, kā aprakstīts ISO 31000:2018 standartā. Atkarībā no riska vadības konteksta un mērķiem ir jāizvēlas vispiemērotākās metodes konkrētai situācijai.

ATSAUCE ISO 31000 STANDARTU Saskaņā ar ISO 31000 standartu risku identificēšana ir pirmais solis risku novērtēšanas procesā.	

Uzdevuma mērķis

Ar šī uzdevuma palīdzību studenti iepazīsies ar dažādām risku identificēšanas metodēm no IEC (Starptautiskā elektrotehnikas komisija) 31010:2019 standarta, pārbaudīs dažas no tām un veiks dažādu metožu salīdzināšanu un to pielietojumu risku pārvaldībā.

UZDEVUMS STUDENTIEM

1. Izveidojiet grupas saskaņā ar pasniedzēja norādījumiem.
2. Katrai grupai ir dota viena metode, kas piemērojama risku identificēšanai saskaņā ar IEC 31010:2019 standartu.
3. Pasniedzēja vadībā definējiet fizisko mērķi, piemēram, ēku vai telpas, vai tās daļu. Mērķim ir jābūt, piemēram, ofisa telpām, skolām, tirdzniecības ēkām, darba vietām, noliktavām utt.
4. Iepazīstieties ar jums piešķirto metodi un sagatavojiet īsu šīs metodes prezentāciju saviem kursa biedriem.
5. Izmantojiet norādīto metodi, lai identificētu jūsu mērķa drošības riskus. Papildus mērķa telpām, īpašumam un cilvēkiem izpētiet, kādas darbības tiek veiktas tajās.
6. Pierakstiet savus izpētes rezultātus saskaņā ar pasniedzēja norādījumiem. Sagatavojieties iepazīstināt kursabiedrus ar savu pētāmo mērķi un iegūtajiem rezultātiem.
7. Prezentējiet kursa biedriem metodi (ko izpētījāt 4. solī), noteikto mērķi un risku identifikācijas rezultātus (ko veicāt 6. solī).
8. Noklausieties savu kursa biedru prezentācijas. Pēc katras prezentācijas savas grupas ietvaros 2 minūtes pārrunājiet dzirdēto. Izvērtējiet, vai prezentācijā izskaidrotā metode būtu piemērota arī jūsu mērķim. Dalieties savās domās ar kursabiedriem. Vai šī metode sniegtu jums atšķirīgus rezultātus?
9. Pēc visām prezentācijām pārrunājiet savā grupā, kura no piedāvātajām metodēm būtu vislabākā jūsu mērķim. Dalieties savās domās ar kursabiedriem.

UZDEVUMS PASNIEDZĒJIEM

1. Pirms nodarbības aprēķiniet studentu skaitu un to, cik grupas izveidosiet (ieteicamais studentu skaits grupā – četri cilvēki). Izlemiet, kādu metodi vēlaties tiem piešķirt.
2. Pirms nodarbības katrai grupai izvēlieties vienu metodi, kas piemērojama risku identificēšanai no IEC 31010:2019 sadaļas "B.2 Riska identificēšanas paņēmieni" (skatiet metožu aprakstus pielikumā).
3. Pēc jūsu izvēles:
   - ja vēlaties, lai identifikācijas uzdevums tiktu veikts klasē, varat studentiem izsniegt rasējumus un citu informāciju par mērķiem. Studenti var izmantot arī tiešsaistes informāciju, piemēram, *Google Maps*, *Google Earth* utt.;
   - ja vēlaties, lai uzdevums tiktu veikts fiziskā vidē, pārliecinieties, ka jums ir piekļuve atbilstošajām izvēlētajām telpām. Varat arī iepriekš sadalīt telpas grupām.
4. Sadaliet studentus grupās pa aptuveni četriem cilvēkiem.
5. Piešķiriet katrai grupai vienu no metodēm no IEC 31010:2019 standarta.
6. Katrai studentu grupai jābūt fiziskam mērķim, piemēram, ēkai vai telpām, vai to daļai. Mērķim ir jābūt, piemēram, ofisa telpām, skolām, tirdzniecības ēkām, darba vietām, noliktavām utt. Varat tās piešķirt pats vai ļaut izlemt studentiem pašiem. Jebkurā gadījumā ir ieteicams apstiprināt katru mērķi, lai tie būtu piemēroti uzdevumam.
7. Uzdodiet studentiem iepazīties ar viņiem piešķirto metodi un sagatavot īsu šīs metodes prezentāciju saviem kolēģiem. Jūs varat izlemt par prezentācijas veidu. Ieteicams ierobežot prezentāciju līdz 5 minūtēm.

8. Uzdodiet studentiem izmantot viņiem piešķirto metodi, lai identificētu drošības riskus savam mērķim. Papildus mērķa telpām, īpašumiem un cilvēkiem viņiem ir jāizpēta, kādas darbības tiek veiktas šajās mērķa telpās. Risku identifikāciju var veikt kā grupu darbu, izmantojot informāciju par mērķi, vai kā fizisku uzdevumu uz vietas – vai jebkuru abu metožu kombināciju.
9. Uzdodiet studentiem pierakstīt savus risku identifikācijas rezultātus. To var izdarīt, piemēram, uz lapām, tāfeles, *PowerPoint* prezentācijas formā, tiešsaistes vidē utt. Uzdodiet studentiem uzdevumu sagatavoties prezentēt savu mērķi un rezultātus kursa biedriem. Jūs varat izlemt par prezentācijas veidu. Ieteicams ierobežot prezentāciju līdz 5 minūtēm.
10. Kamēr studenti gatavo metodes prezentāciju, identificē riskus un gatavo rezultātu prezentāciju, jūsu uzdevums ir atvieglot viņu darbu un palīdzēt, ja viņiem rodas jautājumi, piemēram, par metodi un tās izmantošanu.
11. Uzdodiet studentiem iepazīstināt kursabiedrus ar savu metodi, noteikto mērķi un risku identificēšanas rezultātiem.
12. Prezentāciju laikā vadiet diskusiju un kontrolējiet laiku. Process ir šāds:
    - aptuvenais laiks – 10 minūtes vienai grupas prezentācijai;
    - pēc katras prezentācijas grupām ir dotas 2 minūtes apspriedei savā starpā. Grupām ir jāizvērtē, vai prezentētā metode būtu piemērota viņu mērķim;
    - grupas tiek mudinātas dalīties savās domās. Galvenais jautājums ir: vai metode sniegtu jums atšķirīgus rezultātus?
13. Pēc visām prezentācijām veidojiet diskusiju par to, kura no piedāvātajām metodēm būtu vislabākā attiecīgajiem mērķiem.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

- Spēja strādāt komandā
- Spēja strādāt ierobežotā laikā
- Prezentācijas prasmes un spēja pamatot savu viedokli
- Spēja salīdzināt informāciju un kritiski domāt

PIELIKUMS

IEC 31010 standarta Riska identificēšanas paņēmieni (B.2. sadaļa)

Lai izvēlētos, kuru no metodēm piešķirt katrai no studentu grupām, šeit tiek sniegts neliels ieskats par risku identificēšanas metodēm.

1. Vispārīga pieeja riska identificēšanā

ISO 31010 izceļ vairākas metodes, kas var tikt izmantotas risku identificēšanā, lai aptvertu pēc iespējas plašāku spektru. Šīs metodes ietver:

1. **Pierādījumos balstītas metodes**
   - Šīs metodes izmanto literatūras pārskatus vai vēsturisko datu analīzi, lai identificētu riskus, kas balstīti uz iepriekšējo pieredzi.
   - Piemērs: analizēt iepriekšējo incidentu ziņojumus, lai identificētu līdzīgus draudus.
2. **Empīriskās metodes**
   - Šīs metodes balstās uz testēšanu un modelēšanu, lai noteiktu, kas varētu notikt noteiktos apstākļos.
   - Piemērs: veikt simulācijas, lai novērtētu sistēmas reakciju uz pārslodzi.
3. **Uztveres aptaujas (*Perception surveys*)**
   - Šīs aptaujas apkopo pieredzējušu cilvēku viedokļus par iespējamiem riskiem.
   - Piemērs: organizēt aptaujas starp darbiniekiem, lai noskaidrotu viņu bažas par iespējamiem drošības jautājumiem.
4. **Sistēmiskas metodes**
   - Šīs metodes sadala apskatāmo jautājumu mazākos elementos un analizē tos, uzdodot "Kas būtu, ja...?" jautājumus.
   - Piemēri:
     - *HAZOP* (B.2.4): koncentrējas uz potenciālām kļūdām procesā;
     - *FMEA* (B.2.3): analizē, kā sistēmas kļūdas varētu ietekmēt rezultātus;
     - *SWIFT* (B.2.6): strukturēts grupas process ar "Kas būtu, ja...?" pieeju.
5. **Radošās domāšanas metodes**
   - Šīs metodes veicina iztēles izmantošanu, lai prognozētu nākotnē iespējamās situācijas.
   - Piemērs: scenāriju analīze (B.2.5), kas paredz nākotnes scenārijus, lai identificētu iespējamos riskus.
6. **Kontrolsaraksti vai taksonomijas**
   - Balstīti uz iepriekšējiem datiem vai teorētiskiem modeļiem, lai strukturēti identificētu riskus.
   - Piemērs: PESTLE analīze (politiskie, ekonomiskie, sociālie, tehnoloģiskie, juridiskie, vides faktori).

2. Kontrolsaraksti, klasifikācijas un taksonomijas

Šīs metodes piedāvā sistemātisku pieeju riska identificēšanai, klasificēšanai un analīzei.

Vairāk par SWOT, PESTLE, PMESII-PT, FMEA un scenāriju analīzes metodēm skaties Raimundas Kalesnikas video lekcijā: "Hibrīddraudi drošības risku vadības procesā". Seko saitei QR kodā:

1. **Pārskats**
   - Kontrolsaraksti ir noderīgi, lai strukturētu risku identificēšanu un analīzi.
   - Taksonomijas un tipoloģijas grupē riskus, balstoties uz kopīgām īpašībām.
   - Piemērs: SWOT analīze (Stiprās, Vājās puses, Iespējas, Draudi).
2. **Izmantošana**
   - Var izmantot stratēģiskā vai operatīvā līmenī.
   - Piemēram, PESTLE analīze ir noderīga, lai apsvērtu politiskos, ekonomiskos vai tehnoloģiskos faktorus, kas var ietekmēt riskus.
3. **Ieguvumi**
   - Veicina vienotu izpratni par riskiem starp iesaistītajām pusēm.
   - Ļauj izmantot plašu pieredzi vienkāršā veidā, kas pieejams ne tikai ekspertiem.
   - Nepiemēroti jaunos vai unikālos apstākļos.
   - Koncentrējas uz zināmo, kas var radīt risku, ka nezināmi riski tiek ignorēti.
4. **Rezultāti**
   - Iegūtie rezultāti ir kontrolsaraksti vai riska klasifikācijas, kas veicina labāku riska izpratni.

3. Strukturētas tehnikas

Strukturētas pieejas, piemēram, *HAZOP*, *FMEA* un *SWIFT*, palīdz sistemātiski identificēt riskus, izmantojot definētas darbības. Šīs metodes ir īpaši piemērotas, lai nodrošinātu, ka netiek izlaisti svarīgi riski.

- ***FMEA* (*Failure Modes and Effects Analysis*)**

FMEA ir metode, kas koncentrējas uz sistēmas kļūmju identificēšanu un to ietekmes analīzi. Tā palīdz noteikt potenciālās problēmas, to cēloņus un sekas, lai prioritizētu riska mazināšanas pasākumus.

Galvenie elementi

- **Kļūmes veidi (*Failure Modes*)**: tiek identificētas visas iespējamās kļūmes, kas var rasties konkrētā sistēmas daļā.
- **Cēloņi un sekas**: analizē, kāpēc kļūmes rodas un kā tās ietekmēs sistēmu.
- **Prioritizācija**: kļūmju ietekme, biežums un atklāšanas grūtības tiek novērtētas, lai noteiktu, kuri riski ir vissvarīgākie.
- **Rezultāts**: izveido sarakstu ar prioritārām problēmām un ieteiktajiem risinājumiem.

Piemērs

Mašīnā, kurā ir motors, *FMEA* var identificēt, ka motora pārkaršana ir iespējamā kļūme, tās cēlonis var būt dzesēšanas sistēmas bojājums, un sekas varētu būt pilnīga mašīnas apstāšanās.

- ***SWIFT* (*Structured What-If Technique*)**

SWIFT ir strukturēta metode, kas izmanto "Kas būtu, ja...?" jautājumus, lai identificētu iespējamos riskus. Tā ir elastīgāka un mazāk formāla nekā *HAZOP* vai *FMEA*, tomēr saglabā strukturētu pieeju.

Galvenie elementi

- **Konteksts.** Izmanto plašākām sistēmām vai procesiem, kur var nebūt pieejamas ļoti specifiskas detaļas.
- **Jautājumi.** Tiek izmantoti vadošie jautājumi, piemēram, "Kas būtu, ja piegādes kavētos?" vai "Kas būtu, ja sistēma sabruktu?"
- **Komandas darbs.** Eksperti apspriež iespējamos scenārijus un to sekas.
- **Rezultāts.** Identificēti riski un ieteikti risinājumi.

Piemērs

Ražošanas procesā *SWIFT* varētu uzdot jautājumu: "Kas notiktu, ja tiktu piegādāti nepareizi izejmateriāli?" un analizēt, kā tas ietekmētu ražošanas kvalitāti un laika grafiku.

- ***HAZOP* (*Hazard and Operability Study*)**

HAZOP ir strukturēta un sistemātiska metode, ko izmanto, lai identificētu potenciālos riskus un darbības traucējumus industriālajās sistēmās, procesos un iekārtās. Tā palīdz analizēt, kā un kāpēc var rasties novirzes no paredzētās darbības, un novērtēt to iespējamo ietekmi uz drošību, efektivitāti un ekspluatācijas uzticamību.

HAZOP analīzes pamatā ir komandas pieeja, kurā eksperti sistemātiski pārskata procesu, sadalot to loģiskos posmos un analizējot katru darbību, izmantojot iepriekš noteiktus vadības vārdus (*Guide Words*), piemēram:

***More* (vairāk)** – piemēram, lielāks spiediens vai plūsma nekā paredzēts;
***Less* (mazāk)** – mazāks apjoms vai zemāks temperatūras līmenis;
***No* (nav)** – plūsma vai darbība nenotiek vispār;
***Reverse* (pretēji)** – process norisinās pretējā virzienā nekā paredzēts;
***Other than* (cits nekā paredzēts)** – notiek neparedzēta darbība vai reakcija.

Komanda analizē šos vadības vārdus katram procesa posmam un nosaka potenciālos riskus, kas var rasties noviržu gadījumā. Pēc tam tiek izstrādāti kontroles pasākumi, lai samazinātu vai novērstu identificētos riskus.

***HAZOP* ieguvumi**

- Nodrošina sistēmisku un strukturētu pieeju risku identificēšanai
- Veicina komandas darbu un dažādu ekspertu zināšanu apvienošanu
- Palīdz identificēt ne tikai drošības, bet arī ekspluatācijas problēmas un neefektīvus procesus
- Samazina iespējamās avārijas un finansiālos zaudējumus, ieviešot preventīvus pasākumus

HAZOP ir spēcīgs instruments, kas palīdz uzņēmumiem sistemātiski analizēt un uzlabot procesus, samazinot drošības un darbības riskus, nodrošinot efektīvāku un drošāku darbību.

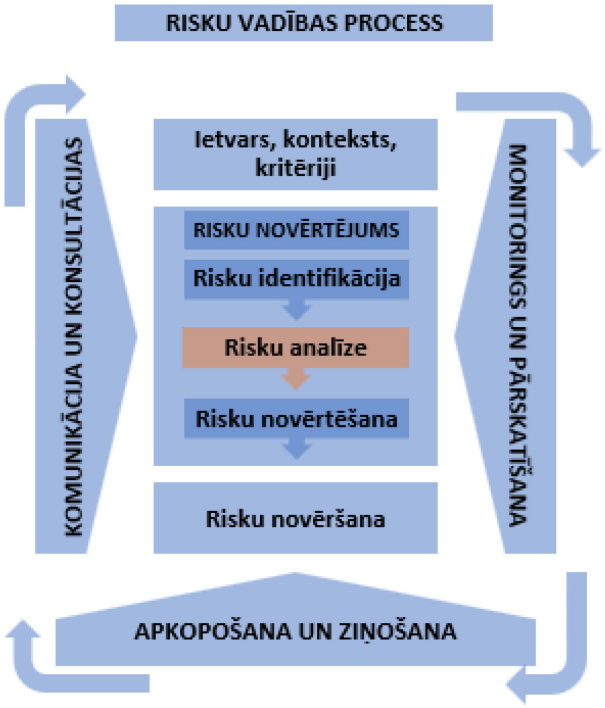
RISKU ANALĪZE UN MODERNĀS TEHNOLOĢIJAS

3. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORS: Javier Dorado, Profilakses un integrētās drošības skola, Spānija

Konteksts

Saskaņā ar ISO 31000 risku analīze sastāv no riska būtības un tā raksturlielumu izpratnes, tostarp, ja nepieciešams, riska līmeņa.

ATSAUCE UZ ISO 31000 STANDARTU	
Risku analīze ietver rūpīgu un detalizētu nenoteiktību, riska avotu, seku, varbūtību, notikumu, scenāriju, kontroles un to efektivitātes izvērtēšanu, piemēram: • notikumu iespējamība un to sekas; • šo seku raksturs un apjoms; • scenārija sarežģītība un savstarpējā saistība; • ar laiku saistīti faktori un nepastāvība; • esošo kontroles mehānismu efektivitāte; • jutīguma un noturības līmenis.	

Uzdevuma mērķis

Veicot šo uzdevumu, studenti varēs veikt risku analīzi scenārijā, kas ietver moderno tehnoloģiju drošības aspektus. Ar modernām tehnoloģijām šajā uzdevumā tiek saprasti droni, mākslīgā intelekta vadītas tehnoloģijas un jebkura cita ierīce, kas var ietekmēt drošības procedūras ikvienā uzņēmumā.

UZDEVUMS STUDENTIEM

1. Izvēlieties savās grupās konkrētu scenāriju. Vispirms izvēlieties, vai situācija tiks analizēta privātā sektorā vai valsts pārvaldē/institūcijās. Kad esat nolēmuši, norādiet, kurā sektorā šī organizācija darbojas (piemēram, uzņēmums, kas organizē pasākumus, vai valsts iestāde – vietējā policija).

2. Kad jūsu grupa ir izvēlējusies scenāriju, padomājiet par vienu drošības procedūru, kas šai iestādei varētu būt jāveic (piemēram, iepriekš minētajam pasākumu organizēšanas uzņēmumam, process, lai kontrolētu piekļuvi pasākumam).
3. Kad ir izlemts gan vispārīgais scenārijs, gan konkrētais konteksts, padomājiet par risku, ko šī situācija varētu radīt. Lai to izdarītu, strādājiet pēc ISO 31000 standartā noteiktajiem soļiem: a) šī notikuma iespējamība un tā sekas; b) šo seku raksturs un apjoms; c) izstrādātā scenārija sarežģītība un savstarpējā sasaiste; un d) ar laiku saistītie faktori.
4. Tagad padomājiet par kādu modernu tehnoloģiju, kas varētu būt noderīga, lai novērstu šo risku. Piemēram, scenārijā, kas norādīts kā piemērs, MI vadīta tehnoloģija personu biometriskai identificēšanai vai drons ar kameru, kas ir iebūvēta piekļuves kontrolei. To darot, ņemiet vērā, ka ISO 31000 standarts ietver šo tehnoloģiju efektivitātes analīzi.
5. Visbeidzot izveidojiet iespējamo risku sarakstu, kas saistīts ar šādu tehnoloģiju izmantošanu. Lai to izdarītu, savā grupā sāciet ar jautājumu: vai šīs tehnoloģijas ir efektīvas? Kāds neparedzēts risks var būt saistīts ar to lietošanu? Normatīvais risks? Risks personu fiziskajai integritātei? Risks procedūrai, kas jānodrošina (šajā piemērā – piekļuves kontrole)?

UZDEVUMS PASNIEDZĒJIEM

1. Izveidojiet studentu grupas, pamatojoties uz dalībnieku kopējo skaitu. Lai diskusija būtu efektīva, katrā grupai vajadzētu būt vismaz trīs studentiem, tomēr ne vairāk kā pieciem.
2. Tā kā šis uzdevums ir vērsts uz risku analīzi ISO 31000 standarta ietvaros, īsi izskaidrojiet koncepciju un darbības.
3. Papildus informācijas sniegšanai par riska analīzes koncepciju paskaidrojiet, ka pirms tās atspoguļošanas un ieviešanas ir jāizvēlas konkrēts scenārijs (kāda veida organizācijas, privātas vai publiskas), kura darbība/sabiedriskie pienākumi ir saistīti ar šo organizāciju, ar kādu galveno risku tās var saskarties ikdienas darbā. Izmantojiet metodi 3K – kurš, ko, kur.
4. Pārliecinieties, ka pirms risku analīzes studenti ir skaidri nodefinējuši 3K - kurš, ko, kur.
5. Uzdevuma pēdējo soli (skatīt punktu nr. 5 studentu uzdevuma aprakstā) var sākt ar konkrētu jautājumu uzdošanu, piemēram: Vai šīs tehnoloģijas ir efektīvas? Kāds neparedzēts risks var būt saistīts ar to lietošanu? Kādi ir normatīvie riski? Vai ir riski personu fiziskajai integritātei? Vai ir procedūru riski?

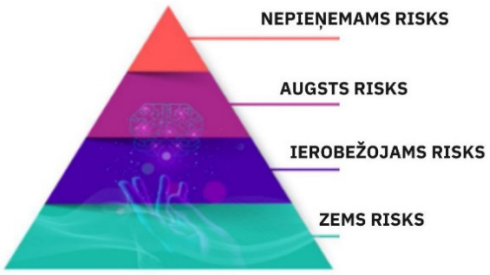
Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Spēja novērtēt modernās tehnoloģijas, novērtēt sekas un ietekmi.

Papildu materiāli

Augsti riski

Šeit atradīsiet ieskatu, kas varētu būt augsti riski saistībā ar moderno tehnoloģiju un MI tehnoloģiju lietošanu.

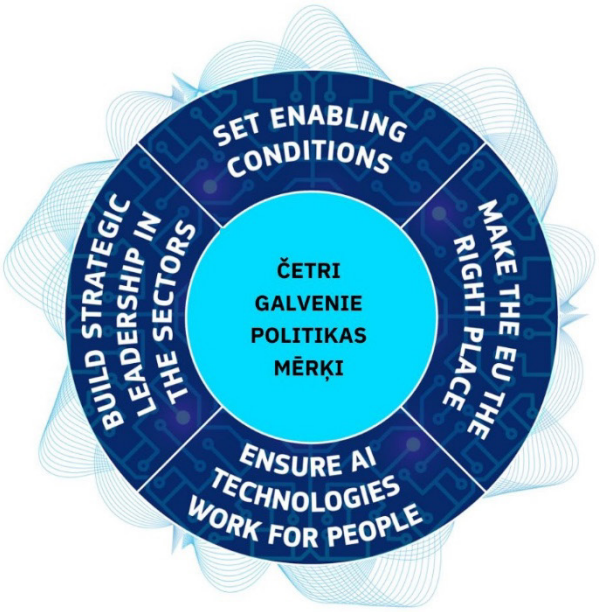
• Kritiskā infrastruktūra (piem., transports), kas varētu apdraudēt iedzīvotāju dzīvību un veselību. • Izglītība vai profesionālā apmācība, kas var noteikt piekļuvi izglītībai un profesionālajai karjerai (piem., eksāmenu vērtēšana). • Drošības komponenti produktiem (piem., MI izmantošana robotizētā ķirurģijā). • Nodarbinātība, darbinieku vadība un piekļuve pašnodarbinātībai (piem., CV šķirošanas programmatūra darbā pieņemšanas procesiem). • Būtiski privātie un publiskie pakalpojumi (piem., kredītreitingi, kas liedz pilsoņiem iespēju saņemt aizdevumu). • Tiesībsargājošās iestādes, kas var ietekmēt cilvēku pamattiesības (piem., pierādījumu ticamības novērtēšana). • Migrācijas, patvēruma un robežkontroles pārvaldība (piem., ceļošanas dokumentu autentiskuma pārbaude). • Tiesu administrēšana un demokrātiskie procesi (piem., likuma piemērošana konkrētos gadījumos).	

Uzticības veidošana, izmantojot pirmo juridisko ietvaru mākslīgajam intelektam. Eiropas Komisija.

Pieejams:

Eiropas Komisijas iniciatīva "Izcilības veicināšana mākslīgajā intelektā"

Eiropas Komisijas iniciatīva "Izcilības veicināšana mākslīgajā intelektā" ir vērsta uz mākslīgā intelekta attīstību, ieviešanu un drošu izmantošanu visā ES. Stratēģija ietver labvēlīgu apstākļu radīšanu inovācijām, līderības veicināšanu augstas ietekmes nozarēs, nodrošinot, ka mākslīgā intelekta tehnoloģijas kalpo cilvēku labā, un padarot ES par globālu uzticama mākslīgā intelekta centru. Tas saskan ar plašāku mērķi nodrošināt digitālo transformāciju, ievērojot ētikas standartus un uzticību.



