

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

By Marija Matotek

UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
I MEĐUNARODNU SARADNJU



KVANTIFIKACIJA RIZIKA
U LANCIMA SNABDEVANJA

Doktorska disertacija

Marija Matotek

Beograd, april 2015.

UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
I MEĐUNARODNU SARADNJU



KVANTIFIKACIJA RIZIKA
U LANCIMA SNABDEVANJA

Doktorska disertacija

Mentor:
Prof. dr Dušan Regodić

Kandidat:
Marija Matotek, MSc

Beograd, april 2015.

SADRŽAJ

1. UVODNE NAPOMENE	...1
1.1. Predmet i problem istraživanja	...2
1.2. Ciljevi istraživanja	...2
1.3. Polazišta – hipoteze	...3
1.4. Primenjena metodologija	...3
1.5. Postignuti rezultati	...5
1.6. Kratak prikaz rada po poglavljima	...5
2. TEORIJSKI OKVIR ISTRAŽIVANJA	...7
2.1. Kategorijalni aparat	...7
2.1.1. <i>Logistika</i>	...7
2.1.2. <i>Lanac snabdevanja</i>	...11
2.1.3. <i>Rizik</i>	...14
2.2. Rizici u lancima snabdevanja	...18
2.2.1. <i>Pretnje i ranjivosti u lancu snabdevanja</i>	...25
2.2.2. <i>Mapiranje poslovnih procesa u lancima snabdevanja</i>	...29
2.2.3. <i>Upravljanje rizikom</i>	...30
2.2.4. <i>Upravljanje rizikom u lancima snabdevanja</i>	...34
2.2.5. <i>Kvantifikacija rizika</i>	...38
2.2.6. <i>Kinney metoda</i>	...39
2.2.7. <i>Softversko rešenje Hestia Risk</i>	...41
2.3. Rezime poglavlja	...50
3. MATEMATIČKI MODEL PROCENE RIZIKA U LANCIMA SNABDEVANJA	...51
3.1. Predlog mera za otklanjanje rizika u lancima snabdevanja	...54
3.2. Rezime poglavlja	...58
4. STUDIJA SLUČAJA PROCENE RIZIKA U LANCIMA SNABDEVANJA PRIMENOM SOFTVERSKOG ALATA HESTIA	...59
4.1. Procesi u lancu snabdevanja	...59
4.2. Ranjivosti i pretnje lanca snabdevanja	...62
4.3. Evaluacija rizika u lancu snabdevanja	...82
4.4. Rezime poglavlja	...93
5. ZAKLJUČNA RAZMATRANJA	...94
6. LITERATURA	...100

Spisak slika

Slika 1: Logistički sistem	...9
Slika 2: Procesi u lancu snabdevanja	...12
Slika 3: Bazični lanac snabdevanja	...12
Slika 4: Evolucija lanca snabdevanja	...13
Slika 5: Identifikacija grupa rizika u lancima snabdevanja u odnosu na okruženje	...20
Slika 6: Kategorije rizika u lancima snabdevanja predložene od strane različitih autora	...21
Slika 7: Korelacija između principa, procesa i okvira upravljanja rizikom	...32
Slika 8: Proces upravljanja rizicima	...33
Slika 9: Integracija lanca snabdevanja podržana upravljanjem rizikom	...34
Slika 10: Okvirni primer SCRM	...35
Slika 11: PDCA model ISMS prema ISO 27001:2005	...42
Slika 12: Funkcionalna shema softverskog alata Hestia	...44
Slika 13: Shema implementacije ISMS	...46
Slika 14: Definisane broj nivoa opasnosti, posledica, pretnji, ranjivosti i rizika	...46
Slika 15: Definisane matrice rizika	...47
Slika 16: Grafički prikaz pojave identifikovanih rizika u lancima snabdevanja po nivoima I – V	...53
Slika 17: Lista procesa u lancu snabdevanja	...60
Slika 18: Grupe rizika u lancu snabdevanja	...61
Slika 19: Lista ranjivosti u lancu snabdevanja	...63
Slika 20: Lista pretnji u lancu snabdevanja	...72
Slika 21: Lista pretnji pridruženih ranjivostima u lancu snabdevanja	...78
Slika 22: Lista predloženih mera za ublažavanje/uklanjanje rizika u lancu snabdevanja	...79
Slika 23: Evaluacija rizika u lancu snabdevanja	...83
Slika 24: Rizici nivoa 5 pre tretiranja	...84
Slika 25: Rizici nivoa 4 pre tretiranja	...85
Slika 26: Rizici nivoa 3	...86
Slika 27: Rizici nivoa 2	...87
Slika 28: Rizici nivoa 1	...88
Slika 29: Preostali rizici nivoa 5 nakon prve iteracije tretiranja predloženim merama	...89
Slika 30: Preostali rizici nivoa 4 nakon prve iteracije tretiranja predloženim merama	...90
Slika 31: Preostali rizici nivoa 3 nakon prve iteracije tretiranja predloženim merama	...91
Slika 32: Statistika procene rizika u lancu snabdevanja	...92

Spisak tabela

Tabela 1: Najčešće definicije rizika koje se upotrebljavaju u poslovnom svetu	...16
Tabela 2: Definicije rizika u okviru zakonskih akata Republike Srbije	...17
Tabela 3: Kategorije rizika u lancima snabdevanja – studija slučaja	...23
Tabela 4: Listing pretnji/izvora rizika u lancu snabdevanja	...26
Tabela 5: Listing ranjivosti lanca snabdevanja	...27
Tabela 6: Metodologija upravljanja rizicima – uslovi i kriterijumi	...28
Tabela 7: Mapiranje poslovnih procesa u lancu snabdevanja	...30
Tabela 8: Bazične SCRM definicije	...36
Tabela 9: Numeričke vrednosti verovatnoća pojave opasnosti/štete po Kinney metodi	...39
Tabela 10: Numeričke vrednosti učestalosti izloženosti delovanju faktora rizika po Kinney metodi	...40
Tabela 11: Numeričke vrednosti težine nastale štete/posledice po Kinney metodi	...40
Tabela 12: Rang rizika po Kinney metodi	...40
Tabela 13: Rang rizika u lancima snabdevanja po Kinney metodi	...51
Tabela 14: Procena rizika u lancu snabdevanja primenom Kinney metode	...52
Tabela 15: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji ljudski faktor	...54
Tabela 16: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji proizvodi i tržišta	...55
Tabela 17: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji infrastruktura	...56
Tabela 18: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji informacije	...56
Tabela 19: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji finansije	...57

1. UVODNE NAPOMENE

Razumevanje bezbednosti sistema kao dinamičnog procesa u odgovoru na savremene poslovne izazove podrazumeva primenu analitičkih procesa i metoda kao segmenta upravljanja rizikom u procesu donošenja odluka u uslovima izvesnosti, rizika i neizvesnosti, što je implicitno uticalo da se upravljanje rizicima prizna kao integralna funkcija upravljanja bezbednošću, kako u velikim privrednim sistemima, tako i u manjim kompanijama. Danas se ljudsko znanje multiplikuje veoma brzo, a čovekova moć nad prirodom deluje samo prividno bezgranična. Međutim, moderan čovek, ipak, danas živi u društvu rizika (Bek, 2001) opsesivno zabrinut za svoju bezbednost i veoma osetljiv na najmanji znak njenog ugrožavanja. Iluziju ranjivosti velikih i moćnih raspršio je događaj od 11.09.2001. godine. Nove sofisticirane tehnologije nose sa sobom i nove mogućnosti za nastanak katastrofalnih događaja. Po nekim autorima one nužno, pre ili kasnije, vode u katastrofu, usled svoje kompleksnosti i čvrste povezanosti elemenata. Dosledno tome da rizik predstavlja "uvertiru" u vanrednu situaciju čije nastupanje nije određeno, sve pripreme u odnosu na negativne događaje imaju svojstvo eventualnosti, zbog brojnosti faktora koji utiču na složenost rizika, sa jedne strane, i sa druge strane njihove stalne promene. U tom smislu može se reći da rizik predstavlja meru devijacije od očekivanog ishoda.

Trend ekstremnog rasta veštine upravljanja rizicima u lancima snabdevanja, tokom poslednje dve decenije, evidententan je u formi, pre svega, modelovanja i analize problematike koja prati razvoj kompleksnih mreža kompanija, kako u zemlji, tako i na globalnom nivou. Navedena problematika je uglavnom usmerena na dizajn, planiranje i koordinaciju materijala (sirovina i finalnih proizvoda) i novčane i informacione tokove kroz lanac snabdevanja. Povećanje dinamičnosti i neizvesnosti poslovnog okruženja postavlja problem rizika na mesto ključnog interesa kompanije. Rizici u lancima snabdevanja, generalno posmatrano, najčešće nastaju usled fluktuacije (promenljivosti nabavke, potražnje i cena), prirodnih nepogoda i kriza izazvanih ljudskim faktorom (npr. teroristički napadi, neetička poslovna praksa i ekonomska recesija). Dalje, kulturološke, infrastrukturne i političke razlike u strategijama outsourcing – a, single sourcing – a i lean prakse, takođe doprinose nastanku ranjivosti lanca snabdevanja. Efektivno upravljanje rizicima postaje centralni problem opstanka i napretka kompanije u konkurentnom poslovnom okruženju. Prema tome, upravljanje rizicima u lancu snabdevanja se pojavljuje kao prirodna ekstenzija upravljanja lancem snabdevanja sa primarnim ciljem identifikovanja potencijalnih pretnji, odnosno izvora rizika, i davanjem predloga održivog akcionog plana mitigacije i potpunog uklanjanja u apstraktnoj percepciji.

Upravljanje rizicima u lancima snabdevanja počine da se formira kao poseban sistematski i kontrolisani proces unutar upravljanja lancima snabdevanja nakon gore pomenute 2001. godine, i to iz dva fundamentalna razloga: intenziviranja događaja izazvanih ljudskom (namernom i slučajnom) greškom i ekspanzijom primene novih poslovnih filozofija.

Domen istraživanja u ovoj disertaciji obuhvata rizike u lancima snabdevanja u smislu njihove kvantifikacije u cilju minimizacije posledica i održanja stabilnosti funkcionisanja sistema kroz konstantne promene poslovnih orijentacija svih tržišnih učesnika.

1.1. Predmet i problem istraživanja

Predmet istraživanja ove disertacije je kvantifikacija rizika u lancima snabdevanja. Procesi identifikovanja, analize i tretiranja rizika u lancima snabdevanja zahtevaju formalizovan pristup korporativnoj kulturi kompanije. Suština ovog procesa zasniva se na pravovremenoj reakciji na promene. Kompanije moraju biti kompetentne za sveobuhvatno sagledavanje potencijalnih rizičnih uticaja na svim nivoima poslovanja, kako bi preventivno njima upravljale. Upravljanje rizicima u lancima snabdevanja predstavlja poslovnu realnost i potrebu. Kao odgovori na potrebe i izazove okruženja, generisani su različiti koncepti modela upravljanja rizicima. Određenjem sistema koji se analizira – lanac snabdevanja, i konstatacije da je u pitanju sistem sa stohastičkim i neizvesnim ponašanjem, uvida se da je taj problem prisutan tokom celog istraživanja. Sistemskim pristupom, problem raznovrsnosti identifikovanih rizika u lancima snabdevanja će se pokušati umanjiti. Ovom disertacijom je dat predlog modela za procenu i upravljanje rizicima u lancima snabdevanja.

Detaljnou deskripcijom rizika u lancima snabdevanja i njihovim upravljanjem dat je doprinos sistematizaciji dosadašnjih saznanja teorije rizika. Takođe je predložen novi model procene i upravljanja rizicima u lancima snabdevanja, koji zapravo predstavlja opravdanost istraživanja sa naučnog stanovišta. Činjenica je da postoji potreba za daljim istraživanjima i upoznavanjem sa karakteristikama rizika u lancima snabdevanja i njihovom upravljanju. Predloženo istraživanje je opravdano i sa društvenog stanovišta, tako što doprinosi identifikovanju i upravljanju stvarnim rizicima u lancima snabdevanja savremenih kompanija.

1.2. Ciljevi istraživanja

Opšti cilj istraživanja ovog rada je sledeći: Unapređenje baze znanja o proceni i upravljanju rizicima u lancima snabdevanja.

Iz ovako definisanog cilja proizilaze sledeći zadaci istraživanja:

- Sistematizacija osnovnih teorijskih principa vezanih za upravljanje lancima snabdevanja, upravljanje rizicima i upravljanje rizicima u lancima snabdevanja.
- Generisanje liste identifikovanih rizika u lancima snabdevanja.
- Mapiranje poslovnih procesa u lancima snabdevanja.
- Generisanje liste pretnji i ranjivosti u procesima lanaca snabdevanja.
- Procena rizika primenom matematičkog modela Kinney metode i predlog mera za njihovo ublažavanje/otklanjanje.
- Procena rizika u lancima snabdevanja primenom softverskog rešenja Hestia.
- Razvoj modela za procenu rizika u lancima snabdevanja.

1.3. Polazišta – Hipoteze

Shodno predmetu i postavljenim ciljevima, istraživanje u doktorskoj disertaciji je bazirano na sledećim relevantnim hipotezama:

- Opšta hipoteza:** Moguće je automatizovati procenu rizika u lancima snabdevanja.
- Posebna hipoteza 1:** Moguće je generisati efikasan model za upravljanje rizicima u lancima snabdevanja, koji će biti kompatibilan sa generalnom strategijom upravljanja rizicima.
- Posebna hipoteza 2:** Definisani model za upravljanje rizicima u lancima snabdevanja, koji će poštovati osnovne teorijske postulate risk menadžmenta imaće potvrdu svoje aplikativnosti u realnim poslovnim sistemima.

1.4. Primenjena metodologija

16

U toku naučnog i istraživačkog rada upotrebljenje su različite metode, kako bi bili zadovoljeni osnovni metodološki zahtevi – objektivnost, pouzdanost, opštost i sistematičnost.

U skladu sa izabranom problematikom, definisanim ciljevima istraživanja i postavljenim naučnim hipotezama radi definisanja naučnih i stručnih zaključaka i iznalaženja 16 gućih rešenja upotrebljena je teorijska analiza uz korišćenje rezultata istraživanja iz međunarodne naučne literature, odnosno saznanja naučnika i drugih autora koji su istraživali problematiku upravljanja rizicima u lancima snabdevanja.

U radu su prikazana istraživanja naučno-teorijskih saznanja, relevantne literature i savremene poslovne prakse primenom sledećih naučnih metoda:

- **Metoda analize dokumenata** – pribavljanje i analiza rezultata istraživanja drugih autora koji se bave upravljanjem rizika u lancima snabdevanja. Pribavljeni podaci potiču iz domaćih i stranih doktorskih disertacija, naučnih radova i dokumentacije ISO standarda.
- **Metodom klasifikacije** je na sistematski način izvršena potpuna podela opsega pojma rizika na posebne 43 ke (rizike u lancima snabdevanja).
- **Deskriptivna metoda** usmerena je prema usavršavanju naučnih saznanja, odnosno 43 ma generalizaciji rizika u lancima snabdevanja. Ona se nije zaustavila samo na opisivanju, prikupljanju i sređivanju podataka, već obuhvata upoređivanje, vrednovanje i interpretaciju podataka.
- Koristeći **induktivno – deduktivnu metodu** rizici u lancima snabdevanja su posmatrani i utvrđeni na makro nivou - na nivou kompanije u celini i/ili pojedinih njenih delova/grana ili pak na mikro nivou – rizici koji prate prirodu, sadržaj, karakter rada, nivoe i funkciju zaposlenih.

- **Metoda kompilacije** – kao postupak preuzimanja tuđih rezultata naučno istraživačkog rada, odnosno tuđih opažanja, stavova, zaključaka i spoznaja, upotrebljena je u kombinaciji sa drugim metodama u naučno istraživačkom radu, uz obavezno navođenje citata svega ono što je od drugih autora preuzeto.
- **Matematička metoda** koja se koristi u ovom istraživanju zasniva se na Kinney metodi procene rizika, za koju su parametri rizika u lancima snabdevanja namenski prilagođeni. Pomoću nje je na egzaktn način prikazan i objašnjen model upravljanja rizicima u lancima snabdevanja.
- **Metoda studije slučaja** istražuje savremene fenomene u kontekstu realnog dešavanja, tako da su postojeća teorijska načela iskorišćena u proučavanju posmatranog fenomena upravljanja rizicima u lancima snabdevanja. Studija slučaja kao istraživačka metoda poseduje jasnu prednost u odnosu na ostale metode u situacijama kada se pitanja „kako“ ili „zašto“ postavljaju u vezi određene grupe aktuelnih događaja nad kojima istraživač poseduje malu ili uopšte ne poseduje kontrolu, što je slučaj u istraživanjima realizovanim u ovom radu.
- **Metoda modelovanja** predstavlja strukturu za rešavanje problema primenom softverskog rešenja Hestia. Metodologija je prikazana u formi niza koraka koji opisuju pojedine faze rešavanja problema, pri čemu broj koraka i redosled njihove realizacije zavisi od konkretne situacije i cilja primene odgovarajuće metodologije. Tako, ova metoda podrazumeva tri koraka:
 - (1) oblikovanje modela;
 - (2) testiranje modela; i
 - (3) analizu nalaza dobijenih upotrebom modela.Modelovanje je proces korišćenja zamene (modela) umesto realnog sistema sa ciljem da se dođe do određenog saznanja. Zamena se koristi u slučaju da je korišćenje realnog sistema teško (ili nemoguće) izvodljivo, ili suviše skupo u smislu novca, resursa, vremena, itd., što je po pitanju rizika potpuno opravdano.

U nastojanju da se istraži međusoban uticaj identifikovanih rizika na funkcionalnost lanca snabdevanja, korišćena su sva četiri tipa analize.

U tom smislu, **procesna analiza** je korišćena u opisu sledećih važnih elemenata lanca snabdevanja: menadžment materijalima, proizvodni proces, transportni proces, upravljanje informacijama, upravljanje finansijama, planiranje i predviđanje potražnje, dizajn procesa, povratni procesi i komunikacija sa okruženjem.

Uz pomoć **strukturalne analize** opisani su rizici u elementima lanca snabdevanja, kroz vrednost uticaja faktora poverljivost, integritet i dostupnost mapiranih procesa lanca snabdevanja na njegovu funkcionalnost i stabilnost.

Kauzalnom analizom opisana je uzročno – posledična relacija između utvrđenih pretnji i slabosti lanca snabdevanja.

Funkcionalnom analizom je ukazano na značaj koji pravovremeno identifikovanje i upravljanje rizicima u lancima snabdevanja imaju po stabilnost poslovanja kompanije.

1.5. Postignuti rezultati

Doprinos doktorske disertacije može se posmatrati sa naučnog i praktičnog aspekta. Teorijski doprinos rada ogleda se detaljnoj sistematizaciji postojećih istraživanja iz oblasti upravljanja rizicima u lancima snabdevanja.

Konkretno, u radu je izvršena sistematizacija osnovnih teorijskih principa iz oblasti logistike, upravljanja lancima snabdevanja, upravljanja rizicima i upravljanja rizicima u lancima snabdevanja, čime je napravljena široka teorijska podloga za definisanje koncepta rizika u lancima snabdevanja i razvoj modela za njihovo upravljanje. Na ovaj način, doktorska disertacija doprinosi postojećoj literaturi kroz pružanje novih informacija vezanih za jasno definisanje koncepta upravljanja rizicima u lancima snabdevanja, kao i informacija o načinima, tehnikama i metodama za njihovu identifikaciju, analizu i tretiranje. Sa metodološkog aspekta, doprinos disertacije ogleda se u razvoju više konceptualnih okvira i modela, kao i u predloženom načinu kombinovanja Kinney metode i softverskog alata Hestia prilikom modelovanja procene rizika u lancima snabdevanja (čija dalja unapređenja mogu da idu u pravcu uspostavljanja standarda za modelovanje i simulaciju u oblasti upravljanja lancima snabdevanja), a zatim i prilikom identifikacije, ocene i tretiranja rizika.

Predloženi konceptualni okviri omogućavaju lakše razumevanje složene strukture koncepta rizika u lancima snabdevanja i principa njihove systemske analize i upravljanja. Na taj način, razumevanjem osnovnih termina i njihovog jasnog razgraničenja i pojmovnog pozicioniranja, povećaće se kapacitet relevantnih sposobnosti neophodnih za rešavanje problema upravljanja rizicima u lancima snabdevanja.

