Integracija sustava upravljanja korporativnom sigurnošću i zaštitom primjenom procesnog pristupa

Forjan, Ernest

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:122:975639

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

University North Digital Repository

Sveučilište Sjever

Diplomski rad br. 069/OMIL/2021

Integracija sustava upravljanja korporativnom sigurnošću i zaštitom primjenom procesnog pristupa

Ernest Forjan, 1471/336D

Koprivnica, lipanj 2021. godine

Sveučilište Sjever

Odjel za Održivu mobilnost i logisitku

Diplomski rad br. 69/OMIL/2021

Integracija sustava upravljanja korporativnom sigurnošću i zaštitom primjenom procesnog pristupa

Student

Ernest Forjan, 1471/336D

Mentor

prof.dr.sc. Krešimir Buntak

Koprivnica, lipanj 2021. godine

Sveučilište
Sjever

SVEUČILIŠTE
SJEVER

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, _____ (ime i prezime) pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog/seminarskog (obrisati nepotrebno) rada pod naslovom
_____ (upisati naslov) te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)

_____
(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, _____ (ime i prezime) neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog/diplomskog (obrisati nepotrebno) rada pod naslovom _____ (upisati naslov) čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)

_____
(vlastoručni potpis)

Predgovor

Ovaj diplomski rad posvećujem svojoj obitelji.

Hvala Vam na podršci i potpori te razumijevanju tijekom studiranja.

Zahvaljujem se prof.dr.sc. Krešimiru Buntaku na stručnoj pomoći, savjetima i potpori prilikom izrade diplomskog rada. Također se zahvaljujem Matiji Kovačiću, mag.ing.traff, suradniku na kolegijima Upravljanje poslovnim procesima u logistici i Upravljanje kvalitetom na bezrezervnoj pomoći i suradnji.

Sažetak

U diplomskom radu govori se o integriranom pristupu sigurnosti i zaštiti u organizaciji što je imperativ s obzirom na sve veće zahtjeve koji izviru iz sve veće turbulentnosti organizacijskih okolina. Međutim, osiguranje i zaštita organizacije potreba je zbog mogućnosti zlonamjernosti organizacijskih zaposlenika, a treba biti sagledavana kroz aspekte ekonomske, ekološke i društvene održivosti. Nadalje, zbog velikog broja različitih normi kao i pozitivnih zakonskih propisa jedan od izazova s kojima se susreću današnje organizacije je integracija sustava upravljanja sigurnosti i zaštitom u organizaciji s obzirom da različite norme kao i različiti pozitivni zakonski propisi postavljaju i definiraju različite zahtjeve koji pokrivaju sve komponente trokuta održivosti. U ovom diplomskom radu opisan je konceptualni model integracije zahtjeva koje postavljaju pozitivni zakonski propisi i norme sustava upravljanja.

Ključne riječi: sigurnost i zaštita, norme sustava upravljanja, održivi uspjeh organizacije

Abstract

The thesis discusses an integrated approach to safety and security in the organization, which is imperative given the growing demands arising from the growing turbulence of organizational environments. However, the insurance and protection of the organization is necessary due to the possibility of malice of organizational employees, and should be considered through aspects of economic, environmental and social sustainability. Furthermore, due to the large number of different standards and positive legal regulations, one of the challenges faced by today's organizations is the integration of security and protection management systems in the organization as different standards and different positive legal regulations set and define different requirements covering all components. sustainability triangle. This thesis describes the conceptual model of integration of requirements set by positive legal regulations and norms of the management system.

Keywords: security and protection, management system norms, sustainable success of the organization

Popis korištenih kratica

IT	Informational technology
ISO	International organization for standardization
FMEA	Failure mode and effects analysis
KPI	Key performance indicators
CSF	Critical success factors

Sadržaj

1. Uvod 1

1.1. Cilj i svrha rada 2

1.2. Sadržaj diplomskog rada 2

1.3. Metodologija 3

2. Održivi rast i razvoj 4

3. Sigurnost i zaštita 8

3.1 Korporativna sigurnost 14

3.2 Rizik i zaštita i sigurnost 18

3.3 Kontinuitet poslovanja i sigurnost i zaštita 24

3.4 Sigurnost i zaštita i troškovi 25

4. Sustav upravljanja sigurnosti 26

4.1 Zakonska regulativa sigurnosti 30

4.2. Norme iz područja sigurnosti 31

5. Komparativna analiza normi i zakona iz područja sigurnosti 33

5.1. Komparativna analiza područja zaštite okoliša 35

5.2. Komparativna analiza područja sigurnosti na radu 41

5.3 Komparacija područja informacijske sigurnosti 46

5.4 Ostali normativni dokumenti 51

6. Proces upravljanja sustavom sigurnosti i zaštite 53

6.1. Evaluacija performansi procesa 57

6.2 Optimizacija i poboljšanje procesa 62

7. Model integriranog sustava upravljanja sigurnosti i zaštitom 67

7.1 Integracija sustava upravljanja 70

72. Metodologija integracije 74

8. Zaključak 78

Literatura 81

Popis slika 83
Popis tablica 84

1. Uvod

Sigurnost i zaštita u današnjim organizacijama postaje imperativ s obzirom na velik broj različitih ugroza. Ugroze se javljaju u prvom redu zbog promjenjivosti organizacijske okoline kao i novih izvora prijetnji koje se mogu pojaviti zbog razvoja znanosti i tehnologije.

S obzirom na uvjete koji prevladavaju u vanjskom ali i unutarnjem okruženju organizacije, današnje organizacije trebaju voditi računa o rizicima koji mogu proizaći iz promjena u organizacijskim okolinama, a identificirane rizike trebaju analizirati kako bi se, na temelju analize, mogle identificirati prijetnje koje mogu ugroziti sigurnost i zaštitu organizacije. Nadalje, kad se govori o sigurnosti i zaštiti, neophodno je napomenuti kako sigurnost i zaštita organizacije može biti ugrožena i zbog zlonamjernosti organizacijskih zaposlenika ali i, s druge strane, organizacijski zaposlenici mogu biti ugroženi zbog načina na koji sustav funkcionira, a što može značiti i sve vrste iskorištavanja zaposlenika ili osiguranja loših radnih uvjeta.

Potrebno je naglasiti kako su zaposlenici jedini živi dio svake organizacije i kao takvi su posebno osjetljivi. Isto tako, budući da su zaposlenici izravno uključeni u gotovo sve organizacijske procese, postoji rizik da njihovo nezadovoljstvo poslom, odnosno nezadovoljstvo statusom u organizaciji rezultira njihovom zlonamjernosti. Zlonamjernost može biti usmjerena prema odavanju poslovne tajne, odnosno može biti usmjerena prema namjernom kršenju postupaka i radnih uputa što će rezultirati ugrožavanjem kontinuiteta poslovanja ali i ugrožavanjem poslovnog rezultata organizacije.

Kao takve, današnje organizacije i njihovo poslovanje oblikovano je nizom zakonskih regulativa, odnosno može biti oblikovano nizom normi koje organizacije dobrovoljno implementiraju. Osiguranje sljedivosti sa zakonskim propisima organizaciji daje osnovu, odnosno omogućuje joj poslovanje budući da su zakonski propisi kao takvi usmjereni prema definiranju minimalnih zahtjeva koje organizacija mora osigurati kako bi mogla poslovati. S druge strane, norme i sustavi upravljanja organizaciji omogućuju stvaranje dodane vrijednosti budući da na već definirane zahtjeve koje na organizaciju postavljaju zakonski propisi definiraju nove zahtjeve koji su često znatno veći u odnosu na zahtjeve koje postavljaju pozitivni zakonski propisi. Osiguranje sljedivosti sa zakonskim propisima kao i osiguranje sljedivosti sa zahtjevima koje definiraju norme sustava upravljanja postaje izazovno s obzirom na usklađivanje i njihovu implementaciju tj. integraciju u organizacijski sustav. S obzirom na to, javlja se potreba za razvojem novih

konceptualnih modela koji će omogućiti tj. dati osnovu za integraciju različitih sustava upravljanja, odnosno različitih zakonskih propisa s kojima organizacija mora osigurati sljedivost. Ovakav pristup predstavlja sustavan pristup osiguranju sigurnosti i zaštite organizacije od internih i eksternih prijetnji kao i što smanjuje mogućnost pojave rizika koji bi mogli ugroziti normalno poslovanje organizacije. Nadalje, potrebno je naglasiti kako sigurnost i zaštita organizacije treba biti u službi osiguranja održivog uspjeha organizacije, a što podrazumijeva osiguranje ekonomske dimenzije održivosti, ekološke dimenzije održivosti kao i socijalne tj. društvene dimenzije održivosti.

1.1.Cilj i svrha rada

Cilj diplomskog rada prikazati je zahtjeve koje pozitivni zakonski propisi, odnosno norme sustava upravljanja postavljaju na današnje organizacije kao i prikazati nedovoljan broj modela koji bi omogućili sagledavanje sigurnosti i zaštite organizacije na sustavan način, odnosno koji bi omogućili integraciju različitih zahtjeva vezanih uz sigurnost i zaštitu u koherentnu cjelinu.

1.2. Sadržaj diplomskog rada

Diplomski rad podijeljen je na poglavlja. U prvom poglavlju diplomskog rada dan je uvod u temu jednako kao i što je opisana potreba integriranog pristupa upravljanju sigurnosti i zaštitom organizacije. Osim toga, u prvom poglavlju opisana je i korištena metodologija.

U drugom poglavlju diplomskog rada opisan je održivi rast i razvoj organizacije kao i značaj koji održivi rast i razvoj ima kako za današnje društvo tako i za organizacije.

Treće poglavlje govori o sigurnosti i zaštiti. Opisana je korporativna sigurnost kao i sve sastavnice korporativne sigurnosti. Osim toga, u trećem poglavlju opisana je potreba i važnost upravljanja rizicima i osiguranje kontinuiteta poslovanja kao i troškovi koji se povezuju uz sigurnost i zaštitu u organizaciji.

U četvrtom poglavlju opisan je sustav upravljanja sigurnosti kao i što su definirane direktne, odnosno indirektne norme. Osim normi, definirani su i pozitivni zakonski propisi koji oblikuju sustav upravljanja sigurnosti.

U petom poglavlju provedena je komparativna analiza normi i zakonskih propisa iz različitih područja kao i što je opisana problematika povezana uz komparativnu analizu.

Šesto poglavlje opisuje proces upravljanja sustavom sigurnosti i zaštite. Osim toga, opisan je način upravljanja procesima koji se odvijaju unutar sustava sigurnosti i zaštite kao i potreba poboljšanja i optimizacije procesa.

U sedmom poglavlju dan je zaključak, definirana su ograničenja istraživanja kao i preporuke za buduće istraživače ovog područja.

1.3.Metodologija

Diplomski rad temelji se na provedenom sekundarnom istraživanju. Sekundarno istraživanje usmjereno je prema identifikaciji svih normi koje su direktne i indirektne, a vežu se uz sigurnost i zaštitu. Direktne norme su norme koje determiniraju izgled sustava sigurnosti i zaštite dok indirektne norme na neizravan način oblikuju spomenuti sustav. Osim norma, u istraživanju su korišteni pozitivni zakonski propisi Republike Hrvatske.

Nakon identifikacije i deskripcije postojećih dostignuća i saznanja iz područja održivosti, rizika i sigurnosti i zaštite, provedena je komparativna analiza normi i pozitivnih zakonskih propisa. Za komparativnu analizu definirani su parametri usporedbe koji su oblikovani tako da su se u obzir uzeli parametri koji su zajednički normama i pozitivnim zakonskim propisima kao i parametri koji su od posebnog značaja za kreiranje konceptualnog modela. Parametri su kreirani tako da se sagledavao zahtjev koji je opisan u normi, odnosno zakonskim propisima, a koji su usmjereni prema dokumentiranju, definiranju kompetentnosti, definiranju ovlaštenja, itd.

2. Održivi rast i razvoj

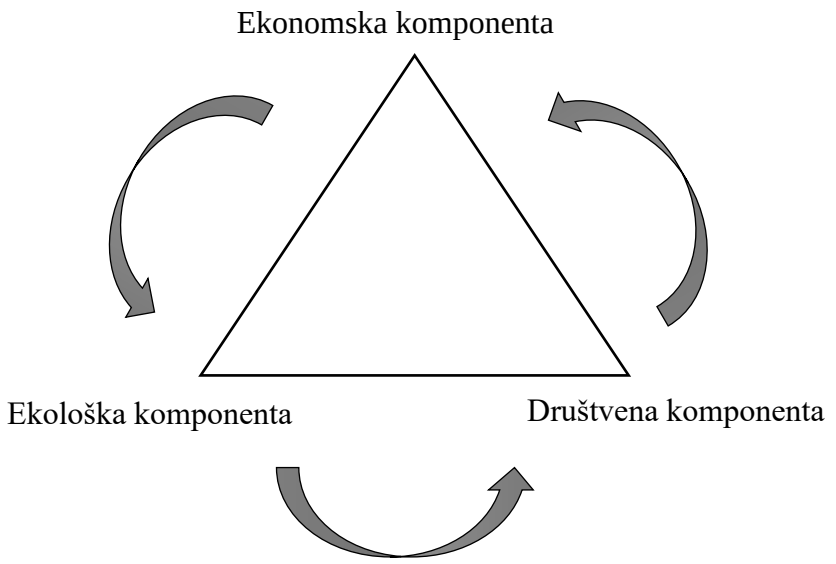
Održivi rast i razvoj podrazumijeva takvu vrstu rasta i razvoja u kojoj se resursi iz okoline racionalno troše, odnosno raspoređuju se tako da se ne ugrožava sposobnost budućih generacija da zadovolje iste potrebe koje imaju trenutne generacije (Hák, et al., 2016). Kao takav, održivi rast i razvoj može simbolički prikazati kroz trokut održivosti koji je prikazan na slici 1. Kao što je vidljivo iz slike 1, održivi rast i razvoj unutar sebe sadržava tri osnovne komponente: ekološku komponentu, društvenu ili socijalnu komponentu i ekonomsku komponentu. Kako bi organizacija uistinu bila održiva neophodno je osigurati sinergiju između svih elemenata trokuta održivosti. Osim toga, potrebno je naglasiti kako su elementi trokuta održivosti međusobno povezani, odnsono koreliraju jedan drugoga. Ekonomska održivost determinira društvenu održivost budući da bez ekonomske održivosti koja je determinirana jednakim rasporedom resursa, odnosno ostvarivanjem većih prihoda u odnosu na troškove, što je jedan od temeljnih uvjeta dugoročne opstojnosti organizacije, nije moguće osigurati dugoročnu društvenu održivost jer se društvo kao takvo ne može održavati bez dovoljne količine financijskih i drugih resursa. Nadalje, bez dugoročne održivosti društvenog segmenta, organizacije ne mogu razvijati dugoročne planove budući da se u pitanje dovodi potražnja za dobrima i uslugama koje nudi organizacija kao i mogućnost da organizacija angažira kompetentne ljudske resurse za normalno odvijanje procesa. Nadalje, društvena i ekonomska održivost determinira ekološku održivost budući da preveliki zahtjevi povezani uz osiguranje dovoljne količine resursa potrebnih za proizvodnju, odnsono normalno odvijanje poslovnih procesa mogu u znatnoj mjeri utjecati na okoliš. Nadalje, bez brige društva o okolišu kao i odgovornog ponašanje povećava se rizik povezan uz značajnije zagađenje okoliša.

Međutim, industrijska revolucija kao i ekspanzija gospodarstva sa sobom dovodi i do povećanja emisija štetnih plinova kao i rizik od nekontroliranog iskorištavanja oskudnih resursa budući da, paralelno s ekonomskom ekspanzijom dolazi i do društvene ekspanzije čime se dovodi u pitanje održivost takvog procesa (Zuo & Ai, 2011).

Ako se održivi rast i razvoj sagledava s aspekta upravljanja organizacijom, neophodno je voditi računa o dugoročnoj održivosti organizacije s ekonomskog aspekta. Drugim riječima, organizacije koje su profitabilne imaju znatno veću vjerojatnost, kroz ulaganja u edukaciju zaposlenika i ulaganje u implementaciju zelenih tehnologija, postići sinergiju svih komponenti trokuta

održivosti za razliku od organizacija koje na raspolaganju nemaju dovoljnu količinu financijskih resursa koje mogu ulagati u implementaciju zelenih tehnologija kao i edukaciju svojih zaposlenika kao i brigu o zaposlenicima čime se u znatnoj mjeri smanjuje njihova fluktuacija.

Slika 1: Trokut održivosti



Izvor: Slika je rad autora

Svaki od elemenata održivosti prikazan slikom 1 podrazumijeva:

- ekonomska komponenta: odnosi se na upravljanje organizacijom tako da menadžment na umu ima ostvarenje većeg prihoda u odnosu na rashode, odnosno osiguranje profitabilnosti organizacije budući da o profitabilnosti organizacije ovisi i mogućnost ulaganja u razvoj ostalih komponenti prikazanih slikom 1,
- ekološka održivost: odnosi se na brigu o okolišu kao i smanjenje negativnog utjecaja kojeg bi organizacija mogla imati na okoliš. Nadalje, odnosi se i na primjenu zelenih materijala, odnosno recikliranje svih materijala koje je moguće reciklirati. Isto tako, ekološka održivost odnosi se na povratnu logistiku kao i uspostavljanje zelenog lanca opskrbe što u znatnoj mjeri smanjuje negativan utjecaj organizacije na okoliš,
- društvena održivost: odnosi se na brigu o zaposlenicima kao i uključivanje zaposlenika u proces odlučivanja ali i poticanje angažmana zaposlenika u svim drugim aktivnostima u organizaciji čime se stvara povoljna organizacijska kultura kao i što se smanjuje fluktuacija zaposlenika kroz organizacijski sustav (Duran, et al., 2015).

Kad se govori o održivosti i sigurnosti i zaštiti, odnosno društvenoj odgovornosti, potrebno je napomenuti kako je sigurnost i zaštita sastavnica izvještaja o društveno odgovornom poslovanju. Drugim riječima, budući da je društveno odgovorno poslovanje usmjereno prema osiguranju ekološke, ekonomske i društvene održivosti, jedna od temeljnih komponenti društvene odgovornosti je briga o sigurnosti, zdravlju i zaštiti organizacijskih zaposlenika. Dakle, svaka organizacija, sukladno smjernicama za društveno odgovorno poslovanje, odnosno izvještavanje o istom, unutar izvještaja treba opisati način na koji brine o sigurnosti i zaštiti svojih zaposlenika, a što može podrazumijevati i sve napore koji su usmjereni prema osiguranje sigurne radne okoline, odnosno edukaciju zaposlenika za rad na siguran način.

Društveno odgovorno poslovanje podrazumijeva:

- poštivanje zakonskih propisa: svaka organizacija mora osigurati sukladnost sa pozitivnim zakonskim propisima koje nalaže zakonodavac, a koji mogu biti povezani uz područje sigurnosti i zaštite na radu, zaštite okoliša, itd. Dakle, kroz osiguranje sukladnosti s minimalnim uvjetima koje definira zakonodavac, organizacija stvara temelj za društveno odgovorno poslovanje, a samim time i smanjuje pojedine rizike koji su povezani uz mogućnost nastanka ozljede na radu.
- Umanjivanje negativnih učinaka poslovanja: organizacija treba nastojati u što je moguće većoj mjeri smanjiti sve svoje negativne učinke kako na društvo u cjelini tako i na zaposlenike koji se nalaze na radnim mjestima u organizaciji.
- Investicije i ulaganja: u prvoj mjeri podrazumijevaju ulaganje u povećanje sigurnosti i zaštite, odnosno ulaganje u poboljšanje pojedinih komponenti u sustavu koje će rezultirati smanjenjem rizika povezanih uz sigurnost i zaštitu, odnosno negativan utjecaj koji organizacija ima na okolinu (Nikolić, et al., 2012).

Kroz sve nabrojene elemente društvene odgovornosti, organizacija u znatnoj mjeri može utjecati i na povećanje brige o sigurnosti i zaštiti organizacijskih zaposlenika.

Nadalje, norma ISO 26000:2018 naglašava kao temeljne komponente društvene odgovornosti:

- Ljudska prava: što se može povezati ne samo uz prava koja su zajamčena zakonskim propisima već i prava koja se odnose na osiguranje sigurne radne okoline kao i svih sastavnica na radnom mjestu koje podrazumijevaju isto,

- Osnovna načela povezana uz rad: što podrazumijeva i načela koja se odnose na osiguranje sigurnih radnih uvjeta, kao i uključivanje zaposlenika u procese i aktivnosti bez njihovog isključenja
- Radna praksa: gdje definira niz pitanja koja su povezana uz zapošljavanje novih zaposlenika u organizaciju kao i oblikovanje radnih mjesta u organizaciji, opisuje sigurnost i zaštitu na radnom mjestu, uvjete rada i socijalnu zaštitu, razvoj ljudskih resursa i edukaciju, itd. (Nikolić, et al., 2012).

Kroz provedeno istraživanje, identificirano je kako postoji nedovoljan broj istraživanja koja bi povezivala društveno odgovorno poslovanje, odnosno održivost organizacije sa sigurnosti i zaštitom na radu što je jedno od područja u poslovanju na koje je potrebno obratiti pozornost zbog činjenice kako organizacija koja nastoji biti društveno odgovorna i održiva treba voditi računa o zaposlenicima kao i osiguranju sigurnih radnih uvjeta. Drugim riječima, ako organizacijski zaposlenici nemaju osigurane sigurne radne uvijete organizacija ne vodit računa o društvenoj komponenti održivosti.

3. Sigurnost i zaštita

Sigurnost se kao takva može definirati kao stupanj u kojem je neki sustav ili komponenta sustava zaštićena od negativnog utjecaja koji može biti povezan uz zlonamjernost drugih sustava ili zlonamjernost drugih pojedinaca. Dakle, sigurnost predstavlja izostanak rizika vezanog uz mogućnost negativnog utjecaja druge ili treće strane, odnosno varijable. Websterov rječnik sigurnost definira kao stanje zaštite od podvrgavanja ili nanošenja ozljeda, ozljeda ili gubitka kao i zaštitu od kvara, loma ili nesreće (Webster dictionary, 2020). S druge strane, zaštita predstavlja zaštitu osobe, infrastrukture, organizacije ili države od prijetnji poput kriminala ili napada stranih zemalja (Cambridge dictionary, 2020).

Nadalje, sigurnost se kao takva može podijeliti na više različitih područja, a kao što su to:

- Industrijska sigurnost: odnosi se na uspostavu sigurnosnog sustava koji je karakterističan za pojedine gospodarske grane, kao što su to građevinarstvo, elektroindustrija, industrija nafte, itd. Potrebno je napomenuti da se svaka od industrijskih grana uvelike razlikuje zbog specifičnosti djelatnosti.
- Gospodarska sigurnost: po svojem obuhvatu značajno je šira u odnosu na industrijsku sigurnost budući da obuhvaća gotovo sve industrije unutar sebe. Drugim riječima, odnosi se na sigurnost svih organizacija koje posluju tj. participiraju na tržištu unutar nekog gospodarstva.
- Poslovna sigurnost: u literaturi se često može naći pod nazivom inteligentna sigurnost, a temelji se na korporativnim normama, kulturi i poslovnoj etici. Nadalje, odnosi se na definiranje postupaka koji će se aktivirati nakon što se u organizaciji dogodi štetni događaj koji bi mogao ugroziti kontinuitet poslovanja organizacije (Mihaljević & Nađ, 2018).

Osim navedene podjele sigurnosti, sigurnost se može podijeliti i kako je to prikazano u tablici 1. Kao što je to vidljivo iz tablice, postoji stanovita razlika između integralne sigurnosti i integrirane sigurnosti što je od posebnog značaja budući da se u literaturi ali i praksi ova dva pojma često zamjenjuju što rezultira nedovoljno dobrim razumijevanjem. Nadalje, ako se organizacija sagledava kroz njezine sastavne dijelove tada se može reći da u organizaciji svaki podsustav treba imati razvijen svoj sigurnosni aspekt. Drugim riječima, može se reći da postoji informacijska sigurnost koja je povezana uz informacije u organizaciji, logistička sigurnost vezana uz logističke

procese koji se odvijaju u organizaciji, fizička sigurnost koja se odnosi na zaštitu infrastrukture, odnosno suprastrukture koja se nalazi u organizaciji, odnosno tehnička sigurnost.

