Pregledni članak
Primljeno: 31. listopada 2024.
https://doi.org/10.46672/zsl.9.10.5

Dražen Kaužljar*

MODEL UPRAVLJANJA POSLOVNOM SIGURNOŠĆU PROMETNIH TOKOVA

Sažetak

Iako i upravljanje poslovnom ili korporativnom sigurnošću i upravljanje sigurnošću prometom imaju u svojem nazivu riječ sigurnost, u praksi se ta dva procesa percipiraju odvojeno. Zbog toga je za studente studija Menadžment poslovne sigurnosti bitno približiti poveznice tih koncepata, a osobito za studente koji u svojim svakodnevnim aktivnostima nemaju dodira sa sigurnošću prometa. U radu se donosi pregled pojmovnog određenja poslovne sigurnosti te se obrađuju područja sigurnosnih procesa i sigurnosnih rizika u prometnom sustavu. U zaključku se naglasak stavlja na važnost znanja u cilju donošenja optimalnih odluka.

Ključne riječi: prometni tok, upravljanje poslovnom sigurnošću, kritična infrastruktura, upravljanje procesima, upravljanje rizicima

1. Uvod

Četverogodišnje iskustvo predavanja na studiju Menadžment poslovne sigurnosti pokazalo je da dio studentica i studenata ne vide jasnu poveznicu studija s kolegijima Sigurnost robnih tokova te Sigurnost prometnica i terminala, ponajviše zato što je poslovna sigurnost danas nužna u svim djelatnostima, pa tako i studenti dolaze iz različitih struka. Veći dio studenata dolazi iz poduzeća koja se bave zaštitom imovine i ljudi te iz Ministarstva unutarnjih poslova. Prva grupa studenata u svojim radnima procesima nije zainteresirana za sigurnost prometa, dok je druga grupa studenata većinom posvećena procesima temeljne policije, a manji dio studenata radi u prometnoj policiji. Dodatni se izazov javlja kad su na predavanjima zajedno redoviti i izvanredni studenti. Redoviti su studenti pretežno mlađe osobe bez radnog iskustva, a izvanredni su studenti starije osobe s višegodišnjim radnim iskustvom, ali izgubljenim navikama učenja. Kako bi se studente različitih struka motiviralo i zainteresiralo za kolegije vezane za sigurnost prometa, potrebno ih je dijelom „personalizirati", odnosno

* dr. sc. Dražen Kaužljar, HŽ Infrastruktura d.o.o., Zagreb, Hrvatska, dkauzljar@libertas.hr

prilagoditi poslovnim zahtjevima svakog studenta. Zbog toga se mogu postaviti dva istraživačka pitanja:

- Kako upravljanje poslovnom sigurnošću utječe na sigurnost prometa i sigurnost prometnih tokova?
- Koja je uloga upravljanja sigurnošću prometnih tokova u upravljanju poslovnom sigurnošću?

Odgovori na prvo istraživačko pitanje nalaze se u drugom poglavlju u kojem se obrađuje upravljanje poslovnom sigurnošću, a u kojem se određuje pojam odnosno teorijski koncept poslovne sigurnosti, a zatim i strategija i proces poslovne sigurnosti. U trećem i četvrtom poglavlju nalaze se odgovori na drugo istraživačko pitanje te su obrađene teme sigurnosnih procesa i sigurnosnih rizika te njihova poveznica s upravljanjem poslovnom sigurnošću. Učinkovito upravljanje procesima i rizicima nužno je radi donošenja kvalitetnih odluka te je u nastavku obrađena poveznica od baze podataka do mudrosti odlučivanja te poveznica od ugroze do donošenja odluke. Ovdje je također obrađena tema kritične infrastrukture.

Globalizacija društva dovodi do sve bržeg razvoja i umrežavanja svijeta gdje značajnu ulogu imaju suvremene prometnice i terminali te prometni tokovi. U takvim uvjetima, a osobito u uvjetima kriznih situacija, sve više dolazi do izražaja upravljanje poslovnom ili korporativnom sigurnošću. Najbolji su primjer nedavne krize prouzročene virusom COVID-19 i potresom u Zagrebu te suvremena ratna događanja i gospodarska kriza. Domovinska sigurnost u takvim uvjetima sve više ovisi o sposobnostima gospodarstva na otvorenom tržištu. Sposobnost gospodarstva ovisi s jedne strane o sigurnosti prometnih tokova, a s druge strane o sigurnosti prometne infrastrukture i terminala.

2. Upravljanje poslovnom sigurnošću

2.1. Pojmovno određenje poslovne sigurnosti

Pojam korporativne ili poslovne sigurnosti relativno je nov te se na različite načine definira i opisuje stoga što se tijekom godina taj teorijski koncept razvijao i nadopunjavao. Dodatan je problem i u samom pojmu sigurnosti jer „Sigurnost koja je jednom u primjeni, u pravilu ostaje dugoročna jer potrebno je puno vremena kako bi se ista prihvatila i mijenjala. Može se reći da je sigurnost jedan od najčešćih upotrebljavanih i najslabije objašnjenih pojmova. Stoga je sigurnost kompleksan, višeznačan i vrlo često politički uvjetovan pojam. Pojam sigurnost nema isto značenje za sve ljude i institucije, pa ga svaka osoba ili zajednica doživljava na svoj način jer svatko ima različite sigurnosne prioritete. Sigurnost treba shvatiti kao uvjet opstanka i razvoj države, društva, nacije i građana, ali ne na način da nešto stvara, već da puno toga omogućava – život, zdravlje, slobodu." (Mihaljević i Nađ, 2018: 21).

U pojmovnom opisu značajna je razlika između engleskih pojmova *security* (opća sigurnost) i *safety* (mjerljiva sigurnost), odnosno pojma *protection* (zaštita). Korporativna sigurnost obuhvaća cijeli niz aktivnosti usmjerenih na osiguravanje zaštite ekonomskih, tehničkih, pravnih i informativnih interesa pojedinog poduzeća. Sve ove mjere provode se kako bi se učinkovito kontrolirali svi poslovni procesi i spriječilo „curenje" informacija koje mogu negativno utjecati na interese gospodarskog subjekta.

Korporativnu sigurnost može se definirati na više načina, a za potrebe ovog rada izdvojene su četiri relevantne definicije kako je prikazano u Tablici 1.