Osnovni praktični (menadžerski) doprinos doktorske disertacije vezan je za praktičnu primenljivost razvijenog modela dokazanu prikazanom studijom slučaja, pri čemu su dalje provere aplikativnosti modela moguće i u realnim privrednim sistemima. Punu praktičnu upotrebljivost predloženog modela za upravljanje rizicima treba tražiti pre svega na planu konsaltinga i podrške odlučivanju, pošto obezbeđuje odličnu startnu poziciju za dalje razmatranje pitanja rizika u lancima snabdevanja.

88

Testiranjem predloženog modela kompanijama će biti pružena mogućnost da u pravo vreme i na pravom mestu reaguju na potencijalne rizike koji bi mogli da poremete ili prekinu neku od poslovnih funkcija. Očekivani rezultat predloženog istraživanja se ogleda u generisanju liste rizičnih događaja koji se mogu pojaviti u nekom od elemenata lanca snabdevanja, a koja će sadržati i predlog mera za njihovo ublažavanje/otklanjanje.

1.6. Kratak prikaz rada po poglavljima

Osnovna ideja autora pri koncipiranju sadržaja ove disertacija bila je da se prezentuje systemsko shvatanje rizika i stvori osnovu za razvoj metodologije za analizu i upravljanje rizikom kompleksnih sistema lanaca snabdevanja. Sledeći osnovnu ideju, materija u disertaciji je obrađena kroz sledeća poglavlja:

KVATNIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Uvodne napomene

U prvom poglavlju – uvodnim napomenama prikazani su predmet i problem istraživanja u oblasti upravljanja rizicima u lancima snabdevanja. U ovom delu disertacije navedeni su i ciljevi istraživanja, osnovna polazišta – hipoteze, primenjena metodologija i postignuti rezultati.

Drugim poglavljem je definisan kategorijalni aparat. U tom smislu predstavljeni su sledeći bazični pojmovi: logistika, lanci snabdevanja, rizici i upravljanje rizicima.

Treće poglavlje sadrži matematički model procene rizika u lancima **7** abdevanja primenom Kinney metode. Kinney metoda, koja se najčešće upotrebljava **za procenu i vrednovanje rizika, usled pojave utvrđenih OH&S opasnosti**, je su u cilju izrade ove teze aplicirana na identifikovane rizike u lancima snabdevanja. Nakon izvršene kvantifikacije, dat je predlog mera za ublažavanje/otklanjanje rizika u lancima snabdevanja.

Četvrtim poglavljem je prikazana studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia, čime se dokazuje jedna od navedenih hipoteza, procenu identifikovanih rizika u mapiranim procesima lanca snabdevanja je moguće automatizovati. Prikazani su dobijeni rezultati i dat je predlog mera za mitigaciju uočenih rizika nivoa 3, 4 i 5.

U poslednjem petom radnom poglavlju istraživanja izneti su zaključci o funkcionalnosti predloženog modela procene rizika u lancima snabdevanja primenom softverskog alata. Preispitana je opravdanost postavljenih hipoteza i razmatrene su moguće implikacije rezultata istraživanja. U ovom delu istraživanja date su i sugestije za eventualna buduća istraživanja u ovoj, kao i u srodnim oblastima.

2. TEORIJSKI OKVIR ISTRAŽIVANJA

2.1. Kategorijalni aparat

U samom naslovu disertacije "*Kvantifikacija rizika u lancima snabdevanja*" nalaze se, kako direktno, 80 o i indirektno, pojmovi koje je neophodno precizno odrediti. U tu svrhu, pojmovi su podeljeni u dve kategorije.

- U prvoj kategoriji su razvrstani pojmovi koji se odnose na opšte oblasti, kao što su: logistika, lanci snabdevanja i rizici.
- U drugoj kategoriji, centralnom mestu ovog istraživanja razvrstani su specifični pojmovi koji se odnose na kvantifikaciju rizika u lancima snabdevanja kroz matematički i softverski model: rizici, pretnje i ranjivosti u lancima snabdevanja; mapiranje poslovnih procesa u lancima snabdevanja; upravljanje rizikom; upravljanje rizikom u lancima snabdevanja; kvantifikacija rizika; Kinney metoda za procenu rizika i softversko rešenje Hestia.

2.1.1. Logistika

14

Za Logistiku se može reći da je veoma stara oblast poslovanja koja se usavršavala paralelno sa razvojem civilizacije. Svakako 14 ve zavisi od toga šta pod njom podrazumevamo. Kao stara oblast poslovanja, logističke aktivnosti srećemo kod velikih seoba naroda i brojnih ratova kojima je bila potrebna logistička podrška. U savremenim uslovima poslovanja logistika se posmatra kao mlada naučna disciplina i istovremeno kao savremena i nova oblast poslovanja (Regodić, 2014).

Logistika kao nauka i kao veština, iako predstavlja snažan alat za povećanje efikasnosti i efektivnosti poslovanja u različitim privrednim sektorima, dugo je za užu i širu naučnu, a posebno za stručnu javnost, predstavljala i još uvek predstavlja nepoznato područje. Iz toga proizlazi da logistika otkriva čitavu jednu novu paradigmu za postizanje konkurentne prednosti i da je optimizacija njenih aktivnosti značajan faktor kreiranja potražnje i proširenja tržišta. Pokretačka snaga logistike transformiše se od orijentacije ka snižavanju troškova i orijentacije na poboljšanje servisa isporuke, na sistemski pristup izučavanju složenih logističkih fenomena. Složenost, kompromisi, efikasna koordinacija, konflikti i potreba da se vodi računa o odnosima van logističkog sistema, kao implikacije sistemskog pristupa izučavanju logističkog sistema i logističkih podistema ukazuju na važnost logistike kao nauke i logistike kao aktivnosti u stvaranju pozitivnog privrednog okruženja za aktivne učesnike logističkog i privrednog sistema, za njihovu afirmaciju, za rast, razvoj, eliminisanje i neutralizovanje brojnih negativnosti logističkog sistema u celosti, koje mogu izazvati subjektivni ili objektivni faktori.

Primena interdisciplinarnih i multidisciplinarnih znanja i veština glavni su uslov za izučavanje i primenjivanje logističkih fenomena, pod kojima treba razumevati sve relevantne sadržaje i elemente koji se odnose na logistiku, odnosno logistički sistem i pripadajuće podsisteme.

Procesi političkog, tehnološkog, privrednog, kulturnog, saobraćajnog i drugog razvoja koji prelaze granice država i kontinenata, ne bi se mogli afirmisati ni dostići pripadajuće vrednosti, da nisu istovremeno praćeni i potpomognuti razvojem složenih logističkih podsistema, i to: megalogistike, globalne logistike, makro – mikro – metalogistike, inter – i intralogistike, servisne logistike, IT logistike, menadžment logistike, primarne logistike, sekundarne logistike, tercijarne logistike i logistike održivog razvoja. Bez konzistentno definisanih, izgrađenih i usaglašenih poslovnih politika (kadrovske, tržišne, proizvodne, finansijske i razvojne politike), logističke kompanije se ne mogu fokusirati na vlastite sposobnosti i mogućnosti iz mikro i makrookruženja, na stabilnost i sigurnost u poslovanju, pa, prema tome, ni na svoje efikasno i efektivno uključivanje u logistički sistem u celini.

Monitornig procesa kretanja proizvoda, usluga i informacija, koji se odvijaju u smeru ka kompanijama, unutar njih i od njih ka krajnjim potrošačima i korisnicima, iako je značajno područje privrednih delatnosti i bitan faktor u kreiranju tržišne politike privrednih subjekata, dugo vremena je bio zanemarivan, a fokus povećanja efikasnosti poslovanja bio je usmeren na područje proizvodnje, tj. tehnologija koje povećavaju efikasnost radne snage, uštedu sirovina, povećanje proizvodnje i sl. Razlog takvom pristupu je viđenje logističkih funkcija kao tradicionalnih, pomoćnih i fragmentisanih funkcija koje nisu pokazivale povratnu informaciju o troškovima ukupnih aktivnosti. Zahvaljujući sve većim mogućnostima modelovanja, a uz sve razvijeniju hardversku i softversku podršku, upravljanje logističkim sistemom kao celinom sve više postaje osnova za povećanje efikasnosti, efektivnosti i fleksibilnosti poslovanja kompanije, a time i konkurentске prednosti (Zelenika & Pupovac, 2001).

Arhaično značenje logistike kao nauke o računanju (grč. *logistikos*, "vešt u izračunavanju"), i dalje postoji u matematici kao logistička ili Fermijeva kriva, ali kao takva deluje nepovezano sa svojim savremenim značenjem. Prvo poznato pojavljivanje pojma logistike u zvaničnoj literaturi u XVIII veku je zabeleženo pri francuskoj vojsci sa značenjima "strategija" i "filozofija rata". Antoine-Henri Jomini, poznati francuski vojni mislioc i pisac, pokušao je da sa preciznošću definiše reč logistika i poveže je sa drugim elementima ratovanja. U delu *Umetnost ratovanja* (Jomini, 1862) logistika je definisana prvi put kroz savremeni okvir kao "praktična veština pomeranja snaga - osim borbe, svega ili gotovo svega u području vojnih aktivnosti". U skladu sa tim, pretpostavlja se da je reč "logistique" izvedena iz oficirskog čina "Major General des Logis", čija je obaveza bila planiranje administrativnih poslova vezanih za premeštanje snaga u francuskoj vojsci. Isto tako, Jomini tvrdi da je pojam logistika nastao od francuske reči *loger*, koja znači "stanovati", "noćiti pod vedrim nebom", "smestiti se", "ukonačiti se", "nastaniti se". Prva naučna monografija sa tematikom logistike je "Précis de l'Art de la Guerre: Des Principales Combinaisons de la Stratégie, de la Grande Tactique et de la Politique Militaire" (Jomini, 1838). Premda nastala u vojsci, radi rešavanja, proučavanja i kreiranja planova za pokretanje trupa i radi njihovog snabdevanja iz pozadine, logistika je napravila snažan prodor u sve privredne delatnosti zbog proširenja tržišta, tendencije pada racionalizacije mogućnosti u proizvodnji, želje za diferenciranjem, servisima isporuke..., da bi rešavala i odstranjivala sve ono što stoji na putu lošoj i skupoj proizvodnji i distribuciji proizvoda i usluga. Takvu tvrdnju potkrepljuje i pojašnjenje reči "logistics" u Cambridge International Dictionary of English (Procter, 2001), "pažljivo organizovanje komplikovanih vojnih i poslovnih aktivnosti tako da se odvijaju učinkovito i efektivno".

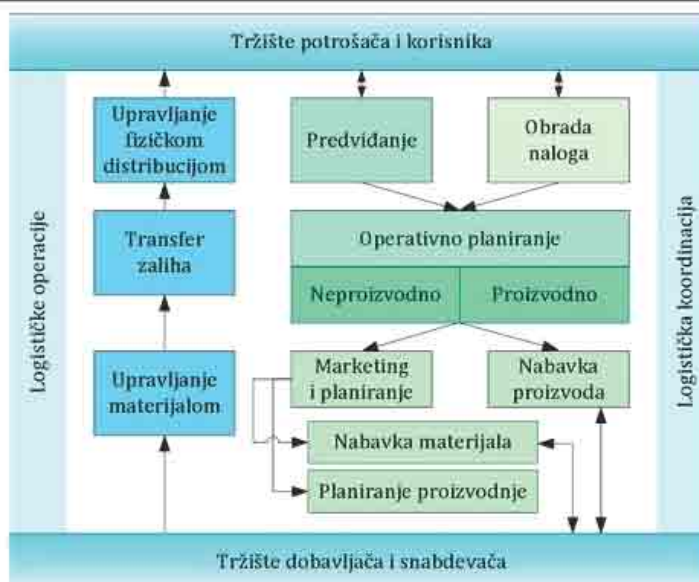
KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Krajem XIX veka izraz logistika "preselio" se i u Sjedinjene Američke Države, pa se u njihovoj vojnoj literaturi koristi u značenju "pozadinski⁷⁸ vojnih službi", odnosno "nauke o pozadinskoj vojnoj službi, tj. transportu i snabdevanju", da bi se u drugoj polovini XX veka "vratio" kao nauka o upravljanju. Logistika se kao nauka i kao veština veoma brzo razvijala i afirmisala u civilnom, odnosno u privrednom sektoru, i to u mnogo širem i suptilnijem značenju, posebno kao interdisciplinarna i multidisciplinarna nauka koja se izučava i primenjuje u gotovo svim ljudskim aktivnostima.

Logistički sistemi doživljavaju ubrzani razvoj tokom II svetskog rata (1939 – 1945). Tokom ratovanja, SAD i članice alijanse su pokazale mnogo veći stepen efikasnosti od Nemaca. Skladišta nemačke vojske bila su konstantno uništavana, a ista ta vojska nije mogla da uzvрати istom merom, između ostalog i zbog dobro poznate taktike vode Adolfa Hitlera. Američke trupe su se mogle snabdeti svim potrebnim resursima, na pravom mestu i na najekonomičniji način. Od tog perioda, tehnike vojne logistike započinju pravu ekspanziju. Postepeno, logistika počinje da se razvija kao veština i kao naučna disciplina.

Slika 1: Logistički sistem



Izvor: Prilagođeno prema: Leo A.P. Moerkens, L., Pollock, W. (2000) *A Structured Approach to Logistics Improvement, Computer Service & Repair*

Danas, logistički eksperti realizuju svoje zadatke zahvaljujući primeni stečenih veština, iskustava i znanja. U savremenom poslovnom sistemu, obaveza menadžera logistike je da obezbedi svrsishodan i efika⁷⁹ logistički sistem. On garantuje da će prava dobra biti dostavljena pravom korisniku, u pravo vreme, na pravom mestu i na najekono mičniji način. Iako izaziva dilemu kod mnogih kompanija, logistika kao naučna disciplina može obezbediti značajnu pomoć. U savremenom poslovnom okruženju, logistika predstavlja

konkurentsku strategiju koja kompanijama može da pruži ostvarenje očekivanja krajnjih korisnika. Logistika obezbeđuje efikasnu integraciju članova lanca snabdevanja. Logistika se ne sastoji od jedne komponente, već uključuje grupe različitih aktivnosti i disciplina poput nabavke, planiranja, koordinacije, skladištenja, distribucije i korisničkog servisa¹.

Logistika se definiše na veliki broj relativno različitih načina, što je posledica visoke dinamičnosti i složene prirode kako samog logističkog konteksta (različite poslovne oblasti) tako i logističkog okruženja. U ovoj disertaciji, fokus će biti na nekoliko definicija, datih od strane udruženja i pojedinaca, za koje autor smatra da na najbolji način doprinose razumevanju koncepta logistike.

"Logistika je upravljanje svim inbound i outbound materijalima, poluproizvodima, sirovinama i gotovim proizvodima. Logistika se sastoji od integrisanog upravljanja nabavkom, transportom i skladištenjem na funkcionalnom nivou. Na nivou kanala, logistiku čini upravljanje u kanalima koji prethode proizvodnji, proizvodnim i postproizvodnim kanalima. Termin logistika treba razlikovati od termina fizička distribucija koji se odnosi samo na postproizvodne kanale." (Cavinato, 1982). Navedena definicija je značajna, jer među prvima pravi razliku između pojmova fizička distribucija i logistika na način da logistiku predstavlja kao širi pojam koji obuhvata ne samo tokove izlaznih materijala, nego i ulazne tokove roba za posmatranu kompaniju (Maslarić, 2014).

8

Institut za logistiku i transport definiše logistiku kao *"proces upravljanja transportom, zalihama, skladištenjem i informacijama o dobrima i materijalima od izvora do mesta finalne potrošnje"* (The Chartered Institute of Logistics and Transport, 1998). Ova definicija inkorporira četiri najveća i najvažnija podsistema logistike – transport, zalihe, skladištenje i informacije.

8

Definicija logistike jednog od najeminentnijih udruženja profesionalaca u oblasti logistike i upravljanja lancima snabdevanja, neprofitne poslovne organizacije glasi: *"Logistika je deo upravljanja lancem snabdevanja koji obuhvata proces planiranja, i kontrole efikasnih i troškovno-efektivnih tokova materijala, skladištenja robe, usluga i njima pripadajućih informacionih tokova od mesta izvora do mesta potrošnje sa ciljem zadovoljenja zahteva krajnjih korisnika"* (CSCMP, 2015).

Evropska logistička asocijacija definiše logistiku kao *"organizaciju, planiranje, kontrolu i realizaciju tokova materijalnih dobara od nabavke sirovina, preko proizvodnje i distribucije do krajnjih korisnika sa ciljem zadovoljenja tržišnih zahteva uz minimalne troškove i minimalno vezan kapital"* (ELA, 2015), dok guru savremene logistike, profesor emeritus Martin Christopher definiše logistiku na sledeći način: *"Logistika je proces strateškog upravljanja nabavkom, transferom i skladištenjem sirovina, poluproizvoda i gotovih proizvoda (i pripadajućih tokova informacija) kroz organizaciju i njene marketinške kanale na takav način koji će maksimizirati sadašnju i buduću profitabilnost preko troškovno efikasnog zadovoljenja zahteva potrošača"* (Christopher, 1998). Poslednje dve definicije govore o neophodnosti realizacije logističkih aktivnosti na način koji će obezbediti što manje trošenje finansijskih sredstava. Navedeno ukazuje na činjenicu da

¹ <http://www.bestlogisticsguide.com/logistics-history.html> [18.01.2015.]

je logistika, pored toga što predstavlja fundamentalnu i esencijalnu odliku svih ekonomskih aktivnosti, i veoma skupa. Okvirne vrednosti troškova logistike se kreću oko 15-20% od ukupnog prometa na nivou kompanija ili oko 10-20% od ukupnog BDP-a, na nivou država (Waters, 2007). Naravno, treba ukazati i na postojanje čuvene "7P" odrednice logistike, koja podrazumeva sve aktivnosti kojima se obezbeđuje da "prava roba, u pravo, vreme, na pravom mestu, u pravoj količini, po pravoj (najboljoj) ceni, pravog kvaliteta, stigne do pravog (odgovarajućeg) kupca", navođene od strane velikog broja autora i nastale iz prvobitne "4P" odrednice logistike: "prava roba, u pravo vreme, na pravom mestu, za pravog kupca".

Podloga za razumevanje poslovne logistike je teorija sistema čija je osnovna zamisao da glavni problem nije u optimizaciji posebnih područja poslovanja, već u optimizaciji poslovnog sistema kao celine (Bulatović, 2013).

Na osnovu prezentovanih definicija može se izvesti generalni zaključak da se pod logistikom podrazumevaju sve aktivnosti vezane za prostornu i vremensku transformaciju roba i usluga.

2.1.2. Lanac snabdevanja

Lanac snabdevanja se sastoji od **26** kompanija koje su uključene (direktno ili indirektno) u zadovoljavanje zahteva potrošača. Lanac snabdevanja ne uključuje samo proizvođača i dobavljače, već transportne i kompanije skladište robu, trgovce na malo i same potrošače. Unutar svake organizacije lanac snabdevanja uključuje sve funkcije koje **26** u vezi sa ispunjenjem zahteva potrošača. Pored ostalog, ove funkcije obuhvataju: razvoj novih proizvoda, marketing, proizvodne operacije, distribuciju, finansije i pružanje usluga potrošačima (Regodić, 2014).

Uopšteno se može reći da lanac snabdevanja čini:

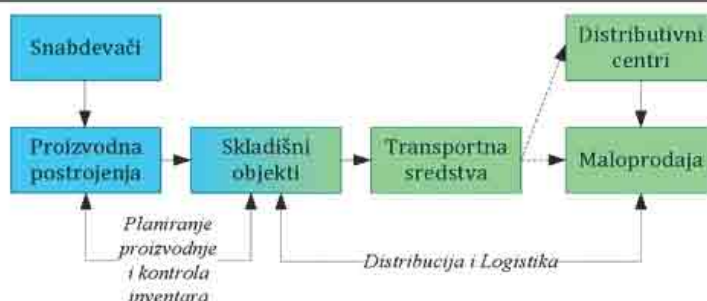
1. niz entiteta (snabdevači, proizvođači, distributeri, prodavci na malo i krajnji korisnici - kupci) koji su fizički i geografski udaljeni, a čija dobra/usluge se skladište ili konvertuju u novčanu vrednost i
2. koordinisani set aktivnosti koji uključuje nabavku sirovina, proizvodnju među - i finalnih proizvoda, kao i njihovu dalju distribuciju do krajnjih korisnika unutar i van lanca (Ravindran & Warsing, 2012).