Tablica 1: Podjela sigurnosti

Vrsta sigurnosti	Opis
Tehnička sigurnost	Odnosi se na implementaciju različitih vrsta tehničkih naprava kako bi se umanjio rizik povezan uz mogućnost pojave neželjenog događaja, odnosno mogućnost da neželjeni događaj kao posljedicu ima stvaranje gubitka ili umanjenja vrijednosti opreme tj. imovine s kojom organizacija raspolaže.
Fizička sigurnost	Odnosi se na fizičku zaštitu osoba i imovine, odnosno na upravljanje tijekom ljudi unutar organizacije kao i upravljanje tijekom ljudi iz organizacije i u organizaciju.
IT sigurnost	Odnosi se na sigurnost povezanu uz informacijsko-komunikacijsku tehnologiju koju organizacija koristi u svakodnevnom poslovanju. Neki od primjera ovakve vrste sigurnosti su sigurnost računala koje organizacija koristi, sigurnost baza podataka, sigurnost internetske mreže unutar organizacije, itd.
Informacijska sigurnost	Odnosi se na sigurnost pohranjenih informacija u organizaciji. Dakle, radi se o sigurnosti svih dokumentiranih informacija koje se nalaze spremljene u arhivama kao i sigurnosti svih informacija koje se nalaze spremljene u bazama podataka.
Integralna sigurnost	To je spoj tehničke zaštite, tjelesne zaštite, nadzora i intervencije. To je sustav koji omogućuje pravovremeno alarmiranje, odnosno pokretanje postupaka zbog prisutnosti neautorizirnog osoblja u štićenim prostorima. U pravilu, ovakav sustav funkcionira tako da dojavni sustav šalje informaciju o neželjenom prisustvu trećih osoba, odnosno o opasnosti od bilo koje vrste krađe. Nakon dojave, službe zadužene za intervenciju reagiraju sukladno identificiranoj prijetnji, a kako bi identificirale treću osobu koja je prisutna u prostoru, odnosno uklonile prijetnju.

Integrirana korporativna sigurnost	Odnosi se na centralizirano upravljanje svim sigurnosnim aspektima unutar organizacije. Dakle, radi se o dizajniranju poslovnih i drugih procesa kako bi oni unutar sebe imali implementirane mehanizme pomoću kojih će se smanjiti rizik povezan uz mogućnost krađe informacija, odnosno rizik povezan uz prisustvo trećih osoba u štićenom prostoru. Drugim riječima, integrirana korporativna sigurnost podrazumijeva zaštitu od požara, protuprovalnu zaštitu, itd.

Izvor: Mihaljević, B., & Nađ, I. (2018). The Basics of Corporate Security.

Kad se govori o uzrocima smanjenja sigurnosti sustava potrebno je napomenuti kako oni mogu biti raznoliki i kako mogu biti determinirani velikim brojem faktora. Neki od faktora koji mogu oblikovati sigurnost, odnosno koji je mogu determinirati mogu se svesti na:

- Pozitivne zakonske propise: nedovoljna briga Zakonodavca povezana uz sigurnost sustava kao posljedicu može imati kreiranje zakonskih propisa u kojima se sigurnost sagledava na nedovoljno dobar način. Drugim riječima, smanjivanje minimalnih zahtjeva koje sustav mora zadovoljiti da bi mogao normalno funkcionirati kao posljedicu ima i manju brigu organizacije povezanu uz brigu oko sigurnosti.
- Zlonamjernost: zlonamjernost predstavlja jednu od najčešćih uzroka ugrožavanja sigurnosti budući da može rezultirati neočekivanim postupcima pojedinaca ili grupe ljudi. Drugim riječima, zaposlenici koji se unutar organizacije organiziraju kako bi svojim djelovanjem nanijeli štetu organizaciji bilo kojeg oblika često se ne mogu na vrijeme identificirati. Zlonamjernost može biti posljedica loših odnosa unutar organizacije kao i nedovoljno dobro definiranih pozitivnih zakonskih propisa što otvara prostor za zlonamjerno djelovanje.
- Viša sila: sigurnost u znatnoj mjeri može biti narušena zbog više sile. U pravilu, organizacija ne može značajnije utjecati na smanjenje mogućnost negativnog utjecaja poplava ili požara budući da intenzitet takvih varijabli se ne može predvidjeti na vrijeme, odnosno ako se predvidi ne može se na vrijeme definirati mjera pomoću koje će se utjecati na smanjenje štete koja može nastati.
- Ostali mogući uzroci: kod ostalih mogućih uzroka potrebno je naglasiti kako loši međunarodni odnosi kao i nelojalnost konkurencije također može biti jedan od uzroka

smanjenja sigurnosti na koje organizacija ne može značajnije utjecati ali s druge strane treba definirati mjere temeljem kojih će smanjiti posljedicu utjecaja takvih varijabli (Mihaljević & Nađ, 2018).

U osnovi, varijable koje mogu ugroziti sigurnost organizacije mogu se podijeliti na unutarnje i vanjske. Unutarnje varijable odnose se na varijable koje se nalaze unutar same organizacije dok se vanjske varijable odnose na one varijable koje se nalaze u organizacijskim okolinama i koje se ne nalaze pod izravnom kontrolom organizacije. Za smanjenje negativnog utjecaja varijabli iz okoline organizacija može definirati mjere za smanjenje štete, odnosno mjere koje će omogućiti osiguranje kontinuiteta poslovanja organizacije. S druge strane, varijable koje se nalaze unutar organizacije trebaju biti analizirane kako bi se identificirao rizik povezan uz mogućnost nastanka događaja koji bi mogao ugroziti sigurnost, a zatim se za takve rizike definiraju preventivne mjere kako se takvi rizici uopće ne bi pojavili tj. ne bi ostvarili.

Potrebno je naglasiti kako organizacije kao takve mogu same postati izvor opasnosti za druge organizacije koje posluju na tržištu zbog svojeg nedovoljno dobro izgrađenog sustava sigurnosti i zaštite, odnosno zbog nedovoljno kompetentnog menadžmenta. U tom slučaju, organizacija može svojim nesavjesnim poslovanjem i ispuštanjem štetnih tvari u okolinu u znatnoj mjeri ugroziti zdravlje i sigurnost neposrednih stanovnika koji se nalaze oko organizacije kao i što može naštetiti drugim organizacijama u njihovom poslovanju. S druge strane, potrebno je napomenuti kako zlonamjernost menadžmenta, odnosno odsustvo poslovne etike u odlukama koje donosi menadžment također može značajno utjecati na loš utjecaj koji organizacija ima na druge organizacije u okruženju kao i gospodarski sustav kao takav. Drugim riječima, nepoštena poslovna praksa, nelojalnost prema konkurenciji, ilegalno zapošljavanje, itd. može predstavljati značajnu prijetnju smanjenju sigurnosti, odnosno može predstavljati varijablu koja u znatnoj mjeri može utjecati na pojavu rizika povezanog uz smanjenje same sigurnosti.

Neodgovarajuća briga organizacije vezana uz ispuštanje štetnih plinova u atmosferu, nedovoljno dobro odlaganje štetnih tvari na odlagalištima, nepoštene trgovačke, odnosno nepoštene poslovne prakse kao i loš odnos prema zaposlenicima ali i društvu koje se nalazi u neposrednoj blizini organizacije može utjecati na održivost poslovanja organizacije. Kao dokaz za to treba spomenuti kako se održivo poslovanje, odnosno održivost kao takva sastoji od ekonomske, društvene i ekološke održivosti, a koje mogu biti značajno narušene ako organizacija primjenjuje

neke od prethodno opisanih poslovnih praksi, odnosno neodgovorno se ponaša prema okolini u kojoj posluje.

Kad se govori o internim prijetnjama koje mogu u značajnoj mjeri ugroziti sigurnost same organizacije, organizaciji se preporučuje posebnu pozornost usmjeriti prema nekim od varijabli koje su opisane u tablici 2.

Tablica 2: Interne prijetnje u organizaciji

Izvor interne prijetnje	Opis
Nekompetentnost	Nekompetentnost kao posljedicu može imati nedovoljno dobro definirane odluke koje će rezultirati štetom za organizaciju. S druge strane, nedovoljna kompetentnost zaposlenika koji obavljaju poslove na radnim mjestima, a na kojima se susreće velik broj rizika, također može rezultirati nastankom neželjenog događaja kao i smanjenju sigurnosti u organizaciji.
Zastarjelost sredstava za rad	Jedan od problema s kojima se može susresti organizacija je i zastarjelost sredstava za rad što može rezultirati pojavom rizika povezanih uz ozljede na radu. Nadalje, zastarjela sredstva zaštite od požara koja se ne servisiraju sukladno preporukama također povećavaju opasnost povezanu uz mogućnost značajnijeg utjecaja neželjenog događaja, poput požara, na organizacijski sustav.
Korištenje energenata	Budući da je sigurnost i zaštita povezana uz održivost, a održivost kao taka ima komponente opisane u poglavlju 2, neophodno je osigurati da organizacija racionalno upravlja svim svojim energentima kao i što je neophodno osigurati da organizacija povećava energetsku učinkovitost podsustava što će rezultirati u dugom roku smanjenjem troškova.
Sklapanje štetnih ugovora	Povezano je uz mogućnost koruptivnih radnji što za organizaciju može značiti generiranje nepotrebnih troškova kao i nepotrebnih obveza prema trećim stranama.
Sukobi unutar organizacije	Loši odnosi unutar organizacije kao posljedicu mogu imati stvaranje loše organizacijske klime koja će rezultirati mogućom

	zlonamjernosti zaposlenika kao i povećanjem fluktuacija zaposlenika čime se može ugroziti sigurnost i kontinuitet.
Profesionalne bolesti	Loša ergonomija prilikom obavljanja zadataka na radnom mjestu kao posljedicu može imati pojavu velikog broja različitih profesionalnih bolesti. Pojava profesionalnih bolesti kao posljedicu može imati i generiranje većih troškova za organizaciju zbog većeg broja bolovanja.
Alkoholizam	Alkoholizam i opijati mogu često biti značajan uzrok nastanka neželjenih događaja u organizaciji. Zaposlenici pod utjecajem spomenutih supstanci često mogu donositi neracionalne odluke, odnosno često mogu imati rizično ponašanje koje može kao posljedicu imati pojavu nesreća ili drugih neželjenih događaja.
Požari	Požari su kao takvi jedan od najčešćih uzroka narušavanja sigurnosti u organizaciji. Zbog toga je od posebne važnosti osigurati adekvatnu opremu koja će omogućiti zaštitu od požara kao i provoditi edukaciju temeljem koje će svi zaposlenici moći postupati sukladno nastaloj situaciji.
Sabotaže	Sabotaže kao takve mogu biti posljedica djelovanja konkurencije kao i djelovanja zaposlenika. Sabotaže mogu rezultirati pojavom troškova povezanih uz nesukladnosti kao i pojavu velike štete zbog potrebe da organizacija ispravi štetu koja je nastala sabotažom.

Izvor: Tablica je rad autora

U tablici 2 navedene su samo neke od ugroza koje su povezane uz internu okolinu organizacije, a koje mogu ugroziti sigurnost. U praksi, svaka organizacija treba analizirati prijetnje unutar svoje interne okoline budući da se organizacije mogu značajno razlikovati jedna od druge zbog organizacijske kulture kao i zbog kompetentnosti menadžmenta prilikom upravljanja organizacijom. Međutim, potrebno je naglasiti kako se organizacijama preporučuje analiza i identifikacija svih značajnih ugroza koje bi mogle prekinuti kontinuitet poslovanja organizacije kao i definiranje mjera za smanjenje štete, odnosno preventivu od takvih događaja.

3.1 Korporativna sigurnost

Korporativna sigurnost jedan je od preduvjeta koje organizacija treba osigurati kako bi mogla dugoročno održivo poslovati. Kao takva, korporativna sigurnost odnosi se na sigurnost svih podsustava od kojih se sastoji organizacija. Drugim riječima, radi se o sigurnosti zaposlenika koji obavljaju aktivnosti u organizacijskim procesima, sigurnosti informacija koje se nalaze spremljene u organizacijskim bazama podataka kao i organizacijskim arhivama, sigurnost informacijskog sustava organizacije, sigurnost imovine, itd. O značaju korporativne sigurnosti u organizaciji govori i činjenica kako se današnjem organiziranju tj. stvaranju organizacije pristupa tako da se korporativna sigurnost smješta u zasebni odjel u organizaciji koji ima svoju autonomiju, a unutar samog odjela nalazi se niz manjih sektora koji su sastavni dio korporativne sigurnosti.

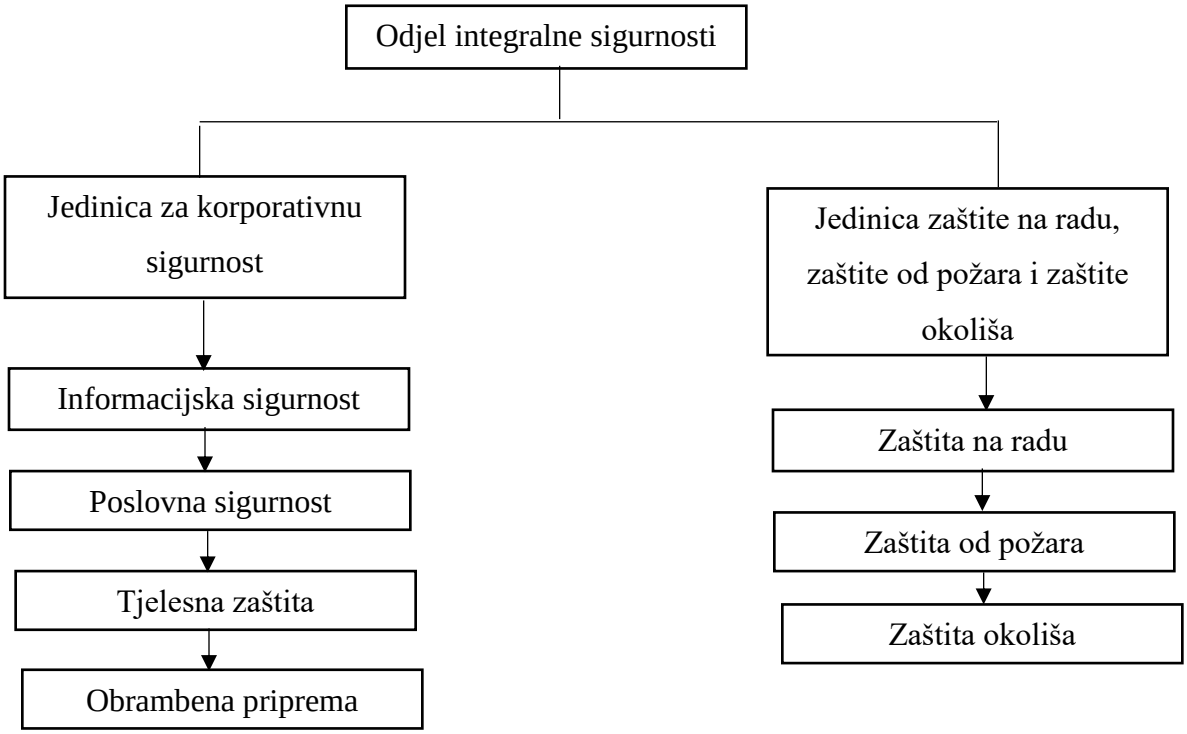
Kad se govori o organizacijama koje dugi niz godina posluju na tržištu, kao i organizacijama koje se mogu klasificirati kao velike organizacije, sigurnost takvih sustava često je izvedena preko tzv. integralne sigurnosti koja unutar sebe obuhvaća zaštitu od požara, odnosno zaštitu osoba i imovine i drugu zasebnu jedinicu koja se bavi korporativnom sigurnosti kao što je to prikazano na slici 1. Iz slike 2 je ujedno i vidljivo koji su to sastavni elementi jedinice korporativne sigurnosti što je od presudne važnosti za shvaćanje ostalih zapažanja opisanih u ovom radu.

Značaj korporativne sigurnosti posebno je naglašen zbog uvjeta u kojima egzistiraju današnje organizacije, a posebice zbog promjena nastalih novom industrijskom revolucijom tzv. Industrijom 4.0 koja naglašava digitalizaciju poslovanja, odnosno poslovanje u oblaku. Takav vid poslovanja sa sobom veže nove izazove povezane uz mogućnost kibernetičkih napada na organizacijske informacijske sustave, a što kao posljedicu može imati ugrozu informacija spremljenih u digitalnim bazama podataka (Pereira, et al., 2017). Nadalje, digitalizacijom i digitalnom transformacijom u znatnoj se mjeri povećava rizik povezan uz mogućnost preuzimanja kontrole od trećih strana koje nemaju autorizaciju, odnosno dopuštenje za upravljanje pojedinim sustavima. Preuzimanje upravljanja nad sustavom ujedno može značiti i rizik od radnji koje bi mogle rezultirati kako štetom za organizaciju tako i štetom za društvo. Jedan od primjera za to je organizacija koja svojim sustavom upravlja posredstvom interneta, odnosno koja za upravljanje postrojenjem koristi CPS (*Cyber physical system*)[1] koji omogućuje upravljanje na daljinu

[1] U slobodnom prijevodu s eng. kiber-fizički sustav

različitim postrojenjima, preuzimanje kontrole nad takvim sustavom kao posljedicu može imati prekid rada postrojenja ili pokretanje pojedinih dijelova postrojenja s namjerom uništavanja djela opreme ili nanošenjem štete kako za društvo tako i za organizaciju.

Slika 2: Odjel integralne sigurnosti



Izvor: Prilagodio autor prema Mikić, M. 2018. Korporativna sigurnost. Sveučilište u Rijeci.

Kad se govori o poslovima korporativne sigurnosti, odnosno o obuhvatu aktivnosti koje se obavljaju unutar odjela korporativne sigurnosti, treba navesti da su to sljedeći poslovi:

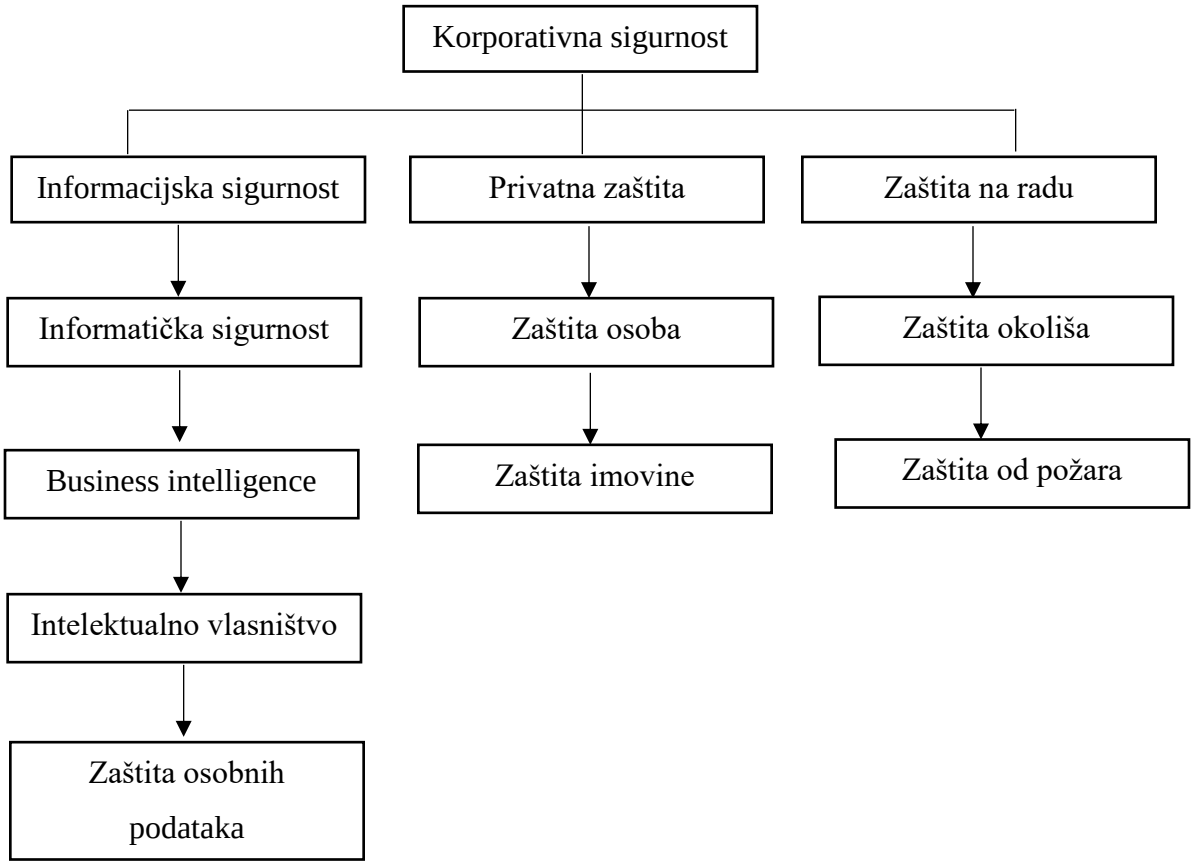
- poslovi administrativne sigurnosti: koji se odnose na uspostavu politika i postupaka koji će biti aktivirani ako dođe do potrebe,
- poslovi informacijske sigurnosti: koji se odnose na sve poslove usmjerene prema osiguranju informacija koje se nalaze u organizaciji. Informacije kao takve mogu biti digitalne ali mogu biti pohranjene i u fizičkom obliku,
- fizičke i tehničke sigurnosti: poslovi koji se odnose na tjelesnu zaštitu objekata, odnosno zaštitu osoba koje su od presudne važnosti za normalno funkcioniranje organizacije, a kao što su to članovi uprave,

- zaštite podataka: poslovi koji se odnose na sve aktivnosti koje su neophodne da bi se zaštitili podatci o zaposlenicima, odnosno da bi se zaštitile poslovne tajne koje su od presudnog značaja za poslovanje organizacije,
- sigurnost vlasništva: odnosi se na sve aktivnosti usmjerene prema uspostavi sustava koji će zaštititi intelektualno vlasništvo organizacije, a kao što su to patenti, inovacije, procesi, postupci, itd. od mogućnosti da treće strane imaju uvid u takve informacije,
- osobna sigurnost: sve aktivnosti koje su usmjerene prema zaštiti na radu, odnosno zaštiti zaposlenika od mogućih ozljeda koje mogu nastati obavljanjem poslova na radnom mjestu. Nadalje, osobna sigurnost unutar sebe obuhvaća i zaštitu od požara kao i zaštitu okoliša od neželjenog utjecaja organizacije,
- edukacije i usavršavanja: osim što korporativna sigurnost podrazumijeva mjere usmjerene prema preventivi, odnosno definiranju mjera koje će biti usmjerene prema sprječavanju mogućeg nastanka problema, korporativna sigurnost treba provoditi aktivnosti koje su usmjerene prema podizanju razine kompetentnosti organizacijskih zaposlenika kako bi organizacijski zaposlenici na vrijeme mogli prepoznati opasnost i spriječiti mogućnost nastanka štete ili ozljede (Mikić, 2018).

Korporativna sigurnost kao takva oblikovana je nizom različitih normativnih okvira koji ovise o tome ima li organizacija implementiran tj. certificiran sustav upravljanja. Nadalje normativni okvir koji determinira korporativnu sigurnost definiran je i temeljnom djelatnosti kojom se organizacija bavi. Postoji stanovita razlika između normativnog okvira za zdravstvene organizacije i normativnog okvira za organizacije koje se bave pružanjem logističkih usluga. Potrebno je naglasiti kako organizacije, kroz osiguranje sukladnosti sa zahtjevima koje na nju postavljaju pozitivni zakonski propisi zemlje, odnosno gospodarstva unutar kojeg egzistira, osigurava minimalne zahtjeve koje organizacija treba ispuniti da bi mogla poslovati. S druge strane, osiguranje sukladnosti sa zahtjevima koje na organizacijski sustav postavljaju norme različitih sustava upravljanja organizaciji omogućuje stvaranje dodane vrijednosti povezane uz podizanje razine sigurnosti i spremnosti organizacije na neplanirani događaj, odnosno na neželjeni događaj. Potrebno je napomenuti kako normativni okvir ovisi o području koje pokriva. Primjerice, postoji stanovita razlika između normativnog okvira povezanog uz informacijsku sigurnost i normativnog okvira povezanog uz sigurnost i zaštitu zaposlenika, odnosno sigurnost na radu.

Kad se govori o poslovima o okviru koji pokriva korporativna sigurnost potrebno je naglasiti kako se korporativna sigurnost može sastojati od tri temeljne djelatnosti, a samim time se ujedno oblikuje i njezin okvir koje pokrivaju poslovi tj. aktivnosti odjela korporativne sigurnosti. Drugim riječima, korporativna sigurnost može se prikazati blok shemom koja je prikazana na slici 3.

Slika 3: Prikaz sastavnica korporativne sigurnosti



Izvor: Darija, I. V., Lidija, K., & Alen, O. (2011). Korporativna sigurnost.

Kao što je to vidljivo na slici 3, korporativna sigurnost unutar sebe objedinjuje niz djelatnosti i vrlo je slična integralnoj sigurnosti. Međutim, potrebno je naglasiti kako, s povećanjem zahtjeva vezanih za korporativnu sigurnost kao i povećanjem broja ugroza koje dolaze iz organizacijskih okolina raste i potreba za uvođenjem tzv. integrirane korporativne sigurnosti koja podrazumijeva uvođenje normi tj. osiguranje sljedivosti sa zakonskim propisima kao i uvođenje sustava upravljanja koji će oblikovati pojedini dio korporativne sigurnosti.

Nadalje, slika 3 prikazuje kako se korporativna sigurnost sastoji od informacijske sigurnosti koja je povezana uz informatičku sigurnost, odnosno sigurnost informatičke i druge opreme.