Tablica 1. Izbor relevantnih definicija koncepta korporativne sigurnosti

„Poslovima korporativne sigurnosti podrazumijevaju se poslovi administrativne sigurnosti, informacijske sigurnosti, fizičke i tehničke sigurnosti, sigurnosti vlasništva, osobna sigurnost. Korporativna sigurnost je strateška funkcija kompanije." (Ivandić Vidović, Karlović i Ostojić, 2011: 34)
„Korporativna sigurnost je poslovna funkcija unutar organizacijske strukture velikih poslovnih sustava uspostavljena s ciljem zaštite temeljnih vrijednosti, odnosno osoba, imovine i poslovanja poduzeća od različitih oblika ugrožavanja. Korporativnu sigurnost u najširem smislu poimanja definiramo kao sigurnosnu mjeru s ciljem ostvarivanja korporativno-organizacijskih ciljeva." (Mihaljević i Nađ, 2018: 18)
„Korporativna sigurnost je integrirani sustav predikcije, upravljanja i ublažavanja sigurnosnih izazova, prijetnji, rizika i posljedica." (Matika, 2018: 9)
„Korporativna sigurnost svojim djelovanjem ostvaruje višestruk doprinos, te služi kako bi zaštitila temeljne vrijednosti gospodarsko-poslovnih subjekata. Stoga je primarni zadatak prvenstveno zaštita zaposlenika, imovine kompanije i kontinuiteta poslovanja, a tek onda doprinos povećanja stupnja sigurnosti u okruženju u kojem kompanija djeluje i posluje. Osim što korporativna sigurnost obuhvaća fizičku i tehničku zaštitu i zaštitu informacijskog sustava, pojam je prepoznatljiv jer označava i zaštitu poslovnih subjekata, a posebno velikih kompanija ili korporacija." (Mihaljević, Nađ, 2018: 35)

Izvor: obrada autora

Korporativna sigurnost, odnosno sustavi nadzora, službenici za sigurnost i druge sigurnosne mjere, od velike je važnosti za zaštitu organizacije od različitih rizika i prijetnji (International Security Journal, 2023). „Korporativna sigurnost koristi ljude, procese i tehnologiju za zaštitu organizacije od negativnih događaja i situacija. Ona identificira, nadzire i odvraća unutarnje i vanjske prijetnje osoblju, imovini i imovini organizacije te upravlja fizičkim krizama kada se dogode. Također procjenjuje rizike za organizaciju, priopćava ih rukovoditeljima i menadžmentu te njima upravlja na odgovarajući način." (Security Executive Council, 2024). Stoga se na temelju navedenih definicija može zaključiti da je temeljna svrha korporativne sigurnosti postizanje poduhvata organizacije, a ne promašene investicije, osobito u današnja nepredvidiva vremena dinamična vanjskog i unutarnjeg konteksta.

Ta se svrha postiže provedbom osnovnih ciljeva korporativne sigurnosti. Osnovni cilj korporativne sigurnosti u poduzeću jest ostvarenje sigurnosti poslovnog uspjeha kompanije, što podrazumijeva eliminaciju svih rizika i ugrožavanja koji mogu utjecati na poslovne aktivnosti i ostvarenje poslovnog uspjeha, svođenje

ugrožavajućih učinaka na najmanju moguću mjeru te prevladavanje kriza i ponovno normalno poslovanje. Unutar svakog poduzeća, osim definiranja vizije, misije, strategije i strateških ciljeva, potrebno je definirati i kreirati sigurnosnu strategiju i sigurnosne poslovne procese, s ciljem uspostave što sigurnijeg poslovnog okruženja (Ivandić Vidović i dr., 2011).

Iako sigurnost prometa nije izričito naglašena niti u jednoj definiciji o poslovnoj ili korporativnoj sigurnosti, jasno je da nema učinkovite poslovne sigurnosti bez učinkovita transportnog procesa, kako izvan organizacije, tako i u samoj organizaciji.

2.2. Strategija korporativne sigurnosti

„Korporativna sigurnost ima za cilj održati povjerljivost, integritet i dostupnost informacija, imovine i osoblja tvrtke, a korporativne sigurnosne strategije također uključuju načine odgovora na prijetnje koje se neočekivano pojavljuju." (International Security Journal, 2024). Nakon utvrđenih ciljeva sljedeći je korak utvrđivanje strategije kako bi se navedeni ciljevi ostvarili. Izrada strategije proces je unaprijed definirana plana pa se implementacija, odnosno provedba strategije, može definirati kao proces zamjene stare strategije novom, pri čemu se mijenjaju mnogi temeljni strateški elementi kao što su vizija i misija poduzeća, ali i različiti resursi nužni za realizaciju planiranih ciljeva i zadataka (Ivandić Vidović i dr., 2011). U suvremenim uvjetima svi kvalitativni i kvantitativni ciljevi vezani su za sigurnosne ciljeve tako da je sigurnost poslovanja usko vezana za sigurnosnu strategiju.

Sigurnosna strategija u pravilu je dugoročna i teško podnosi promjene u kratkom vremenskom razdoblju zato što se sigurnosna strategija provodi putem sigurnosnih politika organizacije. Stoga sigurnosna strategija mora imati jasne ciljeve koji se moraju provesti i mora biti održiva tijekom duljeg razdoblja jer nije smisleno imati ciljeve bez sredstava za njihovu provedbu, ali isto tako nije smisleno ni imati sigurnosnu strategiju koja je u suprotnosti s poslovnom strategijom organizacije (Ivandić Vidović i dr., 2011). Prednosti koje donose definiranje, implementacija i kontrola sigurnosne strategije višestruke su:

- pomažu organizaciji pri njezinu uspješnom korporativnom upravljanju
- neposredno su vezani za poslovnu strategiju, pa organizaciji pružaju smjer i referentnu točku za uspostavljanje prioriteta
- pruža se pomoć pri poslovnom odlučivanju
- zaposlenicima se omogućava bolje razumijevanje važnosti sigurnosti i kako ona može pridonijeti dodanoj vrijednosti kompanije
- pomaže se u proaktivnom pristupu u rješavanju sigurnosnih problema
- pomaže se u zaštiti organizacijskog profita, ugleda, imovine, kupaca, dobavljača i zaposlenika
- poboljšava se korporativna održivost i promjenjivost (Ivandić Vidović i dr., 2011).

Prirodan je slijed utvrđivanje strategije korporativne sigurnosti. Strategija korporativne sigurnosti u poduzeću provodi se na funkcionalnoj razini i pripada jednoj od funkcijskih strategija poslovnog sustava (Ivandić Vidović i dr., 2011). Strategija korporativne sigurnosti ima svoje prednosti kao što su definiranje, implementacija i kontrola. Pritom, kod implementacije sigurnosne strategije jedinstvena provedba podrazumijeva i uspostavu ključnih čimbenika uspjeha te kvalitetu njihove izvedbe koji se odnose na poslovne procese korporativne sigurnosti (Ivandić Vidović i dr., 2011). Upravljanje poslovnim procesima temelj je uspješnosti poslovanja, a proces korporativne sigurnosti ulazi u upravljačke procese poduzeća, a kao što ulazi u upravljačke procese, ulazi i u upravljanje sigurnošću prometa.

2.3. Proces korporativne sigurnosti

Proces se definira kao niz radnji koje se poduzimaju da bi se postigao rezultat. (Cambridge Dictionary, 2024a). U cilju učinkovitog operativnog upravljanja proces korporativne sigurnosti mora proći trima fazama: dizajn procesa korporativne sigurnosti, implementacija procesa korporativne sigurnosti i kontrola procesa korporativne sigurnosti (Ivandić Vidović i dr., 2011).

Dizajn procesa korporativne sigurnosti određen je organizacijskom strukturom koja ovisi o poduzeću i ističe njegove važnosti.