U lancu snabdevanja se manifestuje stalni tok informacija, proizvoda i novca između različitih kompanija. Svaka kompanija u lancu izvršava različite procese i povezana je sa drugim kompanijama u tom lancu. Osnovna svrha postojanja bilo kog lanca snabdevanja jeste da on zadovolji potrebe kupca u procesu stvaranja sopstvenog profita. Aktivnosti lanca snabdevanja počinju sa porudžbinom kupca i završavaju se kada zadovoljan kupac plati kupljenu robu (Regodić, 2014). Cilj svakog lanca snabdevanja je da maksimizira ukupnu proizvedenu vrednost. Vrednost koju generiše lanac snabdevanja jeste razlika između vrednosti finalnog proizvoda za potrošača i izdataka koji nastanu zbog zadovoljenja zahteva potrošača. Kod većine lanaca snabdevanja, vrednost će biti u korelaciji sa profitabilnošću lanca snabdevanja, tj. sa razlikom između ostvarenih prihoda od kupaca i ukupnih troškova lanca snabdevanja. Na slici 2. prikazani su osnovni procesi unutar lanca snabdevanja kroz okvir transformacije sirovina u finalni proizvod.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Slika 2: Procesi u lancu snabdevanja

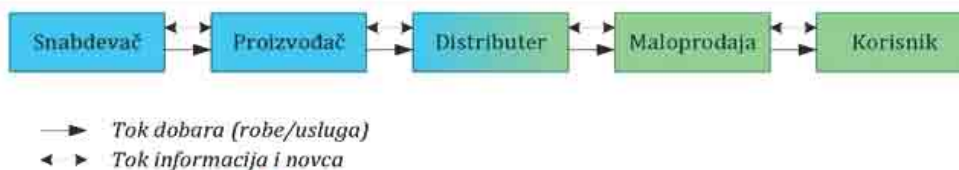


23

Izvor: Prilagođeno prema: Beamon, B. (1998) *Supply chain design and analysis: Models and methods*. International Journal of Production Economics.

Kao posledica međusobnog povezivanja organizacija u cilju povećanja nivoa usluga kupcima, učešća na tržištu i profita, 1980-ih pojavio se pojam lanac snabdevanja. Lanac snabdevanja čine sekventno povezane organizacije, kao i aktivnosti uključene u kreiranje i omogućavanje dostupnosti proizvoda klijentima. Isto tako, lanac snabdevanja se može tretirati kao lanac vrednosti, budući da dobavljači, proizvođači, prevoznici i ostali njegovi članovi dodaju vrednost. Ako se iste aktivnosti posmatraju u obrnutom smeru, lanac snabdevanja se može tretirati i kao lanac tražnje. Umesto uobičajenog linearnog prikazivanja, lanac snabdevanja može da se prikaže kao višedimenzionalna mreža entiteta koji sarađuju (slika 3). Takva mreža može da se potpunije shvati ako se ona tretira kao sistem, s obzirom da sistemski prilaz naglašava interakcije između različitih entiteta (Christopher, 2005).

Slika 3: Bazični lanac snabdevanja



29

Izvor: Prilagođeno prema: Chopra, S., Meindl, P. (2014) *Supply Chain Management: Strategy, Planning, and Operation*. 6th ed. New York: Prentice Hall.

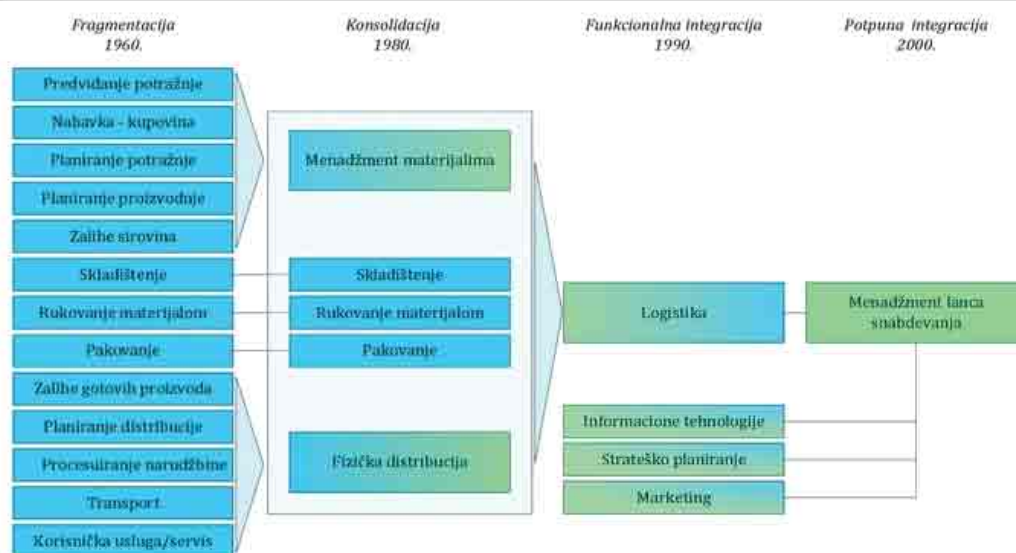
Lanac snabdevanja čine sve neposredno i posredno uključene organizacije, sa ciljem zadovoljavanja potreba krajnjeg korisnika (Chopra & Meindl, 2014).

U teoriji o logistici i lancima snabdevanja ovi različiti entiteti se označavaju kao veze (npr. usluge transporta) i čvorovi (npr. skladišta). Veze i čvorovi mogu, u isto vreme, igrati različite uloge u više lanaca snabdevanja. Isto tako, termin "ešalon" (*echelon*) se ponekad koristi za označavanje različitih delova lanca snabdevanja (Milovanović et al, 2011).

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Slika 4: Evolucija lanca snabdevanja



29

Izvor: Prilagođeno prema: Chopra, S., Meindl, P. (2014) *Supply Chain Management: Strategy, Planning, and Operation*. 6th ed. New York: Prentice Hall.

Kao i kod termina logistike, i kod lanaca snabdevanja važi pravilo da ne postoji jedinstvena definicija. Tokom poslednjih decenija, kako je ova oblast dobijala na značaju, tako se i povećavao naučno priznatih definicija.

APICS (Profesionalna asocijacija za lance snabdevanja i operativni menadžment) opisuje lanac snabdevanja kao "1. procese koji povezuju inicijalne sirovine i krajnje korisnike gotovog proizvoda preko dobavljača, i 2. funkcije unutar i van kompanije koje stvaraju vrednost kompaniji, a krajnjem korisniku obezbeđuju uslugu" (Cox & Blackstone, 1998).

Drugi izvor definiše lanac snabdevanja kao "mrežu entiteta povezanih tokom materijala. Ovi entiteti mogu da uključuju snabdevače, prevoznike, proizvodne lokacije, distributivne centre, trgovce i krajnje korisnike" (Lummus & Alber, 1997).

"Lanac snabdevanja predstavlja skup tri ili više entiteta (organizacija ili pojedinaca) neposredno uključenih u tokove proizvoda, usluga, novca i/ili informacija od izvora do krajnjih kupaca" (Mentzer et al., 2001)

"Lanac snabdevanja predstavlja mrežu organizacija koje su uključene, uzvodnim i nizvodnim vezama, u različite procese i koje stvaraju vrednost u vidu proizvoda ili usluga usmerenih ka krajnjem korisniku ili potrošaču" (Rogers & Tibben-Lembke, 2005).

Zakonodavni okvir Republike Srbije ne poznaje termin lanac snabdevanja, najbližnji ovom terminu je izraz lanac isporuke, koji takođe nije definisan, ali se spominje u kontekstu: "...distributer je pravno lice ili preduzetnik ..., koje je uključeno u lanac

...

69

isporuke...” (Zakon o tehničkim zahtevima za proizvode i ocenjivanju usaglašenosti, 2009).

Na osnovu prezentovanih definicija može se izvesti generalni zaključak da se pod lancem snabdevanja podrazumevaju sve aktivnosti vezane za transformaciju roba i usluga, u cilju zadovoljenja potreba krajnjeg korisnika i stvaranja vrednosti za kompanije, članice lanca.

2.1.3. Rizik

U različitim kulturama, pojam rizik ima različit značaj i konotaciju. Jedna od najstarijih svetskih civilizacija i kultura, kineska, pojam rizik predstavlja kao kombinaciju simbola za opasnost i šansu. S druge strane, moderna američka kultura, izgrađena na preduzetništvu i privatnoj inicijativi, u svoj svakodnevni život je uvela izreku: “*No risk, no profit*”, za koju se pre može reći da rizik posmatra sa pozitivnog stanovišta. Ipak, za srpsku, a može se reći i za kulturu većine evropskih naroda, rizik ima negativnu konotaciju (Molnar & Matotek, 2014).

Pojam rizika je fascinantna do te mere da zaokuplja veliki broj naučnika i teoretičara još od perioda renesanse, pa sve do savremenog doba u kojem je usvojen kao standard. Od izraza koji je označavao otisnuti se u neobeležena mora i u neizvesnost (Vujaković, 1980) do stava u kojem rizik predstavlja poznatu, merljivu i predvidivu kategoriju. Međutim, kvantifikacija rizika samo sa stanovišta ljudske prirode je vrlo kompleksna i zavisi od aspekta posmatranja. U drugoj polovini XX veka došlo je do ekspanzije bihejviorizma koji je takoreći dotakao sve društvene nauke. Sproveden je veliki broj studija i analiza ljudskog ponašanja, stavova i odlučivanja u različitim situacijama. Sklonost ka preuzimanju rizika varira počev od geografskog položaja, kulture, ekonomskog stanja i položaja, sve do individualnih karakteristika svakog ljudskog bića. Ono što se svakako može uzeti kao centralna karakteristika je averzija prema riziku i preuzimanju rizika (Post et al., 2008).

Obzirom na sveprisutnost rizika u svakoj ljudskoj aktivnosti, iznenađujuće je da ne postoji konsenzus o tome kako definisati rizik. U cilju postavljanja jasne granice između merljivih i nemerljivih neizvesnosti, uveden je termin rizik, koji se odnosi na prošla, i termin neizvesnost, koji se odnosi isključivo na buduća stanja posmatranog sistema. U zavisnosti od aspekta posmatranja vanrednih događaja, možemo koristiti sledeće sintagme: “*rizik gubitka*” i “*neizvesnost dobitka*” izražene objektivnom i/ili subjektivnom verovatnoćom nastanka. Zadržavajući nivo opštosti pri određivanju pojma, rizik se može definisati kao “*objektivna verovatnoća gubitka, i neizvesnost kao subjektivna verovatnoća očekivanog povoljnog ishoda*” (Kinght, 1921).

Rizik se može objasniti kao stohastička pojava. Rizični događaj ima veličinu pojave i verovatnoću pojave na nekom području u određenom vremenskom razdoblju. Rizik takode predstavlja potencijalni problem ili potencijalnu priliku. U oba slučaja pojavljuje se u svim sferama poslovanja jedne kompanije, pa ga je stoga neophodno analizirati i pronaći prave načine upravljanja njime. Po ISO terminologiji rizik je *Kombinacija verovatnoće nekog događaja i njegove posledice* (ISO 31000, 2009).

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

2

Oxfordski engleski rečnik definiše rizik kao *verovatnoću ili mogućnost opasnosti, gubitka, povrede ili druge štetne posledice* i u drugim navodima kao *izloženost opasnosti*². U tom kontekstu, rizik se koristi da označi negativne posledice. Međutim, preuzimanjem rizika se može doći i do pozitivnog ishoda. Treća mogućnost je ta da je rizik povezan sa neizvesnošću ishoda (Hopkin, 2012).

2

Dakle, definicije rizika se mogu naći u više verzija. Tradicionalno, rizik se definiše na osnovu neizvesnosti i gubitka. Takva jedna definicija je opisana kao *neizvesnost ostvarivanja gubitka* (Rejda & McNamara, 2014). Ukoliko postoji rizik, moraju postojati makar dva moguća ishoda. Ako se unapred zna da se gubitak neće ostvariti ili da će se ostvariti u potpunosti, onda rizik ne postoji. To je posledica neizvesnosti i nedostatka znanja o budućim dešavanjima. Verovatnoća događaja koji su neo stvarivi jednaka je nuli, dok verovatnoća da će se dogoditi izvesni događaj jednaka je broju jedan. U terminologiji verovatnoće, neizvesnost znači da se verovatnoća procenjuje između 0 i 1. Upravo zbog toga neki autori izjednačavaju neizvesnost i rizik (Ostojić, 2007).

2

Kada je reč o osiguravajućim društvima, rizik se definiše na osnovu određenog broja gubitaka i njihov iznos predstavlja iznos predviđenih gubitaka, pa definicija može glasiti da je rizik *verovatnoća negativnog odstupanja gubitaka od očekivanog ishoda, odnosno, rizik je stanje u kom postoji mogućnost negativnog odstupanja od željenog ishoda koji očekujemo ili kojem se nadamo* (Vaughan & Vaughan, 2000).

2

Alternativne definicije su uvedene iz razloga da se ukaže na široki spektar rizika koji mogu uticati na različite organizacije. Institut za menadžment rizikom³ definiše rizik kao *kombinaciju verovatnoće događaja i njihovih posledica*. Posledice mogu varirati od pozitivnih do negativnih.

2

Međunarodni priručnik koji obuhvata definicije vezane za rizike, ISO Priručnik 73, definiše rizik kao *efekat neizvesnosti u odnosu na ciljeve* (ISO, 2009). Ovaj priručnik objašnjava da efekat može biti pozitivan, negativan ili predstavlja odstupanje od očekivanog. Ove tri vrste događaja povezane sa rizicima mogu biti opisane kao prilika (mogućnost), hazard (opasnost) ili neizvesnost kako se i navodi u tabeli 1. Tu su date neke od definicija koje se široko primenjuju u poslovnom svetu rizika.

2

Rizik u organizacijskom kontekstu je obično definisan kao nešto što može uticati na ispunjenje korporativnih ciljeva. Međutim, korporativni ciljevi nisu u potpunosti navedeni u većini organizacija i teško ih je materijalizovati. Da bi se rizik materijalizovao, događaj se mora dogoditi. Ukoliko se fokus stavi na ove događaje, javlja se i veća verovatnoća uspešne primene procesa rizik menadžmenta. U taj proces spadaju faze poput identifikacije događaja koji mogu uticati na ostvarivanje ciljeva, analize i evaluacije da bi se umanjila ili izbegla šteta nastanka negativnih ishoda. Zatim se izabere adekvatan način upravljanja rizicima. Sve završava fazama monitoringa i pravljenjem izveštaja o uspešnosti ispunjenja zacrtanih ciljeva, uz kontinuiranu kontrolu problematičnih pozicija.

² <http://www.oxforddictionaries.com/definition/english/risk> [10.12.2014.]

³ <https://www.theirm.org> [12.12.2014.]

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Tabela 1: Najčešće definicije rizika koje se upotrebljavaju u poslovnom svetu

ORGANIZACIJE	DEFINICIJE RIZIK
ISO Priručnik 73 ISO 31000	Utica neizvesnosti na ciljeve. Ti efekti mogu biti pozitivni, negativni ili odstupati od očekivanog. Takođe, rizik se često opisuje na osnovu događaja, promene u okolnostima, ili posledica aktivnosti.
Institut za rizik menadžment (IRM)	Rizik je kombinacija verovatnoće događaja i njihovih posledica. Posledice mogu varirati od pozitivnih do negativnih.
„Orange Boo“ iz HM Treasury	Neizvesnost ishoda, u rasponu izloženosti, koja proizilazi iz kombinacije uticaja i verovatnoće potencijalnih događaja.
Institut internih revizora (IIA)	Neizvesnost događaja koji bi se mogao desiti i uticati na ostvarivanje ciljeva. Rizik se meri u smislu posledica i verovatnoće.
Alternativna definicija	Događaj sa mogućnošću uticaja (sprečavanja, povećavanja ili uzrokovanja sumnje) na ispunjenje misije, strategije, projekata, rutinskih procesa, ciljeva, temeljnih procesa i potreba stakeholdera.

Izvor: Prilagođeno prema: Vaughan, E.J., Vaughan, T.M. (2000) *Essentials of insurance : a risk management perspective*. 10th ed. Zagreb: Mate.

Najpopularniji i najpoznatiji akademski rečnik, sa više od pola miliona izraza, Websterov rečnik, na primer, rizik definiše kao „izloženost opasnosti“⁴

Za svaku kompaniju u procesu realizacije poslovanja postoji mogućnost nastupanja nepredvidivih događaja koji mogu direktno uticati na ostvarivanje očekivanih rezultata. Rizik sa svojim štetnim posledicama može onemogućiti uspešno poslovanje i negativno uticati na očekivane poslovne rezultate u razmeni dobara i usluga. Politika osiguranja od rizika, kod savremenih kompanija, predstavlja sastavni deo poslovne politike. Spoznaja rizika, uzroka njihovih pojava i posledica koje prouzrokuju, bitan je uslov za sprečavanje mogućih šteta. Sprečavanje mogućih šteta se postiže odgovarajućim instrumentima i načinima odgovora na rizike.

Različiti autori različito definišu pojam rizika. Takođe, postoje varijacije definicije rizika u zavisnosti od aspekta posmatranja. Zajedničko za sve definicije je da rizik predstavlja događaj koji može uticati na postizanje definisanog poslovnog cilja. S obzirom da se termin rizika najviše vezivao za bankarski i sektor osiguranja, rizik se ranije najčešće posmatrao kao negativna pojava. Za razliku od prošlih vremena, danas se rizik posmatra kao odstupanje od željenog stanja koje može imati pozitivne i/ili negativne efekte na postizanje ciljeva (ISO 31000:2009).

Onoga trenutka kada se na bilo koji način želi utvrditi mera opasnosti od štetnog događaja u nekom sistemu, moraju se utvrditi granice tog sistema, a takođe se mora ograničiti i vreme u kome se mera opasnosti utvrđuje (Adamović et al., 2008). Sistem se može definisati kao totalni skup interaktivnih elemenata, koji je, ukoliko ga posmatramo kao izdvojenu celinu, u interakciji sa određenom sredinom – okruženjem (Černiček & Molnar, 2012). Granice sistema obezbeđuju osnovu za bezbednost svih akcija unutar sistema (Sizemore, 2003).

⁴ <http://www.totodefinition.com/search.php?word=risk> [04.02.2015.]

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Pregled definicija rizika prema zakonodavnom okviru Republike Srbije dat je u tabeli 2.