Nadalje, jedan od vrlo važnih dijelova korporativne sigurnosti je i business intelligence koji je povezan uz aktivnosti usmjerene prema analizi postojećih informacija s kojima organizacija raspolaže kao i analizu svih informacija koje dolaze s tržišta, a analiziranjem kojih organizacija može doći do spoznaja povezanih uz tržišne promjene kao i poteze konkurentskih organizacija, a koji mogu voditi prema pojavi novih ugroza za organizaciju. Isto tako, poslovi u okviru business intelligencea povezani su uz analiziranje velikog broja informacija koje se nalaze spremljene unutar baza podataka tj. tzv. rudarenje podataka (Trieu, 2017). Rudarenje podataka podrazumijeva potragu za informacijama na temelju kojih se mogu razaznati buduća tržišna ili druga kretanja. Ova jedinica unutar korporativne sigurnosti od posebne je važnosti za normalno funkcioniranje organizacije kao i za stvaranje temelja za održivi rast i razvoj organizacije (Madni, et al., 2017).

Osim spomenutog, korporativna sigurnost odnosi se i na poslove privatne zaštite koji su često eksternalizirani drugim specijaliziranim organizacijama, a koje posjeduju kompetentne ljude koji mogu obavljati takve poslove. Riječ je o aktivnostima zaštite objekata, odnosno poslovima tehničke zaštite koji podrazumijevaju postavljanje tehničkih pomagala za praćenje aktivnosti unutar objekta.

Posljednja grupa aktivnosti unutar korporativne sigurnosti su zaštita od požara, zaštita na radu, odnosno zaštita okoliša. Sve tri aktivnosti vrlo su važne za organizaciju budući da su usmjerene prema preventivnim radnjama, a koje će u budućnosti rezultirati smanjenjem troškova koji mogu nastati zbog ozljeda na radu ili požara, a koji će nanijeti štetu organizaciji.

Međutim, osnova za obavljanje svih aktivnosti unutar odjela korporativne sigurnosti procjena je rizika budući da je rizik kao takav izvor prijetnji za organizacijski sustav, odnosno izvor prijetnji koji može ugroziti kontinuitet poslovanja organizacije.

3.2 Rizik i zaštita i sigurnost

Rizik se kao takav može definirati kao učinak nesigurnosti na ciljeve (ISO 9000, 2015). Drugim riječima, rizik povećava vjerojatnost da organizacija neće ostvariti ciljeve koje je definirala u planovima, a što će kao posljedicu imati pad učinkovitosti i djelotvornosti organizacije. Ako se govori o korporativnoj sigurnosti, odnosno o zaštiti i sigurnosti i rizicima, rizici u znatnoj mjeri mogu povećati vjerojatnost da će se u organizaciji dogoditi neželjeni događaj koji će kao posljedicu imati štetu i to s aspekta štete vezane uz ozljede na radu, štete vezane uz umanjenje

vrijednosti imovine ili negativan utjecaj koji može nastati na okoliš zbog pojave rizika, odnosno štete koja nastaje zbog posljedica rizika (Aven, 2016).

S obzirom na to, svaka organizacija treba analizirati rizike povezane uz njezino poslovanje, odnosno rizike koji se odnose na aktivnosti koje se odvijaju tj. obavljaju unutar organizacije.

Kad se govori o rizicima, rizici se mogu podijeliti na:

- financijske rizike: financijski rizici povezani su uz promjenu kamatne stope, odnosno financijska kretanja na tržištu koja će kao posljedicu imati smanjenje vrijednosti imovine organizacije,
- informacijske rizike: ova vrsta rizika povezana je uz mogućnost da informacije koje se nalaze spremljene u organizaciji zbog lošeg upravljanja informacijama budu dostupne trećim stranama, odnosno stranama koje nemaju dopuštenje za njihovo pregledavanje,
- poslovne rizike: poslovni rizici mogu biti povezani uz odluke koje donosi menadžment, a koje kao posljedicu mogu imati smanjenje tržišnog udjela, loš utjecaj na reputaciju organizacije ili pak i narušavanje kontinuiteta poslovanja,
- tržišne rizike: tržišni rizici povezani su uz mogućnost neuspjeha organizacije tj. organizacijskog proizvoda koji je organizacija plasirala na tržište kao i svi drugi rizici koji su povezani uz mogući neuspjeh na tržištu.

Svi navedeni rizici samo su neki od rizika koji mogu značajno utjecati na organizaciju, odnosno koji mogu ugroziti poslovanje organizacije. Međutim, s aspekta korporativne sigurnosti, neki od najznačajnijih rizika mogu biti povezani uz same aktivnosti korporativne sigurnosti, odnosno područja djelatnosti kojom se bavi korporativna sigurnost.

Neki od najznačajnijih rizika, odnosno rizika koji se najčešće susreću, a vezani su uz korporativni sigurnost su rizici na radnom mjestu. Rizici na radnom mjestu povezani su uz nesreće na radu, odnosno aktivnosti koje zaposlenici svakodnevno provode obavljajući poslove na svojim radnim mjestima. Takvi rizici mogu biti posljedica nedovoljno dobre educiranosti zaposlenika kao i zastarjele opreme, odnosno loše zaštite na radu.

S druge strane, rizici od požara kao i rizici lošeg utjecaja na okoliš mogu biti posljedica greške zaposlenika kao i kvara na postrojenjima u organizaciji. Ako organizacija nema definirane mjere temeljem kojih će smanjiti posljedicu rizika, takvi rizici mogu značiti nanošenje velike štete ne

samo organizaciji već i organizacijskim okolinama što će kao posljedicu imati pojavu visokih troškova zbog potrebe da organizacija sanira štetu koja je nastala zbog pojave nekog od rizika.

Od ostalih rizika s kojima se susreće organizacija s aspekta korporativne sigurnosti potrebno je navesti informacijske rizike koji su povezani uz štetu koja može nastati zbog nedovoljno dobrog čuvanja informacija u organizaciji kao i curenje informacija u javnost, a koje mogu biti povezane uz poslovnu tajnu ili planove organizacije.

Kako bi organizacija umanjila posljedice rizika, neophodno je analizirati sve rizike, odnosno rizike za koje organizacija identificira da su od posebne važnosti za osiguranje kontinuiteta poslovanja. Identificirani rizici mogu se analizirati pomoću različitih alata i metoda, a jedan od alata je i FMEA (*Failure mode and effects analysis*) metoda koja je prikazana tablicom 3.

Tablica 3: FMEA metoda

Funkcija, aktivnost	Potencijalni rizik	Potencijalna posljedica	Ozbiljnost	Učestalost	Detekcija	Mjera	Odgovornost

Izvor: Tablica je rad autora

U Tablici 3, nabrojene stavke odnose se na:

- funkcija, aktivnost: označava predmet proučavanja, odnosno predmet analize. U osnovi, može se raditi o funkciji proizvoda, odnosno o aktivnostima koje obavljaju zaposlenici na radnim mjestima na kojima rade,
- potencijalni rizik: odnosi se na rizik povezan uz funkciju,
- potencijalna posljedica: odnosi se na posljedicu pojave rizika koja može biti fatalna ako se radi o zaposlenicima koji su zahvaćeni rizikom, odnosno koja može značiti prekid funkcije proizvoda ili prekid poslovanja organizacije,
- ozbiljnost: odnosi se na procjenu ozbiljnosti rizika, ponderira se ponderima od 1 do 10 gdje je ponder 1 najmanja ozbiljnost, a ponder 10 najveća ozbiljnost. Ozbiljnost se u prvom redu procjenjuje posljedicom za organizaciju. Što je posljedica štetnija za organizaciju to je ujedno i ozbiljnost veća,

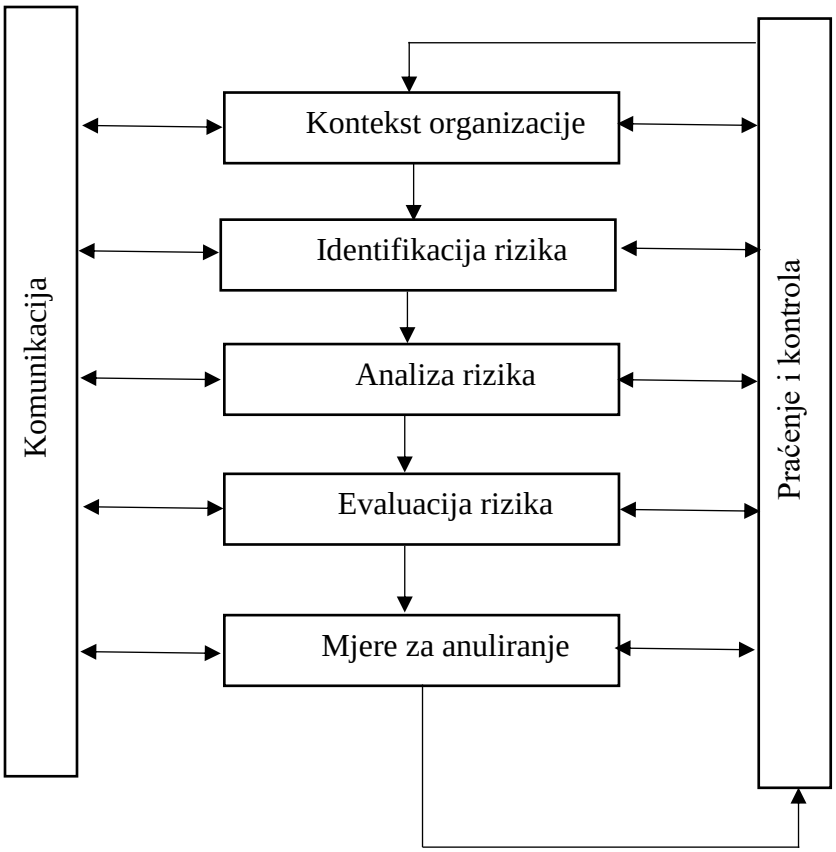
- učestalost: odnosi se na pojavnost pojedinog rizika. Što je mogućnost ponavljanja rizika veća to je i učestalost veća. Jednako kao i ozbiljnost, procjenjuje se ponderima od 1 do 10 gdje je ponder 1 najmanja učestalost, a ponder 10 najveća učestalost, odnosno sigurno je da će se pojedini rizik pojaviti,
- detekcija: odnosi se na vjerojatnost identificiranja rizika. Što je rizik manje vjerojatno detektirati to je i veći ponder koji se upotrebljava za ocjenjivanje. Drugim riječima, ponder 1 definira sigurnu identifikaciju rizika, dok ponder 10 definira rizik koji je gotovo nemoguće identificirati,
- mjera: definira što će organizacija poduzeti kako bi smanjila posljedicu rizika, odnosno kako bi umanjila utjecaj koji rizik ima na organizaciju. Mjera može biti preventivna ili korektivna što je u ovisnosti o tome je li se rizik već pojavio ili ne,
- odgovornost: definira odgovornu osobu koja će biti zadužena za provođenje mjera koje je organizacija definirala. Odgovorna osoba može biti rukovodeća osoba u organizaciji ali može biti i sam zaposlenik koji neposredno obavlja aktivnosti na radnom mjestu (Buntak, et al., 2020).

FMEA analiza preporučuje se provoditi prilikom kreiranja novog radnog mjesta, odnosno periodično za svako radno mjesta kako bi se analizirao rizik povezan uz svako radno mjestu, a samim time i provela adekvatna edukacija zaposlenika koji obavlja aktivnosti na pojedinom radnom mjestu. Nadalje, FMEA analiza preporučuje se provoditi i za sva područja koje pokriva korporativna sigurnost kako bi se identificirao što je mogući veći broj rizika koji mogu nanijeti štetu za organizaciju. Potrebno je napomenuti da se mjera kao takva definira u ovisnosti o visini umnoška pondera za ozbiljnost, učestalost i detekciju. Što je visina umnoška spomenutih pondera veća to je i mjera koju organizacija definira ozbiljnija, odnosno po svojem obuhvatu znatno šira. Međutim, mjere koje organizacija definira kao i značenje pojedinog pondera koji se upotrebljava za ocjenjivanje rizika ovisi o organizacijskoj politici upravljanja rizicima. Svaka organizacija ima drugačiju politiku upravljanja rizicima koja je determinirana organizacijskom otpornosti kao i spremnosti organizacije da se odupre eventualnim prijetnjama.

Kad se govori o identifikaciji rizika i analizi rizika, potrebno je napomenuti kako su to dvije temeljne aktivnosti sustava upravljanja rizicima. Sustav upravljanja rizicima kao i njegova učinkovitost tj. djelotvornost determinira korporativnu sigurnost budući da su rizici kao takvi temeljna prijetnja korporativnoj sigurnosti.

Sustav upravljanja rizicima prikazan je na slici 4.

Slika 4: Sustav upravljanja rizicima



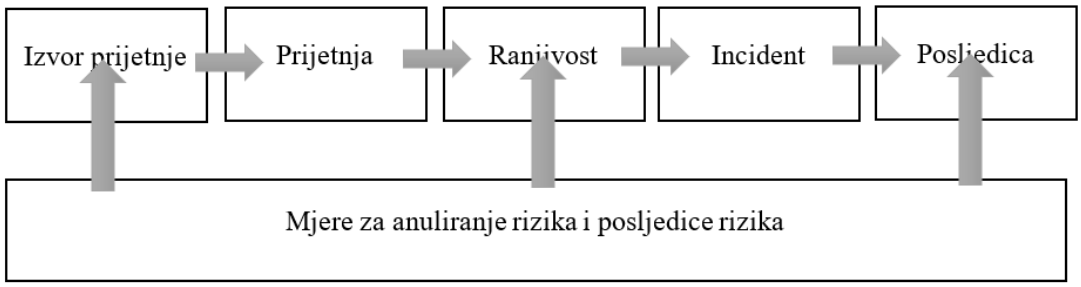
Izvor: Buntak, K., Kovačić, M. 2020. Upravljanje kvalitetom 1. Sveučilište Sjever. Koprivnica

Sustav upravljanja rizikom podrazumijeva stvaranje konteksta organizacije, a koji podrazumijeva analizu internog i eksternog okruženja organizacije kako bi se identificirali svi rizici koji se mogu pojaviti u takvom okruženju. Nakon stvaranja organizacijskog konteksta neophodno je analizirati sve identificirane rizike kako bi se analizirala potencijalna prijetnja koju svaki od definiranih rizika ima za organizaciju. Nakon analize, odnosno nakon evaluacije svih identificiranih rizika neophodno je definirati mjere za anuliranje rizika kao i mjere za anuliranje posljedica rizika. Mjere mogu biti definirane u ovisnosti o tome radi li se o rizicima koji predstavljaju veliku opasnost za prekid kontinuiteta poslovanja organizacije ili se radi o rizicima koji su rutinski rizici i s kojima se organizacija svakodnevno susreće. Potrebno je naglasiti kako organizacija treba voditi računa o adekvatnoj komunikaciji sa svim zainteresiranim stranama kao i što treba pratiti definirane mjere za smanjenje rizika. Ako se ispostavi da mjere koje organizacija

definira nisu adekvatne, neophodno je definirati nove mjere koje će u znatno bolje pokrivati tj. anulirati rizik i posljedice rizika (Buntak & Kovačić, 2020).

Kad se govori o rizicima, a što je posebice važno za razumijevanje sigurnosti i zaštite, neophodno je opisati i način na koji rizici nastaju. Slika 5 prikazuje nastanak rizika u organizaciji.

Slika 5: Nastanak rizika



Izvor: Buntak, K., Kovačić, M. 2020. Upravljanje kvalitetom 1. Sveučilište Sjever. Koprivnica

Kao što je to prikazano na slici 5, rizik nastaje pojavom izvora prijetnje. Drugim riječima, ako u organizaciji ne postoji izvor koji bi bio prijetnja za kontinuitet poslovanja organizacije kao i za normalno odvijanje procesa u organizaciji, rizik se neće pojaviti i obratno. Izvor prijetnje može biti različit i može biti determiniran temeljnom djelatnosti organizacije.

Nadalje, pojavom izvora prijetnje javlja se i sama prijetnja. Prijetnja može biti usmjerena prema nastanku ozljede na radu kao i izbijanja požara, odnosno zagađenja okoliša što je determinirano mjestom na kojem se javlja prijetnja. Ako se pojavi prijetnja, organizacija je ranjiva budući da prijetnje za organizaciju znače slabost sustava, a što može rezultirati štetom za organizaciju, odnosno pojavom rizika (Buntak & Kovačić, 2020).

Kroz ranjivost organizacije postoji vjerojatnost nastanka incidenta. Incident kao takav za organizaciju znači i posljedice koje mogu biti determinirane vrstom incidenta kao i njegovim utjecajem na organizacijski sustav. Što je incident veći, odnosno što je po svojoj snazi veći to je i posljedica koju organizacija može očekivati veća.

Kako bi organizacija smanjila mogućnost nastanka izvora prijetnji kao i same ranjivosti, odnosno posljedica, treba definirati mjere temeljem kojih će utjecati ne samo na izvor prijetnje nego i na same posljedice incidenta, odnosno mjere temeljem kojih će smanjiti ranjivost sustava.

Drugim riječima, ako se govori o korporativnoj sigurnosti, odnosno sigurnosti na radu, rizik povezan uz radno mjesto može biti ozljeda na radu zbog izvora prijetnje koji može biti stroj koji

nema adekvatnu zaštitu, odnosno zaposlenik koji nema adekvatnu edukaciju ili adekvatnu opremu koja bi ga mogla zaštititi od izvora prijetnje. Sukladno tome, zaposlenik postaje ranjiv i postoji vjerojatnost da će se dogoditi incident koji može značiti ozljedu na radu, odnosno štetu za zaposlenika ali i organizaciju u cjelini.

Neki rizici koji mogu značajno utjecati na organizaciju mogu narušiti kontinuitet poslovanja organizacije zbog čega je neophodno da organizacija definira mjere za osiguranje kontinuiteta poslovanja ako dođe do pojave takvih rizika, odnosno posljedica rizika.

3.3 Kontinuitet poslovanja i sigurnost i zaštita

Kontinuitet poslovanja organizacije od presudne je važnosti zbog zadovoljstva zainteresiranih strana s jedne strane ali i s druge strane nastavka odvijanja organizacijskih procesa nakon što se u organizaciji dogodio incident. Rizici koji su po svojoj učestalosti veći, odnosno rizici čije su posljedice za organizaciju veće mogu u značajnoj mjeri ugroziti kontinuitet poslovanja organizacije zbog čega je neophodno definirati mjere koje će omogućiti nastavak poslovanja organizacije nakon nastanka incidenta (Buntak, et al., 2019).

Temelj za definiranje mjera tj. postupaka za nastavak poslovanja organizacije je identifikacija rizika kao i sustav upravljanja rizicima. Nakon što organizacija analizira rizike sukladno opisu danom u poglavlju 3.2., neophodno je definirati mjere koje će biti usmjerene prema stvaranju postupaka, odnosno alokaciji svih resursa koji su neophodni za nastavak poslovanja. Takvi postupci se aktiviraju nakon što dođe do ostvarenja pojedinog rizika, odnosno nakon što organizacija postane podložna posljedicama rizika.

Postupci za osiguranje kontinuiteta poslovanja mogu biti usmjereni prema aktiviranju žurnih službi koje će doći na mjesto poprišta događanja, mogu biti usmjereni prema alokaciji djelatnosti na druga mjesta kako bi se proces nastavio odvijati bez prekida ili većih varijabilnosti, itd.

Osiguranje kontinuiteta poslovanja od posebne je važnosti za organizaciju s aspekta korporativne sigurnosti budući da je usmjereno prema održivosti poslovanja organizacije, odnosno prema sprječavanju prekida poslovanja u slučajevima kada razina rizika postane takva da je vrlo vjerojatno da će rizik moći prekinuti poslovanje organizacije.

Stvaranjem postupaka za oporavak, odnosno za nastavak poslovanja u znatnoj se mjeri može utjecati i na smanjenje troškova koji mogu nastati zbog prekida poslovanja kao i što takvi postupci mogu utjecati na dugoročni poslovni rezultat.

3.4 Sigurnost i zaštita i troškovi

Jedan od aspekata koji treba naglasiti kad je u pitanju sigurnost i zaštita su troškovi. Troškovi su posebno značajna stavka kad je riječ o pojavi rizika koji su povezani uz ugrožavanje kontinuiteta poslovanja kao i kad je riječ o troškovima bolovanja, odnosno ozljeda na radu.

Istraživanje koje je provedeno 2014. godine na razini EU (Europske Unije) pokazalo je kako se na godišnjoj razini na području EU dogodi ukupno 3.2 milijuna nesreća na radu. Kad je riječ o nesrećama na radu koje kao posljedicu imaju fatalni ishod, istraživanjem je identificirano kako je tijekom 2014. godine na području EU bilo ukupno 3.739 fatalnih nesreća na radu (Bađun, 2017). Ovakve brojke ukazuju na visoke troškove s kojima se susreću organizacije na teritoriju EU budući da je neophodno sve ozljede kao i sve zaposlenike adekvatno zbrinuti, odnosno dati im adekvatnu liječničku pomoć kao i osigurati adekvatnu skrb.

Međutim, kad je riječ o ostalim troškovima kao i ostalim kategorijama korporativne sigurnosti i troškovima koji mogu nastati zbog nedovoljno dobrog organizacijskog sustava korporativne sigurnosti treba spomenuti i primjer iz prakse u kojem je jedna zrakoplovna kompanija zbog nedovoljno definiranog sustava zaštite izgubila gotovo 12 milijuna američkih dolara nakon što su u javnost dospjela imena i prezimena kao i svi drugi osobni podatci korisnika koji su koristili usluge aviokompanije (Secude, 2020). Nadalje, kad je riječ o troškovima s kojima se susreću organizacije zbog nedovoljno dobro oblikovanog sustava zaštite okoliša treba spomenuti kako postoji niz primjera iz prakse u kojima je zbog ispuštanja štetnih plinova u okolinu došlo do fatalnih ishoda za neposredne stanovnike koji se nalaze u blizini tvornice koja je ispuštala takve tvari. Isto tako, treba napomenuti kako su posebno izraženi troškovi povezani uz curenje nafte, odnosno puknuće naftovoda u kojima je organizacija, koja polaže prava na eksploataciju, bila dužna sanirati nastalu štetu.

S obzirom na opisano, neophodno je osigurati adekvatan sustav korporativne sigurnosti koji će omogućiti pravovremeno aktiviranje postupaka koji su usmjereni prema umanjenju štete koja je nastala nakon ozljeda na radu, odnosno postupaka koji su usmjereni prema preventivi nastanka pojedinih rizika budući da su troškovi preventive znatno manji u odnosu na troškove provođenja korektivnih radnji.

4. Sustav upravljanja sigurnosti

Sustav upravljanja u organizaciji okvir je koji definira politike s kojima se mora osigurati sukladnost prilikom svih aktivnosti tj. operacija koje se odvijaju u organizacijskom sustavu (Britvić, 2011). Drugim riječima, sustav upravljanja definira postupke, odnosno pravila temeljem kojih se u organizaciji odvijaju poslovni procesi ali i determinira ponašanje organizacijskih zaposlenika kroz oblikovanje organizacijske kulture. Naime, organizacijska kultura oblikuje se na temelju postupaka od kojih se sastoji sustav upravljanja, odnosno oblikuje se na temelju zahtjeva koji se postavljaju na sustav kao takav.

Kad je riječ o sustavu upravljanja sigurnosti potrebno je naglasiti kako on kao takav eksplicitno ne postoji već se kreira na temelju uvođenja različitih sustava upravljanja kao što su to sustav upravljanja okolišem, sustav upravljanja zdravljem i sigurnosti zaposlenika, itd. Isto tako, sustav upravljanja u organizaciji, osim kroz norme, može biti oblikovan i kroz zahtjeve pozitivnih zakonskih propisa koje Zakonodavac definira i postavlja na današnje organizacije.

Tablica prikazuje popis sustava upravljanja koji determiniraju sustav upravljanja sigurnosti u organizaciji. Potrebno je naglasiti kako svaki od navedenih i opisanih sustava upravljanja kao jedan od zahtjeva definira osiguranje sukladnosti s pozitivnim zakonskim propisima. Naime, osiguranje sukladnosti s takvim zahtjevima ujedno je i osnova za certificiranje sustava upravljanja pomoću normi koje su opisane u poglavlju 4.2.

Tablica 4: Popis sustava upravljanja

Sustav upravljanja	Kratki opis
Sustav upravljanja okolišem	Sustav upravljanja okolišem definira način na koji će organizacija oblikovati svoje postupke usmjerene prema smanjenju negativnog utjecaja na okoliš. Ovaj sustav upravljanja definira zahtjeve usmjerene prema pravilnom zbrinjavanju otpada kao i sve aktivnosti povezane uz smanjenje ispuštanja štetnih plinova, otpadnih voda, itd. u okolinu u kojoj organizacija egzistira. Ako se ovaj sustav upravljanja sagledava kroz trokut održivosti on direktno korelira ekološku komponentu održivosti.