Da bi se mogao uspostaviti proces korporativne sigurnosti, potrebno je ustrojiti organizacijske jedinice za korporativnu sigurnost. Organizacijska strukturna jedinica za korporativnu sigurnost ovisi o veličini poduzeća, o broju djelatnika u poduzeću te o teritorijalnoj rasprostranjenosti poslovnih jedinica samog poduzeća. Sami poslovni procesi korporativne sigurnosti svakodnevno su uključeni u mehanizme poslovnog upravljanja i tako štite normalno odvijanje poslovnih procesa poduzeća, stvaraju sigurne radne uvjete i ugodnu radnu atmosferu. Za provedbu aktivne zaštite i mjerljiva, efikasna odgovora na vanjske i unutarnje prijetnje nužne su vještine i kompetencije jer današnja orijentacija tvrtke mnogo je kritičnija, a efikasno vođenje s visokih razina upravljanja imperativ je današnjeg poslovanja. Da bi se model poslovnog procesa korporativne sigurnosti mogao prikazati, potrebno ga je prvo proučiti te modelirati organizacijsku strukturu korporativne sigurnosti u poduzeću (Ivandić Vidović i dr., 2011).

Implementacija procesa korporativne sigurnosti dolazi nakon faze modeliranja trenutnog stanja odvijanja procesa.

Osim što su potrebni modeli poslovnih procesa, potrebno je i dokumentirati poslovna pravila, ali i poboljšati informacijski sustav i educirati sve zaposlenike koji sudjeluju u procesu korporativne sigurnosti. Ako se zaposlenike koji rade na konkretnom procesu aktivno uključi, zaposlenici su motiviraniji za komunikaciju i suradnju te se postiže bolja prihvaćenost procesa od strane zaposlenika. U procesu korporativne

sigurnosti zahtijevaju se različite autorizacije, evidentiranja i praćenja te je u toj fazi sve potrebno testirati (Ivandić Vidović i dr., 2011).

Nakon što se poslovni proces korporativne sigurnosti implementira, potrebno ga je konstantno pratiti, unapređivati i kontrolirati. Iz takve kontrole često se dobiju odgovori na veliki broj pitanja koja se u svakodnevici postavljaju u poslovnome svijetu, postavljenih kako od samih stručnjaka iz područja korporativne sigurnosti, tako i od poslovodstva poduzeća.

Proces upravljanja poslovnom ili korporativnom sigurnošću i proces upravljanja sigurnošću prometa, iako zasebni procesi, imaju niz sličnosti i poveznica te će u budućnosti biti sve više približavanja između njih.

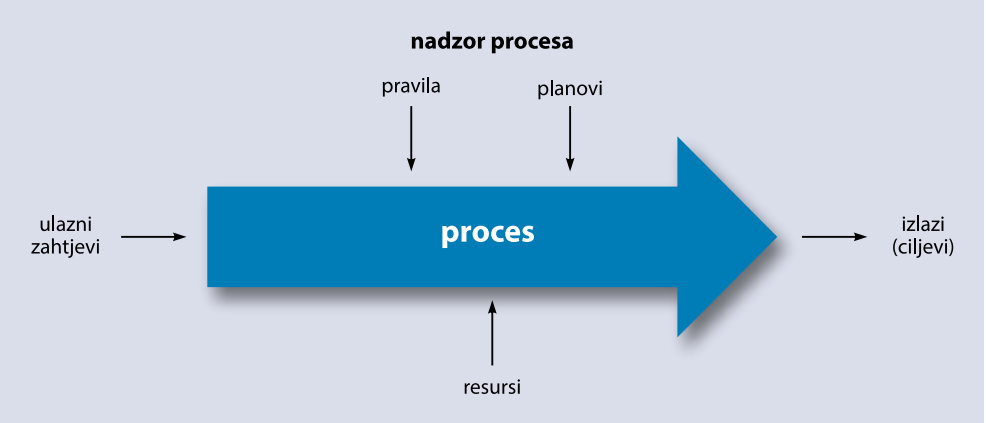
3. Upravljanje sigurnosnim procesima i rizicima

Od postojećih poslovnih procesa u organizacijama u proces korporativne sigurnosti implementiraju se neki od sljedećih procesa: zaštita na radu, zaštita od požara, zaštita okoliša, tjelesna i tehnička zaštita, zaštita imovine i spašavanje, obrambene pripreme, informacijska sigurnost, zaštita intelektualnog kapitala te zaštita podataka, zaštita podataka od državnog značaja i zaštita poslovne tajne.

Uspješnost procesa korporativne sigurnosti ovisi o uspješnosti upravljanja poslovnim procesima u poduzeću, a osobito onima koji su vezani za korporativnu sigurnost. Iako je upravljanje poslovnim procesima prepoznato još u prošlom stoljeću, posebno je naglašeno u ISO standardima prema kojima se proces definira kao skup mjera i aktivnosti koje međusobno utječu jedna na drugu kako bi ulaze pretvorilo u izlaze.[1] Osnovni elementi poslovnih procesa su:

- **ulaz** – jasno utvrđeni zahtjevi, podatci, dokumenti i prilozi koji određuju što se želi ili mora postići u procesu
- **resursi** – elementi procesa neophodni da se zahtjevi na ulazu u proces putem provedbe aktivnosti pretvore u planirane rezultate na izlazu iz procesa
- **izlaz** – rezultati koji prikazuju što se zaista postiglo provedbom procesa
- **pravila** – dokumenti i postupci koji propisuju što, kako i na koji način raditi tijekom izvođenja procesa (opći akti, radne upute)
- **kontrola** – temeljni oblik internog nadzora; metode i postupci ugrađeni u procese, a usvojeni od menadžmenta, radi osiguranja ostvarenja ciljeva.

[1] HRN EN ISO 9001, šesto izdanje, travanj 2016., zamjenjuje HRN EN ISO 9001: 2009, HRN EN ISO 9001: 2009 / Ispr.1: 2010; Sustavi upravljanja kvalitetom – Zahtjevi (ISO 9001: 2015; EN ISO 9001: 2015)



Slika 1. Osnovni elementi procesa (izvor: obrada autora)

Postavljeni izlazni ciljevi moraju biti u korelaciji s ključnim pokazateljima uspješnosti.

Uspostavljeni sustav upravljanja poslovnim procesima zahtijeva kontinuiranu kontrolu i nadzor sustava. Stoga treba periodično izvršiti ocjenu samog sustava.