Tabela 2: Definicije rizika u okviru zakonskih akata Republike Srbije

NAZIV PRAVNOG AKTA	DEFINICIJA RIZIKA
Zakon o vazdušnom saobraćaju (Sl. Glasnik RS, br. 73/2010, čl 3.)	Rizik je kombinacija verovatnoće ili učestalosti ponavljanja određene opasnosti i ozbiljnosti 4.1 edice koju ta opasnost može da izazove;
Carinski zakon (Sl. Glasnik RS, br. 18/2010 i 111/2012, čl 5.)	Rizik je verovatnoća nastajanja događaja u vezi s 4.1 šenjem, iznošenjem, tranzitom, prenosom ili krajnjom upotrebom robe, kao i u vezi s robom koja nema status domaće robe, ...
Zakon o javnom zdravlju (Sl. Glasnik RS, br. 72/2009, čl 2.)	7. rizik jeste određeni nivo verovatnoće da neka aktivnost, direktno ili indirektno, izazove opasnost po životnu sredinu, život i zdravlje ljudi;
Zakon o tajnosti podataka (Sl. Glasnik RS, br. 104/2009, čl 2.)	Bezbednosni rizik je stvarna mogućnost narušavanja bezbednosti tajnih podataka;
Predlog Zakona o klasifikaciji informacija (2007, čl 2.)	Bezbednosni rizik je stvarna mogućnost narušavanja bezbednosti tajnih informacija;
Zakon o zaštiti životne sredine (Sl. Glasnik RS, br. 135/2004, 36/2009, 72/2009 i 43/2011, čl 3.)	Rizik jeste određeni nivo verovatnoće da neka aktivnost, direktno ili indirektno, izazove opasnost 33. životnu sredinu, život i zdravlje ljudi;
Zakon o veterinarstvu (Sl. Glasnik RS, br. 91/2005, čl 3.)	Rizik jeste određeni nivo verovatnoće pojavljivanja 33. izne bolesti ili prisustva štetnih materija, koji direktno ili indirektno u određenom stepenu mogu da ugroze zdravlje životinja ili ljudi;
65. Zakon o bezbednosti i zdravlju na radu (Sl. Glasnik RS, br. 101/2005, čl 4.)	Rizik jeste verovatnoća nastanka povrede, oboljenja 19. štećenja zdravlja zaposlenog usled opasnosti;
Zakon o opštoj bezbednosti proizvoda (Sl. Glasnik RS, br. 41/2009, čl 4.)	Ozbiljan rizik jeste svaki rizik koji zahteva hitno postupanje nadležnih organa, uključujući i rizik čije 19. edice nisu trenutne, odnosno neposredne, a čija se ozbiljnost procenjuje naročito na osnovu ozbiljnosti mogućih posledica po zdravlje i bezbednost potrošača i drugih korisnika, kao i na osnovu učestalosti tih posledica;
Zakon o Fondu za razvoj Republike Srbije (Sl. Glasnik RS, br. 36/2009, 88/2010 i 5/2015, čl 12.)	Rizik je mogućnost nastanka negativnih efekata na finansijski rezultat i kapital Fonda usled promena kamatnih stopa.
Zakon o bezbednosti hrane (Sl. Glasnik RS, br. 41/2009, čl 4.)	78. k jeste faktor verovatnoće štetnog uticaja na zdravlje i ozbiljnost tog uticaja, kao posledice postojanja opasnosti.

Izvor: autor, podaci preuzeti sa <http://www.parlament.gov.rs/narodna-skupstina-.872.html>

Na osnovu izloženog, može se zaključiti da **rizik predstavlja proizvod pozitivne verovatnoće pojave smetnje koja će uticati na funkcionisanje sistema i evidentnih ili neevidentnih posledica po stabilnost sistema**. Autor je stavio akcenat na odrednicu "pozitivna verovatnoća" vodeći se očiglednim postojanjem "crnih labudova" koji podrazumevaju događaje koji su retki (nepredvid 9) i neočekivani. Ili, prema Talebu, crni labud je kombinacija slabe predvidivosti (usled naših zabluda o izglednosti

iznenađenja) i snažnog uticaja. Posmatrano iz drugog ugla, crni labud predstavlja i nešto veoma očekivano⁹ a što se ipak nije dogodilo. Crni labudovi su objašnjivi, ali uvek naknadno (npr. internet, Prvi svetski rat, personalni kompjuter, napad 11. septembra 2001. u SAD-u i slično). Sve što nas okružuje i što je važno za život ljudi podleže dinamici crnog labuda. Dodatnu težinu celoj stvari daje to što ljudi imaju sklonost da se ponašaju kao da crni labud ne postoji (Taleb, 2007).

2.2. Rizici u lancima snabdevanja

Funkcija upravljanja lancem snabdevanja suočava se sa izazovima koje pred nju postavljaju rizici iz internog i eksternog okruženja svih članova lanca snabdevanja. Posledice izazvane rizicima mogu biti različitog intenziteta, od neprimetnih do katastrofalnih. Prema usvojenoj definiciji, rizik predstavlja proizvod pozitivne verovatnoće pojave smetnje koja će uticati na funkcionisanje sistema i evidentnih ili neevidentnih posledica po stabilnost sistema, pri čemu se pod smetnjom u kontekstu lanca snabdevanja mogu grupisati dve kategorije. Prva kategorija smetnji su prirodne i druge katastrofe koje ne predstavljaju rezultat organizovanog sprovođenja poslovne aktivnosti. Drugu kategoriju predstavljaju aktivnosti koje realizuju pojedini članovi lanca snabdevanja, a koje su usmerene ka poslovnim ciljevima.

Ono što je karakteristično za navedene aktivnosti je to da se prilikom njihovog planiranja, organizacije, realizacije i kontrole, rizici ne razmatraju povezano. Ovakva situacija predstavlja plodno tle za pojavu i rast rizika u lancu snabdevanja, gde pojedini članovi lanca ne sagledavaju kako rizike kojima mogu biti direktno izloženi, tako i indirektno rizike povezane sa rizičnim događajima koji se potencijalno mogu ostvariti kod drugih članova u lancu, a čije posledice će imati uticaja i na poslovanje posmatranog člana u lancu (Maslarić, 2014).

Koncept rizika u lancima snabdevanja može se definisati kao izloženost rizičnim događajima koji negativno utiču na operativnost lanca snabdevanja, a samim tim i na njegove performanse kao što su nivo usluge korisniku, troškovi ili mogućnost brzog odgovora (Tummala & Schoenherr, 2011).

Istraživanja rizika u interakciji između pojedinih članova industrijskih logističkih lanaca (odnos kupac-prodavač) su počela polovinom XX veka (Robinson et al., 1967). Krajem XX veka nastaju prvi ozbiljniji radovi na temu odnosa rizika i upravljanja lancima snabdevanja. Osnovni problem na početku svih ovih istraživanja bio je definisanje i razumevanje samog koncepta rizika u lancima snabdevanja.

Pregledom relevantne literature iz oblasti, može se zaključiti da se pod rizicima u lancima snabdevanja najčešće podrazumevaju:

"Događaji koji mogu izazvati odstupanje od planiranih ishoda i ciljanih događaji sa negativnim ekonomskim posledicama" (Pfohl et al., 2010).

"Potencijalni incidenti povezani sa problemima individualnih snabdevača ili poremećajima na tržištu nabavke, čiji ishodi dovode do nemogućnosti kompanije koja nabavlja robu da

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

zadovolji zahteve svojih potrošača ili čak ugrožava njihovu bezbednost" (Klimov & Merkurjev, 2006).

"Štete, definisane verovatnoćom realizacije, koje su posledica događaja unutar kompanija, lanca snabdevanja ili okruženja koje negativno utiču na poslovne procese više od jedne kompanije unutar lanca snabdevanja" (Kersten et al., 2007).

Na osnovu navedenog, moguće je izvesti zaključak da ne postoji jedinstvena definicija rizika u lancima snabdevanja, ali da je moguće izdvojiti dva osnovna pravca u samom razumevanju koncepta rizika: posmatranje rizika kao neizvesnosti (definisanje rizika zasnovano na primeni teorije odlučivanja u uslovima povećane neizvesnosti) i kao određene forme negativnih promena (smetnji) koje utiču na stabilno funkcionisanje sistema (Maslarić, 2014).

Taksonomija rizika u lancima snabdevanja moguća je u odnosu na više kriterijuma. U odnosu na oblast izlaganja, riziku su izloženi:

- ljudski faktor,
- tehnologija,
- okruženje i
- poslovni procesi (Matotek & Regodić, 2015).

U odnosu na izvor rizik može biti operativni – dolazi od funkcionisanja kompanije i teški – dolazi od poslovnih, socijalnih, političkih, ekonomskih i tehnoloških faktora. Spremnost promene je u neposrednoj vezi sa stavovima zaposlenih prema riziku. Stav zaposlenog prema riziku postaje pozitivan ukoliko se razlika između postojećeg stanja i stanja koje će prouzrokovati promena realno opaža, i na osnovu stvarnosti izabere mogućnost koja na najbolji mogući način objašnjava promenu ili problem. Određena verovatnoća kojom se pojedinac uključuje u aktivnost, kao i sopstveno uverenje o ishodu, uz osobine ličnosti, mogu se uzeti kao osnovni preduslovi za formiranje pozitivnog stava prema riziku (Grubić – Nešić, 2005). Ponašanje pojedinca u organizaciji je u funkciji kulturoloških, obrazovnih i ostalih ličnih karakteristika i ne može se uopštavati kao jedinstven obrazac.

Duž lanca snabdevanja, kompanije različitog industrijskog profila, veličine i vlasničke strukture moraju da rade zajedno kako bi postigle zajednički cilj. Njihovi različiti interesi moraju da budu integrisani konzistentnom politikom upravljanja rizikom. Slika 5. ilustruje dve različite vrste rizika u lancu snabdevanja: interne i eksterne rizike. Eksterni rizici su rezultat interakcije lanca snabdevanja sa okruženjem, a interni proizilaze iz interakcije partnera u lancu snabdevanja.

Teorijski okvir istraživanja

[illegible]

Izvor: autor

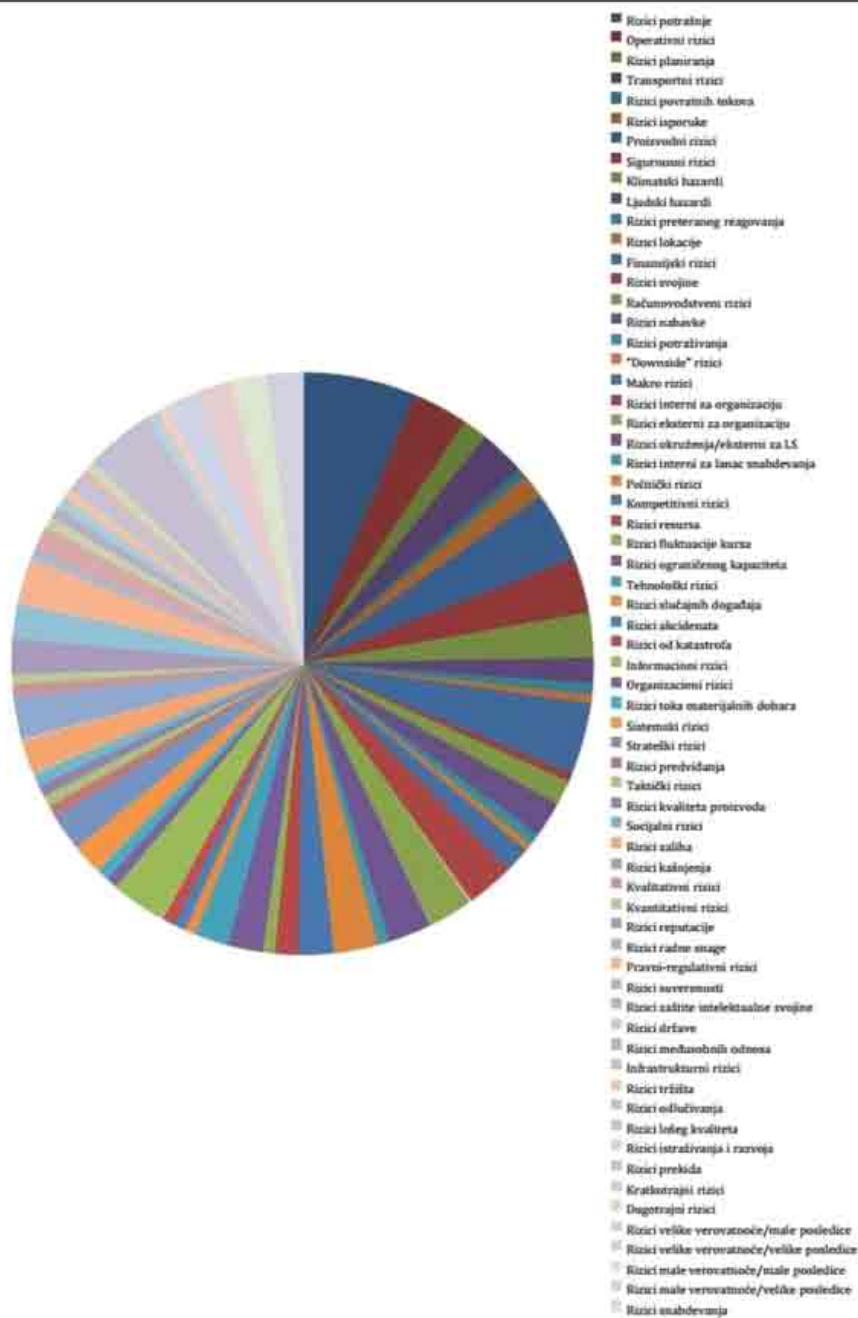
- Vodeni rizici vezani za neizvesnu potražnju ili pogrešno shvaćene zahteve kupca (veleprodaja, maloprodaja) ili krajnjeg kupca.
- Rizici snabdevanja vezani za smetnje u protoku materijala/proizvoda u okviru lanca snabdevanja.
- Rizici okruženja koji su posledica uticaja/šokova izvan lanca snabdevanja.
- Poslovni rizici vezani za različite faktore kao što su finansijska ili stabilnost upravljanja dobavljačima.
- Fizički rizici vezani za stanje fizičkih objekata isporučioaca materijala.

- Rizici neizvesne proizvodnje izazvani prekidom internih operacija ili procesa.
- Poslovni rizici izazvani promenama u menadžmentu, ključnih osoba, strukturom izveštavanja ili poslovnim procesima.
- Rizici planiranja i kontrole usled neadekvatnog planiranja, procene i neefikasnog upravljanja.
- Neadekvatna procena nivoa rizika, nepredviđeni rizici, ublažavanje rizika i ne pridavanje odgovarajućeg značaja.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Slika 6: Kategorije rizika u lancima snabdevanja predložene od strane različitih autora



Izvor: Preuzeto iz: Maslarić, M. (2014) Razvoj modela upravljanja logističkim rizicima u lancima snabdevanja

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Efikasno upravljanje rizicima u lancima snabdevanja direktno implicira njihovu kategorizaciju. Pitanje koje se postavlja jeste na koji način klasifikovati sve te smetnje (događaje) koje mogu da prouzrokuju poremećaj ili prekid stabilnog funkcionisanja sistema – lanca snabdevanja. Analizom relevantne i dostupne literature koja se bavi problematikom kategorizacije rizika u lancima snabdevanja, došlo se do zaključka da postoji više od 70 vrsta strukturno različitih rizika u lancima snabdevanja. Slika 6. prikazuje kategorije rizika predložene od strane različitih autora.

U cilju izrade ove disertacije, autor je klasifikovao rizike u lancima snabdevanja (tabela 3), koji će dalje biti korišćeni kao osnova za procenu rizika matematičkim modelovanjem i rešavanjem problema primenom softverskog alata. Kako bi se izbeglo rasplinjavanje, grupe rizika su podeljene na nekoliko potkategorija, koje su dovoljne da bi se dokazale postavljene hipoteze.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Tabela 3: Kategorije rizika u lancima snabdevanja – studija slučaja

KATEGORIJA/ PODKATEGORIJA RIZIKA	
LJUDSKI RESURSI	Dostupnost stručnog kadra nepotizam, neusklađenost potreba radnog mesta sa obrazovnim sistemom, neadekvatno obrazovanje (veštine/spособnosti, odliv mozgova, rad pod pritiskom, istek ugovora moral i etičnost, odavanje poslovnih tajni, mito i korupcija, nepoštovanje Sistematizacije radnih mesta i ostalih pravnih akata na nivou organizacije/države, pružanje otpora ka usvajanju novih tehnologija/procesa poslovanja, krada informacija/materijalnih dobara kompanije
	Odnosi zajednica životna sredina (otpad, otpadne vode, emisije, iscrpljivanje resursa, zračnjice), terorizam i pretnje (na nivou šire zajednice), reklama, loša reputacija zbog poremećanih međuljudskih odnosa
	Zaštavlje i bezbednost neuspešno krotanje bezbednog radnog okruženja, nepoštovanje propisanih akata iz domena BZR i zaštite od požara, korišćenje neispravne opreme i sredstava za rad (bez atesta, sertifikata i minimuma propisanog)
	Outsourcing gubitak kompetencija, otpuštanje ili prelazak kadrova, neizvesnost među radnicima
	Komunikacije neadekvatna (ili nepostojanje) komunikacija, mobing, neostvarenje planova i prognoza, otpor prema novim tehnologijama (EDI, RFID, SAP, e-mail...)
PROIZVODI I TRŽIŠTA	Pitanja potrošača i tržišni trendovi identifikacija potreba potrošača, dostupnost P/U, primena smernica NBS (kontrola tržišnih rizika), gubitak vrednosti zbog povećanja kamatne stope, nestabilnost izvoznih vrednosti (promena deviznog kursa), odnos cena-kvalitet, servis, uslovi plaćanja, inovacije, uvoznici VS domaći materijal/sirovine, nevidljivost za kupca, odbojnost prema promenama, kompleksnost ECR-a, nekompatibilnost sa trenutnim organizacionim strukturom, briga oko posledica deljenja informacija o poslovanju sa partnerima, različita očekivanja maloprodavaca i proizvođača, nelojalna konkurencija, poprečna procena potreba i zahteva korisnika, promena kamatnih stopa, cena nepokretnosti i vrednosti valuta, crna/siva ekonomija, segmentacija tržišta i diverzifikacija proizvoda
	Spoljna sredina nedostatak distributivnih centara, razvijenost lokalne zajednice, akcidenti, politička neizvesnost, politički pritisci, mere ekonomske prinude (embargo, bojkot i ekonomska blokada), organizovani kr. i ekonomski kriminal, ugrožavanje energetske bezbednosti, politički kriminal, terorizam, sabotaža, ekološki rizici
	Konkurentsko okruženje loš kvalitet P/U, nedostatak sertifikovanih artikala, mali broj proizvoda prilagođenih novim međunarodnim standardima, serije malog obima, gubitak ranije distributivne mreže, nemogućnost kreditiranja prodaje, visina kursa, česte promene ekonomske politike i zaustavljanje reformi zbog izhora, potporani politički i ekonomski odnosi, loš kreditni rejting zemlje, skupi eksterni izvori finansija, globalna finansijska kriza, nepostojanje političke stabilnosti i kontinuiteta u vodenju ekonomske politike, previsok nivo javnih rashoda, glomazna i skupa državna administracija, nepostojanje elektronskih servisa u domenu javnih registara, stajanje monopola ili oligopola, skupe i dugotrajne administrativne procedure, nepovezivanje preduzeća u izvozne klasiere
	Zlonamerni napadi na proizvod ekstremne prevare učinjene od strane trećih lica i zaposlenih, postupci podvale i zloupotrebe, izbegavanje zakona i regulativa, propisi i političke organizacije, brade i prevare, spoljašnji sistem bezbednosti, nečista identifikacija proizvoda, namerna kontaminacija, podnošenje nečasnih izveštaja
	Proizvodni proces :: Kvalitet i rizik nepspravni proizvodni sistemi, zastaralost opreme, nepoznavanje tržišta, nepostojanje prethodnog iskustva, nepovoljna lokacija, nedovoljne količine sirovina/polufabrikata/materijala, nemogućnost obezbeđivanja potrebnih investicija, nizak nivo znanja i odgovornosti, slab kontrola i upravljanje, neplanirana pojava novih trendova u potrošnji, nedostatak ideja i inovacija, zastarevanje opreme i procesa, neracionalni i sablonski rad, ne postoji utvrđen specifični nivo kvaliteta, neuklanjanje uzroka lošeg kvaliteta, nepostojanje kontrole kvaliteta, nepreduzimanje korektivnih mera, U/I nebezbednih proizvoda, neusaglašenih proizvoda
PROIZVODI I TRŽIŠTA	Trgovачke marke :: Brand name erozija ulaganje u neprofitabilne P/U, nesprovođenje strategije diferenciranja i pozicioniranja na tržištu, ne postoji težnja ka autonomiji i koncentraciji u trgovini, paketi ponuda od strane trgovine se ne upotpunjavaju, ekskluzivnosti ponude, postizanje samostalnosti prilikom uvođenja novih proizvoda i povećanje trgovinskih marži uz eliminaciju mera proizvođača, nevidljivost za kupca, pojava supstituta/zamenskih P/U, erozija zbog povećanja konkurencije, nedovoljna ulaganja u nevidljivi kapital od strane top menadžmenta
	Upravljanje sa odnosima klijent nije u centru dogadjanja, loša preglednost u radu, podaci o klijentu nisu strukturirani, nizak stepen automatizacije i nadzora prodajnih i marketinških procesa, smernice dalje saradnje sa klijentima nisu jasno definisane, loša komunikacija sa klijentima, partnerima i dobavljačima, top menadžment se ne bavi CRM, saradnja sa licima/kompanijama koja nemaju ugled, zaključivanje poslova sa licima/kompanijama koja su u vezi ili se mogu dovesti u vezu sa nezakonitim poslovima, netačno i lažno predstavljanje P/U, veliki broj sporova u vezi izvršenja ugovorom preuzetih obaveza, loše interpersonalne veštine i veštine komunikacije
	Marketing i promocije poštovanje marketinga sa oglašavanjem, loša segmentacija tržišta i odabir ciljne grupe, loši odnosi sa stekholderima, nepoznavanje konkurencije, kompanija nije dovoljno usredsređena na tržište i okrenuta kupcima, kompanija ne upravlja dobro odnosima sa svim zainteresovanim stranama, proces marketing planiranja nije adekvatan i primeren uslovima, politika P/U nije dovoljno pooštrjena, napor i umeća koje se ulažu u izgradnju identiteta marke i marketing komunikaciju nisu delotvorni, nedovoljno primenjena dostignuća savremene tehnologije, nepostojanje vertikalnog marketinga i vertikalne integracije partnera u kooperativne marketing odnose, ciljevi promocije nisu jasno određeni, nepostojanje univerzalnih kriterijuma za merenje efikasnosti i moćne ideje o novom P/U se gura uprkos negativnim saznanjima iz istraživanja tržišta, precejena veličina tržišta, proizvod nije dobro dizajniran, nepravilno je pozicioniran na tržištu, nije efikasno oglašavanje ili ima preveliku cenu, troškovi su viši od očekivanog, konkurenti iznerviraju jače od očekivanog, nepostojanje jedinstvenog superiornog P/U, nepostojanje tehnološke i tržišne snerge kao i kvaliteta izrade, kašnjenje u razvoju, neuvrđivanje tehničke izvodljivosti
	Komercijalizacija novih proizvoda veliki procenat oštećene i neekvrentne robe na zalihama, nedostatak zalih, protivrečnost između podataka i stvarnog stanja robe na zalihama, vreme isporuke se produžava preko granice pokrivanja sigurnosnim zalihama, nemogućnost iskorišćenja zalih, zalih padaju ispod sigurnosnih, ne postoji osiguranje ili povećanje sigurnosnih zalih
	Zalhe

...