Sustav upravljanja informacijskom sigurnosti	Informacijska sigurnost sastavni je dio korporativne sigurnosti i od posebne je važnosti za osiguranje kontinuiteta poslovanja. Zbog sve većih zahtjeva povezanih uz poslovanje u virtualnom okruženju kao i zbog sve većih rizika povezanih uz mogućnost ugrožavanja sigurnosti informacija, sustav upravljanja informacijskom sigurnosti predmetom je proučavanja i usavršavanja ISO organizacije, a kako bi se stvorila osnova za sve organizacije vezana uz stvaranje sigurnog okruženja za poslovanje i odvijanje procesa.
Sustav upravljanja sigurnosti i zdravljem zaposlenika	Ovaj sustav upravljanja direktno je povezan uz zaštitu na radu kao i preventivu pojave profesionalnih bolesti koje mogu nastati nakon dugotrajnog izlaganja zaposlenika repetitivnim pokretima, odnosno nedovoljno sigurne radne okoline. Isto tako, ovaj sustav upravljanja na organizaciju postavlja zahtjeve s aspekta stalne edukacije zaposlenika kao i imenovanja povjerenika koji će biti zadužen za poslove zaštite na radu.
Sustav upravljanja protiv mita i korupcije	Ovaj sustav upravljanja sprečava sklapanje štetnih ugovora koji bi mogli narušiti organizacijsku profitabilnost, odnosno njezinu dugoročnu održivost. Ovaj sustav upravljanja potiče jednakost svih zaposlenika kao i jednake mogućnosti za napredovanje. U uskoj je sprezi sa zakonodavstvom koje je kreirano kako bi se spriječile koruptivne i druge radnje, a koje bi kao posljedicu mogle imati neravnopravne odnose između tržišnih dionika kao i neravnopravnost s aspekta mogućnosti napredovanja za sve zaposlenike u organizaciji.
Sustav upravljanja rizikom	Rizik kao takav osnova je za upravljanje sigurnosti u organizaciji. Ovaj sustav upravljanja definira načine na koje organizacija može upravljati rizicima kao i identificirati ih kako bi na vrijeme definirala mjere temeljem kojih će u budućnosti spriječiti pojavu novih rizika, odnosno temeljem kojih će smanjiti posljedice rizika ako se oni ostvare.

Sustav upravljanja kontinuitetom poslovanja	Sustav upravljanja kontinuitetom poslovanja definira način na koji će organizacija osigurati temelj za ostvarenje kontinuiteta odvijanja poslovnih i drugih procesa ako dođe do ostvarenja rizika zbog kojeg bi takav kontinuitet mogao biti prekinut. S aspekta korporativne sigurnosti, ovaj sustav upravljanja definira mjere za oporavak kao i postupke koji se aktiviraju ako dođe do pojave neželjenog događaja u organizaciji.
Sustav upravljanja biološkim rizikom u laboratorijima	Definira niz zahtjeva koje biološki laboratoriji moraju zadovoljiti kako bi mogli poslovati, odnosno kako bi se u njima mogle obavljati aktivnosti vezane uz njihovu temeljnu djelatnost. Implementacija ovakvog sustava upravljanja od posebne je važnosti za sve organizacije koje se bave zdravstvom, odnosno za organizacije koje su u neposrednom kontaktu s biološkim opasnostima.
Sustav upravljanja za privatne sigurnosne operacije	Ovaj sustav upravljanja karakterističan je za sve organizacije koje se bave tj. koje su specijalizirane i čija je temeljna djelatnost pružanje privatne, odnosno tehničke zaštite. Definira niz zahtjeva koji su usmjereni prema poboljšanju postojećih procesa unutar takvih organizacija kao i podizanje kvalitete pružene usluge.
Sustav upravljanja sigurnosti u lancu opskrbe	Ostvarenje sigurnog lanca opskrbe imperativ je za sve organizacije budući da prekidi u lancu opskrbe kao takvi mogu značiti i prekide u kontinuitetu poslovanja organizacije, odnosno prekide u normalnom funkcioniranju organizacije.
Sustav upravljanja sigurnosti hrane	Definira zahtjeve koji se odnose na organizacije koje se bave posluživanjem hrane, odnosno koje se bave preradom hrane. Definira niz mjera, odnosno načina na koje će se smanjiti rizik povezan uz pripremu i posluživanje hrane.

Izvor: Tablica je rad autora

Potrebno je naglasiti kako svi sustavi upravljanja koji su opisani u tablici 4 su dobrovoljni sustavi upravljanja, odnsono organizacija ih implementira u svoje poslovanje na dobrovoljnoj

razini. U zakonskim propisima nije definirana obveza organizacije na implementaciju opisanih sustava upravljanja.

Nadalje, potrebno je naglasiti kako svi nabrojeni sustavi upravljanja mogu biti podijeljeni na sustave upravljanja koji direktno utječu na sigurnost organizacije ali i sustave upravljanja koji indirektno utječu na sigurnost. Sustavi upravljanja koji direktno koreliraju sigurnost organizacije u prvom redu su sustav upravljanja okolišem, sustav upravljanja zdravljem i sigurnosti zaposlenika, sustav upravljanja informacijskom sigurnosti, sustav upravljanja sigurnosti hrane, sustav upravljanja rizikom i sustav upravljanja usmjeren protiv mita i korupcije dok su svi ostali sustavi upravljanja indirektni sustavi upravljanja koji služe kao potpora korporativnoj sigurnosti.

Jednako kao i sustavi upravljanja, pozitivni zakonski propisi također mogu biti direktno i indirektno povezani uz sigurnost i zaštitu, odnsono korporativnu sigurnost. Zakonski propisi, direktni i indirektni, opisani su u poglavlju 4.1.

S obzirom na broj različitih sustava upravljanja kao i opseg svakog od sustava upravljanja nabrojenih u tablici 4, javlja se potreba za međusobnom integracijom, odnosno usklađivanjem svih sustava upravljanja čime se stvara integrirani sustav upravljanja. Budući da se govori o sigurnosti, svaki od sustava upravljanja treba, ako se govori o integraciji, biti uključen u integrirani sustav upravljanja tako da se uzimaju zahtjevi povezani uz rizik koji se susreće u procesu.

Osnova za integraciju sustava upravljanja opisanih u tablici 4 je sustav upravljanja kvalitetom, odnosno zahtjevi koji se postavljaju na menadžment s aspekta kvalitetnog upravljanja organizacijom. Karakteristike kvalitetno upravljane organizacije, a koje trebaju biti uzete u obzir prilikom integracije, su kompetentnost s aspekta tehničke, tehnološke, tehničke i strukturne kompetentnosti, odnosno kompetentnosti ljudskog potencijala, dokumentiranost tj. stvaranje dokumentacije vezane uz upravljanje i upravljivost koja se postiže kroz procesni pristup poslovanju (Buntak, et al., 2019).

Integrirani sustav upravljanja korporativnom sigurnosti razvija se prema fazama, odnosno razvija se sukladno području koje pokriva i može se sagledavati s aspekta zrelosti sustava upravljanja. Zrelost sustava upravljanja podrazumijeva priliku i potrebu za poboljšanjem koja se identificira na temelju mjerenja prilika, odnosno mjerenja trenutnih performansi koje razvijaju procesi organizacijskog sustava upravljanja.

4.1 Zakonska regulativa sigurnosti

Zakonska legislativa povezana uz sigurnost obvezujuća je za sve organizacije koje posluju na području države koja zakonsku legislativu definira. Kao takva, zakonska legislativa definira minimalne zahtjeve koje organizacija treba zadovoljiti kako bi mogla poslovati. Jednako kao i sustavi upravljanja, zakonska legislativa vezana uz sigurnost može biti direktna i indirektna. Direktna zakonska legislativa povezana je uz samu sigurnost u organizaciji, dok indirektna zakonska legislativa na neizravan način definira zahtjeve koje organizacija treba ispuniti kako bi se osigurala sigurnost.

Osim zakonskih propisa postoji i niz pod zakonskih akata kao i niz različitih pravilnika koji također definiraju pojam sigurnosti kao i zahtjeva koji se postavljaju na organizaciju s aspekta sigurnosti. Tablica 5 prikazuje neke od direktnih zakonskih propisa i neke od indirektnih zakonskih propisa koji utječu na oblikovanje sigurnosti u organizaciji.

Tablica 5: Direktni i indirektni zakonski propisi

Direktni zakonski propisi	Indirektni zakonski propisi
Zakon o radu NN 93/14, 127/17, 98/19	Zakon o osiguranju NN 30/15, 112/18, 63/20
Zakon o zaštiti okoliša NN 80/13, 153/13, 78/15, 12/18, 118/18	Zakon o obveznim odnosima NN 35/05, 41/08, 125/11, 78/15, 29/18
Zakon o zaštiti na radu NN 71/14, 118/14, 154/14 , 94/18, 96/18	Zakon o elektroničkom novcu NN 64/18
Opća uredba o zaštiti podataka	Zakon o tajnosti podataka NN 79/07, 86/12
Zakon o informacijskoj sigurnosti NN 79/07	
Zakon o autorskim i srodnim pravima NN 167/03, 79/07, 80/11, 125/11, 141/13, 127/14, 62/17, 96/18	
Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga NN 64/18	

Izvor: Tablica je rad autora

Potrebno je naglasiti kako su zakonski propisi navedeni u tablici 5 samo nekih od najvažnijih zakonskih propisa koji na direktan ili indirektan način oblikuju sigurnost organizacije ali i sigurnost poslovanja, odnosno sigurnost dionika koji su uključeni u poslovanje organizacije.

Kao što je vidljivo, zakonski propisi ne pokrivaju sva područja kojima se bavi korporativna sigurnost, odnosno koje korporativna sigurnost pokriva. Sukladno tome može se reći da postoji nedovoljan broj pozitivnih zakonskih propisa koji bi prisiljavali današnje organizacije na osiguranje minimalnih zahtjeva.

4.2. Norme iz područja sigurnosti

Pozitivni zakonski propisi koji su navedeni u poglavlju 4.1. obvezujući su za sve organizacije dok su norme navedene u ovom poglavlju dobrovoljne za implementaciju i organizacije same odlučuju hoće li implementirati, odnosno certificirati svoj sustav upravljanja pomoću neke od normi ili ne. Jednako kao i zakonski propisi, norme iz područja sigurnosti mogu se podijeliti na direktne norme koje postavljaju izravne zahtjeve povezane uz sigurnost i norme koje su indirektne, a što podrazumijeva neizravno definiranje zahtjeva kojima će organizacija utjecati na povećanje sigurnosti poslovanja. U tablici 6 dan je prikaz normi iz područja sigurnosti.

Tablica 6: Direktne i indirektne norme sustava upravljanja

Direktne norme	Indirektne norme
ISO EN 31000:2018 – norma koja oblikuje upravljanje rizikom	ISO EN 9001:2015 – norma koja oblikuje sustav upravljanja kvalitetom
ISO EN 14001:2015 – norma koja oblikuje sustav zaštite okoliša	ISO EN 5001:2018 – norma koja oblikuje sustav upravljanja energijom
ISO EN 45001:2018 – norma koja oblikuje sustav upravljanja sigurnosti i zdravljem zaposlenika	ISO 30301:2018 – norma koja oblikuje sustav upravljanja zapisima i dokumentiranje informacija u organizaciji
ISO EN 27001:2020 – norma koja oblikuje sustav upravljanja informacijskom sigurnosti	ISO EN 39001:2012 – norma koja oblikuje sustav upravljanja sigurnosti u prometu
ISO EN 22000: 2018 – norma koja oblikuje sustav upravljanja sigurnosti hrane	ISO EN 37001: 2016 – norma koja oblikuje sustav upravljanja protiv mita i korupcije

ISO EN 22301:2018 – norma koja oblikuje sustav upravljanja kontinuitetom poslovanja	ISO EN 19011:2018 – norma koja oblikuje auditiranja sustava upravljanja u organizaciji
ISO EN 28001:2007 – norma koja oblikuje sustav upravljanja sigurnosti u lancu opskrbe	
ISO EN 18788:2015 – norma koja oblikuje sustav upravljanja poslovima privatne zaštite	

Izvor: Tablica je rad autora

Norme koje su prikazane i navedene u tablici 6 koriste se za certificiranje sustava upravljanja koji su opisani u poglavlju 4. Nadalje, iz tablice 6 je vidljivo kako postoji znatno veći broj normi iz područja sigurnosti u odnosu na zakonske propise. S obzirom na to, može se reći da norme kao takve organizaciji osiguravaju dodanu vrijednost u usporedbi s pozitivnim zakonskim propisima s kojima organizacija mora osigurati sljedivost, a koji pokrivaju znatno uže područje u odnosu na norme prikazane u tablici 6.

5. Komparativna analiza normi i zakona iz područja sigurnosti

Temeljni cilj komparativne analize normi i zakona iz područja sigurnosti identificirati je razliku između zahtjeva koje na organizacijski sustav postavlja norma, odnosno zahtjeva koje organizacije mora ispuniti kako bi mogla poslovati na području države koja definira i donosi zakone. S obzirom na raznolikost normi i zakonskih propisa kao i drugačiju formu stvaranja normi, odnosno zakonskih propisa, definirani su zajednički parametri koji će poslužiti kao osnova za usporedbu. Zajednički parametri prikazani su u tablici zajedno s opisima svakog od parametra.

Tablica 7: Parametri komparacije

Parametar usporedbe	Opis parametra
Temeljni cilj	Opisuje svrhu zbog koje je Zakon, odnosno norma nastala jednako kao i njezinu upotrebu.
Pregled pojmova i definicija	Pregled pojmova i definicija od posebne je važnosti budući da determinira terminologiju koja će se koristiti kako u dokumentu tako i u praksi. Pogrešno definirana terminologija može kao posljedicu imati nedovoljno dobro razumijevanje zahtjeva navedenih u dokumentu.
Načela upravljanja	Definiranje načela upravljanja determinira izgled budućih odluka koje će donositi menadžment u organizaciji. Odsustvo načela upravljanja ujedno znači i opasnost da odluke koje donosi menadžment budu nedorečene, odnosno da nisu u sukladnosti s temeljnim ciljem koji je naglašen u normi ili Zakonu.
Odnos s okolinom	Svaka organizacija egzistira u tri osnovne okoline u kojoj se nalaze zainteresirane strane, a koje na organizaciju postavljaju zahtjeve. S obzirom na to, definiranje potrebe analize okoline kao i definiranje dionika iz okoline na koje organizacija treba obratiti pozornost od posebne je važnosti za učinkovito i djelotvorno funkcioniranje sustava upravljanja.
Odgovornosti i ovlaštenja	Ovaj parametar odnosi se na analizu postoji li eksplicitno definirana odgovornost, odnosno eksplicitno definirano ovlaštenje koje se odnosi na radno mjesto ili osobu u organizaciji.

Edukacija i kompetentnost	Permanentno usavršavanje organizacijskih zaposlenika od posebne je važnosti kako bi organizacija mogla zadovoljiti sve zahtjeve koji se vežu uz promjene koje se događaju u organizacijskim okolinama kao i sve zahtjeve povezane uz najnovija dostignuća i otkrića, a koja su vezana uz sustav upravljanja.
Dokumentacija	Parametar usporedbe koji se odnosi na potrebnu dokumentaciju koju organizacija mora imati kako bi osigurala minimalne zakonske uvijete, odnosno kako bi dokazala sukladnost sa zahtjevima koji su definirani u normi.
Utjecaj na okoliš	Specifični parametar koji se primjenjuje samo kod komparacije Zakona o zaštiti okoliša i norme ISO EN 14001:2015, a koji opisuje način na koji se regulira smanjenje negativnog utjecaja na okoliš.
Preventivne mjere	Parametar koji uspoređuje postoje li preventivne mjere koje su obvezujuće za implementaciju u procese, a što ujedno na dugi rok može determinirati i učinkovitost sustava upravljanja kao i smanjenje negativnih posljedica rizika.
Analiza uspješnosti mjera	Parametar koji identificira postoji li zahtjev povezan uz analizu učinkovitosti implementiranih mjera, a što može biti osnova za identifikaciju mjesta na kojima je moguće provesti poboljšanja.
Inspekcijski nadzor	Parametar usporedbe koji je karakterističan za Zakon i koji se ne susreće u normama osim u obliku zahtjeva povezanog za certifikaciju i recertifikaciju sustava upravljanja.

Izvor: Tablica je rad autora

Potrebno je naglasiti kako su se prilikom komparacije u obzir uzele norme koje direktno utječu na sigurnost i zaštitu jednako kao i zakonski propisi koji direktno koreliraju zahtjeve povezane uz osiguranje minimalnih zahtjeva vezanih uz sigurnost i zaštitu.

Nadalje, prilikom usporedbe identificirano je kako postoji nedovoljan broj zakonskih propisa koji bi pratili sva područja koja prate norme, odnosno koji bi obuhvatili jednaka područja koja obuhvaćaju norme koje definira ISO organizacija. Isto tako, tijekom istraživanja identificirano je kako postoji zakonska legislativa koja je zastarjela i koja ne prati novonastale promjene vezane uz tehnološka i druga dostignuća.

5.1. Komparativna analiza područja zaštite okoliša

Prilikom komparativne analize Zakona iz područja zaštite okoliša kao direktni zakon koji determinira zahtjeve povezane uz smanjenje negativnog utjecaja organizacije na okoliš uzet je Zakon o zaštiti okoliša. Posljednja nadopuna Zakona o zaštiti okoliša provedena je 2019. godine, a prilikom analize istoimenog zakona identificirano je kako postoji naglasak na održivosti, odnosno održivom rastu i razvoju.

S druge strane, kao jedna od normi koja je uzeta kao druga varijabla usporedbe je ISO EN 14001:2015. Riječ je o zadnjoj reviziji norme koja je sastavni dio obitelji normi razreda 14. Norme razreda 14 sastoje se od niza drugih normi koje nadopunjuju temeljne zahtjeve navedene u normi ISO 14001:2015.

Potrebno je naglasiti kako je Zakon o zaštiti okoliša obvezujući zakon za sve organizacije koje posluju na području Republike Hrvatske i svaka organizacija mora osigurati sukladnost sa zahtjevima koje definira Zakon. S druge strane, implementacija, odnosno certifikacija sustava upravljanja okolišem dobrovoljna je za svaku organizaciju i menadžment organizacije može ako to smatra potrebni certificirati sustav upravljanja okolišem.

Kao parametri usporedbe uzete su varijable koje su navedene u tablici 7. Potrebno je naglasiti kako Zakon o zaštiti okoliša unutar sebe definira niz zahtjeva povezanih uz inspekcijski nadzor kao i prekršajne odredbe dok norma to ne definira.

Rezultati komparativne analize Zakona o zaštiti okoliša i norme ISO EN 14001:2015 prikazani su u tablici 8. Kao što je to vidljivo iz tablice, postoje parametri usporedbe koje su primjenjive samo u normi jednako kao i što postoje parametri usporedbe koji su karakteristični samo za sustav upravljanja okolišem prema normi ISO EN 14001:2015.

Na temelju usporedbe može se zaključiti kako je Zakon o zaštiti okoliša sveobuhvatan zakon koji na cjelovit način oblikuje odnos organizacije prema zaštiti okoliša kao i što naglašava potrebu analize utjecaja na okoliš koji organizacija ima. Isto tako, u Zakonu su jasno definirana načela koja organizacija mora upotrebljavati prilikom smanjenja, odnosno upravljanja zaštitom okoliša. Međutim, potrebno je naglasiti kako Zakon kao takav eksplicitno ne definira potrebu certifikacije, kao i evaluacije postojećeg sustava kako bi se identificirala mjesta za poboljšanje što je kod norme ISO EN 14001:2015 naglašeno.

Tablica 8: Komparativna analiza Zakona o zaštiti okoliša i norme ISO EN 14001:2015

Parametar usporedbe	ISO 14001:2015	Zakon o zaštiti okoliša	Napomene
Temeljni cilj	Poboljšanje performansi sustava upravljanja okolišem, osiguranje sukladnosti s pozitivnim zakonskim propisima, osiguranje zadovoljenja ciljeva zaštite okoliša	Zaštita zdravlja, zaštita biljaka, zaštita okoliša, ostvarivanje održivosti, unaprjeđenje stanja čovjekova okoliša i zdravlja čovjeka	Norma ne naglašava koncept održivost
Pregled pojmova i definicija	Daje pregled svih pojmova i definicija koji se spominju u normi s detaljnim pojašnjenjem	Daje pregled svih pojmova i definicija koji se susreću u Zakonu s pojašnjenjem	Norma i zakon ne razlikuju se po ovoj točci usporedbe
Načela upravljanja okolišem	Eksplicitno ne definira načela već se poziva na norme koje se nalaze unutar obitelji normi, a koje determiniraju upravljanje okolišem	Definira načela: održivog razvoja, predostrožnosti, zamjene, sanacije štete, očuvanja dobara, cjelovitog pristupa, suradnje, poticaja, itd.	Norma za razliku od Zakona ne definira načela upravljanja već se poziva na druge norme u kojima je detaljno pojašnjeno svako od načela. S druge strane, zakon kao takav definira načela bez njihove nadopune drugim propisima ili aktima.

Odnos s okolinom organizacije	Definira zahtjev povezan uz izradu organizacijskog konteksta, što podrazumijeva analizu svih zainteresiranih strana i njihovih zahtjeva.	Definira dionike koji su uključeni u zaštitu okoliša poput Hrvatskog sabora, Vlade, gradova i županija, pojedinaca, pravnih i fizičkih osoba	Norma na drugačiji način oblikuje identifikaciju zahtjeva iz organizacijske okoline za razliku od Zakona koji točno definira koji su dionici uključeni u proces zaštite okoliša.
Odgovornosti i ovlaštenja	Norma zahtjeva da se organizacijski menadžment opredijeli za upravljanje zaštitom okoliša kao i što zahtjeva definiranje osoblja koje će biti zaduženo za provedbu aktivnosti, odnosno politika.	Zakon definira ovlaštenike koji su zaduženi za provedbu aktivnosti vezanih uz zaštitu okoliša.	Norma jasno postavlja zahtjeve koji su povezani uz opredjeljenje cjelokupne organizacije prema definiranju mjera za zaštitu okoliša dok s druge strane Zakon definira ovlaštenja pojedinaca ali ne traži eksplicitno da se organizacijski menadžment opredijeli za upravljanje okolišem.

Edukacija i kompetentnost	Norma definira kompetentnost kao jedno od bitnih načela upravljanja i zahtjeva od organizacije da osigura kompetentne zaposlenike koji će moći obavljati definirane aktivnosti	Zakon definira potrebu obrazovanja zaposlenika, odnosno povjerenika koji će biti zadužen za provedbu pojedinih mjera tj. aktivnosti vezanih uz zaštitu okoliša	Norma od organizacije zahtjeva kompetentnost čitavog organizacijskog sustava dok Zakon definira potrebu obrazovanja pojedinaca koji će biti uključeni u proces zaštite okoliša. S obzirom na to, norma je po svojim zahtjevima znatno obuhvatnija u odnosu na Zakon.
Dokumentacija	Norma eksplicitno ne definira koje dokumente organizacija treba imati već naglašava da svi dokumenti, odnosno svi planovi koje organizacija izrađuje trebaju biti u sukladnosti sa zahtjevima koji su definirani u normi.	Zakon točno definira koje dokumente, odnosno koje planove organizacija mora imati kako bi osigurala sljedivost sa zakonskim propisima koji se navode u Zakonu.	Zakon jasnije definira dokumente vezane uz zaštitu okoliša međutim ne naglašava da svi ostali dokumenti trebaju unutar sebe sadržavati načela zaštite okoliša. Drugim riječima, može se dogoditi dupliciranje pojedinih dokumenata u kojima se, umjesto da su ti zahtjevi već uvršteni u pojedine dokumente.

Utjecaj na okoliš	Norma eksplicitno ne definira potrebu izrade dokumentacije vezane uz štetan utjecaj na okoliš već definira kako planovi i ostale aktivnosti u organizaciji trebaju biti oblikovane tako da ne djeluju štetno na okoliš.	Zakon definira zahtjeve povezane uz izradu studije utjecaja na okoliš kao i definiranja mjera koje će biti usmjerene prema smanjenju negativnog utjecaja organizacije na okoliš.	Zakon eksplicitno definira zahtjeve za izradom studije utjecaja na okoliš dok norma to ne definira. Međutim, unatoč eksplicitnom ne navođenju i Zakon i norma se ne razlikuju po pristupu.
Preventivne mjere	Norma naglašava važnost identifikacije rizika i definiranja mjera koje će biti usmjerene prema smanjenju negativnog utjecaja na okoliš. Dakle, norma definira pristup utemeljen na rizicima.	Zakon definira nužnost analize i definiranja načina na koji će se spriječiti eventualne nesreće koje bi rezultirale značajnijim zagađenjem.	Norma u svakom svojem zahtjevu koji postavlja na organizaciju jasno definira rizik kao sastavnicu koju organizacija treba uzeti u obzir prilikom oblikovanja svojih aktivnosti dok zakon ne navodi eksplicitno potrebu tj. pristup utemeljen na rizicima.
Analiza uspješnosti mjera	Norma jasno definira zahtjeve koji su usmjereni prema analizi trenutnih performansi sustava	Zakon definira područja koja organizacija treba pratiti, a vezana su uz zaštitu okoliša, odnosno definiranje utjecaja	Zakon i norma jasno definiraju potrebu praćenja performansi, odnosno utjecaja na okoliš s tom razlikom da norma

	upravljanja okolišem i definira potrebu poboljšanja učinkovitosti, odnosno djelotvornosti.	koji organizacija ima na okoliš.	eksplicitno traži pristup utemeljen na stalnom poboljšanju za razliku od Zakona.
Inspekcijski nadzor	Norma ne definira potrebu inspekcijskog nadzora osim potrebe za certifikacijom i recertifikacijom.	Zakon jasno definira inspekcijski nadzor kao i što definira sankcije za sve organizacije za koje se ispostavi da nisu sukladne s definiranim zahtjevima.	Zakon definira jasne sankcije dok norma kao takva ne definira kaznene odredbe vezane uz lošije performanse sustava upravljanja okolišem.