ČETRI GALVENIE POLITIKAS MĒRĶI:
1. NODROŠINĀT LABVĒLĪGUS APSTĀKĻUS
2. VEIDOT STRATĒĢISKO LĪDERĪBU AUGSTAS IETEKMES NOZARĒS
3. PADARĪT ES PAR PIEMĒROTU VIETU
4. NODROŠINĀT, KA MĀKSLĪGĀ INTELEKTA TEHNOLOĢIJAS DARBOJAS CILVĒKU LABĀ

30. attēls. **Izcilības veicināšana mākslīgajā intelektā.** Eiropas Komisija. Pieejams: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en

Attēlā ir atspoguļoti Eiropas Komisijas četri galvenie politikas mērķi saistībā ar mākslīgā intelekta attīstību un izmantošanu. Tā ir daļa no plašākas stratēģijas, kas vērsta uz MI izcilības un uzticamības veicināšanu ES.

Mērķi

1. Nodrošināt labvēlīgus apstākļus MI attīstībai un pielietojumam – tas nozīmē veicināt MI izpēti, inovācijas un plašāku izmantošanu dažādās nozarēs, radot tehnoloģisko un juridisko pamatu tās drošai attīstībai.
2. Veidot stratēģisko līderību augstas ietekmes nozarēs – tas paredz ES atbalstu nozīmīgu nozaru attīstībai, kur MI var būtiski uzlabot procesus, piemēram, veselības aprūpē, enerģētikā, transportā vai ražošanā.
3. Padarīt ES par piemērotu vietu MI attīstībai – šis mērķis uzsver nepieciešamību radīt vidi, kurā uzņēmumi, zinātnieki un investori izvēlas attīstīt MI Eiropā, piemēram, veidojot MI laboratorijas un centrus.
4. Nodrošināt, ka MI tehnoloģijas darbojas cilvēku labā – tas nozīmē koncentrēties uz ētisku un uzticamu MI izstrādi, nodrošinot, ka tehnoloģijas palīdz sabiedrībai un aizsargā cilvēku tiesības.

DROŠĪBAS RISKU PĀRVALDĪBAS CIKLS, IZMANTOJOT ISO 31000 STANDARTU

4. PRAKTISKAIS UZDEVUMS STUDENTIEM

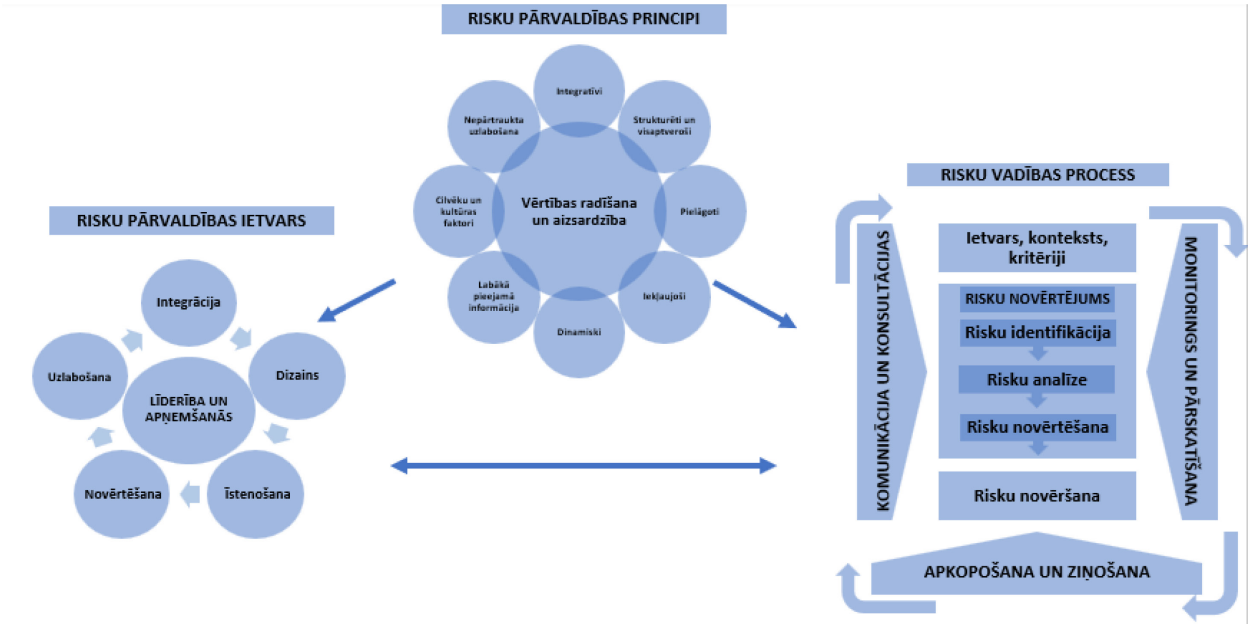
AUTORS: Lambert Bambach, Avans Lietišķo zinātņu Universitāte, Nīderlande

Konteksts

Lai izveidotu ilgtspējīgu pieeju drošības risku pārvaldībai, ir rūpīgi jāizprot ISO 31000:2018 pamatelementi. Atkarībā no organizācijas konteksta un mērķiem tiek sākts ar vienu no blokiem, lai realizētu drošības risku pārvaldību.

ATSAUCE UZ ISO 31000 STANDARTU

Saskaņā ar ISO 31000 standartu galvenie elementi ir risku pārvaldības ietvars, risku pārvaldības principi un risku pārvaldības process.



Uzdevuma mērķis

Studenti iepazīsies ar ISO 31000:2018 standarta elementiem, izmantojot trīs gadījumus, uz kuru pamata ir jāizanalizē: Kur jūs sākat drošības risku pārvaldības ciklu, pamatojoties uz ISO 31000? Kāpēc sāksiet tieši tur? Ko darīsiet? Kas būs jūsu sabiedrotie?

UZDEVUMS STUDENTIEM

1. Veidojiet grupas saskaņā ar pasniedzēja norādījumiem.
2. Katrai grupai ir doti situāciju apraksti, ar kuriem strādāt.
3. Pasniedzēja vadībā definējiet, kur sākt drošības risku pārvaldības ciklu, pamatojoties uz ISO 31000? Kāpēc sāksiet tieši tur? Ko darīsiet? Kas būs jūsu sabiedrotie?
4. Iepazīstieties ar uzņēmuma aprakstu, izvēlieties pamatelementus, ar kuriem sākat darbu, un pierakstiet savas izvēlētās pieejas rezultātus. Ar ko sākt drošības riska pārvaldības ciklu, pamatojoties uz ISO 31000? Kāpēc sākat tieši tur? Ko darīsiet? Kas būs sabiedrotie?
5. Sagatavojiet īsu prezentāciju saviem kursa biedriem par jūsu izvēlētajiem pieejas rezultātiem par iepriekš apskatītajiem četriem jautājumiem.
6. Prezentējiet savus rezultātus kursa biedriem citās grupās.
7. Noklausieties kursa biedru prezentācijas. Pēc katras prezentācijas pārrunājiet 2 minūtes ar savu grupu, vai viņu pieeja gadījumiem būtu piemērota arī jums. Dalieties savās domās ar kursabiedriem. Vai jūsu pieeja katrā gadījumā būtu atšķirīga?
8. Pēc visām prezentācijām pārrunājiet savā grupā, kura no piedāvātajām pieejām būtu vislabākā katram gadījumam. Dalieties savās domās ar pārējiem.

UZDEVUMS PASNIEDZĒJIEM

1. Pirms nodarbības aprēķiniet studentu skaitu un to, cik grupas no četriem studentiem tie veidotu. Izlemiet, kādu metodi vēlaties tiem piešķirt.
2. Pirms nodarbības katrai grupai jābūt ISO 31000:2018 kopijai, studentiem jāiepazīstas ar šajā uzdevumā pielikumā doto informāciju – uzņēmuma aprakstu un vienu no piedāvātajām situācijām.
3. Uzdodiet studentiem analizēt vienu no situācijām un pierakstīt viņu risinājumu. Pierakstus var veikt uz post-it piezīmju lapām, uz tāfeles, *PowerPoint* prezentācijā, tiešsaistes vidē utt. Uzdodiet studentiem sagatavoties prezentēt savus rezultātus. Jūs varat izlemt par prezentācijas veidu. Ieteicams ierobežot prezentācijas ilgumu līdz 5 minūtēm.
4. Uzdodiet studentiem sagatavot prezentāciju par sekojošiem jautājumiem: Kur jūs sākat drošības riska pārvaldības ciklu, pamatojoties uz ISO 31000? Kāpēc sākat tieši tur? Ko darīsiet? Kas būs sabiedrotie? Pasniedzēja darbs ir skaidrot studentiem situāciju un uzdevumu un palīdzēt, ja rodas jautājumi.
5. Aiciniet studentiem prezentēt savu prezentāciju par rezultātiem, iekļaujot atbildes uz šiem jautājumiem: Kur jūs sākat drošības riska pārvaldības ciklu, pamatojoties uz ISO 31000? Kāpēc sākat tieši tur? Ko darīsiet? Kas būs sabiedrotie?
6. Prezentāciju laikā vadiet diskusiju un sekojiet laika rāmim. Process ir šāds:
   - maksimālais laiks vienas grupas prezentācijai – 10 minūtes;
   - pēc katras prezentācijas grupām ir jāapspriež savā starpā jautājumi (aptuveni 2 minūtes). Apspriežamie jautājumi: vai prezentētā pieeja būtu piemērota citu grupu problēmsituācijām?
   - grupas tiek mudinātas dalīties savās domās ar kursabiedriem. Galvenais jautājums: vai pieejas izvēle dos atšķirīgus rezultātus?
7. Pēc visām prezentācijām rosiniet studentus uz kopīgo diskusiju par to, kura no piedāvātajām pieejām būtu vislabākā katrai situācijai.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Prasme strādāt komandā, prasme strādāt ierobežotā laikā, prezentācijas prasmes, argumentēšanas māksla, prasmes salīdzināt un kritiskā domāšana.

UZŅĒMUMA APRAKSTS

Loģistikas kompānija

Konteksts

LOĢISTIKAS KOMPĀNIJAI ir 14 fiziski veikali, interneta veikals un viena nacionālā līmeņa izplatīšanas centra noliktava. LOĢISTIKAS KOMPĀNIJAS apgrozījums ir 370 000 000 eiro gadā, no kuriem 270 000 000 eiro fiziskajiem veikaliem un 100 000 000 eiro interneta veikalam. LOĢISTIKAS KOMPĀNIJAS pozīcija tirgū ir tikpat spēcīga kā tās attiecības ar klientiem. Tāpēc ilgtermiņa attiecības ar klientiem ir tās stratēģijas pamatā.

Vīzija

- Klientu pieredze
- Uz klientu orientēts

Misija

- Empātija (sajūtas): uzņēmums zina klienta individuālās vajadzības.
- Ekspertīze (zināšanas): uzņēmumam ir zināšanas, lai apmierinātu klientu individuālās vajadzības.
- Pieredze (spējas): uzņēmums iepazīstina jūs ar labākajiem elektroniskajiem izstrādājumiem.

Vērtības

- Klients vispirms
- Dari to, ko saki
- Realizē idejas
- Vienmēr labāk

Apsolījumi

- Labāk klientam
- Labāk darbiniekam
- Labāk videi

Biznesa modelis

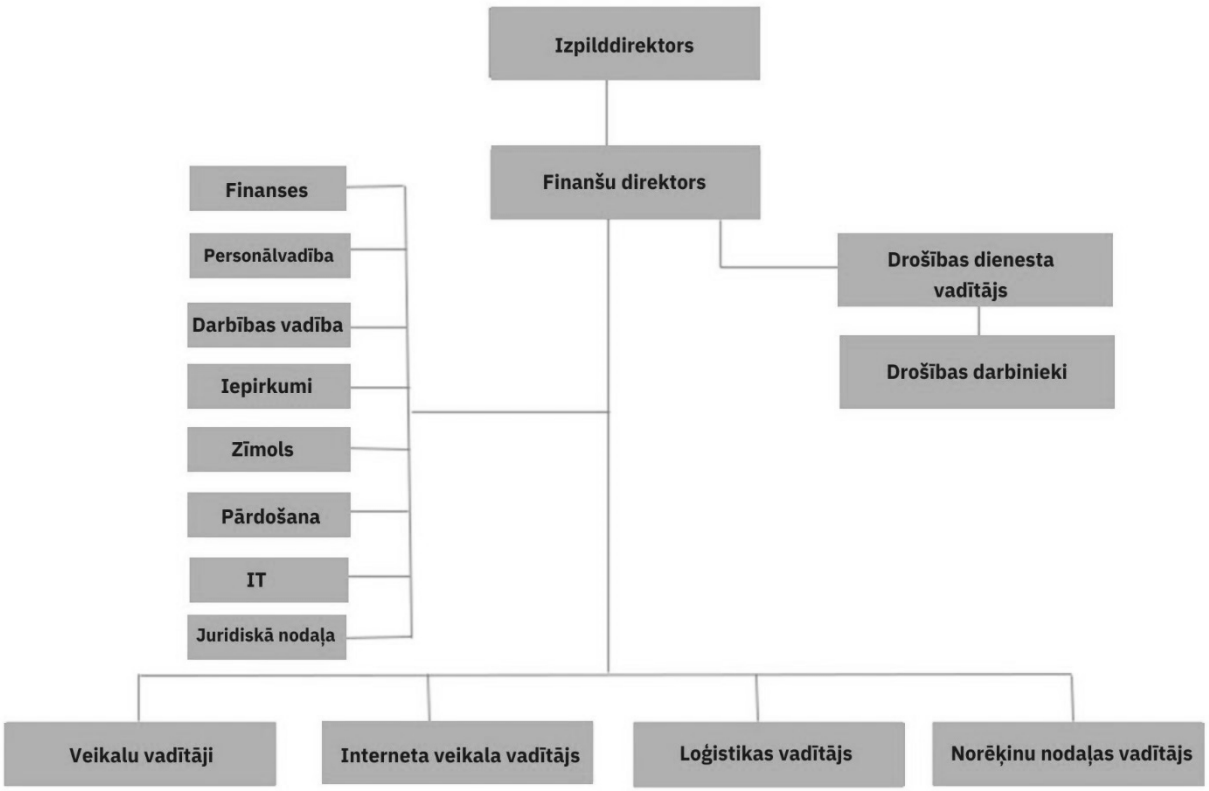
- Zemākas izmaksas
- Spēcīgi zīmoli
- Plašs preču klāsts

LOĢISTIKAS KOMPĀNIJAS pakalpojumu līmenis ir augsts. Īsi piegādes termiņi un zemākā cena, ieskaitot pakalpojumu, nodrošina to, ka LOĢISTIKĀ KOMPĀNIJA rūpīgi skatās uz produktu ieguldījumu peļņas gūšanā.

Attīstība

- Krājumi tiek samazināti līdz minimumam. Izmērāmība ir būtiska neatkarīgi no tā, vai tās ir reklāmas kampaņas, krājumu kontrole vai zaudējumu novēršana;
- LOĢISTIKAS KOMPĀNIJA vēlas ieviest arī visu dokumentu pašskenēšanu, lai palielinātu klienta ērtības;
- Turklāt LOĢISTIKĀ KOMPĀNIJA vēlas panākt peļņas pieaugumu, palielinot pārdošanu tiešsaistē;
- Veikalā un tiešsaistē tiek piemērota viena un tā pati cena. Ja patērētājs citur var pasūtīt vēlamo preci lētāk, LOĢISTIKAS KOMPĀNIJA to piegādās par tādu pašu cenu. Tādā veidā LOĢISTIKĀ KOMPĀNIJA neļauj klientiem kavēties ar pirkuma lēmuma pieņemšanu;
- LOĢISTIKAS KOMPĀNIJA piegādā 24 stundu laikā pēc preču pasūtīšanas;
- LOĢISTIKAS KOMPĀNIJA šobrīd izstrādā *Smart* sistēmu. No mazajiem punktiem tirdzniecības centros tiks veidotas eksperimentālas automātiskās ķēdes, kas nodrošinās ekspres-piegādi. *Smart* veikali atradīsies lielākajos tirdzniecības centros, kur pircēji varēs saņemt mazāku preču klāstu un arī konsultācijas. Viedajos *smart* centros universālais kanāls kļūs par normu. Caur caurspīdīgām sienām veikalos klienti varēs pārbaudīt, vai prece ir pieejama, kā tā izskatās, un veikt pasūtījumus. Kā nākotnes vīziju uzņēmums paredz to, ka šie pasūtījumi tiek piegādāti klientam mājās tajā pašā dienā.

Struktūra



31. attēls. **LOĢISTIKAS KOMPĀNIJAS struktūrshēma**

Veikalu pārvaldība, interneta veikali, loģistikas un izplatīšanas centra noliktavas

Cik zināms, vadītājiem nav būtisku uzdevumu un pienākumu drošības jomā, bet viņi ir atbildīgi par darbinieku vadību drošības jomā veikalos, interneta veikalā un izplatīšanas centra noliktavā.

Vadītāju atbalsta nodaļas

Cik zināms, finanšu, operāciju, iepirkumu, pārdošanas, IT, juridisko nodaļu vadītājiem nav būtisku uzdevumu un pienākumu drošības jomā, bet viņi ir atbildīgi par darbinieku vadīšanu savā nodaļā.

Drošība

Drošība tiek organizēta centrālā līmenī. Drošība ir personāla pakalpojums. Cik zināms, finanšu direktoram nav būtisku uzdevumu un pienākumu drošības jomā, taču viņš joprojām ir atbildīgs par apsardzes dienestu un apsardzes vadītāju. Visi ziņojumi tiek nodoti izpilddirektoram. Drošības dienesta budžets ir noteikts departamenta līmenī. Ikviena LOĢISTIKAS KOMPĀNIJAS struktūrvienība var vērsties pie drošības dienesta, kad uzskata to par nepieciešamu. Izdevumus par ieguldījumiem un uzturēšanas izmaksas sedz LOĢISTIKAS KOMPĀNIJA.

Drošības dienesta vadītājs

Drošības dienesta vadītājs ir atbildīgs par drošības pasākumu vadību, plānošanu un izpildes vadīšanu. Šī kārtība tika izstrādāta galvenajā birojā, risku klasifikācijas process ir daļa no tā. Turklāt drošības dienesta vadītājs un viņa nodaļa atbalsta valsts un vietējo vadību, veicot tādus uzdevumus kā izmeklēšanas, drošības auditi un veikalu, interneta veikala un izplatīšanas centra noliktavas atbilstības novērtējums normatīvajiem aktiem. Turklāt vadītājs pārrauga LOĢISTIKAS KOMPĀNIJAS drošības standartu, instrukcijas, vadlīnijas utt.

Drošības personāls

Drošības dienesta darbinieki veic šādus uzdevumus:

- atbalsta operatīvo vadību drošības jomā;
- palīdz gatavoties revīzijām (iekšējie novērtējumi, izmeklēšana) un atbalsta pēcpārbaudē un pasākumos;
- apkopo informāciju par incidentiem un ziņo par tiem vietējai vadībai;
- atbalsta iekšējās krāpšanas izmeklēšanas;
- izvērtē nozares informāciju un novērtē draudus;
- atbild par LOĢISTIKAS KOMPĀNIJAS drošības standarta, instrukciju, vadlīniju ieviešanu sadarbībā ar Drošības dienesta vadītāju;
- pārbauda uzstādīto fiziskās drošības iekārtu iespējamos defektus vai darbības traucējumus;
- nodrošina vispārīgu drošības informāciju un drošības apmācības darbiniekiem;
- ziņo par šo darbību rezultātiem Drošības dienesta vadītājam;
- veic risku analīzi un atbilstošu pasākumu pielāgošanu.

Drošības dienests ir atbildīgs par:

- jauno darbinieku un darbuzņēmēju pagātnes pārbaudi;
- risku uzskaiti un novērtēšanu (darba procesi, drošība);
- ārējo apsardzes darbinieku vadību;
- sanāksmju organizēšanu par riskiem;
- piekļuves kontroli;
- novērošanas kamerām;
- incidentu izmeklēšanu;
- darbības nepārtrauktības plānošanu;

- risku vadību;
- semināru organizēšanu par informētību, iekšējo apdraudējumu utt.

Veikali, interneta veikals, izplatīšanas centra noliktava

Šobrīd LOĢISTIKAS KOMPĀNIJA sastāv no 14 veikaliem, interneta veikala un izplatīšanas centra noliktavas, kuras savieno loģistikas procesus.

LOĢISTIKAS KOMPĀNIJAI ir savi veikali un franšīzes formula. Franšīzes ņēmēji maksā par formulas izmantošanu. Šiem veikaliem un franšīzes ņēmējiem LOĢISTIKAS KOMPĀNIJA organizē centrālo iepirkumu, sadales centra noliktavu, loģistikas procesu, publicitāti, apkopi, drošību un interneta veikalu. Franšīzes ņēmējs kārto personāla lietas, darba laikus, veikala atrašanās vietu, apdrošināšanu u.c.

Veikali

LOĢISTIKAS KOMPĀNIJAI ir 14 veikali. Veikali ir augstas klases patēriņa preču mazumtirgotāji. Procesu veikalā raksturo preču ienākšana, uzglabāšana un izvešana. Tiek sekots līdzi preču plūsmas ātrumam, reģistrējot produktus, kam beidzies derīguma termiņš. Tiek uzskaitītas preces, kas vēl ir veikala noliktavā un kuras nepieciešams atkārtoti pasūtīt. Veikaliem veic piegādi reizi nedēļā. Veikalos ir jaukts sortiments. Visas preces ir pārdošanā visos veikalos, un tās veikalos ir izkārtotas aptuveni vienā un tajā pašā vietā. Akcijas, kas veikaliem ir noteiktās nedēļās, tiek izceltas veikalu skatlogos. LOĢISTIKAS KOMPĀNIJA veikalā izmanto lietotni, lojalitātes karti un *Wi-Fi* klientu izsekošanu.

LOĢISTIKAS KOMPĀNIJA tic pilnīgai bezsaistes un tiešsaistes integrācijai. Integrējot interneta veikalu un fiziskos veikalus, preces var ātri sasniegt klientu par konkurētspējīgu cenu, piedāvājot arī personīgu apkalpošanu. Uzņēmumam ir pieejami arī produkti, kas ir pieejami tikai caur internetveikalu.

Noliktava

No izplatīšanas centra noliktavas piegādes notiek reizi nedēļā uz LOĢISTIKAS KOMPĀNIJAS veikaliem. Principā interneta veikalā iegādātās preces klientam tiek piegādātas tieši no izplatīšanas centra noliktavas. Ja pircēji internetā pasūtītās preces vēlēsies izņemt veikalā, tās uz veikaliem tiks nogādātas caur izplatīšanas centra noliktavu. Šos pasūtījumus veikalos katru dienu piegādā ārpakalpojuma sniedzējs. Tāpat kā veikalos, arī izplatīšanas centra noliktavā procesu raksturo preču ienākšana, uzglabāšana un izvešana. Izplatīšanas centra noliktavā paletes tiek sakomplektētas un sagatavotas transportēšanai. Šim procesam ir nepieciešama laba sadarbība starp veikaliem, interneta veikalu un izplatīšanas centra noliktavu ar preču saņemšanu (ienākošais) un preču izplatīšanu (izejošo).

Loģistika

Visiem veikaliem ir savi krājumi. Krājumu uzturēšanai veikalos tiek izmantotas trīs sistēmas, proti: *SAP*, *POSFlow* un *TIB*.

Lai pārvaldītu krājumus, LOĢISTIKAS KOMPĀNIJA izmanto *SAP*. *SAP* ir uzņēmuma resursu plānošanas programma, ar kuru KOMPĀNIJA pārvalda visas preču plūsmas. Visas preces tiek reģistrētas *SAP*, ieskaitot specifikācijas un pirkšanas, nodošanas un pārdošanas cenas.

SAP ir saistīts ar POSFlow, LOĢISTIKAS KOMPĀNIJAS POS sistēmu. POS ir sistēma, kas apvieno kases un pārdošanas uzskaites funkcijas. POS sistēma ļauj bez kavēšanās apstrādāt pārdotās preces.

SAP, pamatojoties uz pārdošanu, nosaka, cik liela ir vajadzība pēc noteikta produkta.

Ārējie pakalpojumu sniedzēji

Pasūtīšanas un atgriešanas procesā ir iesaistītas divas ārējās puses: *CEVA* un *DHL*.

CEVA ir viena no pasaulē lielākajām piegādes ķēdes pārvaldības kompānijām. *CEVA* ir līgumi ar LOĢISTIKAS KOMPĀNIJU par preču uzglabāšanu, nosūtīšanu un saņemšanu.

DHL ir transporta uzņēmums, kas pārvadā visas LOĢISTIKAS KOMPĀNIJAS preces.

Drošības dienesta vadītājs uztur labus kontaktus ar citiem līdzīgiem loģistikas organizāciju drošības vadītājiem. Drošības departamentam ir arī labs kontakts ar Valsts policiju.

Krājumi

Iepirkumu nodaļa nosaka, cik daudz krājumu jābūt katrā veikalā. Šis pasūtīšanas veids izveido savienojumu ar lietu internetu (IoT), kas nozīmē, ka objekti, kas savienoti ar internetu, sazinās viens ar otru un automātiski sāk procesu. IoT kļūst arvien svarīgāks loģistikas jomā.

LOĢISTIKAS KOMPĀNIJAS piegādes ķēdē ir divi svarīgi procesi, proti, automātiskais pasūtīšanas process un atgriešanas process.

Automātiskais pasūtīšanas process

Procesu, kurā *SAP* automātiski pasūta produktus, lai uzturētu krājumus, sauc arī par automātisko pasūtīšanas procesu. *SAP* analizē pārdošanas datus un nosaka optimālo pasūtījuma momentu un optimālo pasūtījuma daudzumu. Brīdī, kad SAP konstatē, ka veikalā nav pietiekami daudz preču noliktavā, *SAP* automātiski izveido pasūtījumu attiecīgajam veikalam. *POSFlow* nodrošina *SAP* ar pārdošanas datiem, lai krājumus varētu uzraudzīt.