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

KATEGORIJA/
PODKATEGORIJA RIZIKA

GRUPE AKTIVNOSTI

INFRASTRUKTURA	Akcije Vlade	Vlada ne interveniše na tržištu u cilju stabilizacije kurseva; ne pruža se podrška posrednim kompanijama posebnim olakšicama ili smanjenjem poreza, ne štiti domaće kompanije, tehnologije i sl. kako bi se regulisali makroekonomski uslovi, diskriminacija regulativa, rizik eksproprijacije, kršenje ugovora, masovna nacionalizacija, regulatorne promene, konvertibilnost valute, uticaj vojske u politici, religijske tenzije, poštovanje ustava i zakona, etničke tenzije, demokratska odgovornost, kvalitet birokratije i administracije
	Pravna odgovornost Pravni okvir	neuskladenost poslovnih i opštih akata sa zakonskim i podzakonskim ¹⁹ ima, neprimenljivanje pravnih propisa koji se odnose na ostvarenje i poslovanje kompanija, nepraćenje sudske prakse i loše zastupanje društva pred sudovima i drugim državnim organima, mogućnost gubitaka usled kazni i sankcija prouzrokovanih iz sudskih sporova po osnovu neispunjavanja ugovornih i zakonskih obaveza, kao i usled sankcija izrečenih od strane regulatornog tela, česte promene zakona i propisa
	Skladišta	povrede i druge vrste zdravstvene ugroženosti radnika (prisustvo transportne i pretovarne mehanizacije, manualno rukovanje teretom, odlaganje robe na visinu, ostali zahtevi za realizaciju logističkih aktivnosti, a koji predstavljaju generator potencijalnih povreda), zagađenje atmosfere, stvaranje prašine, isticanje gasa, raspršivanje tečnih materija, buka, požar, neadekvatan smeštaj velike količine robe, zaposleno osoblje slabo poznaje robu koja se skladišti (u javnim skladištima, posebno ako se radi o čuvanju opasne robe), greške u tehnologiji realizacije skladišnih procesa, loša organizacija, upravljanje i kontrola rada, ne pridržavanje predviđenih radnih postupaka i procedura, pad robe sa viših polica, smeštanja robe po radnim prolazima, povećan broj manualnih skladišnih aktivnosti, pretovarna sredstva i oprema koja se koriste u skladištu, prevrtanja i s dani
INFORMACIJE	Nedostatak informacija za donošenje odluka	ločiranje resursa, dinamika proizvodnje, upravljanja zalihama i tokovima transporta, neodređenost traženje, neažurirana informacija o tražnji utiče na delatnost logističke službe, kontakt i razmenu informacija sa članovima službe, arhiviranje dokumentacije, prestanak snabdevanja, nedostatak materijala, prestanak proizvodnje, ne postoji razmena informacija u realnom vremenu, povećanje zaliha, nemogućnost obezbeđenja konkurentskog nivoa
	Gubitak pristupa informacijama	proizvođač nema pristup informacijama o nivou zalih distributera i odgovoran je za kreiranje porudžbine i njihovu isporuku
	Neovlašćen pristup informacijama	vršenje daljinskog ugrožavanja servera, oštećenje brisanje Web-servera nagadanje i provalljivanje lozinki, kopiranje baze podataka, pregledanje osetljivih podataka, uključujući i evidencije platnih spiskova i medicinske informacije, bez ovlašćenja, izvršavanje sniffer programa na radnoj stanici, da bi se ulovila korisnička imena i lozinke, korišćenje, bez dozvole, prilavljene radne stanice na kojoj nema operatera (ili automatizovane radne stanice), gubitak informacija putem kompiuterskog ili unutrašnjih kanala, prihvaćanje poslovnih informacija o konkurentima
FINANSIJE	Dizajn informacione infrastrukture	nepostojanje portfelja usluga, neprepoznavanje poslovnih zahteva, ukupan trošak se ne smanjuje, kvalitet usluge na niskom nivou, konzistencija usluge (ne postoji uskladenost sa korporativnom strategijom), teška implementacija IT usluga, IT usluge nisu usklađene...
	Nestabilnost valute Devizno poslovanje Nestabilnost kamatne stope	fluktuacija kursa valute, cena inputa nije zaštićena, ne postojanje hedžing poslova, solventnost krajnjeg korisnika, povećanje kamate, nestabilnost valute
	Finansijske kontrole	poslovanje se ne obavlja u skladu sa zakonima, oštećenje brisanje internim aktima, ugovor ²² i propisanim postupcima, ne postoji pouzdano, potpuno i blagovremeno finansijsko i poslovno izveštavanje, sredstva se ne koriste pravilno, ekonomično, efikasno i efektivno, zaštita imovine, obaveza i drugih resursa od gubitaka koji mogu nastati neodgovarajućim upravljanjem, nepravilnim trošenjem i korišćenjem, kao i od nepravilnosti i prevara nije regulisana, kontrola se ne sprovodi u skladu sa međunarodno prihvaćenim standardima
	Greške u finansijskim izveštajima	pronevere i kriminalne radnje u poslovanju, značajne greške u ranijim revizijama, odbijanje menadžmenta da izvrši zahteve revizora za otklanjanje grešaka, revizija se radi prvi put, prekid u određenom trendu, prekid rasta pozitivnog trenda rasta neto dobitka, problemi sa pravovremenim izmirenjem dužničkih obaveza, ne postupa se u skladu sa računovodstvenim politikama...
	Predviđanje veličine budžeta kao upravljanje tokovima gotovine	nepostojanje procene budućih rezultata, nepostojanje poslovnog plana, tržišni udeo P/U nije procenjen, nepostojanje projekcije očekivanje potražnje, trendovi u privredi se ne prate, nepoznat ili netačan bilans stanja, mesečna/kvartalna projekcija tokova gotovine za predstojeći period nije pripremljena, loša saradnja sa zahtodavcima, delimična likvidacija osnovnih sredstava
	Cena robe	promena kursa domaće u inostranu valutu, promena tržišnih kamatnih stopa, nabavna cena, konkurencija, kupovna moć, poslovna politika, PDV
	Dostupnost kapitala	nepostojanje kontinuiranih investicija, obim poslovanja ne obezbeđuje dovoljnu zaradu, zavisnost od eksternih izvora finansiranja, pooštreni uslovi kreditiranja, visoke kamatne stope
	Krade inventara : Prevare	falsifikovanje, podmićivanje, pranje novca, iznudivanje, pronevera, pljačka, krađa, zloupotreba imovine kompanije, zloupotreba imovine kompanije, oštećenje imovine kompanije, ostali zloupotrebi i nelegalni akti, krivotvorenje, insajderska trgovina (za svoj račun)
	Vrednovanje imovine	neadekvatno upravljanje imovinom i obavezama, pogrešne procene i evidentiranja, prezertovanje i objavljivanje vrednosti imovine (izvora sredstava društva, prihoda, rashoda i rezultata poslovanja i dr.

Izvor: autor

2.2.1. Pretnje i ranjivosti u lancima snabdevanja

U predmetnoj studiji slučaja rizik predstavlja verovatnoću da će određena pretnja – izvor rizika iskoristiti ranjivost resursa što se manifestuje kroz gubitak poverljivosti, integriteta ili raspoloživosti lanca snabdevanja.

Najpre je potrebno razgraničiti pojmove pretnja i ranjivost sistema – resursa, kako bi se moglo pristupiti daljoj analizi problema.

Resurs (*asset*) - ljudi, veštine, iskustvo i stručnost; sredstva potrebna za svaki korak u procesu upravljanja rizikom; procesi, metode i alati kompanije koji se koriste za upravljanje rizikom; dokumentovani procesi i procedure; informacije i sistemi za upravljanje znanjem; i programe obuke (ISO 31000, 2009). Navedeni resursi obuhvataju materijalne i nematerijalne elemente kojima se može dodeliti vrednost. Nematerijalna ulaganja obuhvataju ugled kompanije i zaštićenost podataka. Informacije mogu uključivati bazu podataka, softverski kod, poslovne tajne i druge nematerijalne elemente.

Resurs je ono što pokušavamo da zaštitimo.

U tabeli 3. dat je pregled grupisanih resursa – procesa u lancima snabdevanja. Za svaki proces je pojedinačno analizirano koji bi uticaj na poverljivost, integritet i raspoloživost mogli da ostvare potencijalni rizici. Nakon analize, svakoj grupi resursa – procesa su pridružene određene grupe rizika (detaljnije o analizi dato je u četvrtom poglavlju disertacije).

Izvor rizika može biti materijalne i nematerijalne prirode (ISO 31000, 2009). Izvor rizika ili pretnja (*threat*) je sve ono što može da iskoristi ranjivost resursa, namerno ili slučajno, pri čemu se narušava stabilnost resursa.

Pretnja je ono od čega pokušavamo da se zaštitimo.

U tabeli 4. prikazan je deo liste pretnji/izvora rizika koji su nakon analize pridruženi konkretnim ranjivostima pojedinih procesa, kao i lanca snabdevanja u celini. U studiji je razmatrana 161 različita pretnja/izvor rizika po poverljivost, integritet i raspoloživost u lancima snabdevanja (kompletna lista je data u Knjizi priloga – Prilog 1).

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Tabela 4: Listing pretnji/izvora rizika u lancu snabdevanja

GRUPA RIZIKA	PRETNJA
Ljudski faktor	Dostupnost stručnog kadra Ponašanje zaposlenih Odnosi zajednica Zdravlje i bezbednost Outsourcing Komunikacija
Proizvodi i tržišta	Pitanja potrošača i tržišni trendovi Spoljna sredina Konkurentsko okruženje Zlonamerni napadi na proizvod Kvalitet proizvodnog procesa Trgovačke marke :: Brand name erozija Upravljanje sa odnosima Marketing i promocije Komercijalizacija novih proizvoda Zalihe
Infrastruktura	Akcije Vlade Pravna odgovornost :: Pravni okviri Skladišta
Informacije	Nedostatak informacija za donošenje odluka Gubitak pristupa informacijama Neovlašćen pristup informacijama Dizajn informacione infrastrukture
Finansije	Nestabilnost valute :: Devizno poslovanje :: Nestabilnost kamatne stope Finansijske kontrole Greške u finansijskim izveštajima Predviđanje veličine budžeta kao upravljanje tokovima gotovine Cena robe Dostupnost kapitala Krade inventara :: Prevare Vrednovanje imovine

Izvor: autor

Ranjivost (*vulnerability*) je slabost sistema – imovine – resursa. Slabost omogućava resursu da bude eksploatisan/iskorišćen od strane jedne ili više pretnji (ISO 27005, 2011).

Ranjivost je jaz u našim naporima zaštite resursa.

Tabela 5. prikazuje deo liste ranjivosti lanca snabdevanja, koje su nakon analize pridružene konkretnim pretnjama po pojedine procese, kao i lanca snabdevanja u celini.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

U studiji je razmatrano 289 različitih vrsta ranjivosti u procesima lanca snabdevanja (kompletna lista je data u Knjizi priloga – Prilog 1).

Tabela 5: Listing ranjivosti lanca snabdevanja

GRUPA RANJIVOSTI	RANJIVOST
Strateška ranjivost	Sindikalni propisi
	Odnosi sa dealerima
	Odnosi sa dobavljačima
	Odnosi sa kupcima
	Lansiranje novih P/U
	Izvor dobavljača
	Tehnološke promene
	Novi ili strani konkurenti
	Oštećenje imovine
	Protivpožarna oprema
Hazardna ranjivost	Udari munje/groma
	Oštećenja od vetra
	Eksplוזija kotla ili mašine
	Gubitak ključnog objekta/postrojenja
	Zagađenje zemljišta, vode, atmosfere
	Gubitak tereta
	Geopolitički rizici
	Poplave
	Sabotaže
	Zemljotresi
Finansijska ranjivost	Dugovi i kreditni rejting
	Likvidnost/gotovina
	Ekonomska recesija
	Nestabilnost finansijskog tržišta
	Fluktuacije valuta i deviznog kursa
	Cena goriva
	Nepovoljne promene u industrijskim propisima
	Kredit
	Krađa
	Greške operatera/slučajne nezgode
Operativna ranjivost	Gubitak ključnih kadrova/osoblja
	Kompjuterski virusi
	Nizak nivo kvaliteta
	Pad IS
	HR rizici
	Gubitak ključnih snabdevača
	Poremećaj logističke rute
	Gubitak ključne opreme
	Pad logističkih provajdera
	Neuspešno obavljena usluga

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Rizik (*risk*), prilagođen ranije usvojenoj definiciji, predstavlja potencijalni gubitak, oštećenje ili uništenje resursa kao rezultat eksploatacije ranjivosti od strane pretnje.

Rizik je raskrsnica resursa, pretnje i ranjivosti.

Prema tome, rizik u ovom smislu možemo izraziti kao

$$R = A + T + V$$

Ukoliko postoji pretnja (stvarna, konceptualna, ili svojstvena), ali ne postoji ranjivost imovine, logično je da je u tom slučaju rizik minimalan. Slično, ukoliko je resurs ranjiv, ali ne postoji evidentna pretnja po funkcionisanje resursa, rizik je takode minimalan. Precizna identifikacija pretnji i ranjivosti od ključne su važnosti za razumevanje procene rizika. Razumevanje razlike između ovih pojmova predstavlja početni korak kvalitetne procene rizika.

U tabeli 6. su prikazani osnovni pojmovi i kriterijumi koji su definisani u metodologiji za upravljanje rizicima, a koja se definiše pre faze procene rizika i ista ne sme biti menjana u toku faza procene rizika i tretiranja rizika. Valjanost metodologije se može analizirati u toku i nakon završetka navedene dve faze u upravljanju rizicima, i ona može biti izmenjena za neke buduće procene rizika (na slici 8. „Monitoring i revizija“).

Tabela 6: Metodologija upravljanja rizicima – uslovi i kriterijumi

IZRAZ/USLOV	OPIS KRITERIJUMA		
T_v - vrednost pretnje	(1-nisko; 2-srednje i 3-visoko)		
V_v - vrednost ranjivosti			
$P = T_v \times V_v$ - verovatnoća	$\forall P \in \{1,2,3,4\} \Rightarrow P_i = P$;		
P_i - nivo rizika	$\forall P \in \{6,9\} \Rightarrow P_i = 5$;		
I_{vx} - impakt faktor	(1- veoma nisko; 2- nisko; 3- srednje; 4- visoko; 5- veoma visoko)		
(x= poverljivost, integritet ili raspoloživost)			
$R_x = I_{vx} \times P_i$ - Rizik	(1- veoma nisko; 2- nisko; 3- srednje; 4- visoko; 5- veoma visoko)		
(x= poverljivost, integritet ili raspoloživost)			
	Nivo rizika	Akcija	Tretiranje rizika
$1 \leq R_x \leq 2$	Veoma nizak	Bez akcije	Zadržavanje
$3 \leq R_x \leq 4$	Nizak	Monitoring rizika	Zadržavanje
$5 \leq R_x \leq 10$	Srednji	Potrebne neke akcije i monitoring	Zadržavanje
$12 \leq R_x \leq 16$	Visok	Potrebne akcije	Redukcija
$20 \leq R_x \leq 25$	Veoma visok	Potrebne akcije	Redukcija

Izvor: Prilagođeno prema: ISO 27005:2011

Iz tabele 6. može se viditi da se rizik izračunava kroz uticaj na tri karakteristike lanca snabdevanja (uticaj na poverljivost (npr. informacija), integritet (lanca snabdevanja u celini) i raspoloživost (npr. usluga koje se nude kroz lanac snabdevanja)).

Usvojicemo i sledeće činjenice:

- pretnje se ne mogu kontrolisati (npr. ne mogu se zaustaviti namere međunarodne terorističke grupe, sprečiti uragan ili cunami unapred. Pretnje treba identifikovati, ali one često ostaju van naše kontrole).
- rizik se može ublažiti (rizikom se može upravljati, bilo na nivou minimalne ranjivosti, bilo na nivou ukupnog uticaja na poslovanje).
- ranjivost se može tretirati (ranjivosti sistema/resursa treba identifikovati i preuzeti proaktivne mere u cilju korigovanja identifikovanih slabosti)

2.2.2. Mapiranje poslovnih procesa u lancima snabdevanja

Sve veća složenost poslovnih procesa, veze između njih i orijentisanost ka zajedničkom cilju zahtevaju da se isti jasno iskažu i povežu među sobom i sa okruženjem. Nažalost, u teoriji, a posebno u praksi, mapiranje procesa se odvija nedovoljno precizno, parcijalno i sa malim informacionim sadržajem.

Razumevanje postojećih procesa je mnogo bitnije od kreiranja novih procesa. Sa tim u vezi se ističe potreba za mapiranjem i merenjem postojećih procesa. Mapiranje daje odgovor na pitanje kako procesi i aktivnosti međusobno utiču jedni na druge u kompaniji i u kakvom su odnosu sa spoljnim okruženjem (Hadžiselimović, 2006). Kroz način odvijanja poslovnih procesa, može se steći i uvid o tome kakve su ostvarene performanse procesa. To će poslužiti kao osnova za identifikovanje postojanja neadekvatnih performansi poslovnih procesa (Arsovski, 2014).

Mapiranje poslovnih procesa (engl. Business Process Mapping) se može koristiti za bolje razumevanje postojećih procesa, kao i za pojednostavljivanje ili eliminisanje onih aktivnosti u okviru procesa koje ne doprinose povećanju vrednosti (Hunt, 1996).