Izvor: Tablica je rad autora

Komparativnom analizom Zakona o zaštiti okoliša i norme ISO EN 14001:2015 identificirano je kako postoje minorne razlike. Međutim, unatoč malim razlikama potrebno je naglasiti kako se organizacijama preporučuje certifikacija sustava upravljanja okolišem normom ISO EN 14001:2015 zbog činjenice kako ona organizaciji osigurava stvaranje dodane vrijednosti i može rezultirati sinergijom. Nadalje, potrebno je naglasiti kako norma prisiljava organizaciju na osiguranje sukladnosti sa zahtjevima Zakona o zaštiti okoliša kao i sve druge legislative iz područja zaštite okoliša zbog čega se može pojaviti spomenuta sinergija.

5.2. Komparativna analiza područja sigurnosti na radu

Komparativna analiza područja zaštite na radu obuhvaća usporedbu Zakona o zaštiti na radu i norme ISO EN 45001:2018. Posljednja revizija Zakona o zaštiti na radu provedena je 2018. godine dok je posljednja revizija norme provedena 2018. godine. S obzirom na istu godinu revizije i nadopune za očekivati je kako će usporedba dati slične, odnosno iste rezultate i kako su oba dokumenta usklađena s posljednjim dostignućima vezanim uz zaštitu na radu.

Jednako kao i što je to bio slučaj kod Zakona o zaštiti okoliša, Zakon o zaštiti na radu obvezujući je zakon za sve organizacije koje posluju unutar gospodarstva Republike Hrvatske. Poseban značaj ovog zakona leži u činjenici kako on determinira minimalne uvjete koje organizacijski zaposlenici moraju ispuniti kako bi mogli obavljati definirane zadatke za pojedino radno mjesto. Nadalje, zakon je povezan s nizom drugih pod zakonskih akata u kojima se definiraju profesionalne bolesti kao i zahtjevi koji se postavljaju na higijensko tehničku zaštitu koju zaposlenici moraju imati na radnom mjestu.

Implementacija i certifikacija sustava upravljanja zdravljem i sigurnosti zaposlenika dobrovoljna je za svaku organizaciju i zahtjeva osiguranje sukladnosti sa svim pozitivnim zakonskim propisima koje definira država unutar čijeg gospodarstva posluje organizacija. Isto tako, implementacija i certifikacija sustava upravljanja zdravljem i sigurnosti zaposlenika organizaciji osigurava dodanu vrijednost kao i što osigurava stvaranje radnog okruženja u kojem zaposlenici imaju znatno manji rizik od nastanka ozljeda, a čime organizacija na dugi rok može smanjiti troškove vezane uz bolovanja i ozljede na radu.

Komparativna analiza Zakona o zaštiti na radu i norme ISO EN 45001:2018 prikazana je u tablici 9.

Tablica 9: Komparativna analiza Zakona o zaštiti a radu i norme ISO EN 45001:2018

Parametar usporedbe	ISO 45001:2018	Zakon o zaštiti na radu	Napomene
Temeljni cilj	Norma jasno definira opseg kao i područje primjene. Norma eksplicitno definira osnovni cilj implementacije sustava upravljanja zdravljem i sigurnosti zaposlenika.	Zakon definira koji je temeljni cilj primjene ovog zakona. Isto tako, Zakon se poziva na Europske norme i propise.	Po ovom parametru usporedbe Zakon i norma se ne razlikuju
Pregled pojmova i definicija	Norma jasno definira sve pojmove i definicije koje će se koristiti u tijelu norme. Svaki pojam, odnosno svaka definicija jasno je i nedvosmisleno pojašnjena.	Zakon jasno i nedvosmisleno opisuje sve pojmove i definicije koje se susreću u tijelu zakona.	Po ovom parametru usporedbe Zakon i norma se ne razlikuju
Načela upravljanja	Norma definira načela upravljanja sustavom osiguranja zaštite zdravlja i sigurnosti zaposlenika kao i što se poziva.	Zakon definira načela prevencije ozljeda na radu koje se temelje na identifikaciji rizika povezanih uz rad, odnosno obavljanje aktivnosti na radnom mjestu.	Po ovom parametru usporedbe Zakon i norma se ne razlikuju

Odnos s okolinom organizacije	Norma jasno definira potrebu izrade organizacijskog konteksta kao i definiranje svih zahtjeva koje zainteresirane strane koje se nalaze u organizacijskim okolinama postavljaju na organizaciju kao i njezin sustav upravljanja zdravljem i sigurnosti zaposlenika.	Zakon ne definira potrebu analize okoline u potrazi za identifikacijom zahtjeva zainteresiranih strana.	Norma u ovoj točci usporedbe znatno šire sagledava zahtjeve koje zainteresirane strane postavljaju na organizaciju kao i što znatno jasnije definira važnost usklađivanja sustava upravljanja sa zahtjevima zainteresiranih strana.
Odgovornosti i ovlaštenja	Norma jasno definira ovlaštenja kao i potrebu organizacijskog menadžmenta da osigura opredijeljenost prema osiguranju sigurne radne okoline, odnosno sukladnosti sa zahtjevima koje norma postavlja na organizacijski sustav upravljanja.	Zakon jasno definira odgovornosti i ovlaštenja u organizaciji, a vezano uz zaštitu na radu.	Po ovom parametru usporedbe Zakon i norma se ne razlikuju

Edukacija i kompetentnost	Norma kao jedan od temeljnih zahtjeva definira potrebu osiguranja kompetentnosti organizacijskih zaposlenika kao i kompetentnost organizacije u cjelini.	Zakon jasno definira potrebu obrazovanja zaposlenika u organizaciji prije no što započnu s obavljanjem zadataka na radnom mjestu koje im je dodijeljeno.	Po ovom parametru usporedbe Zakon i norma se ne razlikuju
Dokumentacija	Norma jasno definira potrebu dokumentiranja, odnosno stvaranja zapisa kao i svih drugih dokumenata temeljem kojih će organizacija moći dokazati osiguranje sljedivosti sa zahtjevima koje postavlja norma.	Zakon definira potrebu dokumentiranja tj. izrade planova i popratne dokumentacije.	Zakon znatno jasnije definira koju dokumentaciju organizacija mora posjedovati, a vezano uz zaštitu na radu u odnosu na Normu koja nalaže potrebu dokumentiranja ali ne definira točnu dokumentaciju koju organizacija treba posjedovati.
Zaštita na radu	Norma ne definira eksplicitno koje mjere organizacija treba poduzeti kako bi smanjila rizik povezan uz ozljede na radu već definira potrebu za	Zakon definira potrebu da svi zaposlenici nose radnu odjeću tj. obuću kako bi bili zaštićeni prilikom obavljanja definiranih zadataka na njihovom radnom mjestu. Isto tako Zakon jasno	Zakon znatno preciznije definira mjere vezane uz zaštitu na radu u odnosu na normu.

	procjenom rizika kao i poduzimanjem svih radnji koje su neophodne kako bi se spriječile moguće ozljede zaposlenika.	definira koji su zahtjevi koje svaki zaposlenik mora ispuniti, a kako bi sigurno obavljao definirane zadatke.	
Preventivne mjere	Norma definira pristup temeljen na rizicima kao i pristup u kojem organizacija treba definirati mjere temeljem kojih će smanjiti mogućnost nastanka ozljede.	Zakon definira potrebu definiranja preventivnih mjera koje će biti usmjerene prema smanjenju rizika povezanih uz poslove koje zaposlenici obavljaju na radnom mjestu.	Po ovom parametru usporedbe Zakon i norma se ne razlikuju
Analiza uspješnosti mjera	Norma jasno definira potrebu vezanu uz evaluaciju trenutnih performansi sustava i analiziranju prilika za poboljšanje	Zakon definira potrebu implementacije mjera temeljem kojih će se rizici povezani uz sigurnost i zdravlje zaposlenika smanjiti.	Po ovom parametru usporedbe Zakon i norma se ne razlikuju
Inspekcijski nadzor	Norma ne definira potrebu inspekcijskog nadzora.	Zakon jasno definira inspekcijski nadzor.	Po ovom parametru, Zakon jasno definira sankcije kao i potrebu za inspekcijskim nadzorom u odnosu na normu koja to ne definira.

Izvor: Tablica je rad autora

Kao što je to vidljivo iz tablice 8, ne postoji značajna razlika između Zakona o zaštiti na radu i norme ISO EN 45001:2018 kao što je to definirano na početku poglavlja. Budući da je Zakon o zaštiti na radu obvezujući za sve organizacije, unutar zakona jasno je definiran inspekcijski nadzor kao i što su definirane prekršajne odredbe. Međutim, parametri usporedbe koji govore o poboljšanju i preventivnim mjerama kao i zaduženjima unutar organizacije, odnosno provođenju edukacije koja će biti usmjerena prema povećanju kompetentnosti organizacijskih zaposlenika koji obavljaju poslove, su jednaki. S obzirom na to, proces oblikovan Zakonom o zaštiti na radu i normom ISO EN 45001:2018 je gotovo identičan. Potrebno je naglasiti kako norma ISO EN 45001:2018 ne predviđa inspekcijski nadzor osim certifikacijskog i recertifikacijskog audita dok s druge strane Zakon to predviđa ali ne definira potrebu certificiranja već isključivo osiguranja sukladnosti i mogućnosti inspekcijske provjere sukladnosti.

5.3. Komparacija područja informacijske sigurnosti

Za komparaciju normativnih dokumenata iz područja informacijske sigurnosti korišten je Zakon o informacijskoj sigurnosti i norma ISO 27001:2020. Zakon o informacijskoj sigurnosti donijet je 2007. godine nakon čega nije bio revidiran i nisu definirana nikakva poboljšanja. S obzirom na napredak tehnologije i napredak na području razvoja informacijske sigurnosti za očekivati je kako će se Zakon o informacijskoj sigurnosti znatno razlikovati u odnosu na normu budući da je norma revidirana 2020. godine.

S obzirom na starost Zakona o zaštiti informacija i njegove isključive namjene za organizacije koje posluju u sklopu javne uprave, normativni okviri koje definira država kao sustav na području informacijske sigurnosti nisu dovoljno razvijeni. To kao posljedicu može imati nedovoljno artikuliranu potrebu organizacija da osiguraju informacije koje se nalaze spremljene tj. dokumentirane u organizaciji.

Međutim, unatoč zastarjelosti zakonske legislative kroz Uredbu o zaštiti osobnih podataka napravljen je značajan pomak prema osuvremenjivanju informacijske sigurnosti. Područje informacijske sigurnosti organizacija u privatnom sektoru prepušteno je menadžmentu takvih organizacija budući da ne postoji sustavno rješenje definirano od strane države.

Tablica 10: Komparacija Zakona o sigurnosti informacija i norme ISO 27001:2020

Parametar usporedbe	ISO 27001:2020	Zakon o informacijskoj sigurnosti	Napomene
Temeljni cilj	Jasno definira temeljni cilj norme kao i što jasno definira područje primjene norme u organizacijama.	Nema eksplicitne definicije temeljnog cilja norme već definira isključivo na što se zakon odnosi.	Norma je po svojem obuhvatu znatno veća i znatno detaljnije navodi temeljni cilj zahtjeva koji su navedeni u normi za razliku od Zakona koji to ne definira.
Pregled pojmova i definicija	Norma jasno definira terminologiju koja se koristi i navodi kroz zahtjeve koji su definirani u normi. Svi termini su jasno i nedvosmisleno objašnjeni.	Zakon definira sve pojmove i definicije koje se koriste u zahtjevima koji se postavljaju na organizacije.	Nema razlike.
Načela upravljanja	Norma jasno definira načela koja se upotrebljavaju za upravljanje informacijskom sigurnosti. Osim toga, poziva se i na druge norme koje se nalaze u sklopu obitelji norme.	Zakon ne definira načela.	Norma po svojem obuhvatu znatno detaljnije opisuje načela kao i što upućuje na druge norme unutar obitelji norme, a koje su povezane uz načela upravljanja.

Odnos s okolinom organizacije	Definira potrebu izrade organizacijskog konteksta kao i identifikaciju svih zahtjeva koje zainteresirane strane iz okoline imaju, a vezane su uz sigurnost informacija u organizaciji, odnosno neovlašteno korištenje istih.	Zakon ne definira eksplicitno odnos s okolinom.	Norma je u ovom parametru usporedbe znatno detaljnije opisala zahtjeve koje postavlja na sustav upravljanja informacijskom sigurnosti u odnosu na Zakon koji taj segment nema dovoljno razvijen.
Odgovornosti i ovlaštenja	Norma jasno definira kako menadžment organizacije mora dokazati sljedivost sa zahtjevima postavljenim u normi kao i što mora dokazati opredjeljenje prema upravljanju informacijskom sigurnosti.	Zakon eksplicitno ne definira odgovornosti i ovlaštenja već navodi tijela zadužena za provedbu Zakona.	Zakon po ovom parametru usporedbe ima znatno uže gledište u odnosu na normu.
Edukacija i kompetentnost	Norma jasno definira potrebu stalnog školovanja, odnosno edukacije svih zaposlenika kao i potrebu	Zakon ne definira potrebu za edukacijom i kompetentnosti.	Vidljiva je stanovita razlika između zahtjeva koje na organizaciju postavlja zakon i

	osiguranja kompetentnosti svih zaposlenika kao i samog sustava kako bi se osigurala optimalna razina sigurnosti informacija.		zahtjeva koje na organizaciju postavlja norma.
Dokumentacija	Norma jasno definira zahtjeve povezane uz dokumentiranje informacija kao i stvaranje zapisa.	Zakon ne definira potrebu izrade dokumentacije.	Po ovom parametru usporedbe norma je po svojem obuhvatu znatno opsežnija, odnosno znatno detaljnije opisuje potrebu za dokumentiranjem informacija.
Preventivne mjere	Norma jasno definira mjere, odnosno potrebu za stvaranjem mjera koje će biti usmjerene prema smanjenju rizika povezanog uz dokumentirane informacije, odnosno informacije koje se nalaze spremljene u bazama podataka koje se nalaze u vlasništvu organizacije.	Zakon ne definira mjere.	U Zakonu nije razvidna potreba da organizacija kao takva definira mjere koje će biti usmjerene prema smanjenju rizika vezanog uz sigurnost informacija.

Analiza uspješnosti mjera	Norma definira potrebu evaluacije definiranih i implementiranih mjera kao i analizu prilika za poboljšanje kako bi se poboljšale performanse sustava upravljanja informacijskom sigurnosti.	Zakon definira potrebu praćenja ali i ne potrebu poboljšanja mjera.	Norma i u ovoj točki znatno detaljnije opisuje zahtjev povezan uz identifikaciju mjera za poboljšanje, odnosno analizu trenutnih performansi sustava kako bi se identificirala mjesta za poboljšanje.
Inspekcijski nadzor	Norma ne definira potrebu za inspekcijskim nadzorom osim prilikom certifikacije i recertifikacije sustava upravljanja informacijskom sigurnosti.	Zakon ne definira eksplicitnu potrebu provedbe inspekcijskog nadzora nad sigurnosti informacija.	U ovom parametru usporedbe norma i Zakon se ne razlikuju.

Izvor: Tablica je rad autora

Kao što je to vidljivo iz tablice 10, postoji stanovita razlika između zahtjeva koje na sustav upravljanja informacijskom sigurnosti postavlja norma i zahtjeva koje definira Zakon o sigurnosti informacija. Potrebno je naglasiti kako Zakon definira isključivo sigurnost informacija vezanu uz državne institucije.

5.4 Ostali normativni dokumenti

Kad se govori o ostalim normativnim dokumentima, identificirano je kako država kao sustav ne definira sva područja sigurnosti, odnsono dokumenata koji na izravan način determiniraju sigurnost. Međutim, postoji niz zakonskih propisa koji neizravno definiraju i oblikuju sustav sigurnosti u organizacijama. S obzirom na to, javlja se izazov povezan uz uspostavu sustava upravljanja sigurnosti u organizaciji ako se organizacija isključivo vodi zakonskim propisima.

Nadalje, jedno od područja koje je zakonski nedorečeno je područje upravljanja kvalitetom budući da ne postoji direktan zakonski okvir koji bi definirao zahtjeve povezane uz kvalitetno upravljanje organizacijom. S druge strane, postoji niz indirektnih zahtjeva koji od menadžmenta zahtijevaju, kao posljedicu oblikovanja planova i odluka, kvalitetan proizvod s aspekta osiguranja minimalnih sigurnosnih uvjeta koje proizvodi koji se stavljaju na tržište moraju ispuniti.

Svaka organizacija koja nastoji stvoriti integrirani sustav upravljanja sigurnosti mora implementirati sustave upravljanja budući da je zakonska legislativa kao takva nedovoljno definirana, odnosno artikulirana.

U osnovi, kad se govori o temeljnoj razlici između zakonskih propisa i zahtjeva koje norma postavlja na organizaciju, treba naglasiti kako je temeljna razlika u obvezujućim zahtjevima koje definira zakon kao i u prekršajnim odredbama koje su definirane u zakonu za sve organizacije koje ne osiguraju sukladnost sa zahtjevima definiranim u zakonu. Međutim, zakonska legislativa kao takva ne definira izgled procesa sustava upravljanja već na njega postavlja samo zahtjeve. S druge strane, norme definiraju i oblikuju procese unutar sustava upravljanja jednako kao i što artikuliraju način njihova odvijanja.

Tijekom komparativne analize identificirano je kako norme postavljaju znatno veće zahtjeve koji su u prvom redu usmjereni prema analizi zahtjeva zainteresiranih strana kao i potrebe stalnog poboljšanja procesa koji se odvijaju u sustavu upravljanja. Nadalje, norme definiraju potrebu permanentne edukacije i naglašavaju kompetentnost kao jedno od načela koje organizacija mora osigurati kako bi mogla certificirati sustav upravljanja nekom od ISO normi.

Zaključno, implementacijom normi sustava upravljanja organizacija može stvoriti temelj za osiguranje sinergije. Budući da zakonska legislativa definira minimalne zahtjeve koji moraju biti ispunjeni kako bi organizacija mogla poslovati, a norma definira preporuke kako poboljšati sustav, odnosno kako ga dodatno učiniti učinkovitijim. Međutim, potrebno je naglasiti kako zahtjevi koje definira norma mogu također biti promatrani kao minimalni zahtjevi koje organizacija mora ispuniti kako bi osigurala certifikat sustava upravljanja. Organizacija može na postavljene zahtjeve definirati dodatne zahtjeve koje uobičajeno oblikuje sam menadžment organizacije, a koji su usmjereni prema uvođenju dodatnih mehanizama, odnosno mjera za dodatno povećanje učinkovitosti i djelotvornosti sustava upravljanja.

Najvažnija razlika između normi i zakonske legislative odnosi se na naglašavanje stalnog poboljšanja procesa po PDCA (Plan – do – check - act) načelu što označava da svaki novi procesni ciklus procesa koji se odvija unutar sustava upravljanja treba biti učinkovitiji od prethodnog procesnog ciklusa što zakon ne definira. To sa sobom povlači niz postupaka koje organizacija treba provoditi. Isto tako, potreba za analizom performansi kao i potreba za analizom zadovoljstva i zahtjeva zainteresiranih strana, odnosno identifikacija prilika za poboljšanje temeljna je karakteristika normi sustava upravljanja koja se ne susreće u zakonskim propisima.

Dakle, zahtjevi koje definira norma obvezuju organizaciju na drugačiji pristup dizajnu procesa kao i drugačiji pristup sagledavanju potrebe za poboljšanjem.

6. Proces upravljanja sustavom sigurnosti i zaštite

Procesni pristup jedan je od temelja za kvalitetno upravljanje organizacijom. Jedan od temeljnih razloga za to je činjenica kako implementacija procesnog pristupa, odnosno poslovnih procesa kao takvih omogućuje organizaciji jednostavnije praćenje transformacije koja se odvija u procesu kao i sam način na koji se dodaje vrijednost sirovinama i materijalima koji se nalaze u samoj transformaciji. Kao takvi, poslovni procesi mogu se definirati kao niz međusobno povezanih radnji tj. aktivnosti koje transformiraju ulazne resurse u izlazne proizvode i usluge pomoću mehanizama, a na temelju pravila i kontrola (Buntak, et al., 2020).

Kad se govori o procesnom pristupu poslovanju, neophodno je napomenuti kako je za uspješno upravljanje poslovnim procesima temelj identificirati zahtjeve zainteresiranih strana. Na temelju zahtjeva zainteresiranih strana, a koji u kontekstu upravljanja sigurnosti i zaštitom u organizaciji mogu biti povezani uz osiguranje sigurnih radnih uvjeta za zaposlenike, smanjenje negativnog utjecaja koji bi organizacija mogla imati na okoliš, itd., organizacijski menadžment definira tj. oblikuje transformaciju koja se odvija u procesu.

Svaki poslovni proces odvija se na temelju PDCA načela što podrazumijeva i pristup stalnom poboljšanju. Drugim riječima, u upravljanju poslovnim procesima, PDCA podrazumijeva:

- Faza planiranja: u fazi planiranja alociraju se resursi koji su neophodni za odvijanje procesa kao i što se definiraju ciljevi koji će se nastojati ispuniti kroz transformaciju u procesu. Nakon završetka planiranja, započinje se s operacionalizacijom plana,
- Faza provedbe: operacionalizacija plana započinje u drugoj fazi PDCA, a što podrazumijeva samu transformaciju resursa koji se nalaze u procesu. Prilikom transformacije neophodno je pratiti performanse na definiranim mjestima tj. kontrolnim točkama u procesu
- Faza kontrole: praćenje performansi odvija se u trećoj fazi PDCA i to pomoću praćenja procesa, odnosno KPI pokazatelja. Neki od parametara koje organizacija može pratiti prilikom odvijanja procesa u učinkovitost procesa, djelotvornost procesa, stabilnost procesa, itd.,
- Faza poboljšanja: u fazi poboljšanja, odnosno fazi djelovanja, organizacija na temelju identificiranih tj. izmjerenih performansi definira mjesta u procesu na kojima je

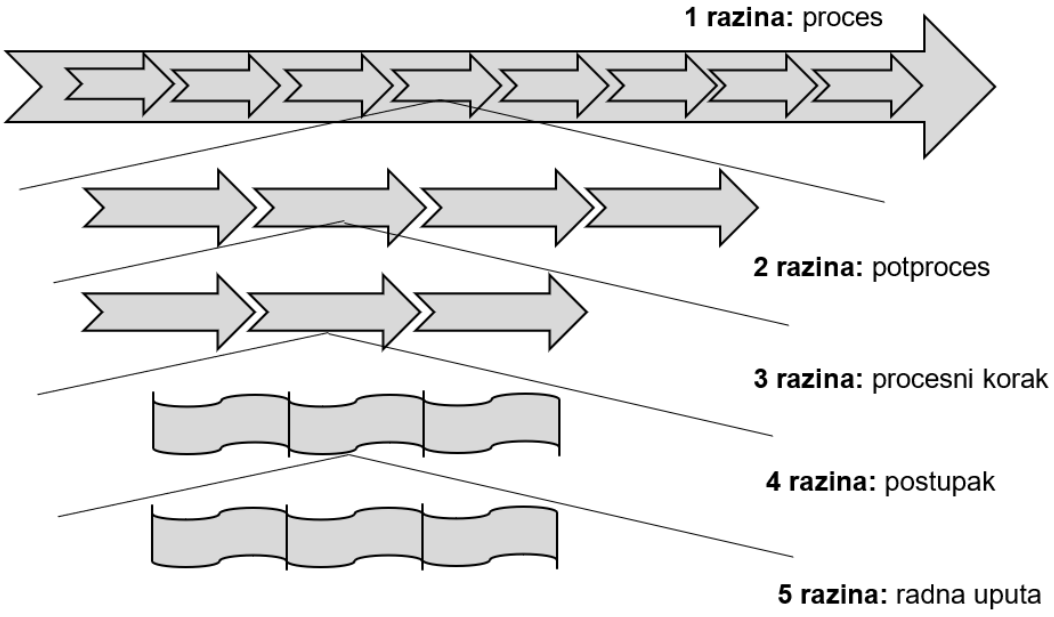
moguće poboljšati proces, a što će direktno utjecati na njegove performanse u novom ciklusu odvijanja procesa (Buntak, et al., 2020).