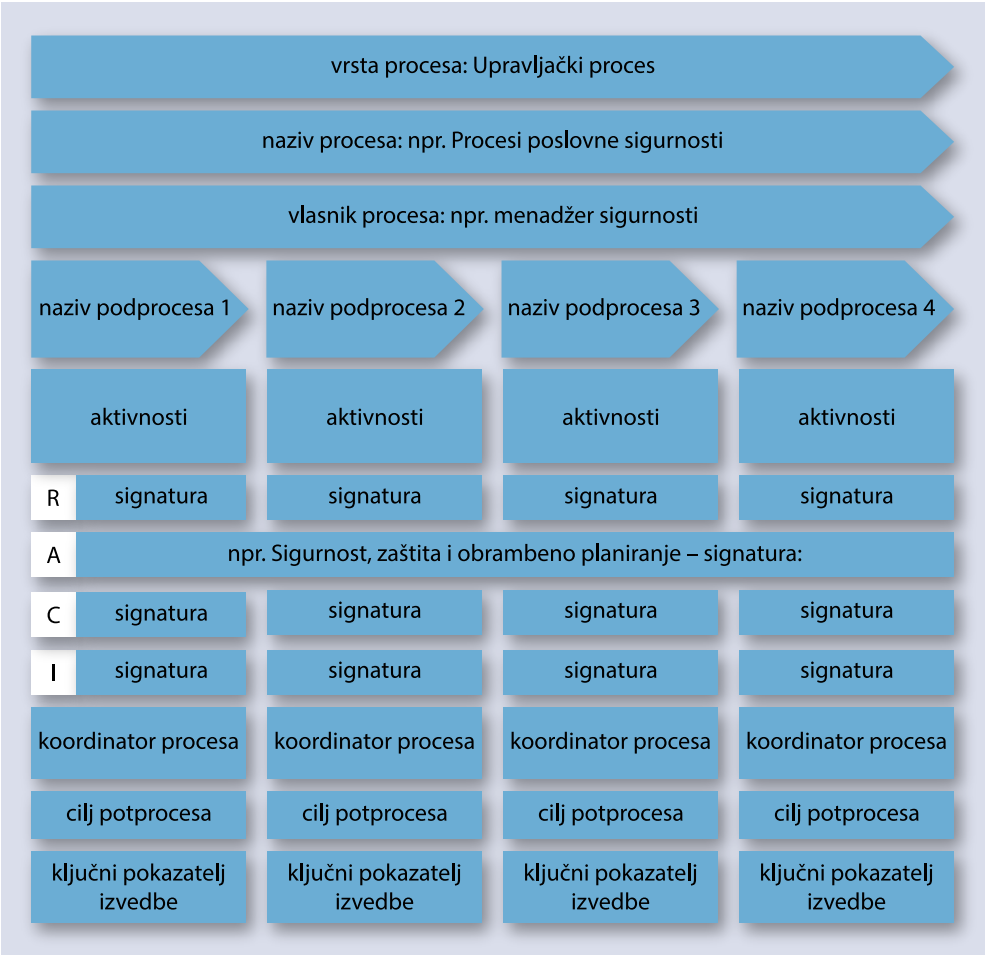
Poslovni procesi dijele se na (*Službeni vjesnik HŽ Infrastrukture*, 2015):

- glavne procese – horizontalni procesi koji su izravno usmjereni na realizaciju proizvoda, zadovoljstvo korisnika i dodavanje nove vrijednosti
- procese podrške – vertikalni procesi koji su neizravno usmjereni na realizaciju proizvoda i zadovoljstvo korisnika putem potpore glavnom procesu
- upravljačke procese – vertikalni procesi koji su usmjereni na upravljanje organizacijom, strateško planiranje, osiguranje resursa, analizu rezultata procesa ili pojedinih faza procesa i njihovo vrednovanje, kao i na njihovo neprestano poboljšavanje.

U organizacijama koje se bave transportnim i logističkim procesima proces sigurnosti prometa i proces korporativne sigurnosti grupira se u upravljačke procese.

Procesni pristup organizacijskoj strukturi nadopunjava funkcijsku organizacijsku strukturu koja u jednoj organizacijskoj cjelini obuhvaća određene aktivnosti vlastitih procesa i drugih procesa koji prolaze kroz nju. Ta poveznica prikazana je RACI matricom sa sljedećim značajkama (*Službeni vjesnik HŽ Infrastrukture*, 2015):

- *responsible* – organizacijska jedinica zadužena za provedbu procesnih aktivnosti
- *accountable* – vlasnik procesa odnosno organizacijska jedinica odgovorna za upravljanje procesom
- *consulted* – organizacijske jedinice koje je nužno konzultirati vezano za promjenu u procesu
- *informed* – organizacijske jedinice koje je dovoljno informirati o procesnim aktivnostima.



Slika 2. Primjer RACI matrice (izvor: obrada autora)

Poslovni proces kao skup uzajamno povezanih ili međusobno djelujućih potprocesa i/ili aktivnosti koje daju zaokružen rezultat i stvaraju prepoznatljivu dodanu vrijednost dijeli se na sljedeće razine (*Službeni vjesnik HŽ Infrastrukture*, 2015):

- potproces – prepoznatljiv dio procesa koji ima svoj ulaz i izlaz unutar osnovnog procesa, a više potprocesa čini proces
- aktivnost – skup povezanih ili međusobno djelujućih radnji koje su dio potprocesa pri čemu više radnih koraka čini aktivnost
- radni koraci – najmanji dijelovi aktivnosti u procesima koji se provode na propisan ili uobičajen način.

Razrada procesa po razinama posebno dolazi do izražaja kad je potrebno krenuti u promjene poslovnih procesa. Tada se poslovni proces analizira te se pokreće, oblikuje, razvija, opisuje, usvaja i implementira promjena. Kad se jednom promjena

implementira u poslovni proces, nužno je njezino održavanje i nadziranje. Promjene su nešto što najteže prolazi u uhodanim organizacijama te je prije implementacije nužno zadovoljiti dva uvjeta:

- tehnološki uvjet – proces mora biti izvodljiv i pozitivno utjecati na druge dijelove poslovanja
- psihološki uvjet – novi postupci redovito znače i nov način rada.

Današnje praćenje procesa omogućeno je brzim i jednostavnim praćenjem poslovanja preko softverskog alata za dizajn i redizajn poslovnih procesa. Najpoznatiji i jedan od najjačih softverskih alata za dizajniranje i upravljanjem poslovnim procesima je ARIS koji pruža potporu upravljanju životnim ciklusom poslovnih procesa te omogućuje praćenje kontinuiranih promjena poslovnih procesa i postizanje izvrsnosti poslovnih procesa. U ARIS-u se organizacijska arhitektura poduzeća promatra kroz organizacijski pogled, pogled funkcija, pogled podataka (dokumenti, baze, materijali), pogled proizvoda i usluga te pogled procesa (integrativni pogled). Takav sustav poslodavcu omogućava jednostavno upravljanje poslovnim procesima te omogućava i lakšu obuku i upravljanje promjenama u poduzeću. Putem sustava kontrole procesa cilj je razviti sustav koji će omogućiti praćenje poslovanja poduzeća, poduzimanje korektivnih akcija zbog samog poboljšanja poslovanja i donošenje upravljačkih odluka (Ivandić Vidović i dr., 2011).

Kad su u pitanju transportni i logistički procesi u zadnjih 40 godina došlo je do niza promjena, kako zbog globalizacije društva, tako i zbog raspada bivše države te širenja Europske unije čija je članica i Republika Hrvatska.