U cilju izrade ovog rada, klasičan pristup mapiranju poslovnih procesa prilagođen je lancima snabdevanja i kao takav prikazan je tabelom 7.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Tabela 7: Mapiranje poslovnih procesa u lancu snabdevanja

POSLOVNI PROCES	AKTIVNOST
Menadžment materijalima	Planiranje materijala Kupovina materijala Skladištenje Kontrola proizvodnje
Proizvodni proces	Pripremni deo proizvodnje Izvršni deo proizvodnje Završni deo proizvodnje
Transportni proces	Utovar Transport I tovar
Upravljanje informacijama	Određivanje potreba za informacijama Prikupljanje i procesuiranje informacija Korišćenje informacija
Upravljanje finansijama	Poslovi pribavljanja i plasmana sredstava Poslovi platnog prometa i likvidature Poslovi finansijskog upravljanja
Planiranje i predviđanje potražnje	Planiranje i predviđanje tražnje Planiranje bezbednosnih zaliha Planiranje mreže snabdevanja Planiranje distribucije Kolaboracija mreže snabdevanja
Dizajn procesa	Utvrđivanje i podela poslova Departmanizacija Delegiranje autoriteta Upostavljanje raspona kontrole
Povratni procesi	Povraćaj Zamena
Komunikacija sa okruženjem i zakonske procedure	Komunikacija Poštovanje zakonskih procedura i standarda iz oblasti

Izvor: autor

4

2.2.3. Upravljanje rizikom

Kao generalni odgovor na pitanje "Šta je upravljanje rizikom?" iz uporedne teorije može se izdvojiti sledeća misao: "Za mnoge analitičare, političare i akademike to je upravljanje prirodnim okruženjem i tehnički generisanim makro rizicima, koji prete našem opstanku" (Kloman, 1999). Generalno posmatrano, upravljanje rizikom se može definisati kao životna disciplina koja podrazumeva mogućnosti da budući događaji mogu izazvati suprotne efekte. Rizik ipak ne mora da bude u potpunosti posmatran kao izbegavajuća kategorija. Prema opšteprihvaćenim normama, upravljanje rizikom predstavlja identifikaciju, ocenu, izdvajanje prioriteta, zatim koordiniranje i ekonomično primenjivanje resursa kako bi se minimizirala, pratila i kontrolisala mogućnost ili uticaj neželjenih događaja i maksimizirala realizacija očekivanih uspeha (ISO 31000, 2009).

...

Upravljanje rizicima je poznato čovečanstvu od davnina. Prva procena rizika zabeležena kroz rad Asipu grupe, u dolini reka Tigar i Eufrat 3200 godine pne. Asipu su pokušavali da daju doprinos proceni rizika po pitanju gradilišta, započinjanja poslovanja, pa čak i pri stupanju u bračnu zajednicu. Asipu su analizirali dostupne faktore rizika, sugerišući alternative i predlažući najbolju soluciju za ublažavanje rizika u kvantitativnom obliku (Covello & Mumpower, 1985). 792 godine pne. "ladarski zajam" (bottomry contracts) je korišten u cilju ublažavanja rizika. Ova forma je sadržala tri elementa, i to: pozajmicu, kamatnu stopu i premiju. Koncept *general average* je razvijen takođe u ovom periodu, da bi kasnije evoluirao u koncept osiguranja. Osiguranje je, dakle, jedan od najstarijih oblika strategije mitigacije (ublažavanja) rizika. Napredak u razvoju teorije verovatnoće tokom XVII i XVIII veka postavlja je na mesto veoma važnog alata za procenu rizika. Od XIX veka teorija verovatnoće se koristi u širokom spektru disciplina, od finansija do inženjerstva, kroz specifične alate i metode.

Upravljanje rizicima znači gledati u budućnost, unapred razmišljati o potencijalnim događajima, učincima i posledicama sa kojima se kompanija može suočiti u budućnosti i pravovremeno preduzimati mere kako bi se rizici minimizirali, a time negativna posledice po poslovanje kompanije izbegle odnosno smanjile. Neophodno je pravovremeno uočiti ključne rizike i preduzeti odgovarajuće kontrolne aktivnosti, odnosno, ući dodatne finansijske izdatke koji će se nužno javiti u cilju saniranja problema, ali i izbegla negativna reputacija zbog propusta u poslovanju.

Menadžeri, ili ovlašćena lica, odgovorni za poslovanje i realizaciju postavljenih ciljeva, istovremeno su i ključne osobe odgovorne za upravljanje rizicima i to treba shvatiti kao sastavni deo svog poslovanja, posebno prilikom donošenja odluka. Sve aktivnosti kompanije uključuju rizike kojima mora upravljati. Proces upravljanja rizicima doprinosi odlučivanju uzimajući u obzir neizvesnost i mogućnost pojave budućih, namernih ili nenamernih događaja i okolnosti i njihovih uticaja na postavljene ciljeve.

Upravljanje rizicima uključuje primenu logičkih i sistematičnih metoda za:

- komuniciranje i konsultacije tokom ovog procesa;
- uspostavljanje organizacionog konteksta za identifikaciju, analizu, procenu, tretman i monitoring rizika vezanih za bilo koju aktivnost, proizvod, funkciju ili proces i
- adekvatno izveštavanje u vezi sa rezultatima (ISO 31000, 2009).

Veza između principa, procesa i okvira kojim se opisuje upravljanje rizikom prikazana je na slici 7.

Upravljanje rizikom se posmatra kao centralni proces upravljanja u kompaniji tako da se rizici razmatraju u smislu uticaja koje mogu imati neizvesnosti u odnosu na ciljeve. Upravljačka struktura kompanije i proces zasnovani su na upravljanju rizicima. Efektivno upravljanje rizicima od strane menadžera smatra se ključnim za postizanje ciljeva kompanije (ISO 31000, 2009). Prema tome, upravljanje rizicima treba da sadrži sledeće principe:

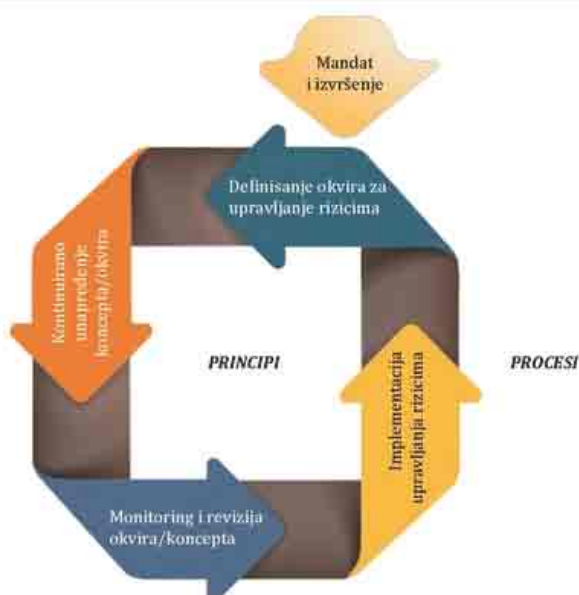
- učešće u stvaranju dodatne vrednosti,
- sastavni deo ostalih poslovnih procesa,
- učešće u donošenju odluka,

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

- izričito adresiranje nesigurnosti,
- sistematičnost, strukturiranost i pravovremenost,
- organizovanje i sprovođenje najbolje dostupne informacije,
- prilagođenost potrebama kompanije i delatnosti gde se koristi,
- uzimanje ljudskih i kulturnih elemenata u obzir,
- transparentnost i inkluzivnost,
- dinamičnost, iterativnost i odgovori na promene i
- omogućavanje stalnog unapređenja i poboljšanja kompanije.

Slika 7: Korelacija između principa, procesa i okvira upravljanja rizikom



Izvor: Prilagođeno prema: ISO 31000:2009

2

U kontekstu organizovanja kompanije postavlja se pitanje gde se sistematizovati proces za upravljanje rizicima. Osim problema bezbednog sprovođenja procesa kontrolinga u kompaniji kroz upravljanje rizicima, postoji još niz pozicija koje se takođe mora upravljati u cilju obezbeđivanja bezbednog (radnog) okruženja. To su npr. strateški i operativni rizici, rizici odvijanja svih ostalih poslovnih procesa, upravljanje aspektima životne sredine, rizicima zdravlja i sigurnosti zaposlenih, IT bezbednost, itd. U svakom slučaju, ovom problemu se treba pristupiti sistematski, jer je nedopustivo da postoji niz nepovezanih upravljanja rizicima u kompaniji, kao i razjedinjeno upravljanje bezbednošću kompanije.

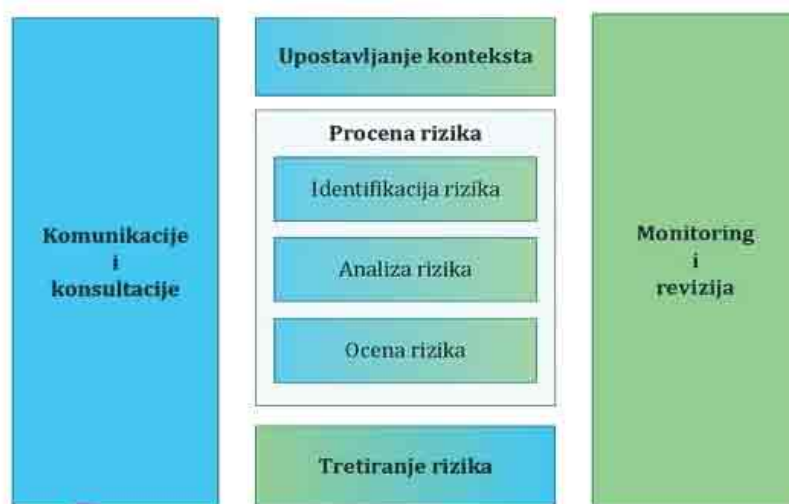
U teoriji, proces upravljanja rizicima izgleda dosledno i jasno. Međutim, praktično iskustvo pokazuje da ne samo da kvantifikacija predstavlja značajne probleme, već i identifikacija rizika na prvom mestu predstavlja gotovo nepremostivi izazov upućen menadžerima. Kvantifikacija, procena verovatnoće nastanka i nivo uticaja, su ograničeni

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

kroz nedostatak podataka o prošlim iskustvima sličnih događaja u drugim kompanijama. Dalje, identifikacija rizika je često predmet nespornosti rukovodilaca da priznaju postojanje rizika u svojim oblastima odgovornosti, pošto se priznavanje prisustva rizika identifikuje kao znak slabosti kompanije. Kada kompanija odluči da implementira rizik menadžment u svoj svakodnevni život, prvo se donosi odluka o organizovanju sistema za upravljanje rizicima koji se odvija putem procesa, kao što je prikazano na slici 8.

Slika 8: Proces upravljanja rizicima



Izvor: Prilagođeno prema: ISO 31000:2009

Na osnovu prethodne slike, elementi za proces upravljanja rizicima se opisuju na sledeći način:

- Komunikacija i konsultacija sa internim i eksternim ulagačima – zainteresovanim stranama, kako je primereno (tehnološki), na svakom stepenu procesa upravljanja rizikom i razmatranje procesa kao celine;
- Utvrđivanje eksternog, internog i konteksta upravljanja rizikom u kom će se odvijati ostatak procesa. Treba utvrditi kriterijume prema kojima će se procenjivati rizik i definisati struktura analize;
- Identifikacija gde, kada, zašto i kako bi se događaji mogli sprečiti, umanjiti, odložiti ili povećati postizanje ciljeva;
- Analiza rizika podrazumeva identifikaciju i procenu postojećih kontrolnih mera. Određivanje posledica i verovatnoće, a zatim nivoa rizika. Ova analiza treba da razmotri područje potencijalnih posledica i njihovu pojavu;
- Vrednovanjem rizika se vrši poređenje procenjenih nivoa rizika sa prethodno utvrđenim kriterijumima i razmatra se ravnoteža između potencijalnih koristi i nepovoljnih rezultata. To omogućava donošenje odluka o obimu i prirodi potrebnih obrada i o prioritetima;

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

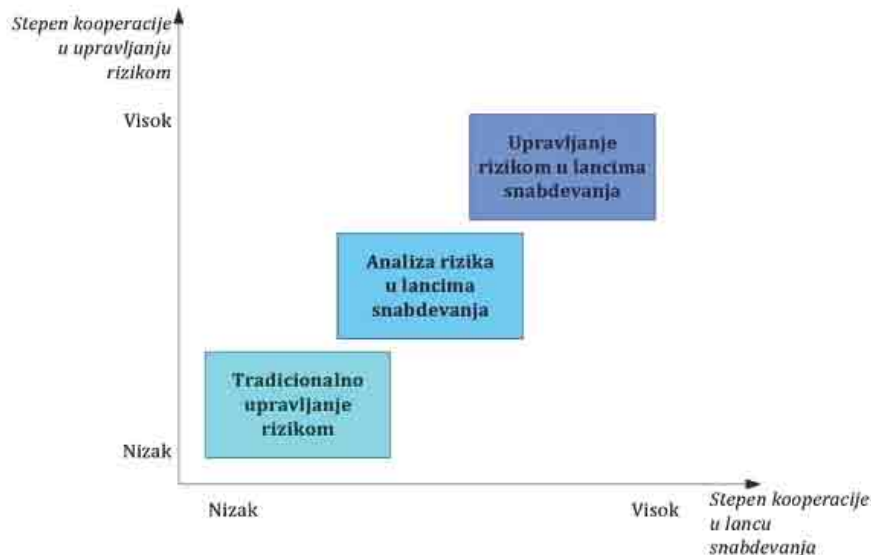
- Obrada rizika obuhvata izradu i primenu specifičnih troškovno-efikasnih strategija i akcionih planova za povećanje potencijalnih koristi i smanjenje potencijalnih troškova;
- Monitoring i revizija se ostvaruju kroz neophodnost praćenja efikasnosti svih koraka procesa upravljanja rizikom. Potrebno je pratiti rizike i efektivnost predloženih mera kako bi se osiguralo da promena uslova ne menja prioritete.

2.2.4. Upravljanje rizikom u lancima snabdevanja

Kao što je već rečeno, upravljanje rizikom je važno sredstvo u obezbeđivanju ekonomskog integriteta organizacije. Ovo posebno važi ako se jasno postave granice organizacije. U okruženju upravljanje lancima snabdevanja postaje zamagljeno, što ne znači da ono zakonski više ne postoji, ali proces identifikovanja linije razdvajanja između dve kompanije postaje veoma težak. Paralelno sa proširenjem obima upravljanja lancem snabdevanja, upravljanje rizikom treba da postane odgovornije (slika 9).

Što je veći stepen integracije duž lanca snabdevanja, obim zahteva za upravljanjem rizicima postaje veći. Upravljanje rizicima u lancima snabdevanja predstavlja integraciju i upravljanje kroz koordinisani pristup među članova lanca u cilju smanjenja ranjivosti lanca snabdevanja u celini (Christopher, 2005). Ranjivost lanca potiče od spoljnih i unutrašnjih rizika po njega.

Slika 9: Integracija lanca snabdevanja podržana upravljanjem rizikom



Izvor: autor

Upravljanje rizikom u lancima snabdevanja (Supply Chain Risk Management, u daljem tekstu SCRM) precizno daje uputstva za proces identifikacije rizika duž lanca

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

snabdevanja, procenu rizika i predlog korišćenja raznih pristupa za njihovo ublažavanje (Park et al., 2013). Primer osnovnog principa upravljanja rizicima u lancima snabdevanja prikazan je slikom 10.

Slika 10: Okvirni primer SCRM



Izvor: Prilagođeno prema: Manuj, I., Mentzer, J.T. (2008) *Global Supply Chain Management*.

Promena u percepciji upravljanja rizicima vođena logistikom je neophodna. Logističke funkcije obezbeđuju konkurentnu prednost kompaniji, bez obzira na to čemu strategija teži. Uz bilo koju od Porterovih strategija rukovođenja ili diferencijacije, logistika pomaže da se ispune ciljevi kompanije i da se pruži dodatnu vrednost za kupca. Upravljanje lancem snabdevanja ima za cilj integraciju partnera u lancu isporuke, skraćivanje protoka materijala, informacija i finansija. Međutim, sa višim stepenom integracije, veća je verovatnoća međuzavisnosti pojedinačnih partnera. Pored toga, globalno poreklo dodaje dalju dimenziju neizvesnosti u pogledu transporta, nestabilnim političkim okruženjima i različitim nivoima posvećenosti kvalitetu i pouzdanosti. Čvrsto povezani internacionalni lanac snabdevanja rezultira složenim procesima koordinacije i administracije partnera u lancu. Različiti nivoi odgovornosti kako zaposlenih, tako i partnera, moraju da budu uzeti u obzir. Fokus upravljanja rizikom nužno se premešta sa kompanije na perspektive lanca snabdevanja. Ovakav razvoj jasno ima uticaj na obim i funkcionalnost kompanija fokusiranih na sistem upravljanja rizicima. Koncept upravljanja rizikom mora da bude aktivan duž celog lanca snabdevanja. To omogućava svim partnerima koji doprinose lancu snabdevanja da ograniče negativne rizike lancu.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Da bi ovaj cilj bio postignut, upravljanje rizikom u lancu snabdevanja mora da se odnosi na:

- tokove materijala, informacija i finansija duž lanca snabdevanja i povezanih procesa;
- granice sistema, koje se trebaju proširiti izvan organizacije da bi se u potpunosti pokrila dužina lanca;
- izazov da se pokrije ne samo strateški nego i operativni nivo, okretanje sistema za upravljanje rizicima od zakonom propisanog izveštavanja ka funkcijama planiranja.

Za SCRM se može reći da predstavlja integraciju i upravljanje kroz koordinisani pristup među članovima lanca u cilju smanjenja ranjivosti lanca snabdevanja u celini (Christopher, 1998). Ranjivost lanca potiče od spoljnih i unutrašnjih rizika po njega.

Kao i u prethodnim poglavljima, ponovo se javlja situacija gde se ne može izdvojiti jedinstvena definicija pojma, u ovom slučaju zbog različitih učesnika u samom lancu snabdevanja, zatim zbog različitih aspekata njegovog posmatranja (ekonomskog, pravnog, zakonodavnog, itd.). Tabelom 8 prikazane su neke od bazičnih definicija pojma upravljanje rizicima u lancima snabdevanja.

Tabela 8: Bazične SCRM definicije

AUTOR(I)	DEFINICIJA SCRM
Jüttner et al.	SCRM se definiše kao identifikacija i upravljanje rizicima za lanac snabdevanja, kroz koordinaciju među članovima lanca, u cilju smanjenja ranjivosti lanca snabdevanja u celini.
Norrman and Lindroth	SCRM primenjuje alate, u saradnji sa partnerima, u procesu upravljanja rizikom, koji se bave izazvanim neizvesnostima ili utiču na resurse i logističke aktivnosti kojima su povezani.
Tang	SCRM se definiše kao upravljanje rizicima u lancima snabdevanja kroz koordinaciju ili saradnju među partnerima lanca isporuke kako bi se osigurala profitabilnost i kontinuitet.
Norrman and Jansson	Fokus upravljanja rizikom u lancima snabdevanja je da se razumeju i pokušaju da izbegnu razorne posledice – katastrofe, koje kao i manji poslovni prekidi mogu imati negativne efekte po stabilno funkcionisanje lanca snabdevanja. Cilj upravljanja rizikom je da se smanji verovatnoća nastanka događaja koji su se nekada već desili i da se poveća otpornost, kroz sposobnost oporavka od prekida.
Giunipero and Eltantawy	SCRM je formalni proces koji uključuje identifikaciju potencijalnih gubitaka, razumevanje verovatnoće mogućih gubitaka i dodeljivanje značaja ovim gubicima.
Supply Chain Council	SCRM je sistematska identifikacija, procena i ublažavanje potencijalnih poremećaja u logističkim mrežama sa ciljem da se smanji njihov negativan uticaj na performanse logističke mreže.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Manuj and Mentzer	U globalu, SCRM je identifikacija i procena rizika i odgovarajućih gubitaka u globalnom lancu snabdevanja, i sprovođenje odgovarajućih strategija kroz koordinisani pristup između članova lanca snabdevanja sa ciljem smanjenja jedne ili više kategorija - gubitaka, verovatnoće, brzine realizacije nepovoljnog događaja, brzine gubitaka, vremena za otkrivanje događaja, frekvencije, odnosno izlaganja, a u cilju postizanja krajnjeg ishoda - usklađivanja stvarnih troškova i profitabilnosti.
Brindley	SCRM se definiše kao upravljanje rizicima u lancu snabdevanja kroz koordinaciju ili saradnju među partnerima lanca snabdevanja kako bi se osigurali profitabilnost i kontinuitet.
Goh et al.	SCRM se definiše kao identifikacija i upravljanje rizicima u okviru mreže snabdevanja i, eksterno kroz koordinisani pristup među članovima lanca snabdevanja, u cilju smanjenja ranjivosti lanca u celini.
Lavastre et al.	SCRM se odnosi na rizike koji mogu da izmene ili spreče efikasan protok informacija, materijala i proizvoda između aktera u lancu snabdevanja unutar organizacije, ili među akterima u globalnom lancu snabdevanja. SCRM može da se posmatra kao sposobnost kompanije da bude agilna.
Tummala and Schoenherr	SCRM je alat koji obezbeđuje menadžerima korisne i strateške informacije, odnosno profile rizika u lancima snabdevanja vezane za datu situaciju. Ovaj način je u suprotnosti sa tradicionalnim upom.