Svaki poslovni proces može se dekomponirati do razine radnog mjesta. Potrebno je naglasiti kako se kroz dekompoziciju procesa može identificirati međusobni odnos između svakog od potprocesa što može biti osnova za promatranje rizika, odnosno za praćenje rizika kroz proces. Primjerice, rizik u jednom od potprocesa može se proširiti na ostale potprocese.

Međutim, najvažnije, dekompozicijom poslovnih procesa organizacija može sagledavati koja su sve radna mjesta potrebna za obavljanje različitih zadataka, odnosno aktivnosti jednako kao i što može definirati potrebne kompetencije bez kojih zaposlenici ne bi mogli na siguran način obavljati definirane zadatke.

Ovakav pristup kreiranju radnog mjesta omogućuje definiranje svih potrebnih znanja i vještina kao i sve potrebne opreme tj. rizika s kojima se susreće zaposlenik na radnom mjestu, a koji mogu značiti pojavu rizika u ostalim potprocesima. Drugim riječima, rizik na jednom radnom mjestu može se proširiti, odnosno kao posljedicu može imati štetu na ostalim radnim mjestima. Dekompozicija poslovnog procesa prikazana je na slici.

Slika 6: Dekompozicija poslovnog procesa



Izvor: Buntak, K., Kovačić, M., Premužić, B. 2020. Upravljanje poslovnim procesima. Sveučilište Sjever.

Kad se govori o poslovnim procesima i njihovoj važnosti, potrebno je naglasiti da se kroz dekompoziciju procesa osim definiranja radnog mjesta, mogu definirati i radne upute u kojima će biti jasno definiran način na koji će zaposlenik obavljati definirane aktivnosti. Drugim riječima, u radnim uputama mogu biti definirane smjernice za rad na siguran način kao i način na koji će zaposlenik upotrebljavati sredstva za rad na radnom mjestu.

Osim toga, kroz postupke može se jasno definirati što će se poduzeti ako dođe do pojave neželjenog događaja u organizaciji, a što može biti usmjereno i prema postupcima koji će biti aktivirani kako bi se osigurao kontinuitet poslovanja organizacije.

Važnost procesnog pristupa u osiguranju sigurne radne okoline, odnosno u upravljanju sigurnosti i zaštitom u organizaciji odnosi se na mogućnost mjerenja i točno definiranog načina na koji će se obavljati pojedine aktivnosti ako dođe do pojave neželjenog događaja.

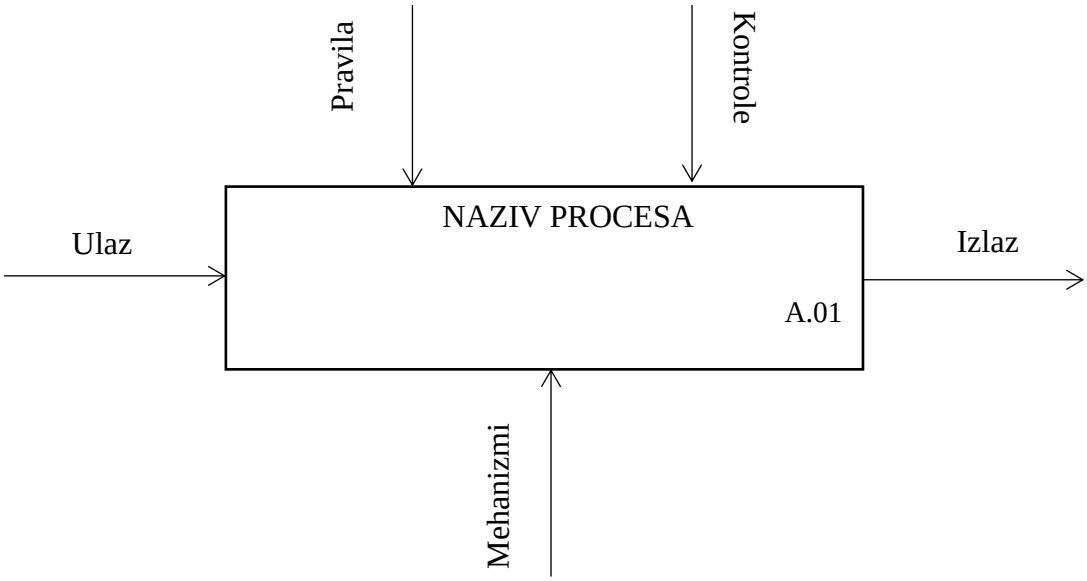
Kad se govori o definiranju i oblikovanju postupaka i radnih uputa, neophodno je napomenuti kako se u radne upute za rad na siguran način ne treba uvrštavati isključivo uputa vezana uz zaštitu na radu već i upute koje su usmjerene prema zaštiti okoliša, zaštiti od požara, zaštiti od neželjenog pristupa informacijama, itd. S druge strane, postupci ne moraju isključivo biti usmjereni prema osiguranju sigurne radne okoline s aspekta zaštite na radu već mogu biti usmjereni i prema prethodno spomenutim područjima sigurnosti i zaštite u organizaciji.

Prilikom izgradnje procesa sustava upravljanja sigurnosti i zaštitom organizacija treba uzeti u obzir pozitivne zakonske propise kao i zahtjeve koje norme sustava upravljanja postaju na organizacijski sustav. S obzirom na to, može se reći da ne postoji jedinstveni način izgradnje sustava upravljanja sigurnosti i zaštitom kao ni jedinstveni način modeliranja procesa unutar spomenutog sustava. Razlog za to je u prvom redu činjenica kako različite organizacije imaju različiti broj, odnosno vrstu sustava upravljanja kao i činjenica da različiti društveni sustavi imaju različito zakonodavstvo koje postavlja različite zahtjeve vezane uz sigurnost i zaštitu.

S obzirom na različitost zahtjeva koji se postavljaju na modeliranje procesa sigurnosti i zaštite, organizacijama na raspolaganju postoji veći broj unificiranih alata za modeliranje procesa, a jedan od njih je i IDEFO metoda. Temeljni razlog za primjenu IDEFO metode leži u činjenici kako ona dekomponira proces sukladno dekompoziciji koja je prikazana na slici 6. Isto tako, metoda definira potrebu opisivanja svih mehanizama koji će se koristiti za osiguranje željenog izlaza iz procesa, odnosno definira sva pravila koja se mogu odnositi na pozitivne zakonske propise kao i zahtjeve normi. Osim toga, IDEFO definira sve kontrole koje su neophodne za kontrolu procesa čime se

ostvaruje pregled svih elemenata procesa koji su od posebne važnosti za stalno poboljšanje procesa sukladno PDCA (Buntak, et al., 2020). Blok shema IDEFO metode prikazana je na slici 7.

Slika 7: IDEFO metoda



Izvor: Buntak, K., Kovačić, M., Premužić, B. 2020. Upravljanje poslovnim procesima. Sveučilište Sjever.

Na slici 7, elementi IDEFO odnose se na:

- Ulazi: odnose se na sve ulazne resurse koji su neophodni za transformaciju koja se odvija u procesu. U najvećem broju slučajeva odnosi se na preporuke za poboljšanje i zahtjeve zainteresiranih strana koje organizacija nastoji ispuniti u procesu kroz transformaciju,
- Pravila: odnose se na sve pozitivne zakonske propise koje se odnose na organizaciju, odnosno koje definira zakonodavac. Isto tako, pravila se odnose i na zahtjeve koje norme sustava upravljanja postavljaju na organizaciju,
- Kontrole: definiraju način na koji će se kontrolirati transformacija u procesu. Mogu se razlikovati u ovisnosti o vrsti transformacije koja se odvija u procesu kao i što mogu biti determinirani ciljevima koji su navedeni u organizacijskim planovima,
- Mehanizmi: odnose se na sve resurse koji se trebaju upotrebljavati kako bi se transformacija u procesu mogla normalno odvijati. Drugim riječima, mehanizmi se odnose na zaposlenike, sredstva za rad, infrastrukturu, itd.

- Izlazi: podrazumijevaju rezultat transformacije koja se odvija u procesu. Izlazi iz procesa mogu biti proizvodi ili usluge, odnosno mogu biti poluproizvodi ili dokumenti koji će se upotrebljavati u drugim procesnim koracima tj. potprocesima (Buntak, et al., 2020).

Za upravljanje poslovnim procesima kao i za upravljanje procesima sustava osiguranja sigurnosti i zaštite, neophodno je identificirati sve rizike kao i što je neophodno sagledavati informacije koje osigurava povratna veza u procesu. Povratna veza osigurava sve informacije koje su od posebne važnosti za analizu mjesta u procesu na kojima se mogu provesti poboljšanja dok rizici definiraju potrebu za stvaranjem mjera temeljem kojih će se smanjiti ili temeljem kojih će se smanjiti posljedica nastalog rizika.

6.1. Evaluacija performansi procesa

S obzirom da je jedan od zahtjeva koji se postavlja na svaki sustav upravljanja povezan uz sigurnost i zaštitu stalno poboljšanje procesa, a stalno poboljšanje procesa treba se temeljiti na evaluaciji trenutnih performansi procesa, neophodno je analizirati trenutne performanse koje proces ima, odnosno analizirati njegovu učinkovitost i djelotvornost (Buer, et al., 2018).

Isto tako, ako se u procesu identificira nesukladnost, odnosno ako se identificira da proces ne ispunjava ciljeve koji su definirani u planovima, potrebno je provesti analizu odstupanja kako bi se identificirao mogući uzrok zbog kojeg je do odstupanja došlo. Potreba analiziranja uzroka odstupanja, odnosno uzroka nesukladnosti od posebne je važnosti budući da odstupanje od plana u kontekstu sigurnosti i zaštite za organizaciju može značiti opasnost, odnosno pojavu novih rizika koji će kao posljedicu imati nova područja koja mogu ugroziti sigurnost i zaštitu.

Kad se govori o evaluaciji procesa sigurnosti i zaštite, neophodno je spomenuti indikatore koje organizacija može upotrebljavati prilikom analize performansi. Neki od indikatora prikazani su u tablici 11. Kao što je to vidljivo iz tablice, indikatori se mogu odnositi na različita područja sigurnosti i zaštite, a što je u ovisnosti o normama koje organizacija ima implementirane kao i o pozitivnim zakonskim propisima koji su obvezujući za svaku organizaciju. Isto tako, indikatori koji su prikazani u tablici 11 nisu generički indikatori tj. različite organizacije mogu upotrebljavati različite indikatore u ovisnosti o planovima koje definira menadžment kao i o politikama koje menadžment upotrebljava prilikom upravljanja i donošenja odluka.

Tablica 11: Indikatori sigurnosti i zaštite

Indikator	Izraz
Broj ozljeda na radu u poslovnoj godini	$\frac{broj\ ozljeda\ na\ radu\ u\ godini\ dana}{broj\ zaposlenika}$
Vrijeme provedeno na bolovanju	$\frac{kumulativ\ vremena\ bolovanja}{broj\ zaposlenika}$
Trošak sigurnosti i zaštite po zaposleniku	$\frac{kumulativ\ uloženih\ sredstava}{broj\ zaposlenika}$
Troškovi tužbe zbog ozljede na radu	$\frac{broj\ tužbi\ zbog\ ozljede\ na\ radu}{broj\ ozljeda\ zaposlenika}$
Broj smrtnih slučajeva zbog ozljeda na radu	$\frac{broj\ smrtnih\ slučajeva}{broj\ ozljeda\ zaposlenika}$
Troškovi školovanja zaposlenika	$\frac{trošak\ školovanja}{broj\ zaposlenika}$
Udio troškova školovanja u ukupnim troškovima	$\frac{kumulativ\ troškova\ školovanja}{ukupni\ troškovi}$
Troškovi pojedinog elementa sigurnosti i zaštite	$\frac{trošak\ elementa}{ukupni\ troškovi\ sigurnosti\ i\ zaštite}$
Udio troškova sigurnosti i zaštite u ukupnim troškovima za kvalitetu	$\frac{ukupni\ troškovi\ sigurnosti\ i\ zaštite}{ukupni\ troškovi\ za\ kvalitetu}$
Broj neželjenih događaja u poslovnoj godini	$\frac{broj\ neželjenih\ događaja}{365}$

Izvor: Tablica je rad autora

Kao što je to vidljivo u tablici 11, evaluacija performansi sustava upravljanja sigurnosti i zaštitom može biti sagledavana nizom različitih indikatora. Svaki od indikatora može ukazati na

učinkovitost trenutnog dizajna procesa sustava upravljanja sigurnosti i zaštitom i može ukazati na potrebu poboljšanja sustava. U tablici 11, indikatori redom se odnose na:

- Broj ozljeda na radu u godini dana: ukazuje na učinkovitost mjera koje organizacija definira, a koje se odnose na zaštitu na radu, odnosno na korištenje higijensko tehničke zaštite kao i svih ostalih mjera temeljem kojih se može povećati sigurnost zaposlenika. Nepovoljan odnos ukazuje na potrebu poboljšanja postojećeg sustava,
- Vrijeme provedeno na bolovanju: može ukazati na potrebu poboljšanja ergonomije radnog mjesta, odnosno na povećano davanje organizacije zbog dugog vremena koje organizacijski zaposlenici provode na bolovanju. Nepovoljan odnos može ukazivati i na loše uvjete rada s aspekta sigurnosti i zaštite,
- Trošak sigurnosti i zaštite po zaposleniku: determinira troškove koje organizacija ima s aspekta osiguranja svih sredstava zaštite za svoje zaposlenike. Visoka davanja, a s druge strane i velik broj ozljeda na radu ili dugo vrijeme bolovanja može ukazati na potrebu promjene mjesta investiranja u povećanje sigurnosti,
- Broj smrtnih slučajeva: ukazuje na broj fatalnih ishoda neželjenog događaja u odnosu na broj ozljeda u godini dana. Može se iskazivati i s obzirom na broj zaposlenika. Što je broj smrtnih slučajeva veći to je učinkovitost sustava sigurnosti i zaštite manja i javlja se potreba za poboljšanjem
- Troškovi tužbe zbog ozljede na radu: ako zaposlenik smatra da su uvjeti na radnom mjestu takvi da je zbog njih nastala ozljeda na radu, zaposlenik može ustati s optužnim prijedlogom protiv organizacije. Velik broj tužba zbog ozljeda na radu ukazuje na potrebu poboljšanja. Ovaj se indikator može sagledavati i po radnom mjestu. Drugim riječima, može se izračunavati za svaku grupu radnih mjesta čime se može procijeniti potreba za poboljšanjem sigurnosti rada na pojedinom radnom mjestu
- Troškovi školovanja zaposlenika: odnose se na financijske resurse koje organizacija izdvaja kako bi povećala kompetentnost organizacijskih zaposlenika s aspekta sigurnosti na radu. Visoki troškovi školovanja, a velik broj ozljeda na radu može ukazivati na nedovoljno učinkovit sustav školovanja, odnosno na potrebu redizajniranja postojećeg obrazovnog programa

- Udio troškova školovanja u ukupnim troškovima: opisuje koliki je postotak troškova koje organizacija ima s aspekta sigurnosti i zaštite i ukupnih troškova u organizaciji. Ovaj indikator može biti korišten prilikom budžetiranja, odnosno alociranja financijskih resursa na početku poslovne godine. Mali udio troškova školovanja, a visok broj ozljeda ukazuje na potrebu povećanja ulaganja u školovanje. S druge strane, visoki udio troškova školovanja, a velik broj ozljeda na radu ukazuje na potrebu redefiniranja načina školovanja,
- Troškovi pojedinog elementa sigurnosti i zaštite: prikazuju kolika su davanja organizacije s aspekta jednog od segmenata sigurnosti i zaštite. Ovaj indikator treba poslužiti organizaciji za analizu svih elemenata sigurnosti i zaštite i to tako da se, primjerice, u odnos stavlja trošak tehničke zaštite i ukupni trošak, trošak povezan uz informacijsku sigurnost i ukupni trošak, itd. Na ovaj način organizacija može identificirati postotak pojedinog troška u ukupnim troškovima. Nadalje, usporedbom pojedinog troška s ostalim indikatorima može se identificirati potreba za poboljšanjem pojedinog segmenta sigurnosti i zaštite u organizaciji.
- Udio troškova sigurnosti i zaštite u ukupnim troškovima kvalitete: davanja koja organizacija ima s aspekta povećanja sigurnosti mogu se klasificirati kao troškovi za kvalitetu. S obzirom na to, moguće je identificirati koliki je postotak troškova sigurnosti i zaštite u ukupnim troškovima kvalitete koje organizacija ima. Visok udio ovakvih troškova ukazuje na potrebu poboljšanja
- Broj neželjenih događaja u poslovnoj godini: indikator koji ukazuje na broj ozljeda na radu, broj proboja u informacijski sustav, itd. kroz poslovnu godinu. Potrebno je naglasiti da se svi pokazatelji moraju računati pojedinačno. Drugim riječima, pokazatelj za broj ozljeda na radu u poslovnoj godini mora se zasebno računati u odnosu na izračun broja požara koji su izbili u godini dana u organizaciji.

Osim indikatora koji su prikazani u tablici 11, organizacija može definirati niz drugih indikatora koji će biti u sukladnosti s potrebama koje organizacija ima. Primjerice, organizacija kao jedan od indikatora učinkovitosti sustava upravljanja sigurnosti i zaštitom može definirati i broj inspekcijskih nadzora u godini dana koji može ukazati da zaposlenici vrlo vjerojatno prijavljuju potrebu za inspekcijskim nadzorom, odnosno da je inspekcija prilikom obilaska organizacije u prošlosti identificirala kako je neophodno ponoviti inspekcijski nadzor u

budućnosti. Nadalje, potrebno je naglasiti kako se svi opisani indikatori mogu prikazivati u apsolutnim, odnosno relativnim brojevima što je u ovisnosti o potrebama organizacije.

Za evaluaciju sustava upravljanja sigurnosti i zaštitom organizacija može definirati i KPI pokazatelje koji neće u odnos stavljati dvije ili više varijabli već će bilježiti broj neželjenih događaja. Neki od KPI pokazatelja koje organizacija može upotrebljavati opisani su u tablici 12.

Tablica 12: KPI pokazatelji

KPI pokazatelj	Opis
Broj ozljeda na radnom mjestu	Identificira koliki je broj ozljeda nastao u promatranom razdoblju na pojedinom radnom mjestu.
Broj fatalnih ozljeda na radnom mjestu	Identificira koliki je broj fatalnih nesreća u odjelu ili funkciji u organizaciji ili na radnom mjestu.
Broj pokušaja penetracije informacijskog sustava	Definira broj pokušaja napada na informacijski sustav. Ovaj KPI može biti povezan uz broj uspjelih napada tj. neautoriziranih ulaza u informacijski sustav.
Broj bolovanja zaposlenika	Definira broj bolovanja koji svaki od zaposlenika ima u godini dana. Može se mjeriti danima ili satima.
Trošak preventive	Odnosi se na sve troškove koje organizacija ima, a povezani su uz davanja usmjerena prema preventivi mogućih ozljeda na radu.
Količina odloženog otpada	Definira količinu otpada koji organizacija odlaže u godini dana. Dugogodišnjom usporedbom može se identificirati trend i identificirani trend može se koristiti za analizu korelacije s definiranim poboljšanjima.

Izvor: Tablica je rad autora

Svi opisani KPI pokazatelji mogu se razlikovati u ovisnosti o organizacijskim potrebama jednako kao i što se mogu razlikovati u ovisnosti o sustavu upravljanja u kojem se sagledavaju. U tablici su navedeni samo neki od indikatora.

Potrebno je naglasiti kako se KPI pokazatelji definirani u tablici mogu koristiti i za integraciju sustava upravljanja sigurnosti i zaštitom. U tom slučaju KPI pokazatelji moraju biti usklađeni sa zahtjevima norme, odnosno pozitivne zakonske legislative.

6.2 Optimizacija i poboljšanje procesa

Indikatori opisani u tablici 12, odnosno tablici 11 osnova su za analizu učinkovitosti sustava upravljanja. Nakon evaluacije tj. analize postojećih performansi sustava upravljanja, na temelju dobivenih informacija neophodno je provesti optimizaciju i poboljšanje. Primjerice, ako se pomoću indikatora prikazanih u tablici 11 identificiralo kako postoji problem povezan uz visoka davanja za osiguranje sigurnosti i zdravlja zaposlenika ali se unatoč tome događaju nesreće na radu kao i što se povećava broj bolovanja u organizaciji, neophodno je provesti analizu i optimizaciju procesa. Optimizacija i poboljšanje procesa može biti usmjereno prema poboljšanju procesa sigurnosti i zaštite, odnosno poboljšanju nekog drugog procesa u organizaciji uz napomenu da proces mora u tom slučaju biti poboljšan u vidu povećanja sigurnosti i zaštite kako sustava tako i zaposlenika koji se nalaze u samom procesu.

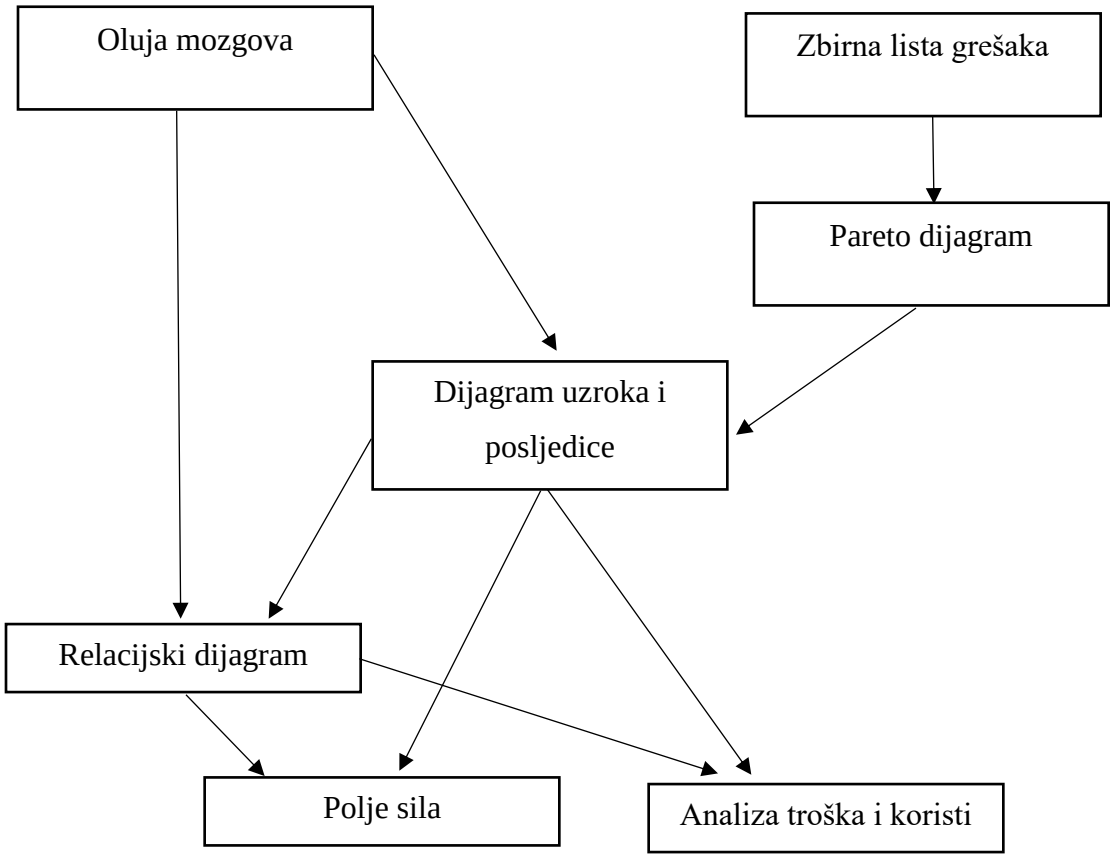
Ako se u organizacijskim procesima identificira nesukladnost, odnosno ako se identificira proboj u informacijski sustav ili dogodi ozljeda na radu, organizacija treba provesti analizu mogućih uzroka zbog kojeg je došlo do proboja ili ozljede na radu. Analiza mogućih uzroka može biti provedena pomoću upotrebe različitih alata i metoda, a kao što su to Pareto dijagram, dijagram uzroka i posljedice, zbirne liste grešaka, itd. Svi spomenuti alati mogu se klasificirati u osnovne alate za upravljanje kvalitetom i svi alati se mogu međusobno kombinirati. Drugim riječima, izlaz iz jednog alata može biti ulaz u drugi alat i samim time organizacija može doći do mogućeg uzroka nastanka problema. Isto tako, potrebno je naglasiti kako se preporučuje sve spomenute alate upotrebljavati u timu, odnosno definirati organizacijski tim koji će analizirati moguće uzroke nastanka problema (Buntak, et al., 2020).

Nakon što organizacijski tim identificira mogući uzrok nastanka problema neophodno je definirati mjere temeljem kojih će se provesti poboljšanje. Ovakav pristup osigurava, sukladno PDCA, stalan pristup poboljšanju. Osim što organizacijski tim može analizirati mogući uzrok nastanka problema nakon što se on pojavio, organizacijski tim može analizirati neke od indikatora koji su definirani u tablicama 11 i 12 i na temelju analize indikatora može definirati mjere usmjerene prema poboljšanju istih.