3.1. Od baze podataka do učinkovitosti procesa

Poslovna sigurnost integrira se u normativnoj sigurnosti („tehnička sigurnost" koja je ugrađena u robu) i preventivnoj sigurnosti (sigurnosni programi). Integriranje posebno dolazi do izražaja u organizacijama u kojima se povezuje ekonomija i sigurnost. Tehnička sigurnost (engl. *safety*) izravno je povezana s kvalitetom proizvoda (Matika, 2018):

- funkcionalnost robe (služi određenoj svrsi)
- pouzdanost robe (nije u kvaru)
- raspoloživost robe
- sigurnost robe – parametri koji se normiraju (standardi ispitivanja robe): bezopasnost, otpornost, žilavost i nekvarljivost.

Utvrđivanje kvalitete proizvoda, robe ili pružene transportne usluge te učinkovitost procesa upravljanja sigurnošću prometnih tokova ima slijed koraka prikazanih u Tablici 2.

Tablica 2. Utvrđivanje kvalitete robe

Korak	Pokazatelj	Opis
1.	baza podataka	skup podataka koji su organizirani tako da je korisniku omogućen brz pristup podatcima, a potom i njihovo brzo pretraživanje
2.	informacija ili obavijest	skup podataka s pripisanim značenjem, osnovni element komunikacije koji, primljen u određenoj situaciji, povećava čovjekovo znanje
3.	znanje	skup stečenih i povezanih informacija koje se mogu odnositi na teorijsko i/ili činjenično znanje
4.	spoznaja	čin, proces ili postupak stjecanja, odnosno proizvodnje znanja i/ili opravdanoga vjerovanja
5.	mudrost	sposobnost čovjekove refleksije nad sobom, svojim mislima i djelima, sposobnost uspješne integracije emocija i razumskog, vještine planiranja i donošenja odluka, razumijevanje drugih ljudi, spremnost na učenje
6.	učinak	posljedica nečega, ono što postoji po drugome kao rezultat neke radnje ili misli

Izvor: obrada autora

4. Upravljanje sigurnosnim rizicima

Stalne promjene u svijetu i u suvremenom poslovanju nužno su uvele proces upravljanja rizicima koji je propisan i Zakonom o sustavu unutarnjih kontrola u javom sektoru (Narodne novine, 2015b; Narodne novine, 2019). „Rizik je mogućnost nastanka događaja koji može nepovoljno utjecati na ostvarenje ciljeva" (Narodne novine, 2015b). U isti se način rizik definira i u stranoj literaturi. Rizik je mogućnost da će pojava nekog događaja nepovoljno utjecati na postizanje ciljeva organizacije (Stanford University, 2024). Rizik kao mjera vjerojatnosti zadobivanja ozljeda ili gubitka ima utjecaj na nesigurnost postizanja ciljeva. Osnovna je korist upravljanja rizicima smanjenje neizvjesnosti i pretvaranje neizvjesnosti u rizik. Neizvjesnost je svaki stupanj nesigurnosti povodom ostvarivanja očekivanih rezultata, odnosno za razliku od rizika, neizvjesnost nema mjerljive atribute, što onemogućavanja sustavno upravljanje. Ostale su koristi upravljanja rizicima bolje odlučivanje, povećanje učinkovitosti, bolje predviđanje i optimiziranje raspoloživih sredstava, jačanje povjerenja u sustav upravljanja pa i razvoj pozitivne organizacijske kulture.

Prvi i najteži korak je percepcija da bi se neki štetan događaj mogao dogoditi. Kad se određeni rizik prepozna, kreće se u sljedeće korake (*Službeni vjesnik HŽ Infrastrukture*, 2021):

- utvrđivanje rizika, odnosno pronalaženje, prepoznavanje i opisivanje rizika; u ovom koraku nužno je važno prepoznati ciljeve kojima prijeti opasnost neostvarenja ako se ne provede utvrđivanje rizika i ne ocijeni njihov utjecaj

- analizu rizika, odnosno shvaćanje prirode rizika i određivanje razine rizika; u ovom koraku razmatraju se uzroci i izvori rizika, njegove pozitivne i negativne posljedice i vjerojatnost da će se te posljedice pojaviti
- procjenu rizika, odnosno utvrđivanje je li rizik i njegova veličina prihvatljiva i podnošljiva; u ovom koraku provodi se rangiranje, utvrđivanje prioriteta i pružanje informacije za donošenje odluka na koje rizike je potrebno više usmjeriti pažnju.

Procjena se rizika sastoji od utvrđivanja vjerojatnosti hoće li se rizični događaj dogoditi, veličine štete u slučaju da dođe do štetnog događaja radi utvrđenog rizika te izračuna ukupne izloženosti.

Primjer upravljanja rizicima moguće je pokazati na organizaciji transporta automobila Unskom prugom uz tehničku zaštitu. Unska pruga naziv je za nekadašnju prugu od Zagreb preko Siska, Bihaća i Knina do Splita. Ovaj je primjer koristan jer obuhvaća dvije zemlje, tri upravitelja infrastrukture (u BiH zasebno je područje Republike Srpske, a zasebno područje Federacije BiH) i zbog toga što uključuje transport automobila što predstavlja najveću tehnološku razinu koju mogu realizirati samo najbolji prijevoznici i logističari.

Mogući rizici vezani za organizaciji transporta automobila Unskom prugom (Zagreb – Sisak – Bihać – Knin – Split) uz tehničku zaštitu:

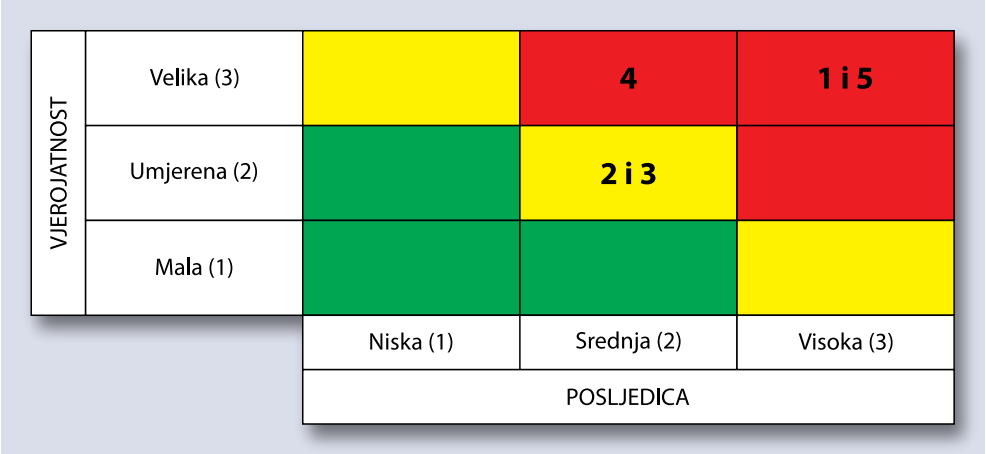
1. rizik: krađa dijelova s automobila
2. rizik: kvar željezničkog prijevoznog sredstva
3. rizik: kvar na željezničkoj infrastrukturi
4. rizik: prevelika birokracija među željezničkim poduzećima
5. rizik: kašnjenje vlaka na iskrcaj u luci.