Atgriešanas process

Papildus automātiskajam pasūtīšanas procesam ir arī atgriešanas process. Katru pirmdienu veikalā tiek izveidota preču atgriešanas atļauja (RMA). RMA sastāv no obligātās atgriešanas un *DOA* gadījumiem (angliski *Dead On Arrival*). *DOA* ir termins, kas norāda, ka pircēja saņemtajai precei tās ierašanās brīdī tika konstatēts defekts vai bojājums. Pēc RMA izveidošanas *DHL* paņem pasūtījumu un nosūta to. Tur preces tiek atdotas trešajai pusei vai uzglabātas noliktavā.

Tiešās piegādes, ko veic ražotāji

Automātiskais pasūtīšanas process nodrošina 60 % veikalu piegādi no izplatīšanas centra noliktavas. Atlikušos 40 % veikalu apgādi nodrošina preču ražotāji, ar kuriem LOĢISTIKAS KOMPĀNIJA ir noslēgusi līgumu. Šo ražotāju pārstāvji paši dodas uz veikaliem, lai pārbaudītu un aizpildītu savas produkcijas plauktus. Turklāt viņi var papildināt krājumus, ja filiālei tie ir nepieciešami. Veikali nepārbauda piegādes saturu, var papildināt plauktus ar krājumiem, ko pārstāvji tur ir piegādājuši. Veikala darbinieki parakstās uz preču pavadzīmes par preču saņemšanu un ievada preces *SAP*. Tās pašas preces var piegādāt arī caur izplatīšanas centra noliktavu ar tādu pašu svītrkodu.

Piegāde un saņemšana veikalā

DHL kurjers novieto piegādes transportu pēc iespējas tuvāk veikalam. Pēc tam viņš izkrauj vajadzīgās preces. Brīdī, kad viņš ienāk veikalā, visu fiksē kameras. *DHL* darbinieks dodas pie veikala darbinieka, kurš dodas uz noliktavu, lai paņemtu preces, kuras jāpaņem kurjeram.

Situāciju apraksti

SITUĀCIJA I

Finanšu direktora viedoklis par drošību

Drošība ir drošības dienesta personāla sniegts pakalpojums. Ņemot vērā, ka veikalos ir svarīgs klienta "labjūtības koncepts", drošības pasākumi nedrīkst traucēt pircēju pieredzi. Klientiem ir jābūt iespējai pieskarties produktiem, arī tiem, kas konkrētajā veikalā atrodas reklāmas nolūkos, bet pieejami ir citos veikalos. Finanšu direktors sagaida, ka veikala darbiniekiem arī būs nozīme veikala drošībā, īpaši ja runa ir par modrību pret klientiem, zādzībām veikalos. Sākotnējā procesā viņš no drošības dienesta sagaida aktīvāku attieksmi: negaidot, kad notiks incidents, bet gan pārvēršot brīdinājuma signālus preventīvā darbībā. Šim nolūkam ir nepieciešams, lai drošības departaments vairāk strādātu ar informāciju, izmantojot galvenos darbības rādītājus, pamatojoties uz pieejamiem iekšējiem un ārējiem informācijas avotiem.

SITUĀCIJA II

Drošības politika

Drošībai trūkst koncepcijas, jo nav skaidras misijas, vīzijas un stratēģijas attiecībā uz drošību. Nav arī politikas plāna vai biznesa mērķu attiecībā uz drošību. Drošības politikas trūkuma dēļ organizācija nespēj efektīvi pārvaldīt savus riskus un aizsargāties pret noziedzību. Tā kā vadības līmenī trūkst virzības un atbildības par drošību, šī rīcība ir radusies operatīvās darbības ietvaros. Šāda rīcība izpaužas kā fakts, ka darbinieki un vadītāji nerīkojas saskaņā ar noteikumiem un procedūrām un neapzinās riskus, ko tie rada.

SITUĀCIJA III

Risku inventarizācija

Uzņēmumam netiek veikta uz drošību orientēta risku analīze. Organizācija uzrauga savus riskus ar drošības auditu. Tomēr šis instruments nesniedz konkrētu informāciju par risku būtību un apjomu. Tas nozīmē, ka netiek veikta analīze par draudiem un to, kādu kaitējumu tie var nodarīt LOĢISTIKAS KOMPĀNIJAI.

Nav arī metodes, ar kuru ārējā informācija un zināšanas tiek inventarizētas, analizētas un pārvērstas politikā. Piemēram, trūkst metodes, ar kuras palīdzību informācija vai pētījumi par noziedzību mazumtirdzniecības sektorā tiek pārvērsti drošības politikā. Tas rada plaisu starp jomas attīstību un LOĢISTIKAS KOMPĀNIJAS pozīciju drošības jomā.

Sakarā ar nepilnīgu draudu un risku inventarizācijas procesā, organizācija nespēj efektīvi saskaņot drošības pasākumus ar drošības riskiem, kuri pastāv organizācijā. Riska inventarizācija pašlaik nav noteicošais faktors, pieņemot lēmumus par drošības pasākumiem. Trūkst pilnīga uzskaitījuma par regulārām pārbaudēm un novērojumiem.

DROŠĪBAS RISKU PĀRVALDĪBAS CIKLA IZMANTOŠANA ORGANIZĀCIJĀ (ISO 31000 UN COSO)

5. PRAKTISKAIS UZDEVUMS STUDENTIEM

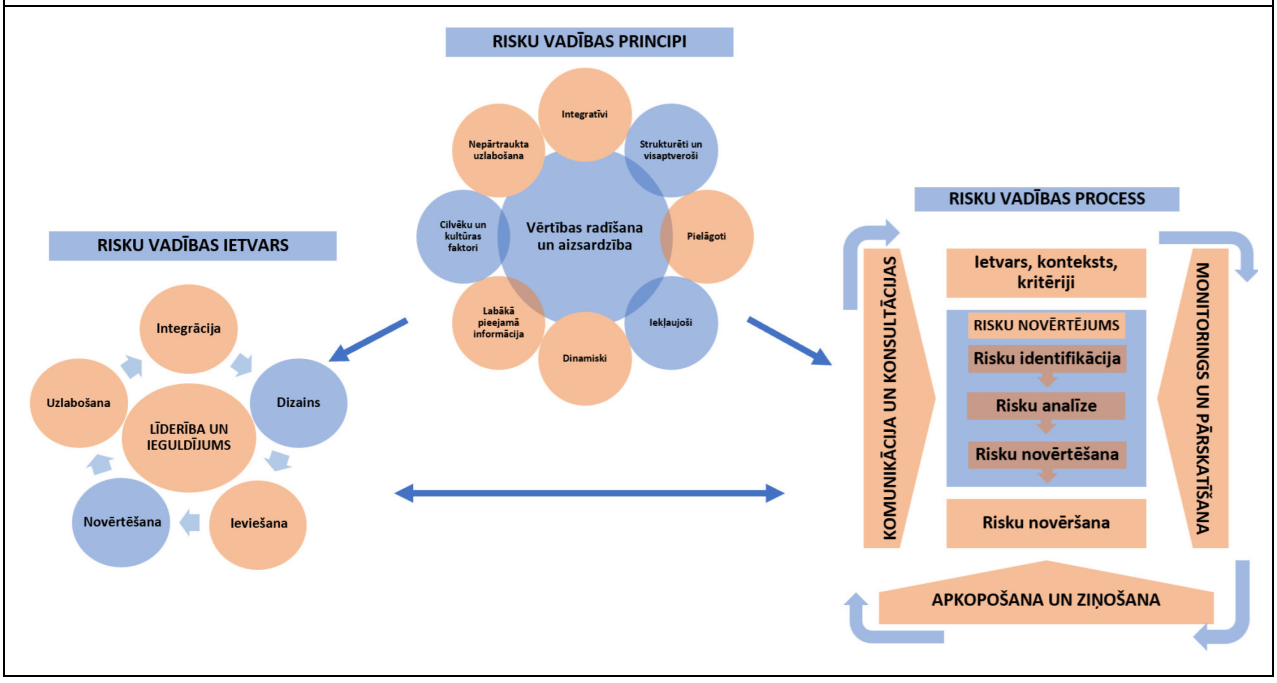
AUTORS: Lambert Bambach, Avans Lietišķo zinātņu Universitāte, Nīderlande

Konteksts

Drošības vadītājam ir jābūt informētam par iekšējās kontroles pasākumu darbību, jo, balstoties uz savām specifiskajām zināšanām par drošību, viņš var veicināt pareizu risku kontroles pasākumu īstenošanu un uzturēšanu. Atkarībā no organizācijas konteksta un mērķiem drošības risku vadības realizācijai sāk ar vienu no ISO 31000:2018 blokiem. Konkrētajā gadījumā ir jāizvēlas vispiemērotākais bloks.

ATSAUCE UZ ISO 31000 STANDARTU

Šajā uzdevumā tiek skarti sekojoši ISO 31000 standarta elementi: Risku vadības process pilnā apjomā; Risku vadības principi – nepārtraukta uzlabošana, integratīvi, pielāgoti, dinamiski, kā arī labākā pieejamā informācija; Risku vadības ietvars – uzlabošana, integrācija, ieviešana, līderība un ieguldījums.



Uzdevuma mērķis

1. Sniegt iespēju studentiem apgūt izstrādes iemaņas organizācijas drošības nodaļām, izmantojot trīs piedāvātos situācijas aprakstus. Ieteikumi ir jāveido, izmantojot ISO drošības risku vadības ciklu.
2. Studentu uzdevums ir pamatoti analizēt:
   - kas jādara katrā gadījumā attiecībā uz administratīvo organizāciju;
   - kas jādara attiecībā uz informācijas vadītu darbu;

- kur sākt drošības risku vadības ciklā;
- kāpēc sākt tieši tur;
- kas ir jādara, kādas darbības jāveic;
- kas būs sabiedrotie.

UZDEVUMS STUDENTIEM

1. Izveidojiet grupas saskaņā ar pasniedzēja norādījumiem.
2. Katrai grupai tiek piešķirti trīs gadījumi (pieejami pievienotajos materiālos), ar kuriem strādāt.
3. Pasniedzēja vadībā nosakiet:
   - kas jādara attiecībā uz administratīvo organizāciju;
   - kas jādara attiecībā uz informācijas vadītu darbu;
   - kur sākt drošības risku vadības ciklā;
   - kāpēc sākt tieši tur;
   - ko jūs plānojat darīt;
   - kas būs jūsu sabiedrotie.
4. Iepazīstieties ar LOĢISTIKAS KOMPĀNIJAS aprakstu un ISO 31000 pamatprincipiem. Tāpat iepazīstieties ar jūsu izvēlētajiem pamatprincipiem, kurus izmantosiet savā pieejā, un pierakstiet rezultātus attiecībā uz:
   - kas jādara administratīvās organizācijas kontekstā;
   - kas jādara informācijas vadīta darba kontekstā;
   - kur sākt drošības risku vadības ciklā un kāpēc;
   - ko jūs plānojat darīt un kas būs jūsu sabiedrotie.
5. Sagatavojiet īsu prezentāciju saviem kursabiedriem no citām grupām par jūsu izvēlēto pieeju un tās rezultātiem.
6. Prezentējiet savu pieeju pārējām grupām.
7. Klausieties citu studentu prezentācijas. Pēc katras prezentācijas 2 minūtes pārrunājiet grupā, vai viņu pieeja būtu piemērota arī jūsu gadījumiem. Dalieties ar savām pārdomām diskusijā. Vai, ņemot vērā citu grupu sniegtos jaunos ieskatus, jūsu pieeja katrā gadījumā būtu atšķirīga?
8. Pēc visu prezentāciju noklausīšanās pārrunājiet grupā, kura no piedāvātajām pieejām būtu vispiemērotākā katram gadījumam. Dalieties savās pārdomās ar pārējiem.

UZDEVUMS PASNIEDZĒJIEM

1. Pirms nodarbības novērtējiet studentu skaitu, lai sadalītu studentus grupās (aptuveni pa četriem studentiem katrā).
2. Pirms nodarbības katrai grupai jābūt pieejamai ISO 31000:2018 standarta kopijai, uzdevuma aprakstam. Studentiem iepriekš ir jāiepazīstas ar pielikumā sniegto LOĢISTIKAS KOMPĀNIJAS aprakstu.
3. Pēc izvēles – uzdevumu varat izspēlēt gan klātienē, gan virtuālā nodarbībā.
4. Nodarbības laikā sadaliet studentus grupās pa aptuveni četriem cilvēkiem.

5. Instruējiet studentus iepazīties ar ISO 31000:2018, uzdevumu un tam pievienotajiem dokumentiem. Tāpat studentiem ir ieteicams iepazīties ar L. Bambaka rakstu par labās prakses piemēru "DROŠĪBAS RISKU PĀRVALDĪBAS ĪSTENOŠANA ORGANIZĀCIJĀ, KAS DARBOJAS KĀ ELEKTROTĪKLA PĀRVALDNIEKS KRITISKAJĀ INFRASTRUKTŪRĀ".
6. Aiciniet studentus pierakstīt savas izvēlētās pieejas rezultātus. To var darīt, piemēram, uz līmlapiņām, tāfeles, *PowerPoint* prezentācijā vai tiešsaistes vidē. Instruējiet studentus sagatavoties prezentācijai. Jūs varat izvēlēties prezentācijas formu, taču ieteicams to ierobežot līdz 5 minūtēm.
7. Kamēr studenti apspriež savu pieeju, viņiem jāpiefiksē savi secinājumi un jāsagatavo prezentācija, atbildot uz šiem jautājumiem:
   - Kas jādara administratīvās organizācijas kontekstā?
   - Kas jādara informācijas vadīta darba kontekstā?
   - Kur sākt drošības risku vadības ciklā?
   - Kāpēc sākt tieši tur?
   - Ko plānojat darīt?
   - Kas būs jūsu sabiedrotie?
8. Jūsu uzdevums ir atvieglot studentu darbu, sniegt konsultācijas un palīdzēt, ja rodas jautājumi.
9. Instruējiet studentus prezentēt savu pieeju kursabiedriem no citām grupām, atbildot uz augstāk minētajiem jautājumiem.
10. Prezentāciju laikā nodrošiniet diskusijas vadību un ievērojiet noteikto grafiku. Process norit šādi:
    - vienas grupas prezentācijai paredzētas ne vairāk kā 10 minūtes;
    - pēc katras prezentācijas grupām 2 minūtes jāapspriež, vai prezentētā pieeja būtu bijusi piemērojama arī viņu uzdevumam.
11. Grupas tiek aicinātas dalīties ar savām domām klasē, atbildot uz galveno jautājumu: vai izvēlētā pieeja dotu atšķirīgus rezultātus?
12. Pēc visu prezentāciju noklausīšanās vadiet kopīgu diskusiju par to, kura no piedāvātajām pieejām būtu vispiemērotākā katrā gadījumā.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Prasme strādāt komandā, prasme strādāt ierobežotā laikā, prezentācijas prasmes, argumentēšanas māksla, prasmes salīdzināt un kritiskā domāšana.

UZŅĒMUMA APRAKSTS
Loģistikas kompānija

Konteksts

LOĢISTIKAS KOMPĀNIJAI ir 14 fiziski veikali, interneta veikals un viena nacionālā līmeņa izplatīšanas centra noliktava. LOĢISTIKAS KOMPĀNIJAS apgrozījums ir 370 000 000 eiro gadā, no kuriem 270 000 000 eiro fiziskajiem veikaliem un 100 000 000 eiro interneta veikalam. LOĢISTIKAS KOMPĀNIJAS pozīcija tirgū ir tikpat spēcīga kā tās attiecības ar klientiem. Tāpēc ilgtermiņa attiecības ar klientiem ir tās stratēģijas pamatā.

Vīzija

- Klientu pieredze
- Uz klientu orientēts

Misija

- Empātija (sajūtas): uzņēmums zina klienta individuālās vajadzības
- Ekspertīze (zināšanas): uzņēmumam ir zināšanas, lai apmierinātu klientu individuālās vajadzības
- Pieredze (spējas): uzņēmums iepazīstina jūs ar labākajiem elektroniskajiem izstrādājumiem

Vērtības

- Klients vispirms
- Dari to, ko saki
- Realizē idejas
- Vienmēr labāk

Apsolījumi

- Labāk klientam
- Labāk darbiniekam
- Labāk videi

Biznesa modelis

- Zemākas izmaksas
- Spēcīgi zīmoli
- Plašs preču klāsts

Stratēģiskie pīlāri

- Spēcīga klientu lojalitāte
- Pieejamo produktu klāsta paplašināšana
- Pārdošana tiešsaistē
- Pievilcīgi produkti
- Korporatīvā atbildība
- Darīt labu mūsu cilvēkiem

Ambīcijas

- Vienmēr labāk
- Apgrozījuma un peļņas pieaugums
- Zaudējumu un izmaksu samazināšana, labāk kontrolējot primāros procesus

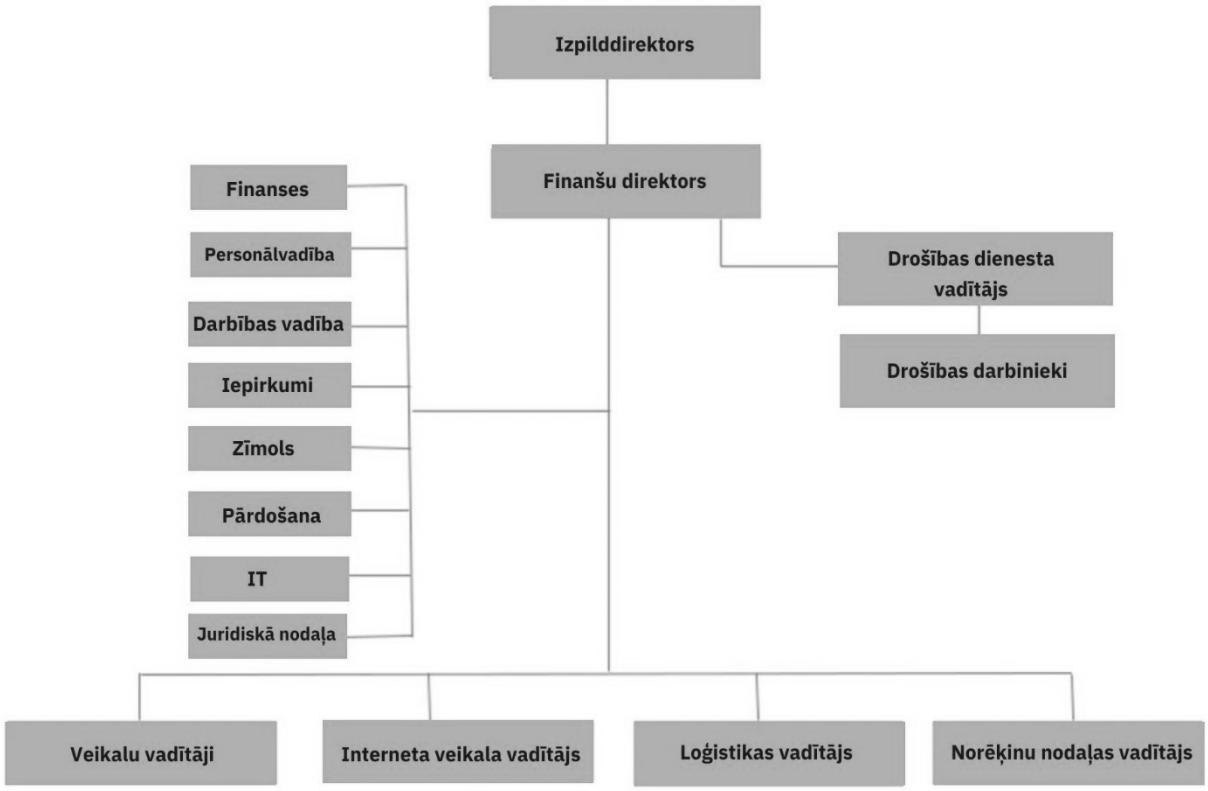
LOĢISTIKAS KOMPĀNIJAS pakalpojumu līmenis ir augsts. Īsi piegādes termiņi un zemākā cena, ieskaitot pakalpojumu, nodrošina to, ka LOĢISTIKAS KOMPĀNIJA rūpīgi skatās uz produktu ieguldījumu peļņas gūšanā.

Attīstība

- Krājumi tiek samazināti līdz minimumam. Izmērāmība ir būtiska neatkarīgi no tā, vai tās ir reklāmas kampaņas, krājumu kontrole vai zaudējumu novēršana.
- LOĢISTIKAS KOMPĀNIJA vēlas ieviest arī visu dokumentu pašskenēšanu, lai palielinātu klienta ērtības.
- Turklāt LOĢISTIKĀ KOMPĀNIJA vēlas panākt peļņas pieaugumu, palielinot pārdošanu tiešsaistē.

- Veikalā un tiešsaistē tiek piemērota viena un tā pati cena. Ja patērētājs citur var pasūtīt vēlamo preci lētāk, LOĢISTIKAS KOMPĀNIJA to piegādās par tādu pašu cenu. Tādā veidā LOĢISTIKAS KOMPĀNIJA neļauj klientiem kavēties ar pirkuma lēmuma pieņemšanu.
- LOĢISTIKAS KOMPĀNIJA preces piegādā 24 stundu laikā pēc preču pasūtīšanas.
- LOĢISTIKAS KOMPĀNIJA šobrīd izstrādā *Smart* sistēmu. No mazajiem punktiem tirdzniecības centros tiks veidotas eksperimentālas automātiskās ķēdes, kas nodrošinās ekspres-piegādi. *Smart* veikali atradīsies lielākajos tirdzniecības centros, kur pircēji varēs saņemt mazāku preču klāstu un arī konsultācijas. Viedajos *smart* centros universālais kanāls kļūs par normu. Caur caurspīdīgām sienām veikalos klienti varēs pārbaudīt, vai prece ir pieejama, kā tā izskatās, un veikt pasūtījumus. Kā nākotnes vīziju uzņēmums paredz to, ka šie pasūtījumi tiek piegādāti klientam mājās tajā pašā dienā

Struktūra



32. attēls. **LOĢISTIKAS KOMPĀNIJAS struktūrshēma**

Veikalu pārvaldība, interneta veikali, loģistikas un izplatīšanas centra noliktavas

Cik zināms, vadītājiem nav būtisku uzdevumu un pienākumu drošības jomā, bet viņi ir atbildīgi par darbinieku vadību drošības jomā veikalos, interneta veikalā un izplatīšanas centra noliktavā.

Vadītāju atbalsta nodaļas

Cik zināms, finanšu operāciju, iepirkumu, pārdošanas, IT, juridisko nodaļu vadītājiem nav būtisku uzdevumu un pienākumu drošības jomā, bet viņi ir atbildīgi par darbinieku vadīšanu savā nodaļā.

Drošība

Drošība tiek organizēta centrālā līmenī. Drošība ir personāla pakalpojums. Cik zināms, finanšu direktoram nav būtisku uzdevumu un pienākumu drošības jomā, taču viņš joprojām ir atbildīgs par apsardzes dienestu un apsardzes vadītāju. Visi ziņojumi tiek nodoti izpilddirektoram. Drošības dienesta budžets ir noteikts departamenta līmenī. Ikviena LOĢISTIKAS KOMPĀNIJAS struktūrvienība var vērsties pie drošības dienesta, kad uzskata to par nepieciešamu. Izdevumus par ieguldījumiem un uzturēšanas izmaksas sedz LOĢISTIKAS KOMPĀNIJA.

Drošības dienesta vadītājs

Drošības dienesta vadītājs ir atbildīgs par drošības pasākumu vadību, plānošanu un izpildes vadīšanu. Šī kārtība tika izstrādāta galvenajā birojā, risku klasifikācijas process ir daļa no tā. Turklāt drošības dienesta vadītājs un viņa nodaļa atbalsta valsts un vietējo vadību, veicot tādus uzdevumus kā izmeklēšanas, drošības auditi un veikalu, interneta veikala un izplatīšanas centra noliktavas atbilstības novērtējums normatīvajiem aktiem. Turklāt vadītājs pārrauga LOĢISTIKAS KOMPĀNIJAS drošības standartu, instrukcijas, vadlīnijas utt.

Drošības personāls

Drošības dienesta darbinieki veic šādus uzdevumus:

- atbalsta operatīvo vadību drošības jomā;
- palīdz gatavoties revīzijām (iekšējie novērtējumi, izmeklēšana) un atbalsta pēcpārbaudē un pasākumos;
- apkopo informāciju par incidentiem un ziņo par tiem vietējai vadībai;
- atbalsta iekšējās krāpšanas izmeklēšanas;
- izvērtē nozares informāciju un novērtē draudus;
- atbild par LOĢISTIKAS KOMPĀNIJAS drošības standarta, instrukciju, vadlīniju ieviešanu sadarbībā ar Drošības dienesta vadītāju;
- pārbauda uzstādīto fiziskās drošības iekārtu iespējamos defektus vai darbības traucējumus;
- nodrošina vispārīgu drošības informāciju un drošības apmācības darbiniekiem;
- ziņo par šo darbību rezultātiem Drošības dienesta vadītājam;
- veic risku analīzi un atbilstošu pasākumu pielāgošanu.

Drošības dienests ir atbildīgs par:

- jauno darbinieku un darbuzņēmēju pagātnes pārbaudi;
- risku uzskaiti un novērtēšanu (darba procesi, drošība);
- ārējo apsardzes darbinieku vadību;
- sanāksmju organizēšanu par riskiem;
- piekļuves kontroli;
- novērošanas kamerām;
- incidentu izmeklēšanu;
- darbības nepārtrauktības plānošanu;
- risku vadību;
- semināru organizēšanu par informētību, iekšējo apdraudējumu utt.