Kad se govori o mogućnosti kombiniranja alata za identifikaciju uzroka problema, slika prikazuje mogućnost kombiniranja različitih alata. Kao što je to vidljivo sa slike, prvi alat koji organizacija može koristiti prilikom analize uzroka problema je oluja mozgova kojom se identificiraju ideje svih zaposlenika koje su usmjerene prema mogućem uzroku problema. U oluju

mozgova može biti uključen i sam oštećeni ako se radi o ozljedi na radu. Osim oluje mozgova, prvi korak u analizi mogućeg uzroka nesukladnosti može biti i zbirna lista grešaka u kojoj je jasno definirano koje su najčešće greške ili uzroci greške u procesu. Nakon identificiranja ideja, odnosno mogućih uzroka problema kroz zbirnu listu grešaka, organizacijski tim može kroz Pareto dijagram analizirati vrlo vjerojatan uzrok problema koji može dodatno analizirati pomoću dijagrama uzroka i posljedice. Osim toga, druga putanja u primjeni alata može biti upotreba relacijskog dijagrama kako bi se identificirao mogući uzrok problema.

Slika 8: Mogući način korištenja alata



Izvor: Slika je rad autora

Potrebno je naglasiti kako se svako definirano rješenje preporučuje analizirati s aspekta troškova i koristi koje organizacija ima prilikom njegove implementacije. Drugim riječima, za implementaciju nekog rješenja organizacija mora izdvojiti određena financijska sredstva, a s obzirom na to svakako se preporučuje sagledati isplativost ulaganja financijskih resursa u predloženo rješenje. Za analizu isplativosti, organizacija može koristiti analizu troška i koristi tj.

tzv. cost-benefit analizu u kojoj sagledava sve troškove koje ima i sve koristi koje dobiva nakon što implementira rješenje. Kad se govori o troškovima i koristima, potrebno je napomenuti kako koristi mogu biti opipljive, u tom slučaju se govori o financijskim koristima, i neopipljive, u tom slučaju se govori o promjenama u organizacijskoj kulturi.

Osim analize troška i koristi, organizacija može koristiti i analizu polja sila u kojoj sagledava sve silnice koje podupiru predloženo rješenje i sve silnice koje se predloženom rješenju odupiru. Ponderiranjem, organizacijski tim dolazi do spoznaje o prihvatljivosti predloženog rješenja.

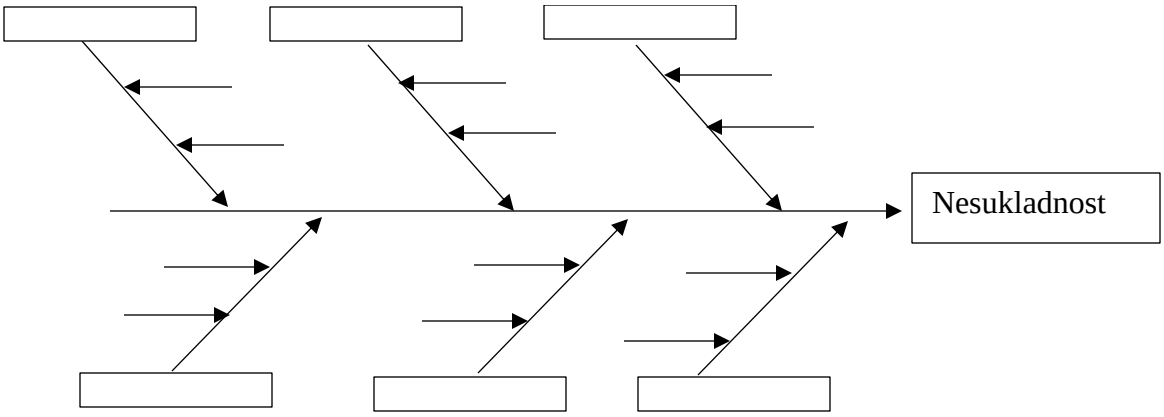
Osim kroz primjenu alata i metoda za analizu uzroka problema, organizacija proces može poboljšati kroz njegovo mapiranje, odnsono mapiranje svih rizika koji se povezuju uz pojedino radno mjesto. U tom slučaju, sagledava se svako radno mjesto za sebe, dokumentiraju se svi rizici koji su identificirani na svakom radnom mjestu i sukladno tome definiraju se mjere koje su usmjerene prema smanjenju rizika ili smanjenju posljedica rizika. Mjere koje se definiraju u pravilu mogu značiti dodatno osposobljavanje zaposlenika, implementaciju dodatnog sustava sigurnosti ako se govori o informacijskoj sigurnosti, implementaciju senzora za identifikaciju dima ako se govori o zaštiti od požara, itd. (Buntak & Kovačić, 2020).

Kroz eliminaciju rizičnog načina obavljanja poslova, odnosno eliminaciju rizika koji mogu biti povezani uz izbijanje požara u znatnoj se mjeri može povećati sigurnosti i zaštita, odnosno može se poboljšati sustav upravljanja sigurnosti i zaštitom.

Mapiranje procesa može biti usmjereno ne samo prema mapiranju rizika već i prema dokumentiranju svih pravila, kontrolnih točaka, odnosno mehanizama pomoću kojih se vrši transformacija u procesu. Na temelju dokumentiranja svih sastavnica procesa može se identificirati potreba za implementacijom novih mjera ili novih indikatora koji će ukazati na postojanje rizika povezanog uz sigurnost i zaštitu.

Kad je riječ o analizi mogućih uzroka nastanka problema o kojoj se piše na početku ovog poglavlja kao i o alatima koji se mogu koristiti, jedan od alata koji je osnova za analizu mogućeg uzroka problema je dijagram uzroka i posljedice koji je prikazan na slici. Dijagram uzroka i posljedice u literaturi je još poznat i po nazivu Ishikawa dijagram, odnosno dijagram riblje kosti. Dijagram uzroka i posljedice može se koristiti za sagledavanje ozljede na radu ili nekog drugog problema povezanog uz sigurnost i zaštitu. Dijagram se koristi tako da se olujom mozgova definiraju mogući uzroci problema nakon čega se definiraju kategorije u koje će se definirani uzroci problema kategorizirati (Buntak, et al., 2020).

Slika 9: Ishikawa dijagram



Izvor: Buntak, K., Kovačić, M., Premužić, B. 2020. Upravljanje poslovnim procesima. Sveučilište sjever.

Kategorije u koje se mogu grupirati generirane ideje su:

- Strojevi i uređaji: nedovoljno zaštićeni strojevi i uređaji kao posljedicu mogu imati ugrožavanje imovine ali i života i zdravlja zaposlenika koji ih koriste prilikom obavljanja aktivnosti na radnom mjestu. U ovu kategoriju može se uvrstiti ergonomija kao jedan od mogućih uzroka problema.
- Zaposlenici: u kategoriju zaposlenici mogu se kategorizirati uzroci poput nekompetentnosti, odnosno zlonamjernosti ako se radi o odavanju informacija zbog čega je narušena informacijska sigurnost u organizaciji.
- Procesi: u procesima postoji niz različitih mogućih uzroka problema kao što su to nedovoljno dobro definirane radne upute, rizici koji nisu identificirani i mapirani, nedovoljno dobro definiran način komunikacije, itd.
- Okolina: u kategoriju okolina moguće je uvrstiti sve uzroke na koje organizacija nema direktan utjecaj tj. moć kontrole. Primjer za takve uzroke su temperatura zraka, poplava, udar groma, itd. Varijable iz okoline, kao što je to prašina, isto tako mogu imati značajan utjecaj na sigurnost i zdravlje zaposlenika ali i indikatore tj. pokazatelje sigurnosti i zaštite.

Osim navedenih kategorija, organizacija može primjenjivati niz drugih kategorija za koje organizacijski tim zaključi da najbolje opisuju identificirane moguće uzroke problema. Nadalje, osim što organizacija može upotrebljavati dijagram uzroka i posljedice, može upotrebljavati i Pareto dijagram koji se temelji na Pareto načelu. Drugim riječima, Pareto načelo govori kako je

80% posljedica rezultat 20% uzroka problema što može biti jedno od načela koje organizacijski tim može uzeti u obzir prilikom sagledavanja mogućeg poboljšanja.

Pareto dijagram moguće uzroke problema svrstava u tri osnovne kategorije:

- Kategorija A: u kategoriju A ubrajaju se svi uzroci koji u kumulativu iznose do 80%
- Kategorija B: u kategoriju B ubrajaju se svi uzroci koji u kumulativu iznose od 80% do 95% svih zabilježenih nesukladnosti,
- Kategorija C: u kategoriju C ubrajaju se svi uzroci koji u kumulativu iznose od 95% do 100% svih zabilježenih nesukladnosti (Buntak, et al., 2020).

Bez obzira o kojem se alatu radilo, organizacijski tim treba pomoću korištenih alata stvoriti podlogu za donošenje odluke o mogućem poboljšanju.

Za poboljšanje procesa organizacijskom timu se preporučuje obilazak svih radnih mjesta kao i svih mjesta u organizacijama na kojima se čuvaju organizacijske informacije, na kojima zaposlenici rade, itd. Nakon obilaska i nakon intervjua sa zaposlenicima moguće je identificirati mjesta na kojima se može poboljšati proces upravljanja sigurnosti i zaštitom kao i što se mogu identificirati novi rizici povezani uz sigurnost i zaštitu.

7. Model integriranog sustava upravljanja sigurnosti i zaštitom

Kroz istraživanje čiji su rezultati izneseni u poglavlju 5 diplomskog rada, nesumnjivo je dokazano kako pozitivni zakonski propisi i norme pokrivaju djelom slična, a djelom različita područja sigurnosti i zaštite. Nadalje, istraživanjem je identificirano kako su norme po svojem obuhvatu i sadržaju znatno opširnije u odnosu na pojedine zakonske propise. No, bez obzira na obuhvat zakonskih propisa, oni moraju biti zadovoljeni u svakoj organizaciji koja posluje na području Republike Hrvatske.

Kad se govori o integriranom sustavu upravljanja, prilikom integracije dolazi do brojnih izazova koji su djelom povezani uz poteškoće integracije zbog različitih sadržaja normi kao i zakona. Različit sadržaj normi je kroz Annex S(L) ujednačen čime se integracija znatno olakšala. Međutim, izazov integracije zakonskih propisa i zahtjeva normi sustava upravljanja u organizacijski sustav i dalje ostaje. S obzirom na to, jedno od rješenja koje se organizacijama preporučuje je nadopunjavanje zahtjeva koje na organizaciju postavlja pozitivna zakonska legislativa normama, a s obzirom na to da su zakonski propisi kao takvi obvezujući.

Budući da je svakoj organizaciji cilj osigurati održivi rast i razvoj i da svaka organizacija teži održivosti, a održivost se može sagledavati kroz tri komponente održivosti, ekonomsku, društvenu i ekološku, svaka organizacija može pomoću implementacije sustava upravljanja i njihovog certificiranja pomoću normi kao i osiguranja sljedivosti sa zahtjevima koje postavljaju pozitivni zakonski propisi stvoriti osnove za osiguranje svoje održivosti.

U tablici je prikazan popis normi, odnosno popis pozitivne zakonske legislative osiguranje sljedivosti s kojom organizaciji omogućuje stvaranje temelja održivosti. Kao što je vidljivo iz tablice, norme koje se odnose na održivost organizacije su norme koje direktno utječu tj. oblikuju sustav sigurnosti i zaštite. S druge strane isto vrijedi i za pozitivne zakonske propise. Pozitivni zakonski propisi koji direktno koreliraju tj. determiniraju izgled sustava upravljanja sigurnosti i zaštitom također su osnova za osiguranje održivosti organizacije.

Budući da se održivost sagledava kroz ekonomsku, ekološku i društvenu održivost, implementacija sustava upravljanja kvalitetom direktno može utjecati na ekonomsku održivost budući da sustav upravljanja kvalitetom postavlja zahtjeve na menadžment, a koji se odnose na način na koji menadžment upravlja organizacijom. S druge strane, sustav upravljanja okolišem može determinirati ekološku komponentu održivosti budući da izravno utječe na zahtjeve koji su

usmjereni prema očuvanju okoliša. Nadalje, sustav upravljanja zdravljem i sigurnosti zaposlenika može utjecati na društvenu komponentnu održivosti.

Tablica 13: Utjecaj normi i zakonskih propisa na održivost

Ekonomska komponenta	Društvena komponenta	Ekološka komponenta
ISO EN 9001:2015	ISO 45001:2018	ISO 14001:2015
ISO 22301:2019	ISO 2200:2018	ISO 50001:2018
	ISO EN 37001: 2016	Zakon o zaštiti okoliša
	Zakon o zaštiti na radu	
	Zakon o radu	
	Opća uredba o zaštiti podataka	
	Zakon o obveznim odnosima	

Izvor: Tablica je rad autora

Kao što je vidljivo iz tablice 13, istraživanjem je identificirano kako postoji znatno veći broj normativnih dokumenata koji oblikuju društvenu komponentu održivosti u odnosu na ostale komponente. Temeljni razlog za to je činjenica kako je društvena komponenta održivosti komponenta koja je najviše osjetljiva. Zatim slijedi ekološka komponenta održivosti u kojoj, osim normi sustava upravljanja, država kao sustav definira niz zakonskih propisa, a kao što je to Zakon o zaštiti okoliša. Međutim, spomenuti zakon samo je jedan od zakonskih dokumenata koji unutar sebe povezuje niz drugih zakonskih propisa koji također mogu oblikovati održivost organizacije.

Kad se govori o integriranom sustavu upravljanja sigurnosti i zaštite potrebno je napomenuti kako se on treba oblikovati tako da u obzir uzima i interne prijetnje unutar organizacije ali i eksterne prijetnje koje dolaze iz organizacijskih okolina. Drugim riječima, organizacijski zaposlenici mogu postati prijetnja za organizaciju ako postanu zlonamjerni, odnosno mogu postati prijetnja ako nisu kompetentni i nisu educirani za obavljanje aktivnosti na siguran način. S druge strane, prijetnje koje dolaze iz vanjske okoline organizacije također mogu umanjiti sigurnost organizacije zbog čega je neophodno definirati mjere za smanjenje rizika.

Kad se govori o smanjenju rizika od unutarnjih prijetnji unutar organizacije, potrebno je naglasiti kako fizička i tehnička zaštita u znatnoj mjeri mogu smanjiti mogućnost da organizacijski zaposlenici načine štetu organizaciji. Nadalje, u slučajevima kada postoji rizik od mogućeg ustupljivanja organizacijskih dokumenata ili organizacijskih informacija neophodno je voditi

računa o uspostavi postupaka vezanih za osiguranje informacijske sigurnosti kao i aktivaciju business intelligence protokola koji će pratiti ponašanje zaposlenika kao i analizirati mogući rizik da informacije koje su važne za organizaciju budu proslijeđene trećim stranama.

S obzirom na to, neophodno je provesti analizu rizika i sukladno identificiranoj razini rizika za svako radno mjesto definirati mjere temeljem kojih će se nastojati spriječiti moguća zloupotreba. Nadalje, posebnu pozornost potrebno je usmjeriti i prema dokumentima koji se nalaze nezaštićeni u uredima u organizaciji, a koji mogu biti dostupni trećim stranama koje nemaju autorizaciju tj. dopuštenje za pregled takvih dokumenata. Isto se odnosi i na industrijsku špijunažu u kojoj postoji rizik da konkurencijski stručnjaci posjete organizaciju pod krinkom posjete zbog razgledavanja i da uvidom u strojeve i uređaje, odnosno tehnologiju otkriju dobiju informacije koje bi mogle narušiti sigurnost poslovanja organizacije.

Sljedeće područje koje može biti zahvaćeno rizikom od mogućeg informacijskog rizika je područje dvorani za sastanke koje mogu biti ozvučene kao i mogućnost da zaposlenici pomoću svojih mobilnih uređaja ili drugih tehničkih naprava snime sadržaj sastanka. To se može odnositi i na nehotično snimanje zbog mogućnosti da treće strane pomoću programa koje postave na tehničke naprave zaposlenika prisluškuju sadržaj sastanka.

Kad se govori o internim prijetnjama potrebno je napomenuti kako postoji opasnost da organizacijski zaposlenici otuđe sredstva za rad ili proizvode iz skladišta ili proizvodnog pogona, odnosno općenito s radnog mjesta. S obzirom na to, neophodno je definirati mjere temeljem kojih će se spriječiti moguće krađe.

Kad je riječ o zaštiti zaposlenika od sustava, potrebno je naglasiti kako sustav kao takav može od zaposlenika tražiti rad na nesiguran način, odnosno zaposleniku ne osigurati sredstva za siguran način rada. Nadalje, jedan od primjera zloupotrebe zaposlenika je prekovremeni rad koji sustav može tražiti od zaposlenika. Prekovremenim radom kao i neosiguravanjem sredstava temeljem kojih će se zaposleniku omogućiti rad na siguran način potrebno je spriječiti budući da će narušiti održivost organizacije ali će i kao posljedicu imati generiranje troškova, odnosno moguću veliku fluktuaciju zaposlenika kroz sustav, a što u dugom roku može postati prijetnja kontinuitetu poslovanja organizacije suočene s ovakvim problemom.

Nadalje, potrebno je napomenuti kako organizacija treba voditi računa i o intelektualnom vlasništvu u organizaciji, odnosno riziku da organizacijski zaposlenici koji posjeduju specifična znanja i vještine napuste organizaciju i odu u druge organizacije. To ujedno može rezultirati i time

da organizacija izgubi jednu komponentu svoje konkurentske prednosti budući da specifična znanja i vještine organizacijskih zaposlenika, organizacija koristi u razvoju kako novih proizvoda tako i normalnom funkcioniranju organizacije. No, svakako je potrebno napomenuti kako kompetentni zaposlenici često mogu iskoristiti svoje kompetencije kako bi iz organizacije iznijeli pojedine informacije ili dokumente koji bi mogli naštetiti organizaciji.

S obzirom na to, neophodno je provesti edukaciju svih zaposlenika kao i definirati mjere temeljem kojih bi se smanjila mogućnost da organizacijski zaposlenici naštete organizaciji. S druge strane, kroz implementaciju sustava koji stvara sigurnosne kopije kao i sustava koji prati aktivnosti koje zaposlenici provode s dokumentacijom kao i podatcima koji se nalaze smješteni spremljeni u bazama informacija.

7.1 Integracija sustava upravljanja

Kad se govori o mogućnostima integracije sustava upravljanja, jedna od mogućnosti koja stoji organizaciji na raspolaganju je integracija pomoću procesnog pristupa. Integracija pomoću procesnog pristupa temelji se na identifikaciji i mapiranju poslovnih procesa koji se odvijaju u organizaciji kao i definiranju svih radnih mjesta u procesu. Osnova za integraciju je implementacija sustava upravljanja kvalitetom budući da on determinira funkcioniranje cjelokupne organizacije, odnosno osnova je za funkcioniranje svih ostalih sustava upravljanja koji se implementiraju u organizaciju.

Osim toga, sustav upravljanja kvalitetom definira i način upravljanja svom dokumentacijom kao i potrebu za stalnim poboljšanjem svih organizacijskih procesa što neminovno dovodi i do poboljšanja procesa karakterističnih za sustav upravljanja sigurnosti.

Dakle, sustav upravljanja kvalitetom postaje temeljni proces u organizaciji koji oblikuje odvijanje svih drugih organizacijskih procesa. To ujedno znači i kako su njegovi zahtjevi implementirani u procese potpore i upravljačke procese, odnsono da menadžment mora organizacijom upravljati po načelima kvalitetnog upravljanja koje nalaže norma. Nadalje, osim osiguranja sukladnosti s načelima kvalitetnog upravljanja, menadžment mora osigurati i sukladnost s načelima upravljanja koje naglašavaju ostale norme sustava upravljanja.

Jedan od izazova s kojim se organizacije mogu susresti prilikom integracije sustava upravljanja je identificiranje točki u procesu u kojima će se vršiti integracije. Točke u procesu mogu biti

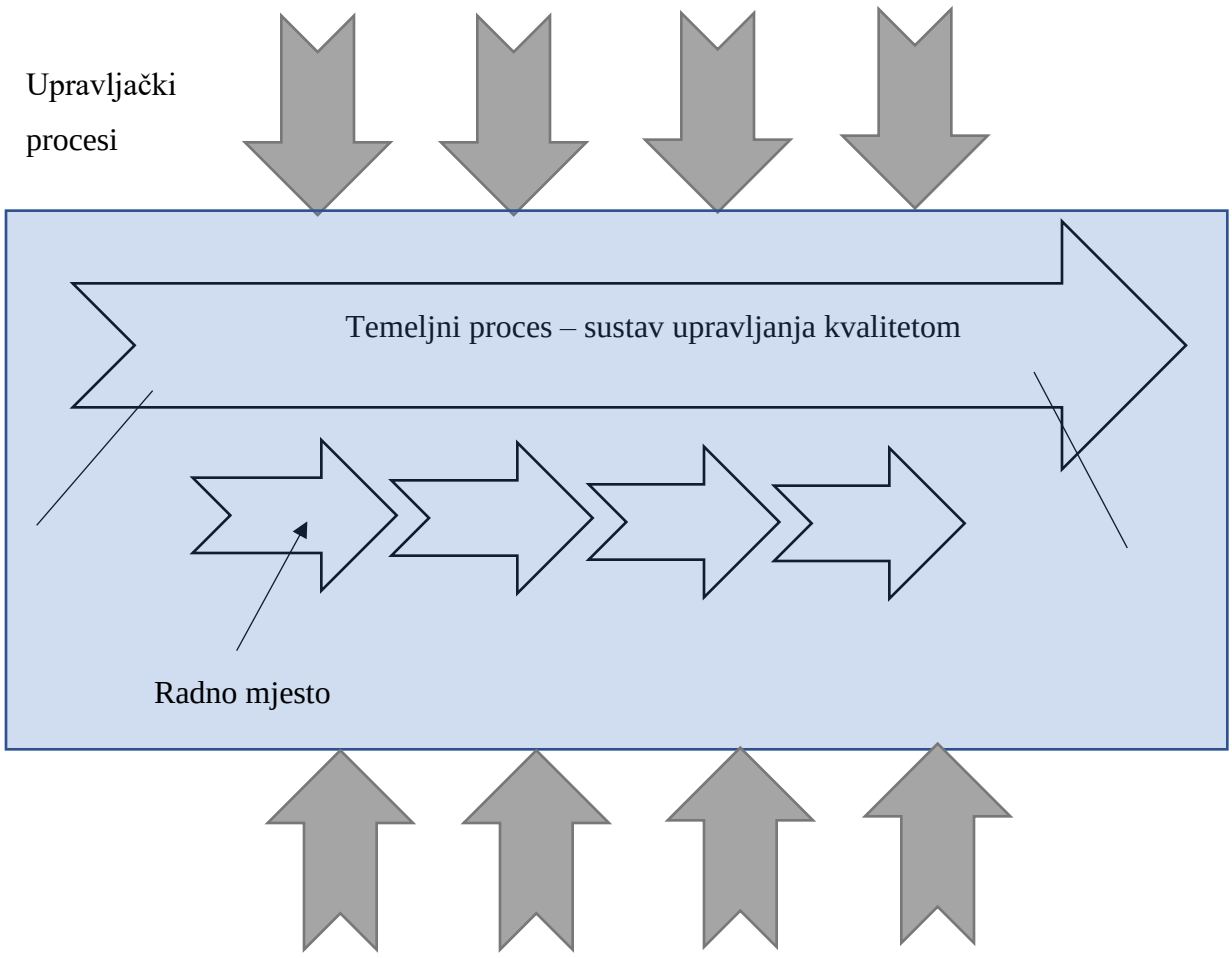
indikatori koje organizacije definira, a koji su u sukladnosti sa zahtjevima pozitivnih zakonskih propisa kao i zahtjeva koje pozitivni zakonski propisi postavljaju na organizaciju.

Ako organizacija definira radno mjesto kao točku integracije, u tom slučaju se analiziraju rizici za svako radno mjesto. Ako se identificira da na pojedinom radnom mjestu postoje rizici vezani uz ozljede na radu, potrebno je uzeti u obzir zahtjeve koje zakonski propisi i norme sustava upravljanja zdravljem i sigurnosti zaposlenika postavljaju na organizaciju i osigurati sukladnost s njima. Isto vrijedi i za sve druge rizike s kojima se organizacijski zaposlenici mogu susresti prilikom obavljanja poslova na radnom mjestu.

S druge strane, ako organizacija za mjesta integracije u obzir uzme točke sukladno indikatorima, potrebno je analizirati ishode sustava upravljanja zdravljem i sigurnosti, odnsono ishode sigurnosti i zaštite u organizaciji i sustav oblikovati tako da se osiguranje sukladnosti sa zahtjevima normi sustava upravljanja, odnosno zakonskim zahtjevima osigura i povoljni indikator.