Tablica 3. Procjena rizika za transport automobila Unskom prugom

Rizik	Vjerojatnost	Posljedica	Ukupno
Rizik 1.	3	3	9
Rizik 2.	2	2	4
Rizik 3.	2	2	4
Rizik 4.	3	2	6
Rizik 5.	3	3	9

Izvor: obrada autora (prema *Službenom vjesniku HŽ Infrastrukture*, 2021)

Slikovni prikaz rizika prikazuje se u matričnom obliku, kao na Slici 3. gdje su visokorizični rizici označeni crvenom bojom, a manje rizični žutom, odnosno zelenom bojom.



Slika 3. Procjena rizika za transport automobila Unskom prugom (izvor: obrada autora prema *Službenom vjesniku HŽ Infrastrukture*, 2021)

Akcijski planovi se utvrđuju i mjere se provode za sve rizike koji imaju ukupnu izloženost 6 i 9, kao i rizici koji imaju malu vjerojatnost (1) i veliku posljedicu (3). U ovom se primjeru mjere provode za utvrđene rizike:

- mjera za rizik 1.: ugovaranje osiguranja od štete
- mjera za rizik 4.: prepuštanje organizacije transporta pouzdanom i kvalitetnom logističaru
- mjera za rizik 5.: ugovaranje osiguranja od plaćanja lučkih i brodskih troškova.

Stoga kad je u pitanju postupanje s utvrđenim rizicima, oni mogu biti (*Službeni vjesnik HŽ Infrastrukture*, 2021):

- prihvaćanje rizika – prihvaćanje postojeće razine rizika
- smanjenje/ublažavanje rizika – poduzimanje radnji i donošenja odluka kako bi se smanjila vjerojatnost i/ili učinak rizika
- izbjegavanje rizika – potpuno ili djelomično izbjegavanje postiže se promjenom aktivnosti odnosno procesa
- prenošenje rizika – prenošenje rizika trećoj strani ili dijeljenje rizika s trećom stranom
- preuzimanje ili povećanje rizika kako bi se iskoristila prilika.

Rizici mogu biti unutarnji ili vanjski, a prema skupinama se dijele na (*Službeni vjesnik HŽ Infrastrukture*, 2021):

- hazardne (čiste) – povezani su s događajima koji imaju samo negativan ishod (nesreća u prometu)
- kontrolne (neizvjesne) – povezani su s nepoznatim i neočekivanim događajima nesigurnog ishoda

- rizike prilika (špekulativni) – povezani su s događajima koji mogu imati pozitivan ishod; sagledavaju se kao rizici opasnosti prihvaćanja mogućnosti i rizici propuštanja prilike; nisu vidljivi i materijalni.

U području sigurnosti prometa prepoznaje se pojam hazarda kao izvora potencijalnog oštećenja ili štete sa štetnim posljedicama na nešto ili nekoga pod određenim uvjetima rada, pa je rizik mjera vjerojatnosti pojavljivanja hazarda.

„Sustav upravljanja rizicima obuhvaća strategije, procese i postupke izvještavanja nužne za identificiranje, mjerenje, praćenje i upravljanje rizicima te kontinuirano izvještavanje na pojedinačnoj i grupnoj osnovi, o rizicima kojima je društvo za osiguranje izloženo ili bi moglo biti izloženo u svom poslovanju te o međuovisnosti tih rizika, a podliježe redovitom unutarnjem pregledu." (Narodne novine, 2014; Narodne novine, 2015a). Kako bi organizacija imala učinkovit sustav upravljanja rizicima nužno je uspostaviti proces upravljanja rizicima kojim se utvrđuju, ocjenjuju i prate rizici vezani za ostvarenje ciljeva organizacije te poduzimanje potrebnih aktivnosti u svrhu smanjenja rizika.

Suvremeno poslovanje i učinkovito upravljanje rizicima nije moguće bez poznavanja konteksta, odnosno stvaranja podloge za utvrđivanje mjerljivih ciljeva, utvrđivanje vanjskih i unutarnjih parametara upravljanja rizikom te određivanje područja i kriterija za rizike u procesu. S aspekta konteksta u području sigurnosti prometa i robnih tokova nužno je prepoznavanje kritične infrastrukture i sustava domovinske sigurnosti.

4.1. Kritična infrastruktura

Suvremeni svijet više ne „ratuje" samo klasičnim oblicima ratovanja, sve više je određena zemlja i određeno gospodarstvo ovisno o funkcionalnosti kritične infrastrukture. „Kritična infrastruktura predstavlja važnu sastavnicu nacionalne sigurnosti svake zemlje (pa tako i Hrvatske) jer ugroza takvih objekata (infrastrukture) dovodi u pitanje normalan tijek života i sigurnosti građana, ali i općenito funkcioniranje države. Kritična infrastruktura i njezina učinkovitost od velikog su značaja za kvalitetu života, gospodarstvo i javni sektor, pa je usklađenost sustava bitna i nužno joj je posvetiti pažnju prilikom donošenja planova, prosudbi i analizi rizika među svim dionicima sustava." (Mikac, Cesarac i Larkin, 2018: 23). U dostupnoj literaturi kritična infrastruktura (kao sustav) i imovina (fizička ili virtualna) vitalni su za državu jer bi nesposobnost ili uništenje takvih sustava i imovine imalo oslabljujući učinak na sigurnost, nacionalnu ekonomsku sigurnost, nacionalno javno zdravlje ili sigurnost ili bilo koju kombinaciju tih pitanja (Computer Security Resource Center, 2024). Najopćenitiji je opis pojma kritične infrastrukture infrastruktura koja uslijed nemogućnosti djelovanja ili oštećenja utječe na nacionalnu sigurnost i sve njezine komponente.

Zbog važnosti funkcionalnosti kritične infrastrukture u Republici Hrvatskoj usvojen je Zakon o kritičnim infrastrukturama (Narodne novine, 2013) koji definira nacionalne kritične infrastrukture. „Nacionalne kritične infrastrukture su sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti." (Narodne novine, 2013; Narodne novine, 2022) Sektori nacionalnih kritičnih infrastruktura, prema navedenom se zakonu dijele na:

- energetiku (proizvodnja, uključivo akumulacije i brane, prijenos, skladištenje, transport energenata i energije, sustavi za distribuciju)
- komunikacijske i informacijske tehnologije (elektroničke komunikacije, prijenos podataka, informacijski sustavi, pružanje audio i audiovizualnih medijskih usluga)
- promet (cestovni, željeznički, zračni, pomorski i promet unutarnjim plovnim putovima)
- zdravstvo (zdravstvena zaštita, proizvodnja, promet i nadzor nad lijekovima)
- vodno gospodarstvo (regulacijske i zaštitne vodne građevine i komunalne vodne građevine)
- hranu (proizvodnja i opskrba hranom i sustav sigurnosti hrane, robne zalihe)
- financije (bankarstvo, burze, investicije, sustavi osiguranja i plaćanja)
- proizvodnja, skladištenje i prijevoz opasnih tvari (kemijski, biološki, radiološki i nuklearni materijali)
- javne službe (osiguranje javnog reda i mira, zaštita i spašavanje, hitna medicinska pomoć)
- nacionalni spomenici i vrijednosti.