Veikali, interneta veikals, izplatīšanas centra noliktava

Šobrīd LOĢISTIKAS KOMPĀNIJA sastāv no 14 veikaliem, interneta veikala un izplatīšanas centra noliktavas, kuras savieno loģistikas procesus.

LOĢISTIKAS KOMPĀNIJAI ir savi veikali un franšīzes formula. Franšīzes ņēmēji maksā par formulas izmantošanu. Šiem veikaliem un franšīzes ņēmējiem LOĢISTIKAS KOMPĀNIJA organizē centrālo iepirkumu, sadales centra noliktavu, loģistikas procesu, publicitāti, apkopi, drošību un interneta veikalu. Franšīzes ņēmējs kārto personāla lietas, darba laikus, veikala atrašanās vietu, apdrošināšanu u.c.

Veikali

LOĢISTIKAS KOMPĀNIJAI ir 14 veikali. Veikali ir augstas klases patēriņa preču mazumtirgotāji. Procesu veikalā raksturo preču ienākšana, uzglabāšana un izvešana. Tiek sekots līdzi preču plūsmas ātrumam, reģistrējot produktus, kam beidzies derīguma termiņš. Tiek uzskaitītas preces, kas vēl ir veikala noliktavā un kuras nepieciešams atkārtoti pasūtīt. Veikaliem veic piegādi reizi nedēļā. Veikalos ir jaukts sortiments. Visas preces ir pārdošanā visos veikalos, un tās veikalos ir izkārtotas aptuveni vienā un tajā pašā vietā. Akcijas, kas veikaliem ir noteiktās nedēļās, tiek izceltas veikalu skatlogos. LOĢISTIKAS KOMPĀNIJA veikalā izmanto lietotni, lojalitātes karti un *Wi-Fi* klientu izsekošanu.

LOĢISTIKAS KOMPĀNIJA tic pilnīgai bezsaistes un tiešsaistes integrācijai. Integrējot interneta veikalu un fiziskos veikalus, preces var ātri sasniegt klientu par konkurētspējīgu cenu, piedāvājot arī personīgu apkalpošanu. Uzņēmumam ir pieejami arī produkti, kas pieejami tikai caur internetveikalu.

Noliktava

No izplatīšanas centra noliktavas piegādes notiek reizi nedēļā uz LOĢISTIKAS KOMPĀNIJAS veikaliem. Principā interneta veikalā iegādātās preces klientam tiek piegādātas tieši no izplatīšanas centra noliktavas. Ja pircēji internetā pasūtītās preces vēlēsies izņemt veikalā, tās uz veikaliem tiks nogādātas caur izplatīšanas centra noliktavu. Šos pasūtījumus veikalos katru dienu piegādā ārpakalpojuma sniedzējs. Tāpat kā veikalos, arī izplatīšanas centra noliktavā procesu raksturo preču ienākšana, uzglabāšana un izvešana. Izplatīšanas centra noliktavā paletes tiek sakomplektētas un sagatavotas transportēšanai. Šim procesam ir nepieciešama laba sadarbība starp veikaliem, interneta veikalu un izplatīšanas centra noliktavu ar preču saņemšanu (ienākošais) un preču izplatīšanu (izejošo).

Loģistika

Visiem veikaliem ir savi krājumi. Krājumu uzturēšanai veikalos tiek izmantotas trīs sistēmas, proti: *SAP*, *POSFlow* un *TIB*.

Lai pārvaldītu krājumus, LOĢISTIKAS KOMPĀNIJA izmanto *SAP*, kas ir uzņēmuma resursu plānošanas programma, ar kuru KOMPĀNIJA pārvalda visas preču plūsmas. Visas preces tiek reģistrētas *SAP*, ieskaitot specifikācijas un pirkšanas, nodošanas un pārdošanas cenas.

SAP ir saistīts ar *POSFlow*, LOĢISTIKAS KOMPĀNIJAS POS sistēmu, kas apvieno kases un pārdošanas uzskaites funkcijas. POS sistēma ļauj bez kavēšanās apstrādāt pārdotās preces.

SAP, pamatojoties uz pārdošanu, nosaka, cik liela ir vajadzība pēc noteikta produkta.

Ārējie pakalpojumu sniedzēji

Pasūtīšanas un atgriešanas procesā ir iesaistītas divas ārējās puses: *CEVA* un *DHL*.

CEVA ir viena no pasaulē lielākajām piegādes ķēdes pārvaldības kompānijām, kam ir līgumi ar LOĢISTIKAS KOMPĀNIJU par preču uzglabāšanu, nosūtīšanu un saņemšanu.

DHL ir transporta uzņēmums, kas pārvadā visas LOĢISTIKAS KOMPĀNIJAS preces.

Drošības dienesta vadītājs uztur labus kontaktus ar citiem līdzīgiem loģistikas organizāciju drošības vadītājiem. Drošības departamentam ir arī labs kontakts ar Valsts policiju.

Krājumi

Iepirkumu nodaļa nosaka, cik daudz krājumu jābūt katrā veikalā. Šis pasūtīšanas veids izveido savienojumu ar lietu internetu (IoT), kas nozīmē, ka objekti, kas savienoti ar internetu, sazinās viens ar otru un automātiski sāk procesu. IoT kļūst arvien svarīgāks loģistikas jomā.

LOĢISTIKAS KOMPĀNIJAS piegādes ķēdē ir divi svarīgi procesi, proti, automātiskais pasūtīšanas process un atgriešanas process.

Automātiskais pasūtīšanas process

Procesu, kurā *SAP* automātiski pasūta produktus, lai uzturētu krājumus, sauc arī par automātisko pasūtīšanas procesu. *SAP* analizē pārdošanas datus un nosaka optimālo pasūtījuma momentu un optimālo pasūtījuma daudzumu. Brīdī, kad *SAP* konstatē, ka veikalā nav pietiekami daudz preču noliktavā, *SAP* automātiski izveido pasūtījumu attiecīgajam veikalam. *POSFlow* nodrošina *SAP* ar pārdošanas datiem, lai krājumus varētu uzraudzīt.

Atgriešanas process

Papildus automātiskajam pasūtīšanas procesam ir arī atgriešanas process. Katru pirmdienu veikalā tiek izveidota preču atgriešanas atļauja (*RMA*). *RMA* sastāv no obligātās atgriešanas un *DOA* gadījumiem (angliski: *Dead On Arrival*). *DOA* ir termins, kas norāda, ka pircēja saņemtajai precei tās ierašanās brīdī tika konstatēts defekts vai bojājums. Pēc *RMA* izveidošanas *DHL* paņem pasūtījumu un nosūta to. Tur preces tiek atdotas trešajai pusei vai uzglabātas noliktavā.

Tiešās piegādes, ko veic ražotāji

Automātiskais pasūtīšanas process nodrošina 60 % veikalu piegādi no izplatīšanas centra noliktavas. Atlikušos 40 % veikalu apgādi nodrošina preču ražotāji, ar kuriem LOĢISTIKAS KOMPĀNIJA ir noslēgusi līgumu. Šo ražotāju pārstāvji paši dodas uz veikaliem, lai pārbaudītu un aizpildītu savas produkcijas plauktus. Turklāt viņi var papildināt krājumus, ja filiālei tie ir nepieciešami. Veikali nepārbauda piegādes saturu, jo var papildināt plauktus ar krājumiem, ko pārstāvji tur ir piegādājuši. Veikala darbinieki parakstās uz preču pavadzīmes par preču saņemšanu un ievada preces *SAP*. Tās pašas preces var piegādāt arī caur izplatīšanas centra noliktavu ar tādu pašu svītrkodu.

Piegāde un saņemšana veikalā

DHL kurjers novieto piegādes transportu pēc iespējas tuvāk veikalam. Pēc tam viņš izkrauj vajadzīgās preces. Brīdī, kad viņš ienāk veikalā, visu fiksē kameras. *DHL* darbinieks dodas pie veikala darbinieka, kurš dodas uz noliktavu, lai paņemtu preces, kuras jānodod kurjeram.

Situāciju apraksti

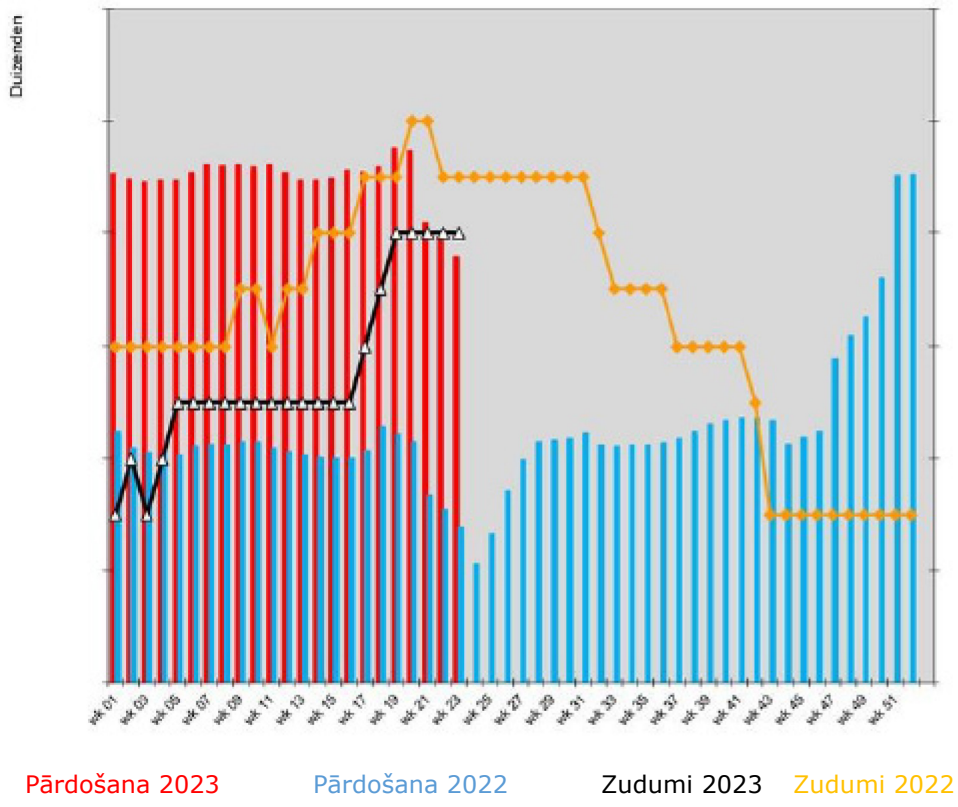
SITUĀCIJA I

Aizdomas par zaudējumiem organizētās noziedzības dēļ

Uzņēmumam ir aizdomas, ka organizētā noziedzība rada tam problēmas. Finanšu direktors vēlas, lai tiktu veikti drošības pasākumi. Finanšu analītiķis norāda, ka neskaidra un līdz šim neidentificēta preču "noplūde" jeb pazušana ir būtiska problēma LOĢISTIKAS KOMPĀNIJAI. Zādzības veido 33 % no kopējiem zudumiem. Salīdzinot ar pagājušo gadu, nenoteikto zudumu apjoms ir ievērojami palielinājies.

Nenoteiktie zudumi netieši ietekmē organizētās noziedzības kartēšanu, jo tā nozīmē, ka zudumi nav identificēti organizācijā un tiek konstatēti tikai vēlāk. Tas rada neskaidru priekšstatu par zaudējumu rādītājiem un apgrūtina organizētās noziedzības ietekmes noteikšanu vai tās apkarošanu. Ja vairāk nekā 50 % zaudējumu nav iespējams izsekot, nav iespējams precīzi noteikt, cik lielā mērā organizētā noziedzība ietekmē šo zaudējumu rādītājus.

Kopējais zaudējumu līmenis ir palielinājies par 6,41 %, salīdzinot ar to pašu periodu pagājušajā gadā. LOĢISTIKAS KOMPĀNIJAS mērķis attiecībā uz zaudējumiem ir 0,20 %. Tas ir kopējais nozagtais preču apjoms (pēc iepirkuma cenas) dalīts ar kopējo bruto apgrozījumu.



33. attēls. **LOĢISTIKAS KOMPĀNIJAS pārdošanas un zudumu dati (mācību uzdevuma attēls)**

Attēls parāda, ka zaudējumu procents 2023. gadā ir zemāks salīdzinājumā ar pagājušo gadu, taču tas ir saistīts ar palielinātu apgrozījumu. Absolūtos skaitļos (summa) zādzības un līdz ar to arī zaudējumi ir pieauguši. Ja šī gada apgrozījums būtu tāds pats kā pagājušajā gadā, zaudējumu līmenis varētu būt dubultojies.

SITUĀCIJA II

Noviržu reģistrācija

LOĢISTIKAS KOMPĀNIJĀ ir radusies situācija, kur procedūras netiek sistemātiski ievērotas. Dažos gadījumos ziņojumi "neiziet" caur Loģistikas nodaļu, kā rezultātā šī nodaļa ne vienmēr ir informēta par ziņojumiem. Citkārt Loģistikas nodaļa dažādu iemeslu dēļ neizskata ziņojumus. Šie faktori ietekmē noviržu reģistrāciju. Tātad precīzu noviržu skaitu nevar norādīt neviena no nodaļām un iesaistītājām pusēm. Loģiski, ka tas rada slēptos skaitļus.

Preces regulāri reģistrē "neautorizēta" persona. Ar "neautorizētu" personu saprotam pagaidu darbinieku, kurš piekļūst sistēmai, lai reģistrētu preces, izmantojot veikala pieejas datus. Tai pat laikā reģistrāciju darbiniekam būtu jāveic, piekļūstot un autorizējoties sistēmā ar savu kases kodu. Netiek pārbaudīts, vai veikali joprojām izmanto veikala (kopīgos) piekļuves kodus, vai arī darbinieku individuālos piekļuves kodus un autentifikācijas līdzekļus. *RMA** numurs netiek paziņots *DHL*. Būtiska problēma ir tā, ka nav kontroles mehānisma.

* *RMA* numurs (*Return Merchandise Authorization*) ir identifikācijas numurs, ko piešķir piegādātājs preču atgriešanai.

SITUĀCIJA III

Riska inventarizācija

LOĢISTIKAS KOMPĀNIJĀ nav drošības orientētas risku inventarizācijas. Organizācija uzrauga savus riskus, izmantojot drošības auditu. Tomēr šis instruments nesniedz specifisku informāciju par risku raksturu un apmēru. Tas nozīmē, ka netiek veikta draudu analīze un novērtēts, kādus zaudējumus tie var radīt LOĢISTIKAS KOMPĀNIJAI.

Tāpat nepastāv metode, ar kuru tiek apkopota, analizēta ārējā informācija un zināšanas, kas vēlāk tiek izstrādātas uzņēmuma drošības politikā. Piemēram, trūkst metodes, kas ļautu informāciju un pētījumus par noziedzību mazumtirdzniecības sektorā izanalizēt un iestrādāt konkrētā uzņēmuma drošības politikā. Tas rada plaisu starp situācijas attīstību nozarē un LOĢISTIKAS KOMPĀNIJAS pozīciju drošības jomā.

Sakarā ar padziļināta draudu un risku inventarizācijas procesa trūkumu organizācija nespēj efektīvi pielāgot drošības pasākumus pastāvošajiem drošības riskiem. Pašreizējā risku inventarizācija nav noteicošais faktors drošības pasākumu izvēlē. Tāpat trūkst pilnīgas regulāro pārbaužu un novērojumu uzskaites.

IETVARS, KONTEKSTS UN KRITĒRIJI DROŠĪBAS RISKU VADĪBĀ

6. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORS: Raimundas Kalesnikas, Kazimiras Simonavičius Universitāte, Lietuva

Konteksts

Drošības risku vadības panākumi būs atkarīgi no vadības sistēmas efektivitātes, kas palīdz efektīvi pārvaldīt drošības riskus, piemērojot riska vadības procesu dažādos līmeņos un konkrētos organizācijas kontekstos. Pirms uzsākt drošības risku vadības sistēmas izstrādi un ieviešanu, ir svarīgi: a) izprast gan organizācijas ārējo, gan iekšējo kontekstu; b) definēt ārējos un iekšējos parametrus riska vadībai; c) noteikt drošības risku vadības procesu apjomu un risku kritērijus, kā aprakstīts ISO 31000:2018 standartā.

ATSAUCE UZ ISO 31000 STANDARTU Saskaņā ar ISO 31000 standartu, ietvara, konteksta un kritēriju noteikšanas mērķis ir pielāgot risku vadības procesu, ļaujot efektīvi novērtēt riskus un piemērot atbilstošas risku novērtēšanas metodes. Ietvars, konteksts un kritēriji ietver procesa darbības jomas definēšanu un organizācijas ārējā un iekšējā konteksta izpratni.	

Uzdevuma mērķis

Studējošie iegūs teorētiskās zināšanas un pilnveidos praktiskās iemaņas par procedūrām un metodēm, kas nepieciešamas organizācijas konteksta izpratnei. Tas ļaus viņiem noteikt drošības risku vadības procesa ietvaru un veikt vides novērtējumu, izmantojot dažādas ISO 31000 metodes, lai organizācija varētu sasniegt savus mērķus drošības risku pārvaldībā.

UZDEVUMS STUDENTIEM

1. Izveidojiet grupas saskaņā ar pasniedzēja norādījumiem. Grupas veidojot, nodrošiniet dažādību (studiju joma, programma, līmenis un studiju gads, darba pieredze, ja tāda ir, utt.).
2. Katra studentu grupa iepazīstas ar notikuma scenāriju un konkrēto uzdevumu, ko piešķir pasniedzējs. Notikums ir jāanalizē organizācijas kontekstā (publiskā vai privātā sektorā), precizējot nozari, kurā organizācija darbojas (piemēram, Valsts robežsardze, uzņēmums, kas attīsta kritisko infrastruktūru utt.).
3. Katra studentu grupa saņem vienu metodi, kas ir piemērojama drošības risku vadības procesa konteksta izpratnei un noteikšanai, piemēram PESTLE vai līdzīgu (skatīt pielikuma materiālos).
4. Iepazīstieties ar jums piešķirto metodi un veiciet uzdevumu, izmantojot prāta vētras metodi saskaņā ar pasniedzēja norādījumiem. Uzdevuma izpildes laika ierobežojums katrai grupai ir 15 minūtes.
5. Sagatavojiet īsu prezentāciju par piešķirto metodi saviem kursabiedriem. Prezentāciju var sniegt dažādos veidos: mutiski, izmantojot līmlapiņas (flipčartu), baltās tāfeles pierakstus, *PowerPoint* u.c.
6. Katra studentu grupa nominē runātāju, kurš prezentēs grupas uzdevuma rezultātus un secinājumus pārējiem studentiem. Prezentācijas laika ierobežojums – līdz 5 minūtēm.
7. Klausieties kursabiedru prezentācijas. Pēc katras prezentācijas apspriediet 2 minūtes savā grupā, vai attiecīgā metode būtu piemērojama jūsu mērķim. Dalieties savās pārdomās ar pārējiem, kad pienāk jūsu kārta.
8. Pēc visu prezentāciju noslēguma pasniedzēja vadībā diskutējiet savā grupā par to, kuri no prezentētajiem parametriem (iekšējie un ārējie) būtu jāņem vērā tālākajā drošības risku vadības procesā. Dalieties par secinājumiem ar pārējiem. Diskusijas laika ierobežojums – līdz 10 minūtēm.

UZDEVUMS PASNIEDZĒJIEM

1. Izveidojiet studentu grupas (ieteicams ne mazāk kā trīs un ne vairāk kā pieci cilvēki vienā grupā). Izlemiet, kādā veidā studenti tiks sadalīti grupās.
2. Izvēlieties kādu draudu scenāriju vai izmantojiet labās prakses piemērā "HIBRĪDDRAUDI UN DROŠĪBAS RISKU VADĪBA" aprakstīto situāciju ar hibrīddraudiem robežas apdraudējuma scenārijā. Sniedziet studentiem īstu ieskatu par analizējamo gadījumu, kas saistīts ar drošības risku vadības procesu. Prezentējiet galvenos principus par konteksta noteikšanu drošības risku vadībā saskaņā ar ISO 31000.
3. Izskaidrojiet katrai studentu grupai piešķirto uzdevumu. Norādiet atsauces uz prasībām, kas saistītas ar konteksta noteikšanu drošības risku vadības procesā, balstoties uz ISO 31000, skatiet informāciju uzdevuma papildu materiālos.
4. Piešķiriet katrai studentu grupai vienu no ISO 31000 noteiktajām pamatnostādnēm, piemēram, organizācijas un tās konteksta izpratne (publiska un/vai privāta organizācija), ārējo faktoru noteikšana (konteksts), iekšējo faktoru noteikšana (konteksts), risku kritēriju definēšana, drošības risku vadības procesa ietvara noteikšana. Atkarībā no studentu grupu skaita uzdevuma saturs var tikt sašaurināts vai paplašināts.

5. Sagatavojiet un nodrošiniet katrai studentu grupai uzdevuma veidlapu (papīra dokumentu). Studenti strādās ar šo veidlapu. Izskaidrojiet, kādus rezultātus sagaidāt no konkrētā uzdevuma.
6. Nosakiet uzdevuma izpildes laika ierobežojumu – 15 minūtes.
7. Sekmējiet studentu darbu un sniedziet palīdzību, ja rodas jautājumi par uzdevumiem.
8. Instruējiet katru studentu grupu sagatavot īsu prezentāciju par uzdevumā iegūtajiem rezultātiem un secinājumiem. Prezentāciju var veikt mutiski, izmantojot līmlapiņas (flipčartu), baltās tāfeles pierakstus, *PowerPoint* u.c. Prezentācijas laika ierobežojums – līdz 5 minūtēm.
9. Pēc visu prezentāciju beigām vadiet diskusiju par to, kuri no prezentētajiem parametriem (iekšējie un ārējie) būtu jāņem vērā drošības risku vadības procesā. Diskusijas laika ierobežojums – līdz 10 minūtēm.
10. Apkopojiet visu studentu grupu uzdevumu izpildes kopējos rezultātus.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Spēja strādāt komandā, spēja strādāt ierobežotā laikā, prezentācijas prasmes, argumentācijas prasmes, kritiskā domāšana.

PAPILDU MATERIĀLI

ISO 31000 – ORGANIZĀCIJAS KONTEKSTA NOVĒRTĒŠANAS METODES

PESTLE analīze

Faktori, kas jāņem vērā, analizējot organizācijas kontekstu attiecībā uz ārējiem faktoriem, izmantojot PESTLE analīzes metodi:

- politiskie (*Political*)
- ekonomiskie (*Economic*)
- sociālie (*Social*)
- tehnoloģiskie (*Technological*)
- juridiskie (*Legal*)
- vides (*Environmental*)

Vairāk par PESTLE analīzi lasi šeit:

ISO 31000

DROŠĪBAS RISKU VADĪBAS PROCESS

IETVARA DEFINĒŠANA

Dažādi organizācijas darbības līmeņi (piemēram, stratēģiskais, operatīvais, programmas, projekta vai citi)

- Mērķi un lēmumi, kas jāpieņem
- Sagaidāmie rezultāti no veicamajiem soļiem procesā
- Laiks, vieta, konkrēti iekļaujamie un izslēdzamie elementi
- Atbilstoši risku novērtēšanas rīki un tehnikas
- Nepieciešamie resursi, atbildība un saglabājamie ieraksti
- Attiecības ar citiem projektiem, procesiem un aktivitātēm

KONTEKSTA NOTEIKŠANA

Vide, kurā organizācija cenšas sasniegt savus mērķus

ĀRĒJAIS KONTEKSTS

Saskaņā ar ISO 31000 standartu ārējā konteksta izpratnē organizācijai būtu jāņem vērā šādi faktori:

- sociālie, kultūras, politiskie, juridiskie, normatīvie, finanšu, tehnoloģiskie, ekonomiskie, dabas un konkurences vides faktori neatkarīgi no tā, vai tie ir starptautiski, nacionāli, reģionāli vai lokāli;
- galvenie virzītājspēki un tendences, kas ietekmē organizācijas mērķus;
- ārējo ieinteresēto pušu attiecības, uztvere, vērtības, vajadzības un gaidas;
- līgumattiecības un saistības;
- tīklu un atkarību sarežģītība.

IEKŠĒJAIS KONTEKSTS

Saskaņā ar ISO 31000 standartu organizācijas iekšējā konteksta izpratnē būtu jāņem vērā šādi faktori:

- vīzija, misija un vērtības;
- pārvaldība, organizatoriskā struktūra, lomas un atbildības;
- stratēģija, mērķi un politikas;
- organizācijas kultūra;
- organizācijas pieņemtie standarti, vadlīnijas un modeļi;
- spējas, kas izprotamas resursu un zināšanu ziņā (piemēram, kapitāls, laiks, cilvēki, intelektuālais īpašums, procesi, sistēmas un tehnoloģijas);
- dati, informācijas sistēmas un informācijas plūsmas, lēmumu pieņemšanas procesi (gan formāli, gan neformāli);
- attiecības ar iekšējām ieinteresētajām pusēm, ņemot vērā to uztveri un vērtības;
- līgumattiecības un saistības;
- savstarpējās atkarības un savienojumi.

RISKU KRITĒRIJU DEFINĒŠANA

- Nenoteiktību veids un raksturs, kas var ietekmēt rezultātus un mērķus (gan taustāmus, gan netaustāmus)
- Kā tiks definētas un mērītas sekas (gan pozitīvas, gan negatīvas) un to iespējamība
- Laika faktori, kas saistīti ar seku iespējamību un/vai pašām sekām
- Mērījumu konsekvence
- Kā tiks noteikts riska līmenis un kad tas kļūst pieņemams vai tolerējams
- Kā tiks ņemtas vērā vairāku risku kombinācijas un secības, un, ja tā, kā un kuras kombinācijas būtu jāapsver
- Organizācijas kapacitāte

PIEMĒRS

Konteksta analīze – draudu identificēšana

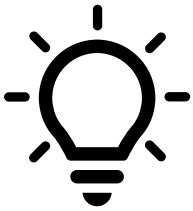
1. solis – IDENTIFICĒ. Identificē draudus.