Osim upotrebe indikatora, organizacija može za integraciju koristiti i točke, koje ne predstavljaju radna mjesta već procesne korake, odnosno potprocese u procesu, i analizirati njihov kontekst. Analiza konteksta procesa podrazumijeva identifikaciju svih prijetnji ali i prilika koje se odnose na mogućnost narušavanja sigurnosti zaposlenika, odnosno narušavanja sigurnosti organizacije u cjelini. Na takvim točkama u procesu se s obzirom na kontekst definiraju mjere na temelju kojih će se smanjiti rizik i osigurati sigurna radna okolina.

Tablica 14: Procesi u organizaciji

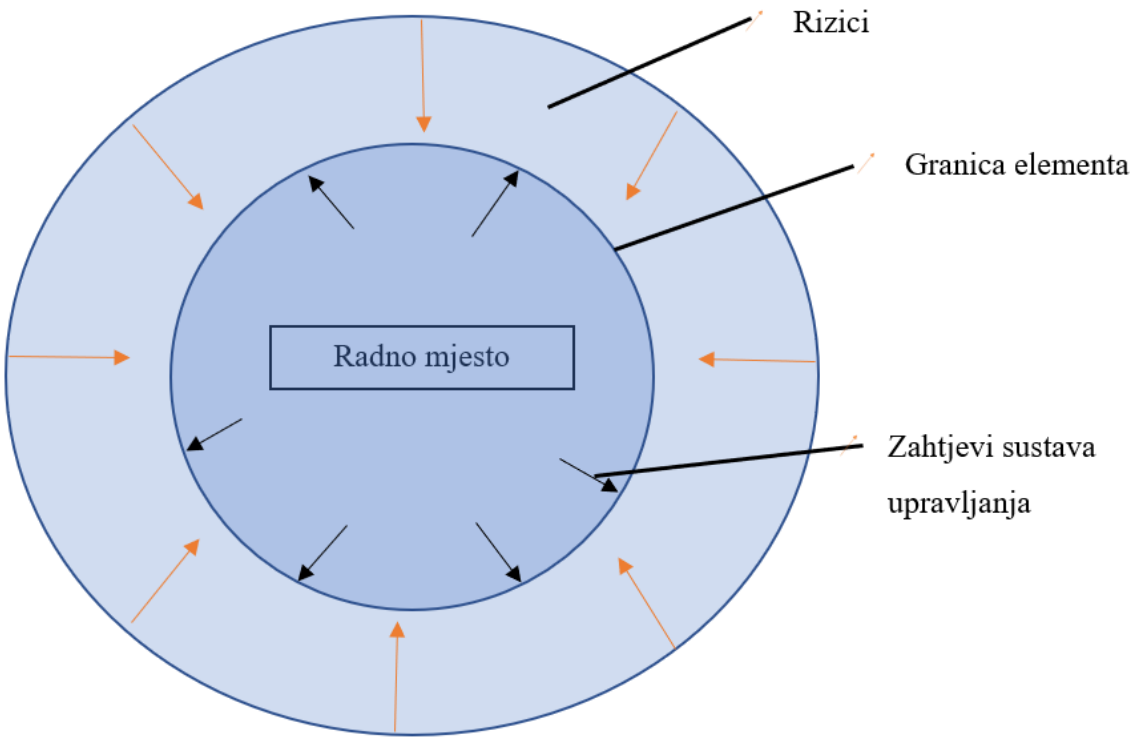


Izvor: Slika je rad autora

Kao što je to prikazano na slici 14, organizacija se sastoji od tri grupe procesa, temeljnog procesa koji je oblikovan normom sustava upravljanja kvalitetom, procesa potpore koji su zaduženi za osiguranje svih resursa neophodnih za normalno funkcioniranje organizacije i upravljačkih procesa koji su zaduženi za upravljanje cjelokupnom organizacijom, odnosno upravljanje temeljnim procesom u organizaciji.

Na slici 14, prikazano je radno mjesto koje je izdvojeno iz jednog potprocesa. Za to radno mjesto na slici 15 prikazan je način integracije sustava upravljanja sigurnosti analizom radnog mjesta, odnosno analizom rizika.

Tablica 15: Radno mjesto i rizici



Izvor: Slika je rad autora

Kao što je to prikazano blok shemom na slici 14, za svako radno mjesto analizira se rizik i temeljem identificiranog rizika definiraju se mjere za smanjenje rizika, odnosno osiguranje optimalne razine sigurnosti. Mjere koje se definiraju determinirane su zahtjevima koje postavlja zakonska legislativa ali i norme sustava upravljanja.

Rizici koji se mogu identificirati na radnom mjestu determinirani su vrstom radnog mjesta, odnosno temeljnom djelatnosti organizacije, a mogu se identificirati primjenom različitih alata i metoda, odnosno na temelju intervjua koji se provodi sa zaposlenikom koji radi na radnom mjestu koje se analizira.

7.2. Metodologija integracije

Kao što je opisano u poglavlju 7.1, prvi korak prilikom stvaranja integriranog sustava upravljanja sigurnosti i zaštitom je implementacija procesnog pristupa u organizaciju. Za implementaciju procesnog pristupa neophodno je identificirati poslovne procese u organizaciji budući da svaka organizacija unatoč tome što nema implementiran procesni pristup. Prilikom identifikacije, odnsono mapiranja poslovnih procesa, organizacija ujedno identificira i radna mjesta u njima. Za svako radno mjesto organizacija može provesti intervju sa zaposlenikom kako bi mogla identificirati za što je zadužen pojedini zaposlenik u organizaciji kao i s kojom se dokumentacijom, odnosno rizicima susreće.

Prilikom implementacije procesnog pristupa, preporučuje se definiranje procesnog toka kroz organizaciju kako bi se mogla pratiti transformacija, odnsono kako bi se mogao pratiti tijek resursa. Ovo je od posebne važnosti za identifikaciju mogućih rizika u svakom procesnom koraku budući da se rizik, sukladno teoriji sustava, može proširiti kroz sve organizacijske procese ako ga se ne kontrolira, odnosno ako se ne definiraju mjere za njegovo smanjenje.

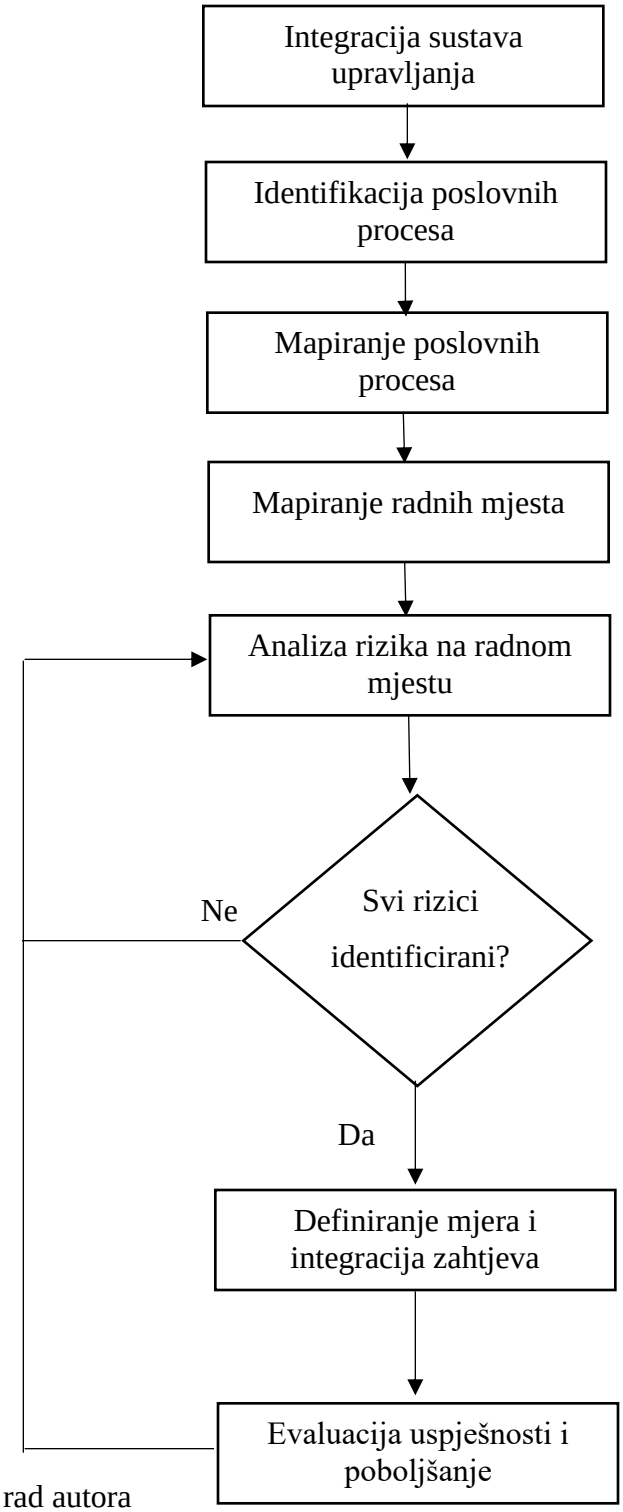
Nakon identifikacije, mapiranja procesa i definiranja radnih mjesta, potrebno je, ako se izabere pristup utemeljen na radnim mjestima, analizirati pojedino radno mjestu u potrazi za svim rizicima koji mogu ugroziti zdravlje i sigurnost zaposlenika, odnosno održivost organizacijskog sustava. Svi rizici trebaju biti analizirani i za svaki rizik potrebno je definirati mjere za smanjenje rizika kao i mjere za smanjenje posljedica rizika.

Potrebno je naglasiti da, ako organizacija kreira radno mjesto, odnsono redizajnira identificirani proces prilikom mapiranja, organizacija mora osigurati sukladnost sa svim pozitivnim zakonskim propisima koji su obvezujući sukladno djelatnosti kojom se organizacija bavi.

Nakon analize i definiranja rizika za svako radno mjesto kao i definiranja mjera koje su u sukladnosti sa zahtjevima normi sustavima upravljanja, organizacija ima prvi stupanj integracije sustava upravljanja sigurnosti i zaštitiom. To podrazumijeva potrebu analiziranja performansi sustava upravljanja temeljem indikatora, odnosno na temelju KPI pokazatelja kao i analize svih neželjenih događaja koji nastaju u procesima pomoću alata i metoda za poboljšanje poslovnih procesa. Kroz poboljšanja i kroz implementaciju novih sustava upravljanja u organizaciju povećava se i razina zrelosti sustava upravljanja.

Dijagram tijeka metodologije integracije sustava upravljanja sigurnosti i zaštitom prikazan je na slici.

Tablica 16: Postupak integracije



Izvor: Slika je rad autora

Kako bi se povećao stupanj zrelosti integracije sustava upravljanja sigurnosti i zaštitom neophodno je provoditi stalno poboljšanje što je ujedno i zahtjev normi kao i pojedinih zakonskih propisa. Nadalje, potrebno je napomenuti kako u modelu integracije nije definiran korak u kojem organizacija analizira organizacijske okoline i definira zahtjeve zainteresiranih strana budući da implementacija samog procesnog pristupa, odnosno implementacija pojedinačnih sustava upravljanja zahtjeva analizu zahtjeva i dokumentiranje istih.

Nakon što se provede integracija, organizacija mora izraditi radne upute u kojima će definirati način na koji će se obavljati poslovi na pojedinom radnom mjestu jednako kao i što treba definirati postupke na temelju kojih će se pokrenuti radnje ako dođe do ugrožavanja sigurnosti organizacije ili njezine održivosti.

Budući da se integracija sustava upravljanja sigurnosti i zaštitom temelji na procesnom pristupu, nakon integracije potrebno je ažurirati knjigu procesa unutar koje je jasno definiran izgled svakog od procesa. Drugim riječima, ako organizacija za prikaz svojih procesa koristi IDEFO metodu neophodno je da ažurira pravila kao i kontrole, odnsono mehanizme. Drugim riječima, pravila su ažurirana na temelju novih radnih uputa kao i na temelju novih zahtjeva koji su sadržani u normama sustava upravljanja. Nadalje, kontrole se ažuriraju na temelju novih kontrolnih točaka na kojima se mjere indikatori učinkovitosti sustava upravljanja dok se mehanizmi ažuriraju s novim sredstvima za rad, odnosno novim sredstvima zaštite ako se takvi upotrebljavaju u procesu.

Kad se govori o integraciji sustava upravljanja kao i certifikaciji sustava upravljanja neophodno je napomenuti kako se integrirani sustav upravljanja certificira, odnosno auditira na znatno drugačiji način u odnosu na pojedinačne sustave upravljanja. Drugim riječima, za certificiranje i auditiranja integriranog sustava upravljanja, auditor mora imati na uvid u kontekst procesa kako bi mogao identificirati s kakvim se rizicima susreće pojedino radno mjesto odnosno organizacija u cjelini. Dakle, prilikom auditiranja integriranog sustava upravljanja govori se o tzv. Više kriterijalnom auditu u kojem se svako radno mjesto, odnosno svaki potproces auditira sukladno drugačijim zahtjevima normi sustava upravljanja. Potprocesi u kojima postoji rizik od zagađenja okoliša ali ne postoji rizik od ozljeda na radu auditiraju se sukladno zahtjevima koje postavlja norma sustava upravljanja okolišem, itd.

Jednako kao i svi drugi sustavi upravljanja certificirani prema ISO normama, integrirani sustav upravljanja podliježe redovitim kontrolnim auditima, odnosno potrebi recertifikacije svake tri

godine od dana dobivanja certifikata. Dakle, pomoću kontrolnog audita nezavisna strana identificira jesu li performanse sustava upravljanja zadovoljavajuće ili ne i sukladno tome definira preporuke za organizaciju. S druge strane, osim audita treće strane, organizacija mora provoditi interni audit kako bi sama identificirala performanse i kako bi povećala zrelost sustava upravljanja, a samim time utjecala i na održivost tj. povećanje sigurnosti.

8. Zaključak

Diplomski rad temelji se na provedenom sekundarnom istraživanju. Sekundarnim istraživanjem identificirale su se posljednje spoznaje iz područja sigurnosti i zaštite u organizaciji. Isto tako, istraživanjem je identificirano kako ne postoji dovoljan broj stručnih i znanstvenih radova koji bi opisivali način na koji će se provesti integracija pozitivnih zakonskih propisa i normi u organizacijskom sustavu kao ni autori koji govore o načinu integracije različitih normi.

Kroz istraživanje je identificirano kako je rizik sastavnica svake organizacijske okoline i kako rizik organizacija treba uzeti u obzir prilikom planiranja kao i prilikom sagledavanja trenutne razine sigurnosti i zaštite u organizaciji. Analiza i dokumentiranje rizika osnova je i za kreiranje plana osiguranja kontinuiteta poslovanja jednako kao i što je osnova za sagledavanje mjera za povećanje trenutne razine sigurnosti i zaštite.

Kroz komparativnu analizu normi i pozitivnih zakonskih propisa iz područja sigurnosti i zaštite, odnosno normi i pozitivnih zakonskih propisa koji na direktni ili indirektni način determiniraju izgled sustava upravljanja sigurnosti i zaštitom, identificirano je kako postoji stanovita razlika između zahtjeva koje na organizacijski sustav postavlja norma i zahtjeva koje na organizaciju postavljaju pozitivni zakonski propisi. Nadalje, kroz komparativnu analizu identificirano je kako pozitivni zakonski propisi na nedovoljno dobar način oblikuju sustav sigurnosti i zaštite budući da su po svojoj reviziji zastarjeli. Jedan od primjera zastarjelog zakonskog propisa je Zakon o sigurnosti informacija koji se odnosi isključivo na državne institucije i ne daje minimalne zahtjeve koje mora zadovoljiti svaka druga organizacija koja se nalazi u privatnom sektoru. To kao posljedicu ima mali broj organizacija koje su svjesne važnosti informacijske sigurnosti, a što posljedično rezultira mogućnosti da organizacije ne štite svoje informacije na dovoljno dobar način što može rezultirati narušavanjem sigurnosti.

Potrebno je naglasiti kako je temeljno ograničenje provedenog komparativnog istraživanja činjenica kako se zakonski propisi koje definira i oblikuje Republika Hrvatske može razlikovati u odnosu na pozitivne zakonske propise koje definiraju druge zemlje u svijetu. S obzirom na to, razvijeni model koji je opisan u poglavlju 7 generički je model što znači da se može prilagoditi različitim organizacijama koje posluju na tržištima različitih gospodarskih sustava.

Model integracije sustava upravljanja sigurnosti i zaštitom temelji se na procesnom pristupu, a što podrazumijeva imperativ uvođenja procesnog pristupa za sve organizacije koje nastoje

provesti integraciju sustava upravljanja. Uvođenje procesnog pristupa ujedno je i osnova za povećanje kvalitete upravljanja organizacijom budući da implementacija procesnog pristupa podrazumijeva i mogućnost boljeg mjerenja performansi, a što znači i mogućnost lakše identifikacije prilika za poboljšanje.

Procesni pristup integraciji sustava upravljanja podrazumijeva definiranje točaka u procesu na kojima će se definirati rizici, a koji će biti smanjeni kroz implementaciju, odnosno osiguranje sukladnosti sa zahtjevima norme i zakonskih prosipa. Drugim riječima, ako organizacija identificira u procesu opasnost povezanu uz informacijsku sigurnost neophodno je osigurati sukladnost sa zahtjevima koje definira norma sustava upravljanja informacijskom sigurnosti. S druge strane, ako organizacija identificira opasnost, odnosno rizik povezan uz mogućnost zagađenja okoliša, neophodno je osigurati sukladnost sa pozitivnim zakonskim propisima iz područja zaštite okoliša kao i sukladnost sa zahtjevima norme sustava upravljanja okolišem.

Kad se govori o oblikovanju točaka u kojima će se vršiti integracija, točke mogu biti definirane na temelju indikatora koji mogu biti oblikovani tako da se sagledava broj ozljeda na radu, broj neautoriziranih pristupa ili pokušaja pristupa informacijama, itd. Osim toga, drugi način integracije odnosi se na sagledavanje i analizu rizika vezanog uz svako radno mjesto. Drugim riječima, analizira se rizik za svakog zaposlenika koji obavlja određeni posao u organizaciji i definiraju se zahtjevi s kojima se mora osigurati sukladnost kako bi se smanjio rizik.

Kad je riječ o negativnom utjecaju na okoliš, odnosno mogućnosti neautoriziranog pristupa, pristup integraciji podrazumijeva analizu mogućih rizika i na temelju identificiranog rizika definiraju se mjere koje moraju biti u sukladnosti sa zahtjevima koje definiraju norme sustava upravljanja.

Zrelost integriranog sustava upravljanja determinirana je brojem sustava upravljanja koji su uključeni u sustav upravljanja sigurnosti i zaštitom. Početna zrelost podrazumijeva isključivo sukladnost s pozitivnim zakonskim propisima bez osiguranja sukladnosti sa zahtjevima normi, odnosno bez implementacije sustava upravljanja.

Budući da je riječ o konceptualnom modelu integracije sustava upravljanja potrebno je naglasiti kako je temeljno ograničenje provedenog istraživanja njegova vrsta, odnosno teorijski pristup definiranju modela bez njegovog testiranja u praksi.

S obzirom na to, budućim istraživačima ovog područja preporučuje se fokusiranje na nadogradnju metodologije integracije sustava upravljanja sigurnosti i zaštitom kao i njegovo testiranje u praksi. Isto tako, preporuka budućim istraživačima fokusiranje je na definiranje indikatora koji bi opisivali svako od područja sigurnosti i zaštite. Drugim riječima, definiranje indikatora koji opisuju informacijsku sigurnost, indikatora koji opisuju sigurnost na radu, indikatora koji opisuju sigurnost okoliša, itd.

Nadalje, preporuka budućim istraživačima je definiranje točka u procesu kao i metode na temelju koje će se definirati točka u procesu na kojoj će se vršiti integracija, a koji, sukladno rezultatima istraživanja, mora biti temeljena na rizicima tj. analizi rizika.

Literatura

1. Aven, T., 2016. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, pp. 1-13.
2. Bađun, M., 2017. Costs of occupational injuries and illnesses in Croatia. *Archives of Industrial Hygiene and Toxicology*, pp. 66-73.
3. Britvić, J., 2011. Moderni sustavi upravljanja u organizacijama. *Praktični menadžment: stručni časopis za teoriju i praksu menadžmenta,* pp. 72-80.
4. Buer, S. V., Fragapane, G. I. & Strandhagen, J. O., 2018. The Data-Driven Process Improvement Cycle: Using Digitalization for Continuous Improvement. *IFAC-PapersOnLine*, pp. 1035-1040.
5. Buntak, K. & Kovačić, M., 2020. *Upravljanje kvalitetom 1*. Koprivnica: Sveučilište Sjever.
6. Buntak, K., Kovačić, M. & Kondić, V., 2020. *Upravljanje kvalitetom 2*. Koprivnica: Sveučilište Sjever.
7. Buntak, K., Kovačić, M. & Micek, B., 2019. INTEGRATION OF THE MANAGEMENT SYSTEM USING PROCESS APPROACH OF THE ORGANIZATION. *21. NACIONALANI I 7.MEĐUNARODNI NAUČNO STRUČNI SKUP SISTEM KVALITETA USLOV ZA USPEŠNO POSLOVANJE I KONKURENTNOST*.
8. Buntak, K., Kovačić, M. & Premužić, B., 2020. *Upravljanje poslovnim procesima.* Koprivnica: Sveučilište Sjever.
9. Buntak, K., Kovačić, M. & Sesar, V., 2019. THE IMPORTANCE OF IDENTIFYING OPPORTUNITIES AND RISK IN ENSHURING BUSINESS CONTINUITY. *ESD conference proceedings*.
10. Cambridge dictionary, 2020. *Security.* [Mrežno] Available at: https://dictionary.cambridge.org/dictionary/english/security [Pokušaj pristupa 09 Rujan 2020].

11. Duran, D. C., Gogan, L. M., Artene, A. & Duran, V., 2015. The components of sustainable development-a possible approach.. *Procedia Economics and Finance*, pp. 806-811.
12. Hák, T., Janoušková, S. & Moldan, B., 2016. Sustainable Development Goals: A need for relevant indicators. *Ecological Indicators*, pp. 565-573.
13. ISO 9000, 2015. *Temeljna načela i terminološki rječnik.* s.l.:an.
14. Madni, H. A., Anwar, Z. & Shah, M. A., 2017. Data mining techniques and applications—a decade review.. *IEEE*, pp. 1-7.
15. Mihaljević, B. & Nađ, I., 2018. *The Basics of Corporate Security.*. s.l.:an.
16. Mikić, M., 2018. *Korporativna sigurnost.* Rijeka: Sveučilište u Rijeci.
17. Pereira, T., Barreto, L. & Amaral, A., 2017. Network and information security challenges within Industry 4.0 paradigm. *Procedia manufacturing*, pp. 1253-1260.
18. Secude, 2020. *10 Data Leaks that have cost Fortune 500 companies a fortune.* [Mrežno]
    Available at: https://secude.com/10-data-leaks-that-have-cost-fortune-500-companies-a-fortune/
    [Pokušaj pristupa 9 Rujan 2020].
19. Trieu, V. H., 2017. Getting value from Business Intelligence systems: A review and research agenda. *Decision Support Systems*, pp. 111-124.
20. Webster dictionary, 2020. *Webster dictionary - word seafty.* [Mrežno] Available at: https://www.merriam-webster.com/dictionary/safety [Pokušaj pristupa 08.09.2020 Rujan 2020].
21. Zuo, H. & Ai, D., 2011. Environment, energy and sustainable economic growth. *Procedia Engineering*, pp. 513-519.

Popis slika

Slika 1: Trokut održivosti 5
Slika 2: Odjel integralne sigurnosti 15
Slika 3: Prikaz sastavnica korporativne sigurnosti 17
Slika 4: Sustav upravljanja rizicima 22
Slika 5: Nastanak rizika 23
Slika 6: Dekompozicija poslovnog procesa 54
Slika 7: IDEFO metoda 56
Slika 8: Mogući način korištenja alata 63
Slika 9: Ishikawa dijagram 65

Popis tablica

Tablica 1: Podjela sigurnosti 9
Tablica 2: Interne prijetnje u organizaciji 12
Tablica 3: FMEA metoda 20
Tablica 4: Popis sustava upravljanja 26
Tablica 5: Direktni i indirektni zakonski propisi 30
Tablica 6: Direktne i indirektne norme sustava upravljanja 31
Tablica 7: Parametri komparacije 33
Tablica 8: Komparativna analiza Zakona o zaštiti okoliša i norme ISO EN 14001:2015 36
Tablica 9: Komparativna analiza Zakona o zaštiti a radu i norme ISO EN 45001:2018 42
Tablica 10: Komparacija Zakona o sigurnosti informacija i norme ISO 27001:2020 47
Tablica 11: Indikatori sigurnosti i zaštite 58
Tablica 12: KPI pokazatelji 61
Tablica 13: Utjecaj normi i zakonskih propisa na održivost 68
Tablica 14: Procesi u organizaciji 72
Tablica 15: Radno mjesto i rizici 73
Tablica 16: Postupak integracije 75