Izvor: Prilagođeno prema: Santos Ceryno, P., Scavarda, L.F., Klingebiel, K., Yüzgülec, G., (2013) *Supply Chain Risk Management: A Content Analysis Approach*

Po Martinu Kristoferu, razumevanje i upravljanje rizicima u lancu snabdevanja obuhvata sledeće korake (Christopher, 2005):

1. Profilisanje na bazi dobavljača:
 - identifikovati svaki materijal/sirovinu,
 - identifikovati strateške materijale i
 - razumeti organizaciju strateških dobavljača.
2. Procena ranjivosti u lancu snabdevanja:
 - scenario šta će se verovatno desiti za svaki od rizika,
 - zašto se dešava neki rizik i
 - mogućnosti/nemogućnosti kompanije da se nosi sa rizicima.
3. Procena posledica:
 - primena simulacionih tehnika.
4. Identifikovanje, ublažavanje i nepredviđeni postupci.
 - radi kontinuiteta u snabdevanju u roku od 24 časa identifikacija poremećaja snabdevanja materijalima, nabavka i kupovina materijala/sirovina iz alternativnih izvora snabdevanja (planiranje i evaluacija brzine povratka kompanije na radne zadatke/aktivnosti).
5. Analiziranje nastalih šteta, troškova i koristi/beneficija:
 - svaki trošak na smanjenju rizika donosi korist smanjenju ukupnih troškova od mogućih šteta i prekida rada i

- pitanje je koliko uložiti u smanjenje rizika.
- 6. Sprovođenje mera i akcija:
 - najvažnije pri upravljanju rizikom lanca snabdevanja je pojašnjenje uloge i odgovornosti svih učesnika,
 - podela bitnih informacija i
 - partnerstvo sa dobavljačima.

Na osnovu iznetog, koncept SCRM može biti definisan kao identifikacija i upravljanje rizicima u lancima snabdevanja kroz koordinisani pristup svih članova lanca snabdevanja u cilju redukcije ranjivosti i povećanja otpornosti lanca u celosti.

2.2.5. Kvantifikacija rizika

Termin kvantifikacija, sa svojim izvornim značenjem određivanje stepena, količine, opsega, obima, prebrojavanja (Antić et al., 2004), kao takav može se preneti na rizike, pa otuda pod sintagmom *kvantifikacija rizika* podrazumevamo određivanje svih mogućih vrednosti promenljive rizika i pozitivne verovatnoće za svaku od njih.

Faza kvantifikacije i analize rizika obuhvata kvantifikovanje i ocenu pojedinačnih rizika kao i skupa rizičnih situacija i interakcije između njih. U okviru ove faze vrši se vrednovanje identifikovanih rizika, kvantifikacija uticaja rizičnih događaja, utvrđivanje verovatnoće njihovog nastajanja, utvrđivanje opsega mogućih vrednosti, definisanje vremena i prostora u kome se rizične situacije mogu dogoditi, kao i analiza osetljivosti na promenu projektnih parametara (Lukić et al., 2009).

Cilj upravljanja rizikom je da se, što je moguće više, smanje negativni uticaji koji mogu remetiti stabilno funkcionisanje posmatranog sistema, kao i da se iskoriste sve mogućnosti za uspešnije i racionalnije izvođenje aktivnosti u nutar sistema.

Proces kvantifikacije predstavlja poseban problem u ukupnom procesu upravljanja rizikom. Svaka vrst poslovne funkcije ima svoje specifičnosti i osobenosti koje ih razlikuju od drugih. Da bi se izvršila adekvatna kvantifikacija rizika potrebno je tvrditi koje ulazne informacije treba sakupiti, kao i koji su njihovi izvori, i ovaj proces treba da se bazira na sledećim podacima:

- trajanje aktivnosti,
- troškovi,
- izvori rizika i
- rizični događaji

Proces kvantifikacije rizika predstavlja primenu određenih metoda i tehnika, u skladu sa opštim karakteristikama izvođenja posla i procesa upravljanja rizikom. Postoji veliki broj različitih metoda i tehnika koje mogu da se koriste u fazi kvantifikacije rizika poput: metode upitnika, metode očekivanog uticaja rizika, analize verovatnoće, simulacije, stabla odlučivanja, Delfi tehnike itd. (Nadrljanski & Nadrljanski, 2014)

Kao izlaz iz faze kvantifikacije rizika očekivano je generisati listu rizičnih događaja koje treba uzeti u razmatranje u fazi definisanja strategije upravljanja rizikom i za njih definisati odgovarajuće strategije, planove, postupke i ostale akcije, kako bi se sprečili negativni efekti ili iskoristile povoljne okolnosti, i listu rizičnih događaja za koje

menadžment treba da primeni strategiju prihvatanja dešavanja ili njihovog ignorisanja. Ovaj metod je koristan za definisanje prioriteta aktivnosti, posebno u slučaju kada postoji veliki broj identifikovanih rizičnih situacija. Kvantifikacija značajno povećava prednosti procene rizika, ali isto tako kvalitativna procena rizika nije uvek dovoljno dominantna činjenica koja će da ubedi top menadžment u neophodno investiranje u program kontrole rizika. Kvantitativna procena rizika je upravo ta koja povećava svest o postojanju i mogućim posledicama rizika unutar kompanije.

2.2.6. Kinney metoda

Proces procene rizika je od vitalnog značaja i podrška procesu donošenja odluka u svakoj kompaniji. Različite kompanije koriste različite metode za procenu rizika, čiji nivoi sofisticiranosti u samom procesu variraju. Kinney metoda za procenu rizika uvedena je prvi put u upotrebu 1976. godine u okviru tehničke dokumentacije Vojnopomorskog oružanog centra u Kaliforniji, SAD. Autori metode, Kinney i Wiruth, u početku rada su imali za cilj prevenciju rizika od eksplozija u vojnoj industriji. Kao takav, metod je naišao na opšti uspeh širom Evrope. Većina relevantnih literaturnih izvora upravo ovu metodu kvalifikuje kao bazičnu metodu procene rizika.

Evalvacija i rangiranje rizika, po ovoj metodi, nastavlja da bude lider u oblasti širom država članica EU. Na primer, u Belgiji je Kinney metoda univerzalan alat, kako u velikim kompanijama, tako i u malim i srednjim preduzećima (Koob & Malchaire, 2003).

Po Kinney metodi procena rizika se posmatra kroz tri parametra:

- verovatnoća pojave opasnosti ili štete (događaja) – V,
- učestalost (vreme izlaganja opasnostima/štetnostima) – U i
- težina nastale posledice – P.

Verovatnoća nastanka štete tokom izlaganja faktorima rizika je isključivo nenamernog, stohastičkog i neizvesnog karaktera. Izvorno je definisano sedam klasa verovatnoće (pojave opasnosti ili štetnosti) kojima je dodeljena numerička vrednost, kao što je prikazano u tabeli 9 (Kinney & Wiruth, 1976).

Tabela 9: Numeričke vrednosti verovatnoća pojave opasnosti/štete po Kinney metodi

VEROVATNOĆA (V)	OPIS
0,1	Praktično nemoguće
0,2	Skoro nemoguće
0,5	Verovatno, prihvatljivo
1	Malo verovatno, moguće u granicama
3	Neobično, ali moguće
6	Moguće
10	Predvidivo

Izvor: Prilagođeno prema: Kinney, G.F., Wiruth, A.D. (1976) *Practical risk analysis for safety management*

Učestalost izloženosti resursa delovanju faktora rizika izraženo je vremenskim intervalom koji pripada jednoj od šest klasa kao što je prikazano u tabeli 10.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Tabela 10: Numeričke vrednosti učestalosti izloženosti delovanju faktora rizika po Kinney metodi

UČESTALOST (U)	OPIS
0,5	Veoma retko (ređe od jednom godišnje)
1	Retko (godišnje)
2	Mesečno
3	Povremeno (nedeljno)
6	Redovno (dnevno)
10	Permanentno

Izvor: Prilagođeno prema: Kinney, G.F., Wiruth, A.D. (1976), op. cit.

Težina nastale posledice/štete izražena je kroz pet klasa, kao što prikazuje tabela 11.

Tabela 11: Numeričke vrednosti težine nastale štete/posledice po Kinney metodi

POSLEDICA (P)	OPIS	VRSTE POSLEDICA
1	Niska	Povreda zaposlenog, bez prekida proizvodnog procesa
3	Značajna	Povreda zaposlenog, sa prekidom proizvodnog procesa
7	Visoka	Invalidnost zaposlenog
15	Veoma visoka	Jedna ljudska žrtva
40	Katastrofalna	Više ljudskih žrtava

Izvor: Prilagođeno prema: Kinney, G.F., Wiruth, A.D. (1976), op. cit.

Autori preporučuju da proces procene treba da počne od vrha menadžmenta, kroz definisanje svakog radnog zadatka. Tek nakon identifikacije rizika može se pristupiti kvantifikaciji. Međutim, ako proces procene obavlja jedno lice, konačan rezultat neće biti validan upravo iz razloga subjektivnosti procenjivača, samim tim preporučuje se formiranje multidisciplinarnog tima. Nakon završetka faze identifikacije, pristupa se razvijanju scenarija rizika. Na osnovu postavljenog konteksta, numeričke vrednosti se dodeljuju verovatnoći, učestalosti i težini posledice. Konačni rezultat proizvoda ova tri faktora će formirati rang rizika. Vrednosti ranga rizika, prikazane su u tabeli 12.

$$R = V \times U \times P$$

Tabela 12: Rang rizika po Kinney metodi

RANG	NIVO RIZIKA	OCENA	MERE KOJE TREBA PREDUZETI
I	Prihvatljiv	$R \leq 20$	Ne preduzimati dodatne mere
II	Mali	$20 < R \leq 70$	Potreban oprez, rešiti ga redovnom procedurom – radnim upustvom
III	Umereni	$70 < R \leq 200$	Potrebne mere, moraju se utvrditi odgovornosti
IV	Visoki	$200 < R \leq 400$	Potrebna brza reakcija od strane višeg rukovodstva
V	Ekstremni rizik	$R > 400$	Prekinuti aktivnost. Potrebna momentalna akcija od strane najvišeg rukovodstva

Izvor: Prilagođeno prema: Kinney, G.F., Wiruth, A.D. (1976), op. cit.

U trećem poglavlju disertacije data je procena rizika u lancima snabdevanja po Kinney metodi, koju je autor prilagodio propozicijama matematičkog modelovanja koje važe za ovu metodu i primenio je na identifikovanim rizičnim događajima za koje smatra da su najbitniji u lancima snabdevanja.

2.2.7. Softversko rešenje Hestia Risk

U izradi ove teze korišćena je modifikovana verzija softverskog alata Hestia Risk (koji distribuira hrvatska firma Bluefield d.o.o.), integralno softversko rešenje za upravljanje rizicima primenom kvalitativne metodologije. Autor teze je iskoristio fleksibilnost i parametrizaciju softvera kako bi ga prilagodio za procenu rizika u lancima snabdevanja. U okviru ovog poglavlja date su informacije o osnovnom Hestia Risk softverskom alatu. Primena modifikovane verzije (za lance snabdevanja), izveštaji i komentari izloženi su u četvrtom poglavlju ove teze.

Postojanje informacionih sistema ni u kom slučaju nije započelo kompjuterskom erom. Informacioni sistemi postoje praktično od kada su poznate delatnosti i rad ljudi, od najstarijih vremena pa do danas. U opštem smislu, pod informacionim sistemom se smatra skup resursa, pravila i organizacija sprovođenja aktivnosti vezanih za generisanje, obradu, prenos, arhiviranje i upotrebu informacija. Kao što se može zaključiti, glavni objekat oko kog se sve vrti u jednom informacionom sistemu je svakako informacija. Postoji niz raznih definicija pojma informacije, koje su manje ili više slične, ali za potrebe ovog rada može se pojednostavljeno reći da informacija predstavlja svaki podatak koji ima neku vrednost za korisnika. Čim se radi o vrednosti, onda se u prvom redu smatra da je moguće svaliti informaciju valorizovati i izraziti neku meru, kroz odgovarajuću novčanu vrednost. Automatski se nameće zaključak da nešto što ima neku vrednost predstavlja imovinu za vlasnika. U tom smislu i standard ISO 27001 definiše informaciju kao *imovinu prema kojoj se u organizaciji treba odgovarajuće odnositi, kao i prema bilo kojoj drugoj imovini*. Kada je reč o materijalnoj imovini problem očuvanja vrednosti iste je u suštini dosta jednostavno definisati (onemogućiti krađu, onemogućiti oštećenja, osigurati pravilnu upotrebu, itd.). Sa druge strane, materijalna imovina je opipljiva i relativno je jednostavno shvatanje njenog očuvanja. Međutim, informacija je apstraktni pojam te je problem očuvanja njene bezbednosti unutar informacionog sistema teže prikazati. Tu značajnu ulogu igra standard ISO 27001:2005 u kom se kaže da se očuvanje informacije, odnosno njene vrednosti može ostvariti u okviru informacionog sistema tako što će se obezbediti tri osnovna zahteva:

- poverljivost – informacija mora biti dostupna samo ovlašćenim korisnicima;
- integritet – sadržaj informacije se ne sme promeniti bez dozvole vlasnika, i
- dostupnost – do informacije se može doći od strane ovlašćenog korisnika kada i gde je to potrebno.

Za informacioni sistem koji obezbeđuje ova tri aspekta bezbednosti u kontekstu standarda ISO 27001:2005 se kaže da je siguran, te da se u njemu čuva informaciona vrednost. No, ISO 27001 pored toga zahteva da se način uspostavljanja ova tri aspekta sigurnosti informacija ostvaruje kroz organizovani sistem i da se stanje sigurnosti stalno unapređuje. To se mora ostvarivati procesnim pristupom, a do unapređenja se dolazi tzv. PDCA krugom (slika 11). Poštovanjem ovih zahteva kaže se da kompanija ima sistem

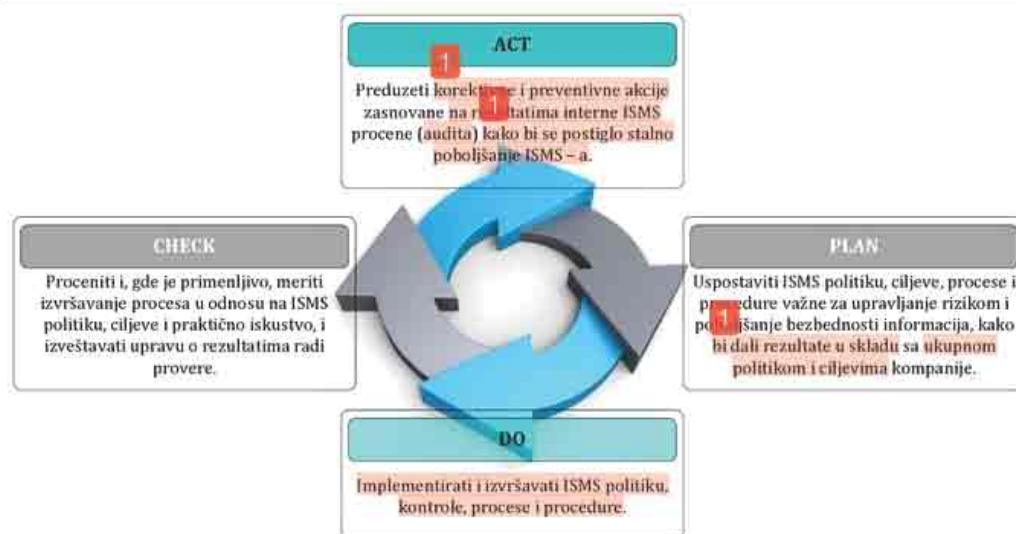
KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

za upravljanje bezbednošću informacija, poznat po akronimu ISMS (*Information Security Management System*).

Uspostavljanje ISMS u kompaniji je izuzetno složeno i ozbiljan posao koji mora uključiti tim specijalista. Uz to, sam proces vremenski dugo traje zbog obima posla i teškoća koje se tek pojavljuju. To znači, ukoliko se želi implementirati ISMS po pravilu se treba pokrenuti projekat s identifikovanim parametrima: ciljem (kvalitet realizacije), budžetom i vremenskim planom realizacije. Nakon završetka projekta implementacije ISMS u kompaniju i dobijanja sertifikata prema standardu ISO 27001, sam projekat automatski prelazi u proces upravljanja i unapređenja ISMS.

Slika 11: PDCA model ISMS prema ISO 27001:2005



Izvor: Prilagođeno prema: ISO 27001:2005.

Slikom 11. su prikazane faze PDCA modela za uspostavljanje i održavanje – unapređenje ISMS prema ISO 27001:2005. Početak implementacije (faze P i D) se definišu kao projekat implementacije. Nakon uspešno izvršenog projekta implementacije ISMS poziva se akreditaciono telo koje sertifikuje ISMS u kompaniji. Nakon toga nastavlja se životni ciklus ISMS prema PDCA krugu (faze C i A), te se ponovno prelazi na početnu fazu P. Međutim ta faza više ne predstavlja deo projekta, već deo uspostavljenog procesa sveukupnog upravljanja i poboljšanja ISMS. Važno je naglasiti da je standard ISO 27001:2005 u potpunosti usaglašen sa osnovnim standardom ISO 9001:2000, ali i sa ISO 14001:2004. To znači da se matično definisani zahtevi u pogledu uspostavljanja sistema upravljanja u okviru ISMS moraju apsolutno poštovati. Ovo dovodi do nužne integracije QMS i ISMS, i ta se integracija prvenstveno ogleda kroz jedinstveno i zajedničko rešavanje pitanja kao što su:

- upravljanje dokumentima i zapisima,
- upravljanje auditom (nezavisnom ocenom kvaliteta),

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

- korektivne i preventivne akcije,
- upravljanje imovinom i
- analiza.

Realizacija pojedinih faza projekta implementacije ISMS u kompaniju, a kasnije i poboljšanje sistema je vrlo kompleksno, prvenstveno zbog potrebe stalne procene rizika kao osnovnog pokazatelja šta i koliko treba preduzimati da bi se postigao odgovarajući stepen sigurnosti, ali i redovne pojave da je informacioni sistem vrlo dinamičan i podložan stalnim promenama kako po volumenu, tako i po sadržaju elemenata koji ga određuju.

1

Softverskim rešenjem Hestia se omogućava kvalitetna implementacija ISMS prema zahtevima standarda ISO 27001:2005 u svim fazama od planiranja do sertifikacije, a i kasnije u toku održavanja i unapređenja. Primenom programa Hestia ISMS korisnik ima sve potrebne alate za uspešno i optimalno uvođenje ISMS i kasnije upravljanje.

U svojoj strukturi softver Hestia ima nekoliko celina koje se međusobno funkcionalno i namenski bitno razlikuju. Njih čine:

- Sistemski deo – namenjen je za podešavanja, i aktivnosti vezane za funkcionisanje aplikacije. Tu spadaju npr. odabir jezika, podešavanje sigurnosti rada, itd.
- Opšti aplikativni deo – namenjen je za podešavanje podataka koji su zajednički za sve vrste upravljanja rizicima koji su zastupljeni u aplikaciji. To su podaci o korisniku aplikacije, organizaciona struktura, spisak osoba relevantnih za podršku upravljanja rizicima, definisanje opcija obrade rizika, tabela kritičnosti, razlozi primene kontrole, itd.
- Deo upravljanja rizicima - sadrži sve relevantne podatke vezane za upravljanje rizicima određenog tipa, odnosno namene. Tako npr. tu spadaju upravljanje operativnim rizicima, strateškim rizicima, rizicima informacija, rizicima kontinuitetom poslovanja, itd. Svaki od tih sistema upravljanja rizicima može imati posebna pravila, metodologiju, kriterijume koji se koriste.