2. solis – NOVĒRTĒ. Novērtē draudus un nosaki savas organizācijas risku līmeni (ievainojamību).

3. solis – IZSTRĀDĀ. Izstrādā stratēģiju, lai mazinātu riskus un ievainojamību.

34. attēls. **Draudu identifikācijas shēma**

Vardarbīgi draudi	Organizatoriskie draudi	Vides draudi
1) Mērķtiecīgs bruņots uzbrukums 2) Nemērķtiecīgs bruņots konflikts 3) Nolaupīšana 4) Terorisms 5) Auto nolaupīšana 6) Seksuāla vardarbība 7) Pilsoniskie nemieri 8) Reliģiska vardarbība 9) Noziedzība 10) Citi vardarbības veidi	11) Reputācijas risks 12) Finanšu risks (banku sistēma, valūtas maiņa, zādzība, piesavināšanās) 13) Korupcija 14) Juridiskais risks (darba atļaujas, atbilstība vietējiem likumiem, pretestība interešu aizstāvībai) 15) Politiskais risks 16) Vardarbība vai diskriminācija darbavietā 17) Kultūras izaicinājumi	18) Dabas katastrofas (laikapstākļi, zemestrīces, plūdi) 19) Medicīniskie riski (pieejamība piemērotai medicīniskai aprūpei personālam) 20) Ar veselību saistīti jautājumi (pārtika, ūdens, slimības, stress) 21) Satiksmes un ceļu negadījumi 22) Citi negadījumi 23) Ugunsgrēki



NODERĪGI! *Frontex* tīmekļa vietnē iespējams iepazīties ar Kopējo integrēto risku analīzes modeli (CIRAM), kas izstrādāts, lai palīdzētu *Frontex*, kā arī Eiropas Savienības un Šengenas valstīm sagatavot risku analīzes. CIRAM veicina vienotu izpratni par risku analīzi un skaidro, kā šis rīks var veicināt lielāku saskaņotību ārējo robežu pārvaldībā.

CIRAM izmanto vadības pieeju riska analīzei, definējot risku kā draudu, ievainojamības un ietekmes funkciju. Šī pieeja atspoguļo Šengenas Robežu kodeksa un Eiropas Robežu un krasta apsardzes regulējuma garu, kas uzsver riska analīzi kā galveno rīku resursu optimālai sadalei budžeta, cilvēkresursu un aprīkojuma ierobežojumu ietvaros.

Šeit ir pieejama arī CIRAM brošūra dažādās valodās, tai skaitā latviešu valodā.

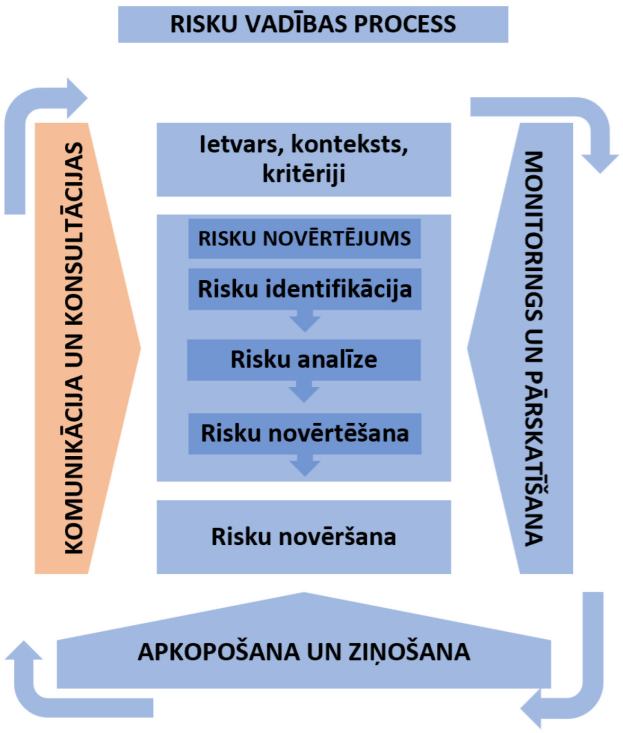
PUBLISKO VIETU TERORISMA RISKU NOVĒRTĒJUMS

7. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORE: Elizabeta Garsija Rulla, Prevencijas un integrētās drošības skola, Spānija

Konteksts

Saskaņā ar ISO 31000 Eiropas Savienībā (ES) ir publicēts raksts "Publisko telpu terorisma riska novērtējums praktiķiem", kas ir ļoti noderīgs rīks pilsētas amatpersonām un drošības jomas darbiniekiem. Šajā rakstā ir iekļauts ES ievainojamības novērtējuma kontrolsaraksts valsts un drošības iestādēm. Kontrolsaraksts ir ļoti noderīgs rīks. Lasi vairāk par to, skenējot QR kodu.

ATSAUCE UZ ISO 31000 STANDARTU	
Saskaņā ar ISO 31000 riska analīze ietver ievainojamības novērtējumu. ES ievainojamības novērtējuma kontrolsarakstā valsts un drošības iestādēm ir noteikti daži neaizsargātības aspekti, kas jāņem vērā.	

Uzdevuma mērķis

Studenti iepazīsies ar risku analīzes procesā vērtējamo ievainojamības novērtēšanu terorisma jomā.

UZDEVUMS STUDENTIEM

1. Veidojiet grupas saskaņā ar pasniedzēja norādījumiem.
2. Jūsu uzdevums ir izvēlēties lielu, pazīstamu laukumu savā pilsētā vai jebkurā citā pilsētā. Iedomājaties, ka pastāv liels teroristu uzbrukuma risks, kurā terorists izmanto transportlīdzekli kā ieroci. Izmantojot šo informāciju, jūsu grupas uzdevums ir analizēt sava izvēlētā objekta ievainojamību. Izmantojiet kontrolsarakstu, kas pievienots uzdevuma pielikumā.
3. Nākamais uzdevums ir izveidot informatīvu materiālu, kas ir viegli saprotams un vizuāli pievilcīgs. Materiāla izveidei iesakām izmantot vizuālās rediģēšanas rīkus, piemēram, *Canva*, *Infogram* vai *Piktochart*. *Canva* nodrošina arī izveidoto materiālu bezmaksas lejupielādi. Iesācēju apmācību videoklipus varat atrast vietnē *YouTube*: https://www.youtube.com/playlist?list=PLATYfhN6gQz8GiTG_nUxVar8ycrt9hJxL.
4. Prezentējiet savu materiālu un izskaidrojiet tajā iekļauto informāciju:
   Kāpēc izvēlēta tieši šī mērķa grupa, kāpēc materiālā iekļautā informācija ir svarīga konkrētai mērķa grupai un kādas zināšanas mērķa grupa iegūs, iepazīstoties ar informatīvo materiālu.

UZDEVUMS PASNIEDZĒJIEM

1. Izveidojiet studentu grupas (ieteicams ne vairāk kā četri cilvēki vienā grupā).
2. Izskaidrojiet uzdevumu studentiem, uzsverot, cik svarīgi ir attīstīt prasmes, lai efektīvi nodotu drošības informāciju kolēģiem un sabiedrībai. Ieteicams prezentēt pētījuma rezultātus par jauno drošības speciālistu prasmēm. Skenējiet kvadrātkodu, lai uzzinātu vairāk.
3. Palīdziet studentiem izvēlēties mērķa grupu un informatīvā materiāla fokusu. Ja nepieciešams, sniedziet piemērus un norādījumus.
4. Ja studentiem trūkst pieredzes un prasmju, izmantojot vizualizācijas rīkus, piemēram, *Canva*, *Infogram* vai *Piktochart*, sniedziet pamatapmācību par kādu no šiem vizuālās rediģēšanas rīkiem.
5. Izvērtējiet studentu izstrādātos informatīvos materiālus un pārrunājiet to saturu, sniedzot ieteikumus uzlabojumiem.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Spēja strādāt komandā limitētos laika rāmjos, prezentācijas prasmes, spēja efektīvi sazināties, digitālās prasmes (vizuālās rediģēšanas prasmes).

PIELIKUMS

Informācija no Eiropas Komisijas izstrādātā publisko telpu terorisma riska novērtējuma. Pieejams: https://ec.europa.eu/newsroom/pps/items/674909/en

Ievainojamības novērtējums

Ievainojamība ir potenciālā mērķa raksturīgās nepilnības. Kritiska ievainojamības izvērtēšana uzbrukuma scenāriju kontekstā palīdzēs lēmumu pieņēmējiem izstrādāt efektīvus atturēšanas un mazināšanas pasākumus, palīdzēs izstrādāt stratēģijas seku mazināšanai, ārkārtas situāciju pārvaldības plānus un paaugstināt noturību. Ievainojamība ir atkarīga no draudu specifikas, situācijas un laika.

35. attēls. **Eiropas Komisijas izstrādātā publisko telpu terorisma riska novērtējuma shēma**

ES ievainojamības novērtējuma kontrolsaraksts uzsver virkni faktoru, kas jāņem vērā, vērtējot vājās vietas. Tajā ir arī praktiski jautājumi, kas jāuzdod, veicot dažādu veidu publisko telpu ievainojamības novērtēšanu saistībā ar plašu apdraudējumu klāstu.

Publiskās telpas ievainojamība tiek klasificēta atbilstoši dažādām piekļuves/ieejas/izejas publiskajai telpai, fāzēm un ir saistīta ar iespējamiem uzbrukuma scenārijiem un apsvērumiem. Ir pieejamas papildu ievainojamības novērtēšanas matricas iekšējās drošības apdraudējumiem un dronu uzbrukumiem. Ievainojamības aspekti, kas jāņem vērā:

Pievedceļi konkrētai vietai

- Vājās vietas, sašaurinājumi (iespējams transportlīdzekļa izraisīts sprādziens, arī blakus gājēju satiksmei)
- Alternatīvi piebraucamie/izbraucamie ceļi
- Tuvums galvenajai ceļu infrastruktūrai, dzīvojamiem rajoniem, citai transporta infrastruktūrai
- Piekļuve lieliem/smagiem transportlīdzekļiem

Autostāvvieta un transporta iespējas

- iebraukšanas plūsmu īpatnības (tuneļi, maršruta autobusi, šauras joslas)
- blakus esošās sabiedriskās vietas
- stāvvietu/transporta iekārtu stāvoklis attiecībā pret publisko vietu

Gājēju piekļuve

- Vājās vietas, sašaurinājumi (iespējamas cilvēku improvizēto spridzekļu eksplozijas, aktīvo šāvēju incidenti)
- Apkārtējās būves, kuras var izmantot teroristi
- Sabiedriskais transports

Ieejas/izejas punkti

- Pūļa drūzmēšanās
- Neaizsargātība pret uzbrukumiem ārpus aizsargātā perimetra
- avārijas izejas
- Elektroniski darbināmas iekārtas (lifti, mobilās barjeras u.c.)

Piekļuves kontrole

- Piekļuves kontroles izvietošana tā, lai neizraisītu pūļa drūzmēšanos
- Iespēja izlauzties cauri piekļuves kontrolei

Atklātas piekļuves publiskās vietas

- Iespēja pārorientēt pūļa plūsmu
- Pūļa neaizsargātība ieejas un izejas punktos ārpus publiskās telpas
- Patvēruma klātbūtne pret iespējamu apšaudes/transportlīdzekļa taranēšanas uzbrukumu
- Aizsardzība pret dronu uzbrukumiem

Strukturālā noturība

- Fragmentu/konstrukciju daļu sabrukšanas iespēja
- Citas ēkas/būves tuvumā

Iekšējās drošības pasākumi

- Līdzekļi uzbrucēju pārbaudei/apturēšanai
- Apkalpojošā personāla/transportlīdzekļu kontrole
- Iekšējie draudi un iekšējā kontrole

Sistemātiska un nepārtraukta terorisma risku novērtēšana publiskajām telpām ir būtiska prioritāšu noteikšanai, plānošanai un efektīvu seku mazināšanas risinājumu ieviešanai. Praksē nav uzbrukumiem drošu risinājumu un vienmēr būs pieņemams riska faktors. Tomēr teroristu mērķis ir ar savu uzbrukumu panākt visaugstāko haosu, līdz ar to viņi bieži izvēlas publisko telpu atklāto ievainojamību. Seku mazināšanas pasākumu īstenošana, kas sistemātiski analizē riskus, nodrošinās lielāku noturību teroristu uzbrukuma gadījumā, un šādu pasākumu īstenošana var atturēt teroristus no konkrētā uzbrukuma mērķa izvēlēšanās.

KOMUNIKĀCIJA KRĪZES SITUĀCIJĀS

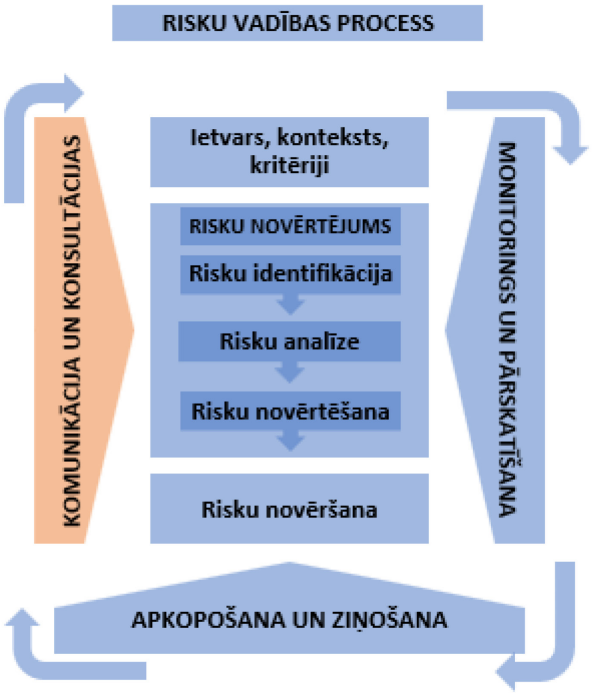
8. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORS: Uģis Začs, Biznesa augstskola *Turība*, Latvija

Konteksts

Sešu valstu eksperti 2022. gada nogalē veiktajā pētījumā uzsvēra, ka drošības speciālistiem trūkst zināšanu un prasmju informēt un skaidrot drošības jautājumus un drošības risku nozīmi gan kolēģiem, gan sabiedrībai kopumā. Skaidrs, ka bez kolēģu izpratnes un iesaistes drošības nodrošināšana organizācijā vai uzņēmumā kļūst neiespējama. Vēl jo svarīgāk tas ir svarīgi krīzes situācijās. Tāpēc viens no drošības speciālista uzdevumiem organizācijā vai uzņēmumā ir spēt nodrošināt pareizu komunikāciju krīzes situācijā.

Ar pilnu ziņojumu par prasmēm var iepazīties šeit: https://security.turiba.lv/2022/12/06/what-skills-young-security-specialists-are-missing/

ATSAUCE UZ ISO 31000 STANDARTU Saskaņā ar ISO 31000 standartu komunikācijai ir ārkārtīgi liela nozīme efektīvā risku pārvaldībā. Komunikācijai ir izšķiroša nozīme visos risku pārvaldības procesa posmos, tostarp risku identificēšanā, analīzē, novēršanā un uzraudzībā.	

Uzdevuma mērķis

Viens no svarīgākajiem drošības risku vadības aspektiem ir prasme organizēt ātru un precīzu komunikāciju krīzes situācijās. Šī uzdevuma mērķis ir apmācīt studentus īsi un kodolīgi komunicēt par krīzes situāciju un sagatavot saprotamu vēstījumu.

UZDEVUMS STUDENTIEM

1. Sagatavojiet savus mobilos telefonus.

2. Saskaņojiet ar pasniedzēju saziņas metodi (SMS, *WhatsApp* vai cits veids).
3. Noskatieties video kopā ar pasniedzēju.
4. Iedomājieties, ka jūs esat Drošības nodaļas vadītājs. Jums ir jāsagatavo skaidrs informatīvs ziņojums par situāciju. Jums ir svarīgi informēt visus uzņēmuma darbiniekus, tostarp jāsniedz informācija, ko darīt, kā rīkoties, ko nedrīkst darīt, ja iestājas šāda krīze un informācija par uzņēmumu parādās medijos.

UZDEVUMS PASNIEDZĒJIEM

1. Pasniedzējs vienojas ar studentiem par saziņas metodi – e-pasts, SMS, *messenger*, *WhatsApp* vai cita metode. Pasniedzējs norāda saziņas kanāla numuru vai nosaukumu.
2. Pasniedzējs demonstrē video par krīzes situāciju. Var izvēlēties jebkuru video, kas parāda kādu krīzes situāciju, īpaši tādu, kas varētu nonākt medijos un radīt uzņēmumam negatīvu publicitāti. Var izmantot, piemēram, *YouTube* video, skenējot QR kodu.
3. Šo videoklipu var atrast arī vietnē *YouTube*, meklējot "Domino picas krīze, netīra Dominos pica".
4. Noskatieties šo video kopā ar studentiem.
5. Pasniedzējs lūdz studentus sagatavot un pa iepriekš izvēlēto kanālu nosūtīt ziņu. Studentam jāgatavo ziņu tā, it kā viņš būtu apsardzes priekšnieks, detalizēti norādot, kā viņi informētu uzņēmuma darbiniekus pēc šāda video parādīšanās medijos.
6. Pēc ziņu saņemšanas pasniedzējs analizē atbildes un sniedz atgriezenisko saiti un ieteikumus par to, vai komunikācija bija skaidra, vai norādījumi darbiniekiem bija skaidri un konsekventi un vai no ziņojuma bija skaidrs, ko darīt, kā rīkoties un kā sazināties ar plašsaziņas līdzekļiem.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Spēja pieņemt lēmumus; prasme formulēt informāciju un viedokli.

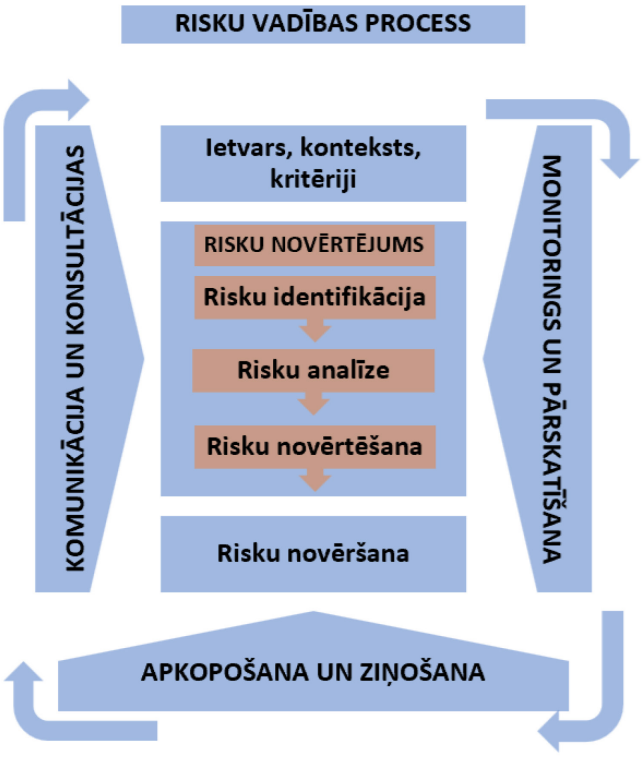
RISKU IDENTIFICĒŠANA UN PRIORITĀŠU NOTEIKŠANA, IZMANTOJOT RISKU VARBŪTĪBAS UN IETEKMES MATRICU

9. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORS: Uģis Začs, Kristīne Neimane, Biznesa augstskola *Turība*, Latvija

Konteksts

Risku pārvaldība prasa rūpīgu risku identificēšanu kā vienu no pirmajiem procesa soļiem, kā aprakstīts ISO 31000:2018 standartā. Turpmākie soļi ietver risku analīzi un novērtēšanu, kas prasa spēju noteikt to prioritāti.

ATSAUCE UZ ISO 31000 STANDARTU Saskaņā ar ISO 31000 standartu risku identificēšana ir pirmais solis riska novērtēšanas procesā. Nākamie soļi ir riska analīze un novērtēšana.	

Uzdevuma mērķis

Viens no svarīgākajiem drošības risku pārvaldības aspektiem ir spēja identificēt un prioritizēt riskus. Lai attīstītu un uzlabotu šīs prasmes, ir svarīgi trenēt šo prasmi ar praktisku uzdevumu palīdzību. Šī konkrētā uzdevuma mērķis ir palīdzēt studentiem iemācīties identificēt iespējamos drošības riskus, kas saistīti ar dažādiem stacionāriem objektiem, un tad tos prioritizēt. Šādā veidā studenti var iejusties drošības dienestu vadītāju lomā un izprast, kā efektīvi mazināt šos riskus.

UZDEVUMS STUDENTIEM

1. Studenti izvēlas vienu fizisku objektu.
2. Nākamais solis ir identificēt 20 drošības riskus, kas varētu būt saistīti ar konkrēto objektu.
3. Novērtējiet šos riskus pēc diviem kritērijiem: varbūtība un sekas. Izmantojiet skalu no 1 līdz 5, kur 1 ir "neiespējamas/mazas sekas" un 5 apzīmē "noteikti notiks / lielas sekas, kas var izraisīt organizācijas slēgšanu".

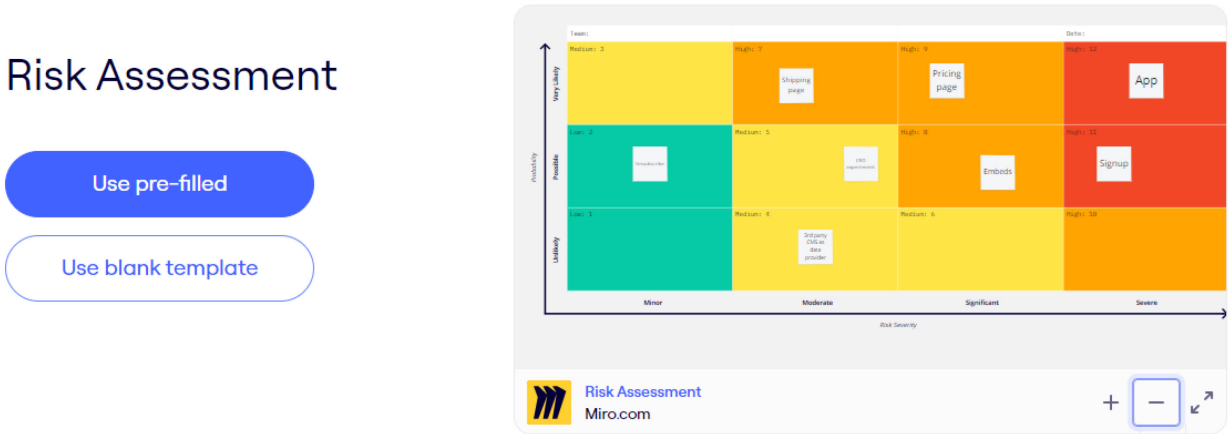
   Piemērs

Risks	Varbūtība	Ietekme	Koeficients
Ugunsgrēks objektā	2	4	8

   Riska koeficientu aprēķina, reizinot varbūtību ar sekām.
4. Pamatojoties uz koeficientiem, nosakiet piecus svarīgākos riskus, prioritizējiet tos. Tālāk jau analizējiet, kā tos varētu samazināt. Sagatavojiet prezentāciju par paveikto darbu.

UZDEVUMS PASNIEDZĒJIEM

1. Ja ir seši vai vairāk studentu, tie jāsadala pa pāriem. Ja ir mazāk, tad katrs students var strādāt individuāli.
2. Piešķiriet vai izlozējiet katram studentam vai pārim kādu no šādiem stacionāriem objektiem: banka, iepirkšanās centrs, skola, degvielas uzpildes stacija, pārtikas veikals, autoserviss, kazino, restorāns, viesnīca, naktsklubs, kokzāģētava, vēstniecība, lidosta, dzelzceļš, stacija, biroju ēka, sporta halle, klientu apkalpošanas centrs, kino, jahtklubs, piena kombināts, zoodārzs, autosalons vai slimnīca.
3. Pēc tam, kad studenti ir pabeiguši savus uzdevumus, pasniedzējs var analizēt risku novērtēšanas matricu un studentu aprēķinātos koeficientus. Pasniedzējs var noteikt, vai koeficienti ir reāli, vai arī atsevišķos gadījumos varbūtības un seku novērtējums nav ticams. Turklāt pasniedzējs var sniegt atgriezenisko saiti par studentu identificētajiem risku samazināšanas priekšlikumiem.
4. Pasniedzējs var ieteikt studentiem izmantot digitālo risku novērtēšanas matricu. Piemēram, piedāvā *Miro.com* veidni risku novērtēšanai.



36. attēls. **Varbūtības risku matrica**
Risku novērtēšanas matrica pieejama *Miro.com*

Vairāk par varbūtības–ietekmes risku matricu varat lasīt šeit:

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Darbs grupā, salīdzināšanas prasmes un kritiskā domāšana, izmantojot digitālo matricu – digitālās prasmes.