Iz navedenog pregleda sektora nacionalnih infrastruktura, s aspekta sigurnosti prometnih tokova, prepoznaju su energetika, promet, komunikacijska i informacijska tehnologija, hrana te proizvodnja, skladištenje i prijevoz opasnih tvari. Središnje tijelo državne uprave zaduženo za zaštitu i spašavanje redovito prati, procjenjuje ugroze i predlaže operativne i druge mjere za procjenjivanje kritičnosti, a vlasnici, odnosno upravitelji utvrđenih kritičnih infrastruktura izravno su odgovorni za upravljanje i zaštitu kritičnih infrastruktura u svim uvjetima.

U konačnici nacionalna kritična infrastruktura izravno je povezana sa sustavom domovinske sigurnosti. „Sustav domovinske sigurnosti čine:

1. središnja tijela državne uprave nadležna za unutarnje poslove, obranu, vanjske poslove, civilnu zaštitu, zaštitu okoliša, zdravstvo, financije i pravosuđe, uključujući i tijela iz njihova djelokruga te tijela sigurnosno-obavještajnog sustava Republike Hrvatske

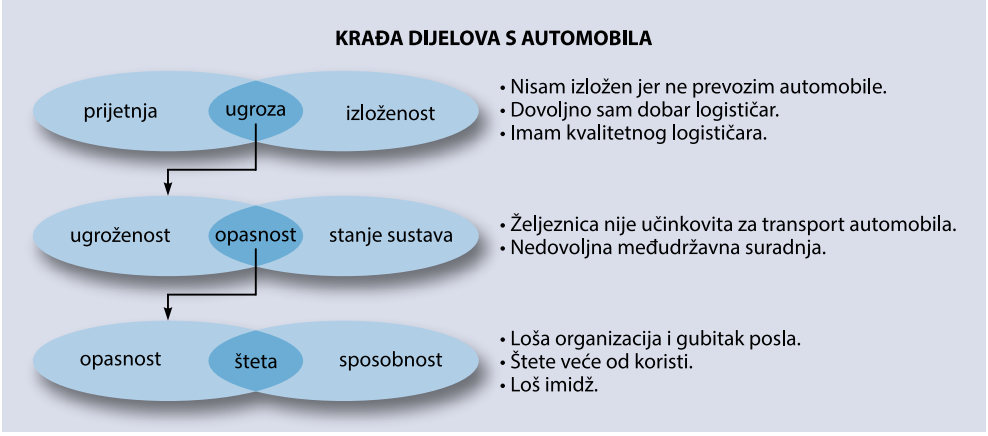
2. središnja tijela državne uprave koja u svojem djelokrugu imaju kritične infrastrukture, uključujući i tijela iz njihova djelokruga koja sudjeluju ili mogu sudjelovati u aktivnostima procesa upravljanja sigurnosnim rizicima
3. druga središnja tijela državne uprave." (Narodne novine, 2017)

4.2. Donošenje odluka

Prilikom donošenja odluka rizik se promatra kao osobna posebnost donositelja odluke, a donositelj odluke može biti sklon riziku, nesklon riziku ili neutralan po pitanju rizika. S obzirom da je rizik odlučivanja svjesna kategorija i ne može se isključiti, a nesklonost riziku često je rezultat neobaviještenosti, neznanja i problema u komunikaciji, koordinaciji i organiziranosti procesa kojim se upravlja, da bi se lakše donijela kvalitetna odluka nužno je prepoznati sljedeće pojmove:

- ugroza[2] – prijetnja kojoj je organizacija izložena
- opasnost – stanje sustava nije zadovoljavajuće i sustav se ne može suprotstaviti ugrozi
- šteta – nesposobnost u suprotstavljanju opasnosti izaziva štetu jer nije dostatna otpornost postojećeg sustava.

Primjer moguće štete u transportu automobila prikazan je na Slici 4.

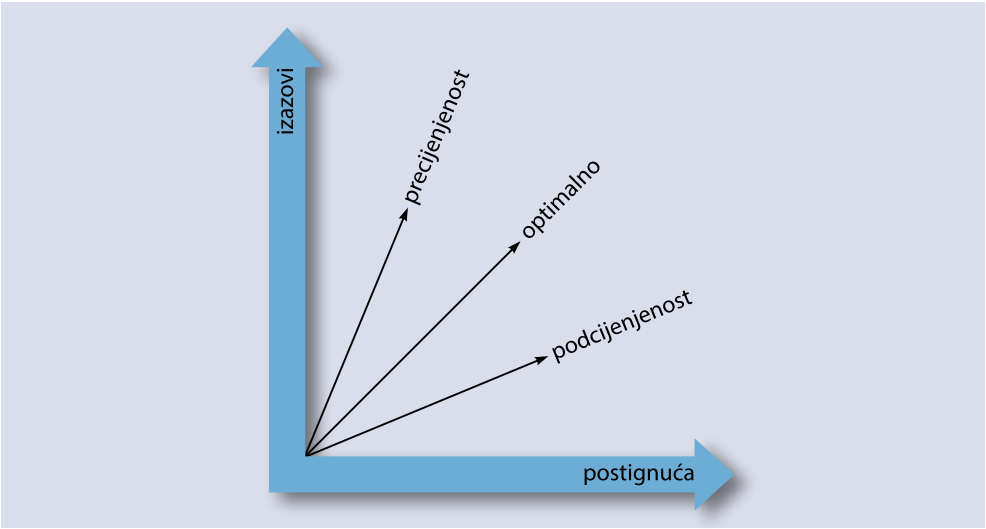


Slika 4. Šteta prouzročena zbog krađe dijelova na automobilima (izvor: obrada autora)

Pri donošenju odluka nužno je osvijestiti izazove s kojima se organizacija susreće te s postignućima organizacije, a može biti (Matika, 2018):

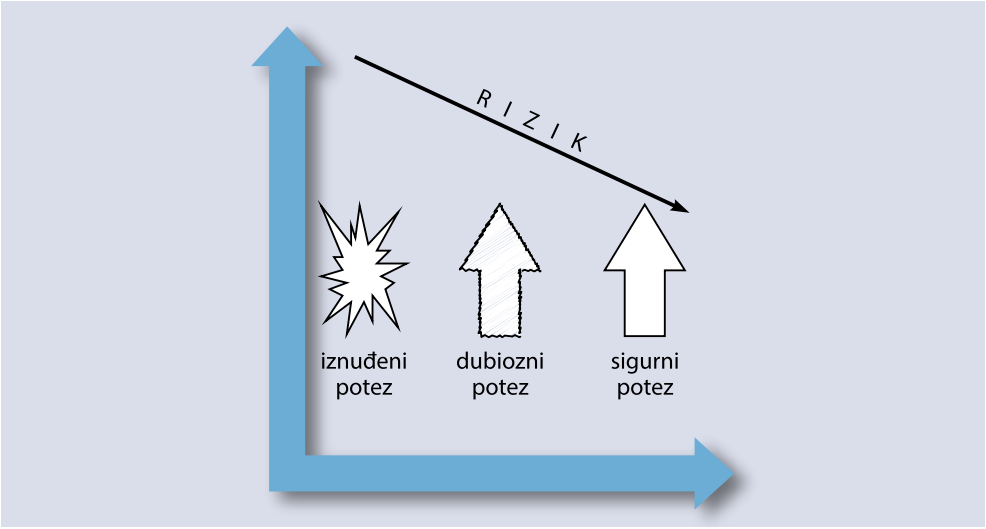
- podcijenjenost – niži izazovi od postignuća
- precijenjenost – veći izazovi od postignuća
- optimalno – izazovi u skladu s postignućima organizacije.