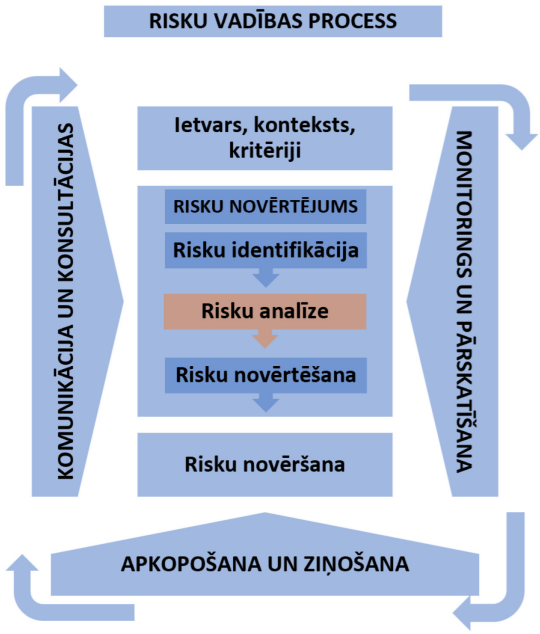
RISKU ANALĪZE

10. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORS: Oskari Lahtinen, Laurea Lietišķo zinātņu universitāte, Somija

Konteksts

Efektīva risku vadība prasa pareizu identificēto risku analīzi. Saskaņā ar ISO 31000:2018 standartu tā ir vidējā risku novērtēšanas posma sastāvdaļa. Lai nodrošinātu efektīvu risku analīzi, vienmēr ir svarīgi izmantot dažādus rīkus.

ATSAUCE ISO 31000 STANDARTU ISO 31000:2018 standartā riska analīze ir attēlota kā vidējais posms risku novērtēšanas procesā un kā visa procesa centrālā daļa.	

Uzdevuma mērķis

Studenti iepazīsies ar risku analīzes metodēm un rīkiem, kas aprakstīti IEC 31010:2019 standartā, un izvēlēsies trīs rīkus vienai no trim analīzes jomām: seku, iespējamību vai risku līmeņa novērtēšanai. Pēc tam studenti analizēs un salīdzinās metožu efektivitāti un pielietojumu.

UZDEVUMS STUDENTIEM

1. Izveidojiet grupas no 4 līdz 5 cilvēkiem.
2. Katrai grupai tiks piešķirti trīs rīki – pa vienam katrai kategorijai (sekas, iespējamība un riska līmenis), kā aprakstīts IEC 31010:2019 standarta A.3 punktā*.
3. Pasniedzējs jums piešķirs mērķa objektu un risku sarakstu.
4. Izpētiet jums piešķirtos rīkus un sagatavojieties īsai prezentācijai par tiem, kā arī par analīzes rezultātiem, ko prezentēsiet studiju biedriem.

5. Izmantojiet jums piešķirtos rīkus, lai analizētu dotos riskus, ņemot vērā mērķa darbību un darbības vidi. Jūs varat izvēlēties, kuru rīku izmantot katram riskam, taču nav nepieciešams analizēt katru risku ar visiem rīkiem.
6. Pierakstiet analīzes rezultātus un sagatavojieties to prezentēšanai.
7. Prezentējiet izmantotos rīkus, piešķirto mērķa objektu un jūsu analīzes rezultātus.
8. Noklausieties pārējās prezentācijas un pēc katras sagatavojiet komentārus un jautājumus par to, kā jūsu metodes atšķiras, kuru metodi jūs uzskatāt par labāko un kāpēc.
9. Kad visas prezentācijas būs pabeigtas, jums būs iespēja apspriesties savā grupā par rīku atšķirībām. Diskusijas noslēgumā katra grupa prezentē savas atziņas pārējiem.

UZDEVUMS PASNIEDZĒJIEM

1. Pirms nodarbības novērtējiet, cik grupu būs, un sagatavojiet pietiekamu skaitu risku analīzes rīku, kas atbilst uzdevumam un izvēlētajam scenārijam, katrai kategorijai (sekas, iespējamība un riska līmenis), katrai grupai, izmantojot IEC 31010:2019 standarta tabulu A.3.*
2. Pirms nodarbības sagatavojiet izdomātu vietu un sarakstu ar vismaz četriem identificētiem riskiem. Pietiek ar objekta plānojuma shēmu un tā darbības aprakstu. Varat arī izmantot pielikumos iekļautos piemērus.
3. Nodarbības laikā instruējiet studentus izveidot grupas no 4 līdz 5 cilvēkiem, ja nepieciešams, varat izmantot jebkuru vēlamo metodi, lai sadalītu studentus grupās.
4. Piešķiriet katrai grupai trīs analīzes rīkus (no A.3 tabulas) – pa vienam katrai kategorijai, kā arī sagatavoto mērķi un identificētos riskus.
5. Instruējiet studentus izpētīt savus piešķirtos trīs rīkus un iepazīties ar tiem. Informējiet studentus, ka viņiem jāizmanto piešķirtie rīki, lai analizētu viņiem piešķirtās vietas riskus, un atgādiniet par darbības apraksta izlasīšanas nozīmi un tā ievērošanu analīzē. Atgādiniet studentiem, ka viņiem jāizvēlas, kuru rīku izmantot katram riskam, un iesakiet neanalizēt katru risku ar visiem rīkiem.
6. Informējiet studentus, ka pēc analīzes viņi prezentēs savus trīs rīkus un analīzes rezultātus kursabiedriem. Izvēlieties jebkuru prezentācijas metodi, kas jums šķiet piemērota. Prezentācijai jābūt ne garākai par 5 minūtēm (atkarībā no studentu skaita šo laiku var saīsināt vai pagarināt), un tai jāiekļauj ne vairāk kā 6 slaidi vai 2 lapas atkarībā no izvēlētās prezentācijas metodes.
7. Atgādiniet studentiem pierakstīt savus secinājumus jebkurā izvēlētajā veidā. Pieņemami ir visi prezentācijas formāti, piemēram, *Word*, *Miro*, pieraksts uz papīra vai *PowerPoint*.
8. Kamēr studenti analizē riskus un gatavo savas prezentācijas, jūsu uzdevums ir uzraudzīt procesu un palīdzēt studentiem ar jautājumiem par prezentācijas metodi vai analīzes rīkiem.
9. Instruējiet studentus prezentēt savus trīs rīkus un risku analīzes rezultātus. Informējiet viņus par prezentāciju secību un izveidojiet grafiku, kur katra prezentācija ilgst 5 minūtes, un pēc katras tiek atvēlētas 2 minūtes komentāriem.
10. Prezentāciju laikā jūsu uzdevums ir sekot līdzi laikam un nepieļaut, ka to pārsniedz. Sniedziet atsauksmes diskusiju laikā un vadiet diskusiju. Ja studenti nelabprāt iesaistās diskusijā, varat sniegt pirmos komentārus kā piemēru un piedāvāt studentiem tēmas, par kurām var diskutēt. Ja nepieciešams, strukturējiet komentāru sadaļu, nosakot kārtību, kurā studenti sniedz savus komentārus.

11. Kad visas prezentācijas ir pabeigtas, dodiet studentiem laiku apspriesties savās grupās un pēc tam vadiet kopīgu diskusiju par rīku atšķirībām un par to, kuru katra grupa uzskata par vislabāko un kāpēc.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Darbs komandā, komunikācija grupas ietvaros, prezentācijas prasmes, darbs ierobežotā laikā, salīdzināšana un konstruktīvas atsauksmes sniegšana.

Pielikumi

1. Plānojuma shēma 1.
2. Plānojuma shēma 2.
3. Uzņēmuma apraksts plānojuma shēmā un identificētie riski 1.
4. Uzņēmuma apraksts plānojuma shēmā un identificētie riski 2.

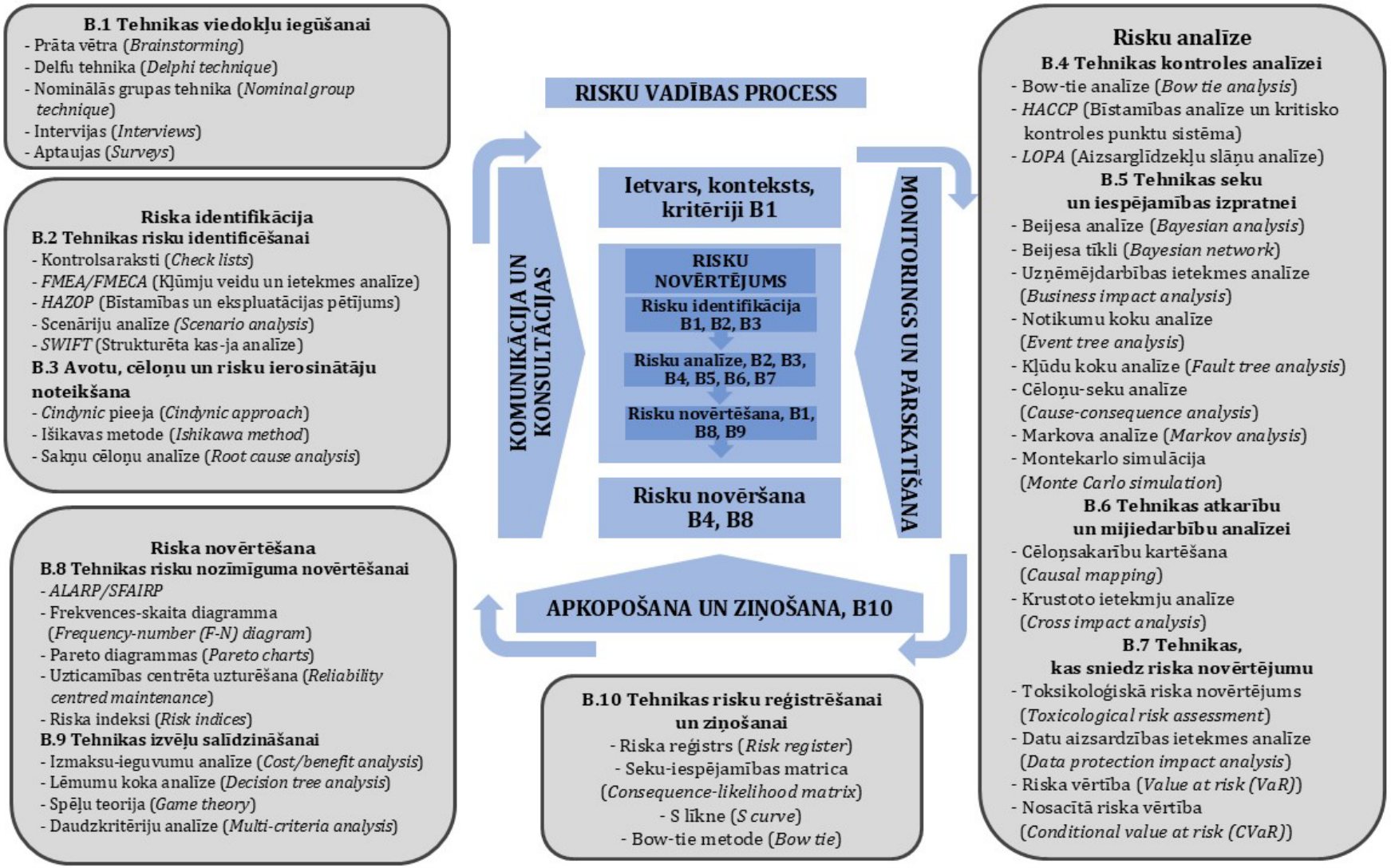
* Skaidrojums par trīs risku analīzes kategorijām IEC 31010:2019 standarta ietvaros

Saskaņā ar IEC 31010:2019 standartu risku analīze ietver dažādu risku aspektu novērtēšanu, izmantojot dažādus rīkus. Šajā procesā tiek izdalītas trīs galvenās kategorijas:

- **sekas (*Consequence Analysis*)** – novērtē iespējamās risku ietekmes smagumu, ja tie iestājas;
- **iespējamība (*Likelihood Analysis*)** – nosaka, cik ticami vai bieži riski varētu iestāties;
- **risku līmenis (*Risk Level Determination*)** – apvieno seku un iespējamības analīzi, lai noteiktu kopējo risku līmeni.

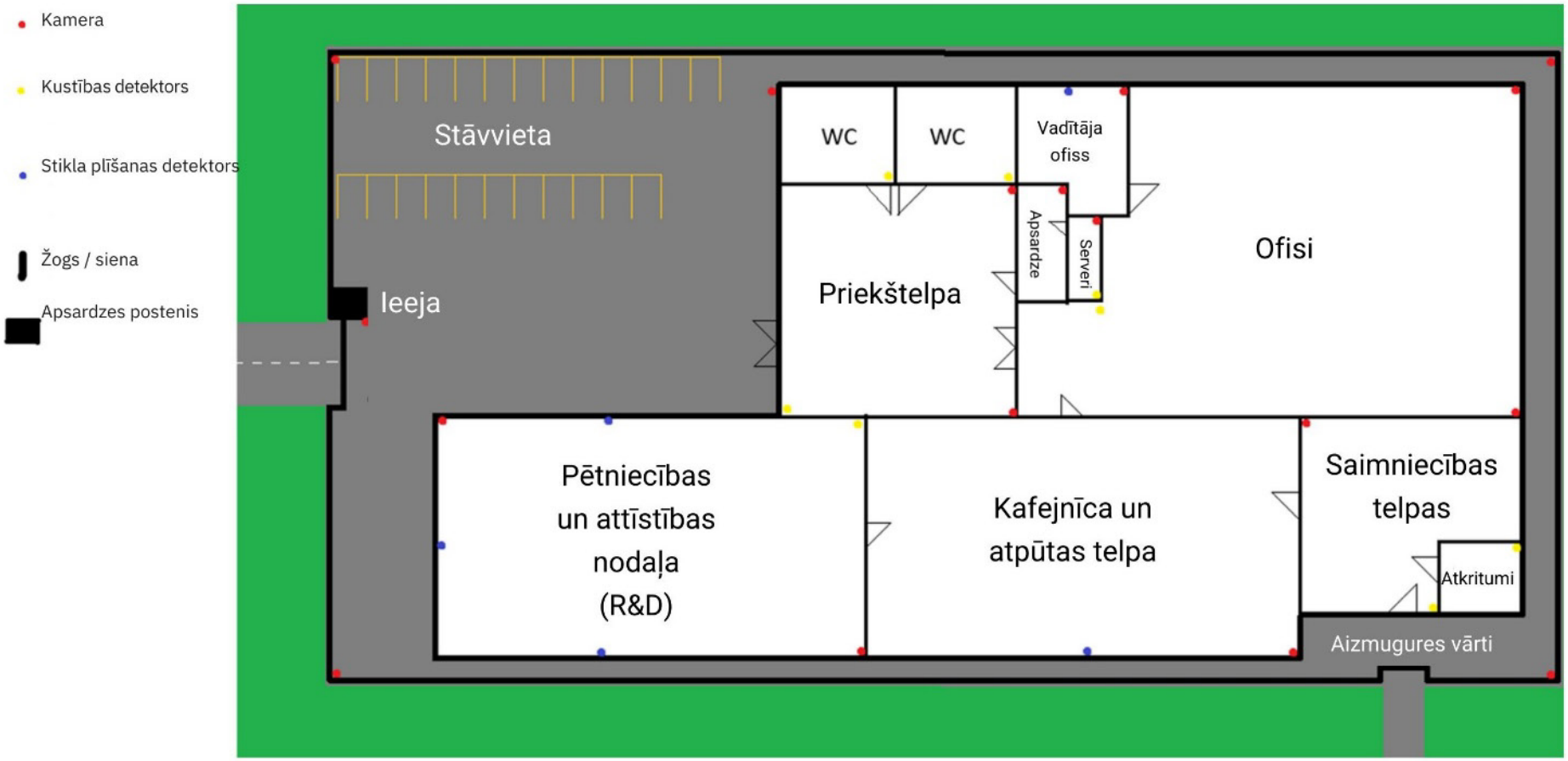
A.3 Tehniku izmantošana ISO 31000 procesā

IEC 31010:2019 standartā tabula A.3 parāda, cik lielā mērā katra tehnika ir piemērojama dažādām riska novērtēšanas fāzēm, proti: risku identifikācijai, risku analīzei un risku novērtēšanai.

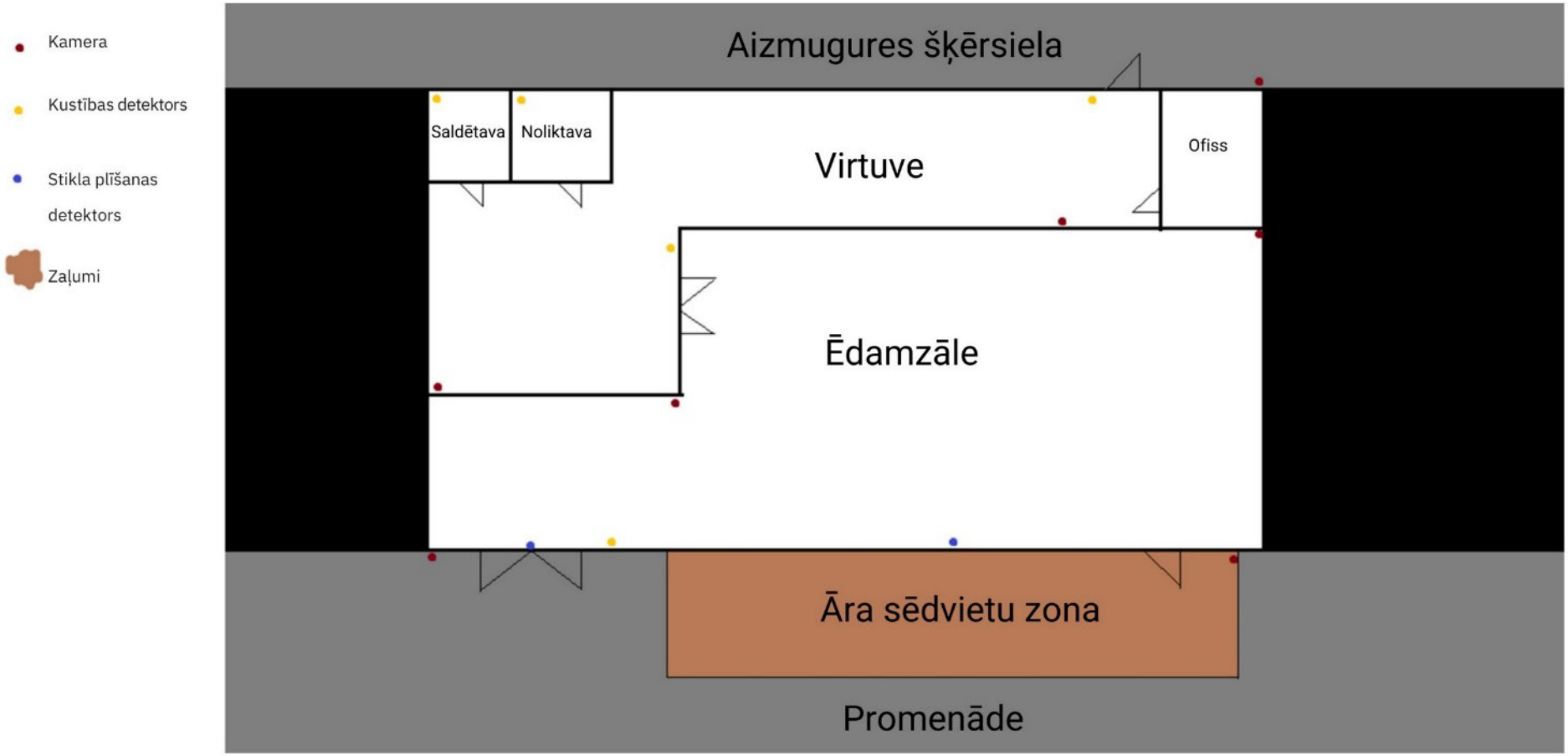


Neliels ieskats par *HAZOP*, *SWIFT* un *FMEA* metodēm pieejams 2. uzdevuma pielikumā.

Plānojuma shēma 1



Plānojuma shēma 2



Uzņēmuma apraksts plānojuma shēmā un identificētie riski 1

Neliels specializēto tehnoloģiju ražotājs ar 30 darbiniekiem.
Ēka atrodas Dienvidsomijā, to ieskauj mežs un rūpnieciskais rajons.
Aptuveni 15 minūšu brauciena attālumā no pilsētas centra, un apkārtējie uzņēmumi galvenokārt ir saistīti ar automašīnu ražošanu un metālapstrādi.

Identificētās problēmas

- Slīdēšanas risks pie aizmugurējiem vārtiem ziemā.
- Nepietiekams drošības aprīkojums darbiniekiem pētniecības un attīstības (R&D) nodaļā.
- Nav apsardzes ārpus darba laika, un policijas ierašanās laiks pēc trauksmes ir aptuveni 20 minūtes.
- Durvis starp vestibilu un biroja telpām nav aizslēgtas. Pastāv nepiederošu personu iekļūšanas, "pleca novērošanas" un citu fiziskās spiegošanas metožu risks.

Uzņēmuma apraksts plānojuma shēmā un identificētie riski 2

Uzņēmums ir neformāls restorāns, kas piedāvā labu ēdienu un alkoholu.
Restorāns atrodas pašā pilsētas centrā, kurā dzīvo vairāk nekā 10 miljoni iedzīvotāju un valda silts klimats.
Apkārtējie uzņēmumi galvenokārt ir modes preču veikali un kafejnīcas.

Identificētās problēmas

- Ugunsgrēka trauksmes signāls ēdamzālē ir bloķēts ar galdu.
- Aizmugures ejas durvju slēdzene ir bojāta. Tās var aizslēgt, bet tās var atvērt ar spēku kratot.
- Neapstrādāta gaļa tiek uzglabāta blakus gatavai gaļai saldētavā.
- Terases koka lakas pārklājums lietus laikā klūst loti slidens.

DROŠĪBAS RISKU VADĪBA UN NOTURĪBA

11. PRAKTISKAIS UZDEVUMS STUDENTIEM

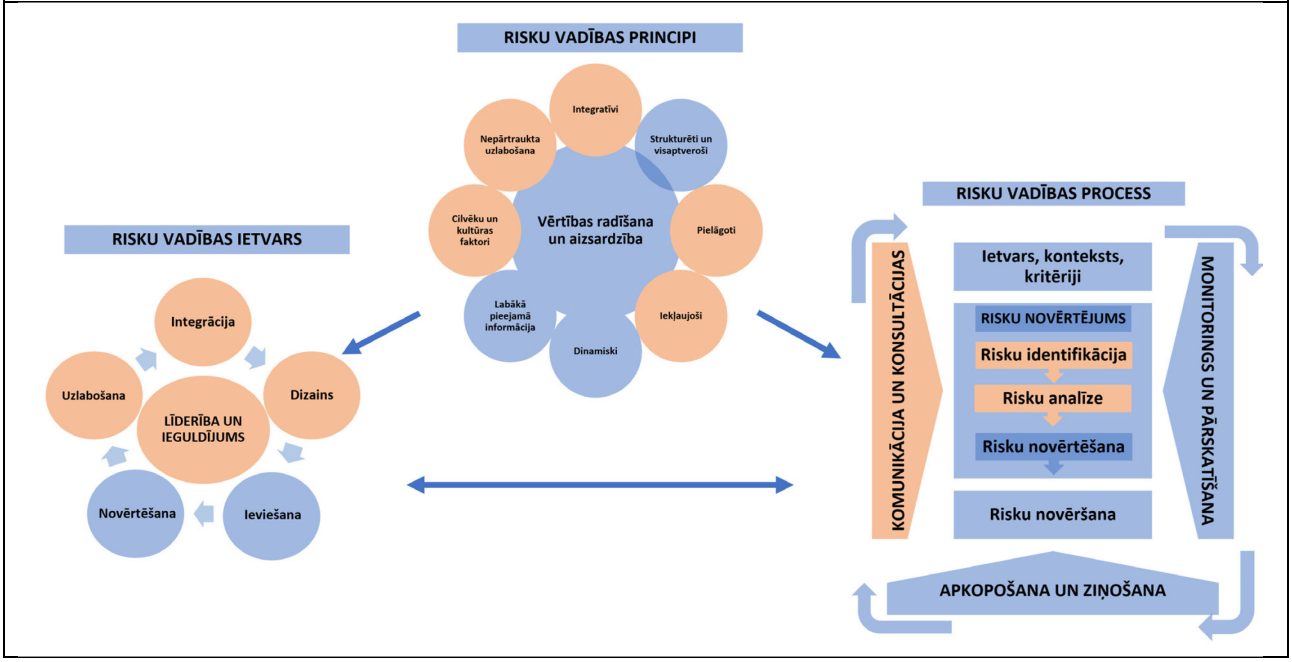
AUTORS: Lambert Bambach, Avans Lietišķo zinātņu Universitāte, Nīderlande

Konteksts

Lai gūtu priekšstatu par drošības risku pārvaldības ieguldījumu organizācijas noturības nodrošināšanā, ir jāveic seši soļi – apspriediet neveiksmes, apsveriet savienojumus, saprotiet, kas ir svarīgi, nosakiet ietekmes sliekšņus, veiciet stratēģiskas izvēles un veiciet stresa testus *(Discuss for failure, Consider the connections, Understand what is important, Set impact thresholds, Make strategic choices and Conduct stress testing)*. Lai gan organizācijas konteksts un mērķi var atšķirties, studenti šajā uzdevumā iepazīsies ar sešiem soļiem, kas tiem palīdzēs izprast organizāciju un noskaidrot, kā drošības risku pārvaldība var palīdzēt organizācijai.

ATSAUCE UZ ISO 31000 STANDARTU

Šajā uzdevumā tiek aplūkoti sekojoši ISO 31000 standarta elementi: uzlabošana, integrācija, vadība un apņemšanās, dizains (Risku vadības ietvars), cilvēciskie un kultūras faktori, nepārtraukti uzlabojumi, integratīvi, pielāgoti, iekļaujoši (Risku vadības principi), komunikācija un konsultācijas, risku identificēšana un risku analīze (Risku vadības process).