[2] Sugestija da će se dogoditi nešto neugodno ili nasilno, osobito ako se ne slijedi određena radnja ili naredba (Cambridge University, 2024b)



Slika 5. Odluka temeljena na ambiciji (izvor: obrada autora prema Matika, 2018.)

Precijenjenost ili podcijenjenost prilikom donošenja odluka značajno utječe na upravljanje rizicima u sigurnosti robnih tokova. Optimalnim odnosom izazova i postignuća organizacije dolazi se do sigurnih odluka, kao što se vidi na Slici 6.



Slika 6. Upravljanje rizicima na temelju sigurnih poteza
(izvor: obrada autora prema Matika 2018)

Bez izvrsnog poznavanja i upravljanja procesima poslovne sigurnosti i procesa sigurnosti prometa nije moguće osigurati kvalitetu, a time ni sigurnost robnih tokova te sigurnost prometnica i terminala potrebnih za prometne tokove.

5. Zaključak

Model upravljanja sigurnošću prometnih tokova koji obuhvaća i sigurnost prometnica i terminala spoj je procesa upravljanja poslovnom (korporativnom) sigurnošću i procesa upravljanja sigurnošću prometa. Zbog toga je u radu napravljeno pojmovno određenje poslovne sigurnosti i procesa koje obuhvaćaju te njihova poveznica sa sigurnošću prometa.

Upravljanje sigurnošću u suvremenim uvjetima poslovanja nije moguće bez učinkovitog upravljanja poslovnim procesima koje obuhvaća djelovanje temeljeno na bazama podataka, informacijama, znanjima, spoznajama i mudrosti te na upravljanju rizicima u skladu s donošenjem optimalnih i sigurnih odluka.

Sve to nije moguće bez dobrog teorijskog i praktičnog poznavanja izazova s kojima se susrećemo suvremene organizacije. Bila koja organizacija i svi studenti studija Menadžmenta poslovne sigurnosti, neovisno o struci kojom se bave, u svojem svakodnevnom radu susrećemo se s prometnim tokovima i sigurnošću prometa te je stoga nužno podizanje svjesnosti o važnosti znanja za njihove buduće poslovne izazove.

Literatura

1. Computer Security Resource Center (2024). Critical Infrastructure. https://csrc.nist.gov/glossary/term/critical_infrastructure (10. prosinca 2024.)
2. Cambridge Dictionary (2024a). Process. https://dictionary.cambridge.org/dictionary/english/process (10. prosinca 2024.)
3. Cambridge Dictionary (2024b). Threat. https://dictionary.cambridge.org/dictionary/english/threat (15. prosinca 2024.)
4. International Security Journal (2023). What is Corporate Security? https://internationalsecurityjournal.com/what-is-corporate-security/ (10. prosinca 2024.)
5. Ivandić Vidović, D., Karlović, L. i Ostojić, A. (2021). *Korporativna sigurnost*. Zagreb: HUMS.
6. Matika, D. (2018). *Integracija sigurnosti u poslovnim procesima (neobjavljeno predavanje)*. Zagreb, Libertas međunarodno sveučilište.
7. Mihaljević, B. i Nađ, I. (2018). *Osnove korporativne sigurnosti*. Zagreb: HUMS.
8. Mikac, R., Cesarac, I. i Larkin, R. (2018). *Kritična infrastruktura*. Zagreb: Jesenski i Turk.
9. Narodne novine (2013). Zakon o kritičnim infrastrukturama. NN 56/2013, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html (10. prosinca 2024.)
10. Narodne novine (2014). Pravilnik o sustavu upravljanja rizicima. NN 154/2014, https://narodne-novine.nn.hr/clanci/sluzbeni/2014_12_154_2923.html (10. prosinca 2024.)
11. Narodne novine (2015a). Odluka o upravljanju rizicima. NN 30/2015, https://narodne-novine.nn.hr/clanci/sluzbeni/2015_01_1_22.html (10. prosinca 2024.)
12. Narodne novine (2015b). Zakon o sustavu unutarnjih kontrola u javnom sektoru. NN 78/2015, https://narodne-novine.nn.hr/clanci/sluzbeni/2015_07_78_1492.html (10. prosinca 2024.)

13. Narodne novine (2017). Zakon o sustavu domovinske sigurnosti. NN 108/2017, https://narodne-novine.nn.hr/clanci/sluzbeni/2017_11_108_2489.html (10. prosinca 2024.)
14. Narodne novine (2019). Zakon o izmjenama i dopunama Zakona o sustavu unutarnjih kontrola u javnom sektoru. NN 102/2019, https://narodne-novine.nn.hr/clanci/sluzbeni/2019_10_102_2049.html (10. prosinca 2024.)
15. Narodne novine (2022). Zakon o izmjeni Zakona o kritičnim infrastrukturama. NN 114/2022, https://narodne-novine.nn.hr/clanci/sluzbeni/2022_10_114_1698.html (10. prosinca 2024.)
16. Security Executive Council (2024). What is Corporate Security? https://securityexecutivecouncil.com/insight/corporate-security-career/what-is-corporate-security-2097 (11. prosinca 2024.)
17. *Službeni vjesnik HŽ Infrastrukture* (2015). Uputa o upravljanja poslovnim procesima. Br.5/2015. Zagreb: HŽ Infrastruktura.
18. *Službeni vjesnik HŽ Infrastrukture* (2021). Uputa o upravljanja rizicima. Br. 7/2021. Zagreb: HŽ Infrastruktura.
19. Stanford University (2024). Definition of Risk. https://ocro.stanford.edu/enterprise-risk-management-erm/key-definitions/definition-risk (12. prosinca 2024.)

Management Model of Traffic Flow Corporate Security

Abstract

Although both corporate security management and traffic security-management contain the word security, in practice these two processes are managed separately. It is important for students of Corporate Security Management to bring their links closer, and especially for those students who don't have any contact with traffic security in their daily activities. In the paper, there is an overview of the conceptual definition of corporate security and the areas of security processes and security risks in the transport system were covered. In conclusion, emphasis is placed on the importance of knowledge in order to make optimal decisions.

Key words: traffic flow, corporate security management, critical infrastructure, process management, risk management