Uzdevuma mērķis

Studenti iepazīsies ar sešiem soļiem, kas var palīdzēt izprast organizācijas noturību. Studenti spēs noteikt, kas ir nepieciešams no drošības risku vadības viedokļa, lai veicinātu organizācijas domāšanu noturības stiprināšanai. Studenti var pielietot sešu soļu metodi un ar to saistītos jautājumus. Skatīt sešu soļu metodi pielikumā.

UZDEVUMS STUDENTIEM

Mājas darbs. Pirms šī uzdevuma uzsākšanas grupā students ir individuāli aptaujājis un savā organizācijā apkopojis informāciju par noturību, pamatojoties uz sešiem soļiem (jautājumi pievienotajā tabulā).

1. Veidojiet grupas saskaņā ar pasniedzēja norādījumiem.
2. Katrā grupā ir trīs četri studenti.
3. Pasniedzēja vadībā definējiet, kā jūs interpretējat sešus soļus? Sarindojiet soļus pēc grūtības pakāpes atbilstoši pūlēm, kas bija nepieciešamas, lai iegūtu atbildes uz jautājumiem. Pārdomājiet, kāpēc tas, iespējams, bija tik grūti vai nebija grūti? Pārrunājiet, ko iegūtā informācija nozīmē drošības risku pārvaldības atbalstam organizācijā un organizācijas noturībai?
4. Sagatavojiet īsu prezentāciju saviem kursa biedriem par aptaujas rezultātiem. Prezentācijā jāiekļauj: seši soļi, par kuru(-iem) soli(-ļiem) bija visvieglāk ievākt informāciju un kāpēc? Par kuru(-iem) soli(-ļiem) bija visgrūtāk iegūt informāciju un kāpēc? Ko tas, jūsuprāt, drošības risku pārvaldībā var dot organizācijas noturības stiprināšanai? Skaidri norādiet, kā drošības risku pārvaldībai būtu jāsniedz savs ieguldījums noturības stiprināšanā, kādai vajadzētu būt pieejai?
5. Iepazīstiniet ar savu prezentāciju savus kursa biedrus.
6. Klausieties kursa biedru prezentācijas. Pēc katras prezentācijas divas minūtes pārrunājiet savā grupā, vai piedāvātā pieeja būtu piemērota arī jums un kāpēc?
7. Pēc visām prezentācijām savā grupā pārrunājiet, kurām no piedāvātajām pieejām jūs kā grupa dodat priekšroku un kāpēc? Dalieties savās domās ar pārējiem.

UZDEVUMS PASNIEDZĒJIEM

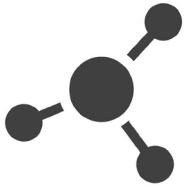
1. Pirms nodarbības pārbaudiet, vai mājasdarbs ir izpildīts. Atļaujiet uzdevumā piedalīties tikai tiem studentiem, kuri ir vismaz uzsākuši vai ir pabeiguši mājasdarbu. Studenti, kuri to nav izdarījuši, var izmantot laiku mājasdarba veikšanai.
2. Pirms nodarbībām apziniet studentu skaitu un to, cik grupas var veidot, lai tajās būtu ne vairāk par četriem studentiem. Grupu izveidei varat pielietot jebkuru metodi.
3. Pirms nodarbības katrai grupai ir jāsaņem Labās prakses raksta kopija par drošības riska pārvaldību un noturību (L. Bambaks "Kā drošības risku pārvaldība var veicināt organizācijas noturību").
4. Pēc izvēles – uzdevumu varat izspēlēt gan klātienē, gan virtuālā nodarbībā.
5. Auditorijā sadaliet studentus grupās ne vairāk par četriem studentiem katrā grupā.
6. Uzdodiet studentiem iepazīties ar sešiem soļiem un pievienotajiem jautājumiem.
7. Uzdodiet studentiem pierakstīt diskusiju rezultātus, piemēram, uz piezīmēm, uz tāfeles, *PowerPoint* prezentācijā, tiešsaistes vidē utt., ietverot jautājumus: Kā jūs interpretējāt sešus soļus? Sarindojiet soļus pēc grūtības pakāpes atbilstoši pūlēm, kas bija nepieciešamas, lai iegūtu atbildes uz jautājumiem? Pārdomājiet, kāpēc tas, iespējams, bija tik grūti vai nebija grūti? Pārdomājiet, ko drošības risku pārvaldība dod organizācijas noturībai?
8. Uzdodiet studentiem sagatavoties prezentēt savus rezultātus saviem kursa biedriem. Jūs varat izlemt par prezentācijas veidu. Prezentāciju ieteicams ierobežot līdz 5–10 minūtēm.

9. Uzdodiet studentiem sagatavot īsas prezentācijas par aptaujas rezultātiem saviem kursa biedriem. Grupas prezentē sešus soļus, par kuru(-iem) soli(-ļiem) bija visvieglāk ievākt informāciju un kāpēc? Par kuru(-iem) soli(-ļiem) bija visgrūtāk iegūt informāciju un kāpēc? Ko drošības risku pārvaldība var dot organizācijas noturības stiprināšanai? Kā drošības risku pārvaldībai būtu jāsniedz ieguldījums noturības stiprināšanā, kādai vajadzētu būt pieejai?
10. Prezentāciju laikā vadiet diskusiju un skatieties, lai grupas ievēro iepriekš dotos uzdevumus. Process ir šāds:
    - ne ilgāk kā 10 minūtes vienai grupas prezentācijai;
    - pēc katras prezentācijas 2 minūtes grupas savā starpā pārrunā, vai piedāvātā pieeja būtu piemērota katrai no tām un kāpēc?
    - grupas tiek mudinātas dalīties savās domās ar pārējiem. Galvenais jautājums ir: vai pieejas izvēle būtu piemērojama jūsu organizācijai un/vai sniegtu jums atšķirīgu viedokli par atbalstu, ko drošības risku pārvaldība sniedz noturības veicināšanai?
11. Pēc visām prezentācijām vadiet diskusiju ar studentiem par dažādām pieejām un to, kas viņiem varētu būt piemērots.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Prasme strādāt komandā, prasme strādāt ierobežotā laikā, prezentācijas prasmes, argumentēšanas māksla, prasme salīdzināt un kritiskā domāšana.

Pielikums. Sešu soļu metode

 1. Apspried neveiksmes	 2. Apsver saiknes	 3. Saproti, kas ir svarīgi	 4. Nosaki ietekmes sliekšņus	 5. Veic stratēģiskās izvēles	 6. Veic stresa testēšanu
Lai izvairītos no pašapmierinātības un veicinātu "nākotnes domāšanu", **apspriediet neveiksmes**. Uzdodiet jautājumus "Kas būtu, ja?" un "Kas būs tālāk?". Iedrošiniet savus darbiniekus izteikties.	**Apsveriet saiknes** starp "pieciem kapitāliem"*, lai izprastu iespējamo traucējumu ietekmi uz ieinteresētajām pusēm, organizāciju un plašāku sabiedrību.	**Saprotiet, kas ir svarīgi** ieinteresētajām pusēm un sabiedrībai, proti, "būtiskos rezultātus", kuriem nepieciešama augsta noturības pakāpe.	**Nosakiet** būtisko rezultātu **ietekmes sliekšņus**, lai noteiktu pieļaujamās robežas, kuras nevajadzētu pārsniegt, ņemot vērā ietekmi uz visiem "pieciem kapitāliem".	**Veiciet stratēģiskas izvēles** attiecībā uz noturības pasākumiem, līdzsvarojot kontroli, elastību, efektivitāti un inovācijas.	**Veiciet stresa testēšanu**, lai noteiktu, vai spējat saglabāt ietekmes sliekšņus neatkarīgi no draudiem.
Kādi pieņēmumi par neveiksmēm pastāv organizācijā?	Kādu ieguldījumu organizācijas paaugstinātā noturība dos kopējai jūsu nozares, kopienas un sabiedrības noturībai?	Kā tiek nodrošināti būtiskie rezultāti?	Kas veidotu nepieņemamu ietekmi uz būtiskajiem rezultātiem?	Cik progresīva vai aizsardzības orientēta ir organizācijas domāšana?	Kā tiks sasniegti būtiskie rezultāti stresa vai traucējumu laikā?
Vai cilvēki atklāti apspriež iespējamās neveiksmes, potenciālas problēmas un kļūdas?	Kā organizācijas rīcība vai bezdarbība var ietekmēt "piecus kapitālus" (dabas, cilvēku, sociālo, uzbūvēto un finanšu) pašlaik un nākotnē?	Kas varētu kavēt būtisko rezultātu nodrošināšanu vai atjaunošanu?	Kā būtisko rezultātu traucējumi ietekmētu dažādas klientu grupas, organizāciju un plašāku nozares sistēmu?	Cik elastīgs vai konsekvents ir organizācijas dizains attiecībā uz noturību?	Kāda pārliecība jums ir, ka alternatīvie līdzekļi un ārkārtas plāni ļaus jums sasniegt būtiskos rezultātus pieļaujamās ietekmes robežās sarežģītos, bet ticamos scenārijos?
Kā darbiniekiem tiek uzticēts pamanīt izaicinājumus, pārmaiņas vai iespējamos traucējumus nākotnē?		Vai būtiskie rezultāti varētu tikt nodrošināti ar alternatīviem līdzekļiem?		Kā jūs līdzsvarojat spriedzes un izmantojat "gan/gan" domāšanas veidu?	Kā jūs pārbaudīsiet nākotnes iespējas un izvēles, kuras jums būtu (vai nebūtu) jāizdara šodien? Kā šīs izvēles varētu ierobežot jūsu iespējas pēc vairākiem gadiem?
Kādas nākotnes tendences varētu radīt jaunas iespējas organizācijai? Kādas priekšrocības jūs varētu attīstīt?		Vai mums ir pietiekama elastība, lai nodrošinātu būtiskos rezultātus pat sarežģītos vai ārkārtējos scenārijos?		Kādi papildu ieguldījumi ir nepieciešami, lai uzturētu būtiskos rezultātus pieņemamu tolerances sliekšņu robežās?	

* "Piecu kapitālu" teorija ir ietvars, kas izstrādāts, lai novērtētu organizācijas ilgtspējību, ņemot vērā piecus galvenos resursu veidus: dabas, cilvēku, sociālo, uzbūvēto un finanšu kapitālu. Šī pieeja palīdz organizācijām izprast savu darbību ietekmi uz dažādiem resursiem un veicināt ilgtspējīgu attīstību.

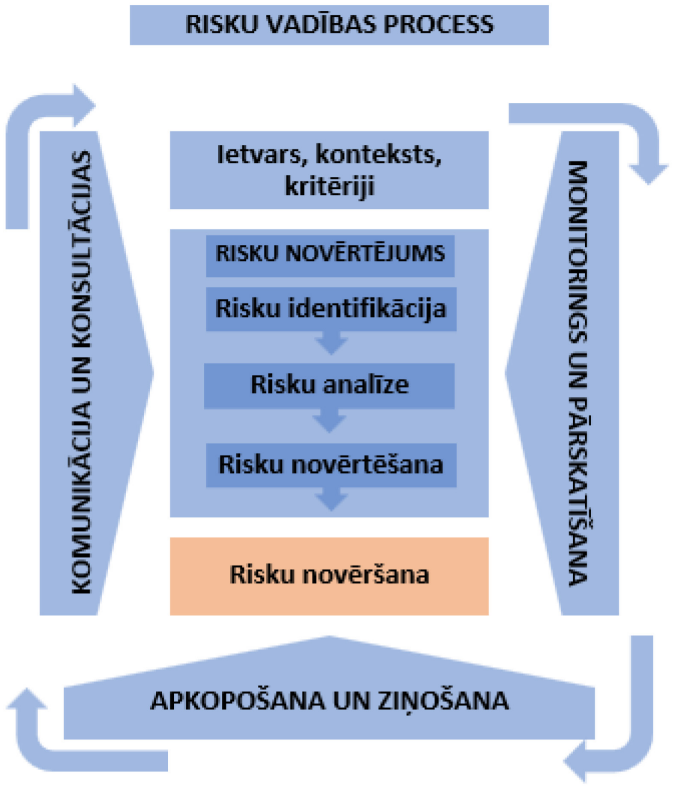
RISKU NOVĒRŠANA DROŠĪBAS RISKU PĀRVALDĪBAS PROCESĀ

12. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORS: Raimundas Kalesnykas, Biznesa augstskola *Turība*, Latvija

Konteksts

Drošības risku pārvaldības process ietver organizācijas politikas, procedūru un prakses sistemātisku piemērošanu komunikācijas un konsultāciju darbībām, konteksta noteikšanu un drošības risku novērtēšanu, uzraudzību, pārskatīšanu, reģistrēšanu un ziņošanu par to. Visas organizācijas darbības ir saistītas ar risku. Organizācijas pārvalda drošības riskus, tos identificējot, analizējot un pēc tam izvērtējot, vai risks ir jāveic darbības risku apstrādei un novēršanai. Risku mazināšana ir organizācijas stratēģiju un darbību īstenošanas plāns, lai atbilstoši risinātu drošības apdraudējumus un tos efektīvi pārvaldītu. Risku apstrādei vienmēr jāiet roku rokā ar citiem drošības risku pārvaldības procesiem, kas iekļauti ISO 31000:2018 standartā.

ATSAUCE ISO 31000 STANDARTU	
Saskaņā ar ISO 31000:2018 standartu riska apstrādes mērķis ir izvēlēties un ieviest drošības riska risināšanas iespējas. Riska apstrāde ietver iteratīvu drošības riska pārvaldības procesu, kas ietver: (a) riska ārstēšanas iespēju formulēšanu un atlasi; b) riska apstrādes plānošanu un īstenošanu; c) šīs ārstēšanas efektivitātes novērtēšanu; d) izlemt, vai atlikušais risks ir pieņemams; un e) ja tas nav pieņemams, veic turpmāku ārstēšanu.	

Uzdevuma mērķis

Studenti iegūs teorētiskas zināšanas un izpratīs risku mazināšanas ietekmi drošības risku vadības procesa plānošanā. Tāpat viņi apgūs, kā formulēt un izvēlēties riska novēršanas iespējas, pamatojoties uz identificētajiem draudiem organizācijai, izmantojot drošības risku matricu, un kā izstrādāt riska novēršanas plānu atbilstoši ISO 31000:2018 prasībām.

UZDEVUMS STUDENTIEM

Izveidojiet grupas pēc pasniedzēja norādījumiem. Saglabājiet dažādību grupu veidošanā (studiju virziens, programma, studiju līmenis un gads, darba pieredze – ja tāda ir, utt.).

1. Katra studentu grupa iepazīstas ar gadījuma aprakstu un konkrēto uzdevumu, ko uzdod pasniedzējs. Gadījums jāanalizē organizācijas kontekstā (publiskā, privātā), norādot sektoru, kurā organizācija darbojas (policijas dežūrpunkts, tiesu ēkas un telpas, biznesa uzņēmums kritiskās infrastruktūras attīstībai u.c.). Katrai grupai tiks piešķirta 5x5 risku novērtējuma matrica (skatīt pielikumā) ar identificētajiem draudiem atbilstoši riska nopietnībai un tā rašanās iespējamībai.
2. Katrai studentu grupai tiek dota viena metode, kas piemērojama: a) lai noteiktu riska līmeni – no iespējamas un ļoti iespējamas iestāšanās līdz nozīmīgai un smagai seku pakāpei; b) lai formulētu un atlasītu riska novēršanas iespējas/vai pasākumus riska novēršanai; c) veiktu pasākumus un plānotu risku novēršanas pasākumu ieviešanu. Lūdzu, ievērojiet ISO 31000:2018 5. punktā noteiktās prasības.
3. Iepazīstieties ar jums piešķirto metodi un izpildiet uzdevumu, izmantojot "prāta vētras" metodi saskaņā ar pasniedzēja norādījumiem. Uzdevumu izpildes laiks katrai grupai – 15 min.
4. Sagatavojiet īsu metodes prezentāciju. Prezentācija tiek sniegta pēc izvēles, izmantojot šādus veidus: mutiski, izmantojot piezīmes (*flipchart*), uz tāfeles, *PowerPoint* u.c.
5. Katra studentu grupa izvirza runātāju, kurš iepazīstinās savus kursabiedrus ar grupas rezultātiem/secinājumiem par sniegto uzdevumu. Prezentācijas laiks līdz 10 min.
6. Noklausieties kursa biedru prezentācijas. Pēc katras prezentācijas pārrunājiet (2 minūtes) ar savu grupu, vai viņu metode būtu piemērota jūsu mērķim. Dalieties savās domās ar auditoriju.
7. Pēc visām prezentācijām un lektora vadībā savā grupā pārrunājiet, kuri no piedāvātajiem parametriem (iekšējais un ārējais) tiktu ņemti vērā turpmākajā drošības riska pārvaldīšanas procesā. Dalieties savās domās ar auditoriju. Diskusijas laiks līdz 10 min.

UZDEVUMS PASNIEDZĒJIEM

1. Izveidojiet studentu grupas (ieteicams ne mazāk kā 3 un ne vairāk kā 5 cilvēki vienā grupā). Izlemiet, kādā veidā studenti tiks sadalīti grupās.
2. Sniedziet īsu pārskatu par gadījuma aprakstu, kas saistīts ar drošības riska pārvaldības procesu. Iepazīstiniet ar drošības risku risināšanas variantu izvēles un ieviešanas galvenajiem noteikumiem saskaņā ar ISO 31000:2018.
3. Izskaidrojiet katrai grupai uzdoto uzdevumu. Atsauces uz drošības risku apstrādes prasībām sniegtas ISO 31000:2018 standartā.
4. Katrai studentu grupai piešķiriet vienu vai jauktus nosacījumus no 31000:2018, t.i.: a) izvēlieties augstus riskus – no iespējamas un ļoti iespējamas iestāšanās līdz nozīmīgai un nopietnai smaguma pakāpei; b) uzdodiet sakārtot riskus prioritārā secībā, sākot no visaugstākā; c) aiciniet studentus formulēt un izvēlēties piemērotus pasākumus, lai novērstu risku, pamatojoties uz identificētajiem draudiem organizācijas drošībai; d) uzdodiet studentiem plānot darbības risku novēršanai, izlemjot, vai augstais risks ir pieņemams vai ne.
5. Atkarībā no studentu grupu skaita uzdevumu saturu var sašaurināt vai paplašināt.

6. Pirms uzdevuma veikšanas Izstrādājiet un nodrošiniet veidlapu/paraugu (papīra dokumentu) katrai studentu grupai atkarībā no uzdevuma. Kā paraugu var izmantot papildmateriālos pievienotos paraugus. Katrai studentu grupai uzdodiet strādāt pie kādas no veidnēm (papīra dokumenta). Paskaidrojiet, kādi rezultāti ir sagaidāmi saskaņā ar doto uzdevumu.
7. Katrai studentu grupai nosakiet uzdevuma izpildes laika limitu (15 min.).
8. Veiciniet studentu darbu un palīdziet, ja viņiem ir jautājumi par sniegto uzdevumu.
9. Uzdodiet katrai studentu grupai sagatavot īsu rezultātu/secinājumu prezentāciju saskaņā ar sniegto uzdevumu. Prezentāciju var veikt mutiski, piezīmēs (*flipchart*), uz tāfeles, *PowerPoint* u.c. Prezentācijas laiks līdz 10 min.
10. Pēc visām prezentācijām vadiet visu studentu diskusiju par risku novēršanas iespēju izvēles pamatojumu, tostarp paredzamajiem ieguvumiem drošības risku pārvaldībā. Diskusijas laiks līdz 10 min.
11. Apkopojiet visu studentu grupu uzdevumu kopējos rezultātus.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

Spēja strādāt komandā; spēja strādāt ierobežotā laikā, prezentācijas prasmes, argumentācijas prasmes, kritiskā domāšana.

Papildmateriāli

ISO 31000	**DROŠĪBAS RISKU VADĪBAS PROCESS**
RISKU NOVĒRŠANA ir kopīgs termins organizācijas drošības politikām un/vai stratēģijām, kas izvēlētas, lai reaģētu uz konkrētu risku, lai sasniegtu vēlamo rezultātu saistībā ar apdraudējumu drošībai	
• drošības risku modifikācijas process • var radīt jaunus riskus vai modificēt esošos riskus • apzīmēti kā "drošības riska mazināšana", "drošības riska izsaukšana", "drošības riska novēršana", "drošības riska mazināšana"	
RISKU NOVĒRŠANAS PROCESS	
SOĻI	**KRITĒRIJI / PRASĪBAS**
1. **"PRĀTA VĒTRA" UN** **RISKU NOVĒRŠANAS IESPĒJU IZVĒLE** Izvēloties vispiemērotāko drošības risku novēršanas iespēju(-as), jānodrošina līdzsvars starp potenciālajiem ieguvumiem mērķu sasniegšanā un izmaksām, ieguldījumiem vai ieviešanas trūkumiem.	Drošības risku novēršana var ietvert vienu vai vairākas no zemāk skatītajām darbībām. 1. Izvairīšanās no riska, nolemjot neuzsākt vai neturpināt darbību, kas rada risku; • riska pieņemšana vai palielināšana, lai izmantotu kādu iespēju; • riska avota novēršana; • iespējamības izmaiņa, lai samazinātu riska iestāšanās varbūtību; • darbības, lai mazinātu negatīvās sekas; • riska dalīšana (piemēram, izmantojot līgumus vai apdrošināšanu);

	• riska saglabāšana, pieņemot to apzināta lēmuma rezultātā. 2. Drošības riska novēršanas iespējas jāizvēlas, balstoties uz detalizētu analīzi, ņemot vērā tādus faktorus kā organizācijas kopējā drošības riska stratēģija, pieejamie resursi, mērķi, kā arī paredzamās izmaksas salīdzinājumā ar ieguvumiem. 3. Drošības riska novēršanas iespēju izvēlei jāatbilst organizācijas mērķiem, riska kritērijiem un pieejamajiem resursiem.
2. **DROŠĪBAS RISKU NOVĒRŠANAS PLĀNOŠANA UN ĪSTENOŠANA** Drošības risku novēršanas plāna mērķis ir noteikt, kā izvēlētās novēršanas iespējas tiks īstenotas, lai iesaistītās puses skaidri saprastu pasākumus un varētu uzraudzīt plāna īstenošanas progresu. Drošības risku novēršanas plānā skaidri jānorāda, kādā secībā risku novēršanas tiks īstenota. Drošības risku novēršanas plānam jābūt integrētam organizācijas drošības risku vadības stratēģijā un procesos, sadarbojoties ar atbilstošajām ieinteresētajām pusēm.	Drošības risku novēršanas plānā sniegtajai informācijai jāietver: • pamatojums izvēlētajām riska novēršanas iespējām, tostarp sagaidāmie ieguvumi; • personas, kas ir atbildīgas un pilnvarotas apstiprināt un īstenot plānu; • plānotās darbības riska novēršanai; • nepieciešamie resursi, tostarp rezerves risinājumi; • veiktspējas novērtēšanas kritēriji; • ierobežojumi un iespējamie šķēršļi; • nepieciešamā atskaišu sniegšana un uzraudzība.
3. **RISKU NOVĒRŠANAS EFEKTIVITĀTES NOVĒRTĒŠANA** Tas ietver drošības risku novēršanas plāna un ieviesto pasākumu novērtēšanu, lai noteiktu, cik labi tie darbojas drošības risku pārvaldībā. Šis process nodrošina, ka risku novēršana samazina drošības riskus līdz pieņemamam līmenim un sasniedz vēlamo rezultātu.	Risku novēršanas efektivitātes novērtēšana ietver: • veiktspējas mērīšanu, t.i., izmantojot metriku un indikatorus, lai novērtētu, cik labi darbojas riska novēršanas pasākumi, kā arī sekot līdzi drošības risku notikumu biežumam un ietekmei; • atlikušo risku novērtēšanu, t.i., noteikt drošības riska līmeni, kas saglabājas pēc riska novēršanas pasākumu īstenošanas; • salīdzināšanu ar organizācijas mērķiem, t.i., pārbaudīt, vai atlikušo drošības risku līmenis atbilst organizācijas riska pieļaujamības līmenim un mērķiem; • uzraudzību, pārskatīšanu un pielāgošanu, t.i., ja riska novēršana nav efektīva, identificēt jaunas stratēģijas vai pielāgot esošās, lai labāk pārvaldītu drošības riskus.
4. **LĒMUMA PIEŅEMŠANA PAR RISKA LĪMEŅA PIEŅEMAMĪBU** Lēmuma pieņemšana par to, vai atlikušie drošības riski ir pieņemami, ietver atlikušo risku, kas saglabājas pēc visu risku novēršanas pasākumu īstenošanas, novērtēšanu. Ja atlikušie drošības riski tiek uzskatīti par pieņemamiem, tas nozīmē, ka organizācija ir gatava sadzīvot ar šo risku, ņemot vērā papildu riska novēršanas pasākumu izmaksas un ieguvumus.	Lēmumu pieņemšanas process par to, vai atlikušie drošības riski ir pieņemami, ietver: • atlikušo drošības risku līmeņa noteikšanu pēc risku novēršanas pasākumu īstenošanas; • atlikušo risku salīdzināšanu ar organizācijas risku pieļaujamības un tolerances līmeņiem; • atlikušo drošības risku potenciālās ietekmes un iespējamības analīzi, kas palīdz izprast risku smagumu un to iestāšanās varbūtību; • lēmuma pieņemšanu, vai atlikušie drošības riski ir pieņemami vai nepieciešami papildu pasākumi to tālākai mazināšanai.

5. **JA ATLIKUŠAIS RISKS NAV PIEŅEMAMS, VEIKT PAPILDU PASĀKUMUS RISKU NOVĒRŠANAI** Tas nozīmē, ka atlikušo drošības risku līmenis joprojām ir pārāk augsts un var potenciāli kaitēt organizācijai vai tās mērķiem. Šādos gadījumos ir nepieciešami papildu pasākumi, lai samazinātu risku līdz pieņemamam līmenim.	Organizācijas lēmumu pieņēmējiem jāapzinās atlikušo drošības risku būtība un apmērs pēc risku novēršanas pasākumu īstenošanas. Atlikušie drošības riski ir jādokumentē un jāpakļauj uzraudzībai, pārskatīšanai un, ja nepieciešams, turpmākai novēršanai.

Dokumentu piemēri

Risku novērtēšanas matrica

5x5 drošības risku novērtēšanas matrica sastāv no piecām rindām un piecām kolonnām, kur kolonnas attēlo riska nozīmīgumu, bet rindas – tā iestāšanās iespējamību. Riska līmeņi tiek kategorizēti 25 dažādās šūnās, pamatojoties uz riska nozīmīgumu un tā iespējamību. Spektrs svārstās no maznicama un nenozīmīga riska līdz ļoti ticamam un nozīmīgam riskam.

	Nenozīmīga ietekme	Neliela ietekme	Vidēja ietekme	Liela ietekme	Katastrofāla ietekme
Ikdienišķa	Zems-vidējs	Vidējs	Vidējs- augsts	Augsts	Augsts
Regulāra	Zems	Zems-vidējs	Vidējs	Vidējs- augsts	Augsts
Bieža	Zems	Zems-vidējs	Vidējs	Vidējs- augsts	Vidējs- augsts
Vidēja	Zems	Zems-vidējs	Zems-vidējs	Vidējs	Vidējs- augsts
Reta	Zems	Zems	Zems-vidējs	Vidējs	Vidējs

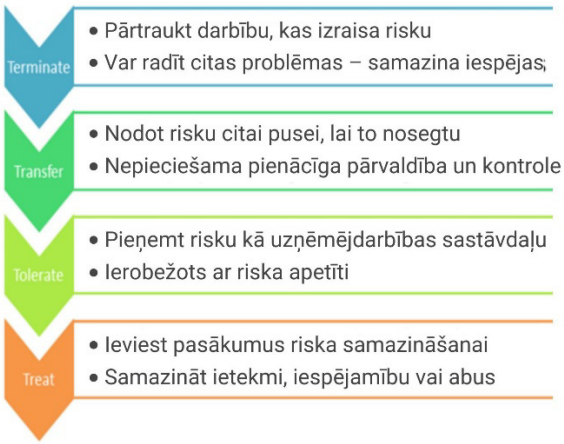
Risku novēršanas plāns

Riska veids	Ietekmes nozīmīgums	Iestāšanās iespējamība	Riska mazināšanas stratēģija	Atbildīgais	Laika periods
X	Augsts	Vidējs			
X	Augsts	Vidējs			
X	Vidējs	Augsts			
X	Vidējs	Vidējs			
X	Zems	Zems			

Risku novēršanas plāna piemērs

Aktīvs	Drauds	Ievainojamība	Riska novēršanas stratēģija	Ieviešanas instrukcijas
Serveris	Ugunsgrēks	Nepietiekams ugunsdzēšamo aparātu daudzums	1) Samazināt risku 2) Dalīt risku	Iegādāties papildu ugunsdzēšamos aparātus, iegādāties apdrošināšanas polisi pret ugunsgrēka bojājumiem
Portatīvais dators	Nesankcionēta piekļuve datoriem	Nedrošas paroles	Samazināt risku	Izstrādāt un ieviest paroļu veidošanas politiku, iegādāties paroļu pārvaldības programmatūru
Sistēmas administrators	Administrators dodas ilgstošā atvaļinājumā vai pamet uzņēmumu	Nav pietiekami apmācīta aizvietotāja	Samazināt risku	Pieņemt darbā un apmācīt otru sistēmas administratoru

Drošības risku novēršanas iesējas



Riska izvairīšanās: izvairīties no darbībām, kas izraisa risku; tas var nozīmēt projekta pārtraukšanu vai procesa maiņu, ja tas ir pārāk riskants.

Riska samazināšana: ieviest papildu kontroles vai pasākumus, lai samazinātu riska iespējamību vai ietekmi, piemēram, uzlabojot drošības protokolus, pastiprinot drošības pasākumus vai modernizējot tehnoloģijas.

Riska pārnešana: pārnest risku uz citu iesaistīto pusi, piemēram, izmantojot apdrošināšanu vai ārpakalpojumus, t.i., finanšu ietekmi no riska uzņemas cita vienība.

Riska dalīšana: sadalīt risku starp vairākām pusēm, piemēram, izmantojot partnerības vai kopuzņēmumus, kur risks tiek kopīgi uzņemts.

NODERĪGI! **Varbūtības risku matrica**

Seko QR kodam un gūsti padziļinātu ieskatu riska novēršanas stratēģijās. Mājaslapā tiek aplūkotas dažādas pieejas, kā organizācijas var reaģēt uz identificētajiem riskiem, lai samazinātu to negatīvo ietekmi vai pat gūtu no tiem labumu.

Šo interneta vietni izveidojis uzņēmums *Continuity2*, kas specializējas biznesa nepārtrauktības pārvaldības programmatūras izstrādē.

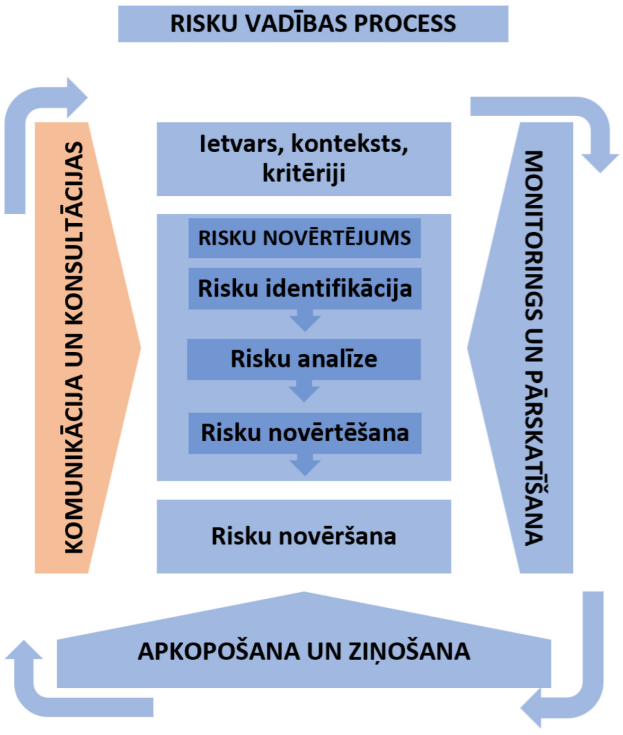
KRĪŽU TIPOLOĢIJA UN VEIKSMES FAKTORI KRĪŽU VADĪBĀ

13. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORE: Ensieh Roud, Nord Universitāte, Norvēģija

Konteksts

Krīžu vadītājiem ir jābūt skaidrai izpratnei par krīzes veidu, ar kuru viņi saskaras, un tās iespējamām sekām. Efektīvai krīzes pārvaldībai ir jāsabalansē improvizācija ar iepriekš plānotām stratēģijām un jāizmanto gan formālie, gan neformālie tīkli. Šis uzdevums uzsver komunikācijas un zināšanu apmaiņas būtisko lomu organizācijās, saskaņojot to ar principiem, kas izklāstīti ISO 31000:2018 riska pārvaldības sistēmā. Veiksmīga reakcija uz krīzi ir vērsta uz efektīvu sadarbības tīklu veidošanu, ko raksturo tādi galvenie elementi kā savstarpīgums, kopīgu lēmumu pieņemšana un kopīga vadība. Šie faktori ir saistīti ar krīzes sarežģītības pārvarēšanu un koordinētas reakcijas nodrošināšanu.

ATSAUCE UZ ISO 31000 STANDARTU	
Saskaņā ar ISO 31000 standartu komunikācijai ir ārkārtīgi liela nozīme efektīvā risku pārvaldībā. Komunikācijai ir izšķiroša nozīme visos risku pārvaldības procesa posmos, tostarp risku identificēšanā, novērtēšanā, novēršanā un uzraudzībā.	

Uzdevuma mērķis

Sniegt studentiem dziļāku izpratni par galvenajiem faktoriem, kas ir saistīti ar efektīvu sadarbību un komunikāciju krīzes reaģēšanas posmā. Vispirms apzinot krīzes veidu, apjomu un iespējamās sekas, studenti attīstīs kritiskas prasmes krīzes situāciju novērtēšanā un pārvaldībā. Izmantojot gadījuma izpēti, viņi praktizēsies klasificēt incidentus un precīzi noteikt būtiskus veiksmes faktorus efektīvai krīzes pārvaldībai.

UZDEVUMS STUDENTIEM

1. Pēc pasniedzēja norādījumiem veidojiet grupas (3–4 cilvēki grupā).
2. Visām grupām tiek dota gadījuma izpēte, pie kuras strādāt.
3. Pasniedzēja vadībā iepazīstieties ar krīzes tipoloģijām.
4. Savā grupā sagatavojiet īsu prezentāciju, kurā atbildiet uz šādiem jautājumiem:
   - kategorizējiet šo krīzi, pamatojoties uz dotajām tipoloģijām;
   - kāpēc to var uzskatīt par veiksmīgu risinājumu?
   - kādi bija izaicinājumi šajā pasākumā?
5. Prezentējiet savu prezentāciju saviem kursabiedriem citās grupās.
6. Pēc visām prezentācijām pārrunājiet un dalieties savās domās ar auditoriju.

UZDEVUMS PASNIEDZĒJIEM

1. Pirms nodarbības aprēķiniet studentu skaitu un to, cik grupas var izveidot no aptuveni četriem studentiem katrā. Ja izmantojat digitālo platformu, varētu būt piemērota studentu sadalīšana pa virtuālajām telpām (*breakout rooms*).
2. Pirms nodarbības lietas un krīzes tipoloģijas materiāls jānosūta studentiem. Lai iepazīstinātu viņus ar krīzes tipoloģiju. Varat ieteikt viņiem noskatīties video ar nosaukumu “Krīzes vadība”, kas pieejams šeit: https://security.turiba.lv/video/

   Varat izvēlēties gadījumu, kas atspoguļo krīzes situāciju. Divi krīzes situāciju piemēri ir atrodami labās prakses piemēru rakstos: "Sadarbības reakcija Gjerdrumas zemes nogruvuma laikā Norvēģijā" un "Mācīšanās no Northguider zemes nogruvuma pieredzes". Abi raksti ir pieejami šeit: https://security.turiba.lv/best-practice-cases/.
3. Uzdodiet studentiem sagatavot prezentāciju, balstoties uz dotajiem uzdevumiem.
4. Prezentāciju laikā noteikti vadiet diskusiju un ievērojiet, lai grupas iekļaujas noteiktā grafika ietvaros. Process ir šāds:
   - apmēram 5 minūtes vienai grupas prezentācijai;
   - pēc visām prezentācijām grupām jāapspriež/jādiskutē 10 minūtes savā starpā.
5. Varat izmantot digitālos rīkus, piemēram, *LearnLab*, lai izveidotu vizuālu kopsavilkumu par studentu prezentācijām un kopīgotu to ar viņiem.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

- Iesaistīšanās efektīvā grupu darbā, lai atrisinātu sarežģītus krīzes scenārijus.
- Efektīva uzdevumu veikšana ierobežota laika apstākļos, simulējot reaģēšanu uz krīzi reālajā pasaulē.
- Prezentāciju sniegšana un to analīzes un lēmumu aizstāvēšana ar pamatotiem argumentiem.
- Prasmju uzlabošana, salīdzinot dažādas krīzes reakcijas, novērtējot stratēģijas un kritiski domājot, lai noteiktu labāko praksi.

MĀKSLĪGĀ INTELEKTA RISKA NOVĒRTĒJUMS UN APSTRĀDE, IZMANTOJOT ISO 31000

14. PRAKTISKAIS UZDEVUMS STUDENTIEM

AUTORI: Rita Lankauskienė, Kazimieras Simonavicius Universitāte, Lietuva

Konteksts

Straujā ģeneratīvā mākslīgā intelekta tehnoloģijas izaugsme un plašā radošo MI risinājumu izmantošana ir izraisījusi jaunu riska veidu strauju parādīšanos. Tas jau tā sarežģītos MI izveides un ieviešanas procesus padara vēl mazāk paredzamus. Arvien vairāk problēmu rodas mākslīgā intelekta (nepareizas) izmantošanas dēļ.[152] Šīs problēmas skar daudzus cilvēkus, grupas un valdības visos līmeņos (nacionālajā, starptautiskajā un globālajā). Izmantojot riska pārvaldības metodi, lai atrastu riskus, analizētu tos, novērtētu un ārstētu tos, riska pārvaldības praksē tiek mēģināts tikt galā ar galvenajām neskaidrībām. Šajā uzdevumā ISO31000 standarta metodoloģija ir modificēta un piemērota, lai novērtētu MI risku reālos MI gadījumos, lai modelētu MI riska novēršanas plānus.

ATSAUCE UZ ISO 31000 STANDARTU ISO 31000 standarts piedāvā sistemātisku riska pārvaldības metodiku, kas var tikt pielāgota konkrētām MI drošības prasībām, lai ieviestu MI riska novērtējumu konkrētos apstākļos.	

[152] MI incidentu datu bāze (2024). Iegūts no https://incidentdatabase.ai/

Uzdevuma mērķis

Studenti mācīsies pielietot ISO31000 standarta metodoloģijā balstītu loģiku, lai novērtētu MI riskus atsevišķos reālās dzīves MI gadījumos un modelētu MI riska novēršanas plānus.

UZDEVUMS STUDENTIEM

1. Izveidojiet grupas saskaņā ar pasniedzēja norādījumiem un sadaliet pienākumus grupā:
   - Kurš vadīs visu diskusijas procesu, sekojot uzdevuma anketai un atbalsta materiālam?
   - Kurš rakstveidā fiksēs diskusijas kopsavilkuma akcentus?
   - Kurš iepazīstinās pārējos ar grupas darba gala rezultātiem?
2. Iepazīstiniet sevi un savus grupas biedrus ar riska novērtēšanas loģikas pamatelementiem, kas iestrādāti ISO31000 standartā. Pēc pieprasījuma meklējiet papildu materiālus, lai iegūtu paraugprakses vadlīnijas, ko izstrādājis Lietu interneta drošības institūts (IoTSI) par to, kā veikt MI drošības riska novērtējumu, izmantojot ISO 31000.
3. Atlasiet mākslīgā intelekta (ne)lietošanas gadījumu no MI incidentu datu bāzes (2024) https://incidentdatabase.ai/. Neaizmirstiet piefiksēt vispārīgo informāciju par izvēlēto gadījumu, kā norādīts anketas vadlīnijās.
4. Veiciet MI drošības riska novērtējumu izmantojot ISO 31000 metodoloģiju: pakāpeniski ieviesiet visas drošības novērtējuma darbības jūsu izvēlētajam MI (nepareizas) izmantošanas gadījumam. Uzmanīgi sekojiet anketai. Esiet elastīgs, veidojot atbalstošus jautājumus pēc vajadzības.
5. Apspriediet grupā un izvēlieties vienu identificēto risku, lai sagatavotu riska novēršanas plānu.
6. Vienojieties par savas grupas galarezultātu un sagatavojiet līdz 10 minūtēm garu prezentāciju, kas ietver šādus aspektus:
   - izvēlētā gadījuma nosaukums un avots;
   - komandas dalībnieki, kas strādāja pie plāna sagatavošanas;
   - izraudzītā MI (nepareizas) izmantošanas gadījuma vispārīgs apraksts (līdz 5 teikumiem);
   - MI (ne)lietošanas iekšējais un ārējais konteksts;
   - MI riska novērtēšanas galvenie soļi: identificēšana, analīze un novērtēšana;
   - riska novēršanas plāns (scenārija veidošana) izvēlētajam riskam: darbības, resursi un pienākumi;
   - kopsavilkuma atsauksmes par sarežģītākajiem un veiksmīgākajiem ISO31000 metodoloģijas piemērošanas posmiem mākslīgā intelekta riska mazināšanas un novērtēšanas plānošanai.
7. Klausieties citu grupu prezentācijas. Pēc katras prezentācijas iesaistieties divu minūšu diskusijā ar savu grupu, lai noteiktu, vai viņu pieeja izvēlētajiem gadījumiem būtu bijusi piemērota arī jums. Pēc apspriedes izsakiet savu viedokli pārējiem kursabiedriem.
8. Pēc visu prezentāciju pabeigšanas pārrunājiet savā grupā, kura no piedāvātajām pieejām būtu vispiemērotākā katram gadījumam. Lūdzu dalieties savās domās ar pārējiem kursabiedriem.

UZDEVUMS PASNIEDZĒJIEM

1. Pirms nodarbību sākuma aprēķiniet grupu skaitu auditorijā, ņemot vērā esošo studentu skaitu, lai grupā būtu 5–7 studenti.
2. Katrai grupai jābūt pieejamam atbalsta materiālam (atkarībā no klātienes vai attālinātas dalības):
   - MI drošības riska novērtējuma tabula, pamatojoties uz ISO 31000 vadlīnijām (1. pielikums);
   - ISO 31000: 2018 ietvars;
   - internets, lai pirms nodarbības sākuma MI incidentu datubāzē (pieejams: https://incidentdatabase.ai/) atlasītu MI (ne)lietošanas gadījumu;
   - A1 formāta papīra loksne, krāsainas piezīmju lapiņas un marķieri (vai līdzvērtīga programmatūra attālinātā režīmā).
3. Sadaliet studentus grupās, kurās ir 5–7 studenti.
4. Uzdodiet studentiem iepazīties ar ISO 31000:2018 standartu, kā arī gadījumu "AI drošības izaicinājums un riska novērtējums, izmantojot ISO 31000".
5. Norādiet studentiem, kā reģistrēt viņu izvēlētās pieejas rezultātus, ievērojot 1. pielikumā sniegto "MI drošības riska novērtējuma tabulu, pamatojoties uz ISO 31000 vadlīnijām". Atgādiniet, ka šī tabula ir izstrādāta no gadījuma "AI drošības izaicinājums un riska novērtējums, izmantojot ISO 31000", kas studentiem jau jāpārzina. Diskusiju rezultātus var sasniegt, izmantojot dažādas metodes, piemēram, pēc piezīmes, *PowerPoint* prezentāciju, tāfeli vai tiešsaistes vidi. Studenti jāinformē par to, kā sagatavoties savu rezultātu prezentācijai. Sniedziet norādījumus, kas jāiekļauj prezentācijā (skatīt iepriekš). Atgādiniet studentiem, ka prezentācija var ilgt ne vairāk kā 10 minūtes.
6. Prezentāciju laikā nodrošiniet, lai diskusija tiktu vadīta un prezentācija tiktu demonstrēta tai atvēlētajā laikā. Procedūra ir šāda:
   - viena grupas prezentācija ir paredzēta ne vairāk kā 10 minūtes;
   - pēc katras prezentācijas grupām jāiesaistās divu minūšu diskusijā savās attiecīgajās grupās, lai noteiktu, vai piedāvātā pieeja būtu bijusi piemērota viņu pašu pieejai;
   - auditorija tiek mudināta uzklausīt citu grupu viedokļus;
   - pamatjautājums ir šāds: vai izstrādātie riska novēršanas plāni noved pie sagaidāmajiem rezultātiem?
7. Sekojiet katrai prezentācijai, veicinot diskusiju starp visiem studentiem par visefektīvāko pieeju.

Papildu prasmes, kuras students iegūst, veicot šo uzdevumu

- Darbs grupā
- Darbs ierobežotā laikā
- Prezentācijas sniegšana un gadījumu argumentēšana
- Salīdzināšanas prasmes un kritiskā domāšana

Šī darbība ir vērsta uz riska novērtēšanu, un tās galvenais mērķis ir visaptverošs to risku novērtējums, kas saistīts ar mākslīgā intelekta pieaugošo ieviešanu noteiktos kontekstos. Šajā procesā studenti ne tikai iepazīsies ar ISO31000 standarta metodoloģiju un loģisko ietvaru, bet arī iemācīsies to pielāgot, kritiski izvērtējot MI izaicinājuma sekas un ietekmi reālās dzīves gadījumos, dažādās cilvēka darbības sfērās.

Materiāli

MI incidentu datu bāze (2024). Iegūts no https://incidentdatabase.ai/

IoT Analytics. State of IoT, Summer 2024. Market Report. Iegūts no https://iot-analytics.com/product/state-of-iot-summer-2024/

MI drošības riska novērtējuma veikšana, izmantojot ISO 31000 (2024). IoTSI. Iegūts no https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/155-conducting-an-ai-security-risk-assessment-using-iso-31000

ISO 31000:2018. Risk management – Guidelines (2018). Iegūts no https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

1. pielikums

MI drošības riska novērtējuma tabula, pamatojoties uz ISO 31000 vadlīnijām

Informācija par gadījumu Nosaukums: Saite uz izvēlēto lietu: Piekļuves datums:		
Informācija par grupas dalībniekiem Moderators: Referents: Prezentētājs (i):		
MI DROŠĪBAS RISKA NOVĒRTĒŠANAS PROCEDŪRA		
	Saturs	Piezīmes
Konteksta noteikšana		
Iekšējais konteksts:	• Regulējošais ietvars • Tirgus un tehnoloģiju tendences • Draudu aina	
Ārējais konteksts:	• Organizatoriskā struktūra • Riska vadības politikas • Riska apetīte un tolerance	
MI riska novērtējums		
MI riska identificēšana	Datu riski: • pārkāpumi (*breaches*), • datu manipulācija (*data poisoning*), • datu integritāte (*data integrity*). Modeļa riski: • pretrunīgi uzbrukumi, • modeļu zagšana, • modeļa neobjektivitāte. Operacionālie riski: • sistēmas kļūmes, • drošības konfigurācija, • trešo pušu riski.	
MI riska analīze	Ietekmes novērtējums: • finansiālā ietekme, • darbības ietekme, • ietekme uz reputāciju. Varbūtības novērtējums: • vēsturiskie dati, • ievainojamības analīze, • apdraudējuma dalībnieku spējas.	
MI riska novērtēšana	Riska matrica: • augsts, • mērens, • zems. Lēmumu pieņemšana: • visi iesaistītie, • atsevišķas iesaistītās ieinteresētās personas, • iesaistītās ieinteresēto personu grupas.	

Risku novēršanas plāns		
Mērķis — skaidri definējiet, kas konkrēti ir jādara, piemēram, lai samazinātu datu noplūdes risku vai vājinātu naidīgu uzbrukumu sekas.	Mērķis:	
Darbības — norādiet, kas ir jādara, piemēram, jāievieš vairāku faktoru pieteikšanās, jāšifrē dati vai jāveic regulāras drošības pārbaudes.	Darbības:	
Nodrošiniet riska novēršanas pasākumus ar saprātīgiem resursiem, personālu un tehnoloģijām, kas nepieciešamas, lai tos īstenotu.	Resursi:	
Skaidri norādiet pienākumus riska novēršanas plāna izpildei, nodrošinot atbildību un uzraudzību	Pienākumi:	
Riska novēršanas plāna piemērs: lai mazinātu modeļa novirzes risku, plāns var ietvert apmācības datu dažādošanu, taisnīguma metrikas piemērošanu un regulāru auditu veikšanu, lai identificētu un labotu novirzes.		

Avots: izstrādājis autors, pamatojoties uz IoTSI norādījumiem (2024). MI drošības riska novērtējuma veikšana, izmantojot ISO 31000. Pieejams: https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/155-conducting-an-ai-security-risk-assessment-using-iso-31000

PĒCVĀRDS

Šī grāmata tika radīta ar nolūku sniegt padziļinātu izpratni par drošības risku vadību, piedāvājot ne tikai teorētiskas zināšanas, bet arī praktiskus uzdevumus un labās prakses piemērus dažādās nozarēs no vairākām valstīm. Mūsdienu sarežģītajā un dinamiskajā vidē drošības jautājumi ir kļuvuši par neatņemamu uzņēmumu, organizāciju un sabiedrības daļu. Mēs ceram, ka šī grāmata palīdzēs studentiem attīstīt nepieciešamās prasmes un zināšanas, kas būs noderīgas viņu profesionālajā karjerā, kā arī dos iespēju praktiski apgūt ISO 31000 standarta pielietojumu drošības jomā. Pasniedzējiem tā kalpos kā vērtīgs resurss, piedāvājot reālus piemērus un praktiskus uzdevumus, ko izmantot lekcijās un semināros, savukārt drošības profesionāļiem tā padziļinās izpratni par risku vadību un iepazīstinās ar dažādu organizāciju pieredzi un risinājumiem.

Drošības riski un izaicinājumi nemitīgi mainās, tāpēc zināšanas un prasmes šajā jomā ir jāattīsta un jāpilnveido nepārtraukti. Mēs aicinām izmantot šo grāmatu ne tikai kā pamatu, bet arī kā atspēriena punktu turpmākai attīstībai, kas motivēs dalīties ar pieredzi un ieviest labās prakses risinājumus savās organizācijās. Zināšanas par risku vadību nedrīkst palikt tikai teorētiskas – tās ir jāpielieto ikdienas darbā, lai uzlabotu drošības līmeni, novērstu iespējamos apdraudējumus un veidotu stiprākas un noturīgākas organizācijas. Mēs ceram, ka šo izdevumu novērtēs izglītības iestādes un integrēs tā saturu savās mācību programmās, tādējādi veicinot nākamās paaudzes speciālistu sagatavošanu drošības risku vadības jomā. Mūsu vēlējums – lai drošība būtu prioritāte un iegūtās zināšanas kalpotu kā stabils pamats, uz kura balstīt ilgtspējīgu organizācijas attīstību.