U softveru Hestia implementirano je nekoliko obrazaca upravljanja rizicima za specifična područja primene, kao npr. za ISMS, za EMS, za OHSAS, za BCM, za strateške rizike, za operativne rizike, za projektne rizike, za kritične infrastrukture, itd. Svaki od tih pojedinih sistema upravljanja rizicima ima neke specifičnosti i u softveru se za njih definišu posebni metodološki pristupi procene rizika. Pored toga, moguće je otvoriti više istih tipova upravljanja rizicima, ali s različitim (ili istim) metodološkim elementima.

U praksi su se u pojedinim sistemima upravljanja rizicima postigli različiti nivoi definisanosti kako u smislu prateće dokumentacije, tako i u smislu metodološkog pristupa. U softveru Hestia primenjena je najbolja praksa i unificirana svim sistemima upravljanja rizicima.

Softversko rešenje Hestia se zasniva na primeni međunarodnog standarda ISO 31000, ali i ostalih srodnih smernica, kao npr. ISO/IEC 27005, ISO 22301, itd. Neka područja primene su: Bezbednost informacija (ISO/IEC 27001), Servis menadžment (ISO/IEC 20000), kontinuitet poslovanja (ISO 22301), zaštita okruženja (ISO 14001), projektni rizici, operativni rizici, strateški rizici, kritične infrastrukture, itd. Međunarodni standard ISO 31000 obezbeđuje principe i generičke smernice za upravljanje rizicima. Mogu ga

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

koristiti bilo koja javna ili privatna preduzeća, organizacije, udruženja, grupe ili pojedinci. Zato, ovaj standard nije namenjen nekoj specifičnoj industriji ili području.

Na slici 12. je prikazana blok shema funkcionalnih mogućnosti softvera Hestia. Kao što se može videti softver Hestia ima šest glavnih modula sa sledećim funkcijama:

- ISMS – upravljanje rizicima za potrebe sistema upravljanja sigurnošću informacija, zasnovano na normama ISO 27001 i ISO 27005;
- OHSAS – upravljanje rizicima prema normi OHSAS 18001;
- EMS – upravljanje rizicima za zaštitu životne sredine na temelju normi ISO 14001 i ISO 31000;
- PROCES – upravljanje rizicima na poslovnim procesima bazirano na normi ISO 31000;
- PROJEKAT – upravljanje rizicima na projektima prema PMBOK i normi ISO 31000;
- OPERATIVNI – upravljanje operativnim rizicima zasnovano na ISO 31000;
- INCIDENT – upravljanje incidentima za bilo koju vrstu rizika prema normi ISO 27035;
- DOKUMENT – upravljanje dokumentacijom prema normi ISO 9001, ISO 10013, ISO 27001;
- KOMUNIKACIJA – upravljanje komunikacijama između zainteresovanih strana;
- ADMINISTRACIJA – modul za administrativno održavanje softvera, određivanja prava rada, itd.

Slika 12: Funkcionalna shema softverskog alata Hestia



Izvor: Prilagođeno prema: Adelsberger, Z. (2014)

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Ovako široka funkcionalnost softvera Hestia posledica je praktičnih potreba koje se pojavljuju u kompanijama. Naravno, da pojedini korisnici ne koriste sve module, već se na početku primene koncentrišu na jedno područje, ono koje im je u tom trenutku primarno, a onda ta iskustva proširuju na ostala područja kako im potrebe i pozitivno iskustvo nalažu.

Glavni moduli programa Hestia ISMS su:

- Modul za definisanje opcija programa i pravila kojima se izvršava program kod korisnika;
- Modul za administraciju (održavanje baze podataka, arhiviranje baze, evidencija i prava korisnika, itd.);
- Modul matičnih podataka (evidencije osoblja, organizacija, partnera, poslovnih procesa, itd.) relevantnih za informacioni sistem kompanije;
- Modul za upravljanje informacionom imovinom;
- Modul za definisanje pravila procene rizika (ranjivosti, pretnje, sigurnosne mere);
- Modul za optimalnu selekciju kontrola za pretnje i ranjivosti prema klasifikaciji informacione imovine;
- Modul upravljanja rizicima (procena rizika, obrada rizika);
- Modul za automatsko generisanje dokumenta "Izjava o primenljivosti" (SoA);
- Modul za izveštavanje i komunikaciju sa zainteresovanim stranama;
- Modul za upravljanje dokumentacijom;
- Modul za izradu šablona (template) za politike, procedure, uputstva i zapise;
- Ugrađen tekst procesor za obradu dokumenata (kompatibilan s MS Wordom);
- Ugrađen grafički program za crtanje dijagrama toka (Flow Chart);
- Modul za import baza "najbolje prakse" za politike i procedure, ali i ostale tipove dokumenata.

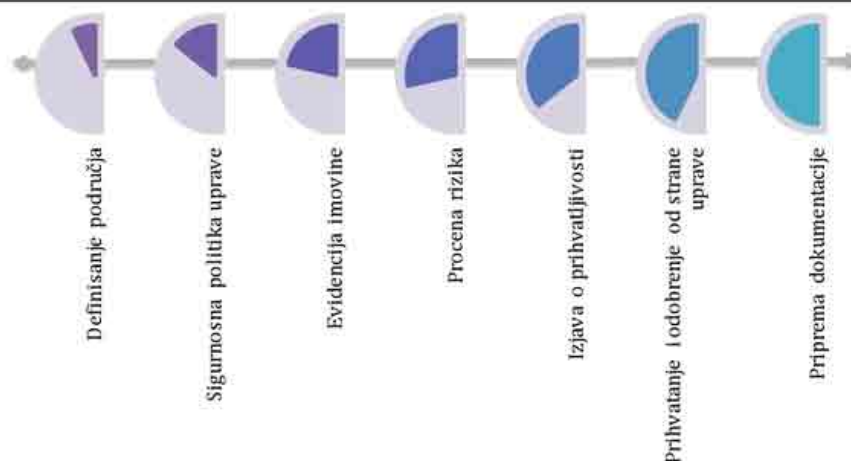
Svi ugrađeni moduli u funkcionalnom smislu u potpunosti zadovoljavaju prvenstveno sve zahteve koji za te poslove traže standardi (ISO 27001, ISO 27002, BS 7799-3, ISO 9001, itd.).

Posebna pažnja je poklonjena jednostavnosti rada primenom najnovijih programskih tehnika što je dovelo do intuitivnog rešenja koje korisnici vrlo lako prihvataju. Zbog svoje konfiguracije i tehnike realizacije, program HESTIA se može koristiti i za obuku ili treninge tima koji vrši implementaciju. Platforma na kojoj program radi su od MS XP do WIN 2K servera kao deljena aplikacija ili u modu client/server, pa se može pokretati i preko intraneta/interneta. Sama tehnika primene programa Hestia u prvom redu se svodi na poštovanje procedure implementacije kako je manje više zadata i zahtevana standardom ISO 27001:2005. Na osnovu tih zahteva proces implementacije – uvođenja ISMS u kompaniju se može prikazati kao što je prikazano na slici 13.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Slika 13: Shema implementacije ISMS



Izvor: Prilagođeno prema: ISO 27001:2005.

Ne postoji unapred određeno pravilo koliko nivoa bi trebalo odabrati za rangiranje parametara, ali što je veći broj dobija se i veće polje vrednosti rezultata. Ali sa druge strane veći broj nivoa ranga otežava opis kojim bi se razlikovali susedni nivoi ranga. Zato se najčešće odabiraju skale koje imaju 3 ili 5, a ređe i više nivoa ranga.

Slika 14: Definisane broja nivoa opasnosti, posledica, pretnji, ranjivosti i rizika

Options

Risk: ☐ Količina prihvatljivosti ☐ Broj nivoa opasnosti / ranjivosti

Preporuka / Broj nivoa opasnosti: ☐ 3 ☐ 5 ☐ 7

Procena nivoa ranjivosti: ☐ Pritužba: ranjivost, posledica ☐ Vjerojatnost: posledica

Vrednost: ☐ Očekivati iznosnu posledicu na proceni

Nivni posledica:

- C -
- I -
- A -
- Posledica X:
- Posledica Y:
- Posledica Z:

Opasnost posledica:

Vrednost	Naziv	Financijska vrednost	Opis
1	Very Low	0.00	ISMS
2	Low	0.00	ISMS
3	Medium	0.00	ISMS
4	High	0.00	ISMS
5	Very High	0.00	ISMS

Prilagođeno

Prilagođeno

Prilagođeno

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Pored toga preporuka je da te dve tabele imaju isti broj nivoa jer su ta dva parametra definisana za matricu rizika prema ISO 31000, koja je uobičajeno kvadratnog oblika. Slika 14. prikazuje način definisanja broja nivoa u softveru Hestia.

Na osnovu gornje dve skale može se izračunati rizik prema formuli

$$\text{Rizik} = \text{Opasnost} \times \text{Posledica}$$

Prema ISO 31000, dobijene vrednosti rizika se moraju rangirati. U tu svrhu se koristi tabela rangiranja rizika koja opet može imati manji ili veći broj nivoa ranga. S praktične strane zadovoljava rangiranje na tri ili pet nivoa. Na osnovu tabele rangiranja rizika može se dobiti matrica rizika koja je prema ISO 31000 osnovni alat menadžmenta za definisanje i merenje sigurnosne politike. Način definisanja matrice prikazan je na slici 15.

Slika 15: Definisanje matrice rizika



Izvor: autor

Softver Hestia čine sledeće celine:

- Opšti podaci – podaci koji su zajednički za sve module, kao npr. registar zaposlenih, organizacionih jedinica, itd.
- Upravljanje dokumentacijom - modul kojim se u potpunosti može upravljati dokumentacijom, sa svim relevantnim zahtevima koji su definisani kroz niz ISO standarda.
- ISMS upravljanje rizicima – modul specijalizovan za upravljanje rizicima u području IT bezbednosti.
- Upravljanje rizicima u poslovnim procesima – modul specijalizovan za upravljanje rizicima koji su identifikovani i mapirani u kompaniji.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

- Upravljanje operativnim rizicima – modul koji je posebno prilagođen BASEL II.
- Servis podataka – više modula kojima se vrši servisiranje aplikacije, kao npr. arhiviranje podataka, reorganizacija baze podataka, evidencija korisnika programa i definisanje njihovih radnih procedura, itd.

Da bi se uspešno radilo sa programom, pretpostavka je da korisnik ima osnovna znanja o upravljanju rizicima i da ima uvid u zahteve i preporuke najbolje prakse koji se nalaze u pojedinim relevantnim međunarodnim i/ili nacionalnim standardima.

U okviru softverskog alata Hestia koristi se kvalitativna metoda procene rizika, jer problematika za upravljanje rizicima na koju se odnosi program praktično se ne može tretirati nekom drugom metodom, osim u ekstremnim specijalnim slučajevima.

Fizički model procene rizika se zasniva na primeni sledećih pojmova: objekat procene rizika, pretnje, ranjivosti, posledice i kriterijum prihvatljivosti rizika. Osnovni element modela procene rizika je objekat procene rizika. On može biti poslovni proces, projekat, neka aktivnost, neka oprema, ugovor sa partnerom, zaposleni, saradnici, itd. U skladu sa definicijama i značenjem pojedinih elemenata procene rizika fizički model procene rizika se može opisati na sledeći način: *“za bilo koji odabrani objekat procene rizika važi pravilo: ako postoji bilo kakva vrednost tog objekta (finansijska, poslovna, funkcionalna ili bilo kakva druga), onda postoje veće ili manje pretnje iz raznih izvora koje nastoje naneti štetu vlasniku objekta”*. To u žargonu sistema za upravljanje rizicima znači da postoji realna šansa da će neka pretnja (jedna ili više) u nekom trenutku iskoristiti ranjivost objekta i izazvati štetne posledice. Što znači: svaki objekat egzistira u uslovima hazarda, odnosno obavlja svoju funkciju u uslovima nesigurnosti za ispunjenje poslovnih ciljeva vezanih za taj objekat. Do posledica, realizacije rizika, može doći samo u slučaju da jedna ili više pretnji iskoristi ranjivost objekta. Ukoliko objekat nije ranjiv za te pretnje, tada ne može doći do realizacije rizika, odnosno do incidenta (Adelsberger, 2010).

Glavna funkcija procene rizika je odrediti nivo te nesigurnosti, odnosno koliki je rizik za odabrani objekat da će doći do pojave incidenta. Svaka kompanija po prirodi stvari nastoji poslovati sa što manjim rizicima. Smanjivanje rizika na niži nivo znači po pravilu i veću investiciju. Nivoi tih investicija mogu biti izuzetno veliki čak do finansijske nepodnošljivosti u kompaniji. Zbog toga se od strane top menadžmenta definišu, kroz sigurnosnu politiku, stav i odnos, kao i ciljevi koji se žele postići u smislu rizika, odnosno nesigurnosti poslovanja. To je uvek kompromis između mogućnosti i želja. Kako god bilo, svaka kompanija koja formalno brine o rizicima ima definisani prag prihvatljivosti rizika. Svi rizici ispod tog praga su prihvatljivi, za razliku od onih koji su preko tog praga. Za sve rizike koji su iznad praga prihvatljivosti rizika treba sprovesti tzv. obradu rizika, odnosno nastojati ako je to ikako moguće, smanjiti rizik na prihvatljiv nivo.

Da bi se moglo izvršiti vrednovanje rizika koristi se sledeća matematička formula:

$$R = T \times V \times I$$

gde su: R – rang rizika (*risk*),
T – veličina pretnje (*threat*),
V – veličina ranjivosti (*vulnerability*) i
I – veličina posledice (*impact*).

• • •

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Teorijski okvir istraživanja

Matematički model procene rizika se zasniva na tzv. kvalitativnom modelu. Razlog za to je činjenica da parametri koji se koriste za vrednovanje rizika nemaju temelj u egzaktnim vrednostima, već se po pravilu procenjuju koliki bi mogli biti. Osnovu za to čine iskustvo procenitelja, statistički, istorijski podaci i relevantna literatura.

Evaluacija rizika se bavi procenom verovatnoće i posledica pojedinih pretnji na imovinu.

Kod procene rizika prvi korak je popunjavanje polja za pretnje i ranjivosti koje su unapred definisane. Tada je potrebno za svaku ranjivost upisati vrednosti za pretnju, te se na osnovu kalkulacije automatski izračunava rizik za tu ranjivost. Za svaku procenjenju ranjivosti nudi se mogućnost obrade rizika. Obrada rizika je proces donošenja odluke. Za svaki rizik, obrada rizika se sastoji od odabira jednog od četiri moguća stanja:

- prihvatanje rizika (zadržavanje rizika) – predstavlja uobičajeni metod rešavanja rizika, kada pojedinac ili kompanija ne preduzima ništa (svesno ili nesvesno) da izbegne, umanjí ili prenese rizik,
- izbegavanje rizika – rizik se izbegava kada pojedinac ili kompanija ne žele da prihvate rizik,
- prenos rizika – rizik se može preneti sa jednog pojedinca (operacije ili kompanije u slučaju lanca snabdevanja) na drugog koji je spremniji da snosi rizik ili
- smanjivanje rizika – koje se postiže sprečavanjem ili kontrolom.

Ukoliko se odabere bilo koja opcija, osim prihvatanja rizika, tada je potrebno uneti kontrolne mere kojima će se odabrani rizik rešiti.

Kod obrade rizika potrebno je odabrati kontrolnu meru, odgovornu osobu, definisati budžet, datum početka i završetka sprovođenja kontrole, svrhu sprovođenja kontrole, te koje su očekivane vrednosti pretnje i ranjivosti nakon sprovođenja kontrolnih mera, nakon čega se automatski izračunava preostali rizik. Preostali rizik je onaj rizik koji ostaje nakon sprovedenih mera za otklanjanje rizika.

Kontrola je bilo koja administrativna, upravljačka, tehnička ili pravna metoda korišćena za upravljanje rizikom, a koja uključuje praksu, politiku, proceduru, programe, tehnike, tehnologije, uputstava i organizacione strukture.

Pretnja je potencijalni događaj. Kada pretnja pređe u stvarni događaj, može prouzrokovati neželjeni incident. Neželjeni je zato što može naštetiti kompaniji ili sistemu.

Ranjivost je slabost imovine ili grupe imovina. Ta slabost može biti iskorišćena od strane jedne ili više pretnji. Moguće je definisati neograničen broj grupa ranjivosti.

Povezivanje pretnji i ranjivosti omogućava visoki stepen automatske procene rizika kod evaluacije rizika.

Grupe rizika se koriste za grupisanje srodnih pretnji. Koriste se kod definisanja grupa imovine, da bi se odredilo koje pretnje i ranjivosti mogu biti iskorišćene za ugrožavanje imovine u toj grupi. Na ovaj način ubrzava se postupak dodeljivanja pretnji i ranjivosti imovini. Broj grupa rizika takođe je neograničen.

2.3. Rezime poglavlja

Logistika predstavlja novu paradigmu za postizanje konkurentnosti kompanije u različitim proizvodnim i uslužnim sektorima. Pokretačka snaga logistike transformiše se od projektovane minimizacije troškova i maksimizacije kvaliteta usluge i/ili finalnog proizvoda, na sistemski pristup izučavanju složenih logističkih fenomena. Složenost, kompromisi, efikasna koordinacija, konflikti i potreba da se vodi računa o odnosima van logističkog sistema, kao implikacije sistemskog pristupa izučavanju logističkog sistema i logističkih podsistema ukazuju na važnost logistike u cilju kreiranja pozitivnog privrednog okruženja.

Pred svakom međunarodno orijentisanom kompanijom dominantan značaj, u odnosu na ostale faktore poslovnog uspeha, ima upravljanje lancima snabdevanja, jer je obezbeđivanje raspoloživosti zahtevanog proizvoda u pravo vreme, na pravom mestu i po prihvatljivim troškovima daleko teže ostvariti u planetarnim nego u nacionalnim okvirima.

Primarna svrha lanca snabdevanja je povezivanje glavnih poslovnih funkcija i procesa između kompanija u konzistentan poslovni model sa maksimalnim učinkom. Iako još uvek ne postoji opšte prihvaćena definicija lanca snabdevanja, niti model njegovog upravljanja, može se okvirno reći da lanac snabdevanja predstavlja skup kompanija koje međusobno podržavaju realizaciju materijalnih tokova i sa njima povezanih informacionih i novčanih tokova.

Funkcija upravljanja lancem snabdevanja suočava se sa izazovima koje pred nju postavljaju rizici iz internog i eksternog okruženja svih članova lanca snabdevanja. Posledice izazvane rizicima mogu biti različitog intenziteta, od neprimetnih do katastrofalnih. Prema usvojenoj definiciji, rizik u lancu snabdevanja predstavlja proizvod pozitivne verovatnoće pojave smetnje koja će uticati na funkcionisanje sistema i evidentnih ili neevidentnih posledica po stabilnost sistema.

Efikasno upravljanje rizicima u lancima snabdevanja direktno implicira njihovu kategorizaciju. Analizom relevantne i dostupne literature koja se bavi problematikom kategorizacije rizika u lancima snabdevanja, došlo se do zaključka da postoji više od 70 vrsta strukturno različitih rizika u lancima snabdevanja.

Dakle, upravljanje rizikom je važno sredstvo u obezbeđivanju ekonomskog integriteta kompanije, posebno ukoliko se jasno postave granice kompanije. U okruženju upravljanje lancem snabdevanja postaje zamagljeno, što ne znači da ono zakonski više ne postoji, ali proces identifikovanja linije razdvajanja između dve kompanije postaje veoma težak. Paralelno sa proširenjem obima upravljanja lancem snabdevanja, upravljanje rizikom treba da postane odgovornije.

3. MATEMATIČKI MODEL PROCENE RIZIKA U LANCIMA SNABDEVANJA

Kinney metoda, koja se u praksi najčešće upotrebljava za procenu i vrednovanje rizika, usled pojave utvrđenih OH&S (*Occupational safety and health* – Bezbednost i zdravlje na radu) opasnosti, je u cilju izrade ove teze primenjena na identifikovane rizike u lancima snabdevanja.

Kao što je objašnjeno u drugom poglavlju, Kinney metoda se bazira na:

1. Verovatnoći pojave i realizacije mogućeg nepovoljnog događaja – (V),
2. Učestalosti (vreme izlaganja opasnostima/štetnostima) – (U) i
3. Posledicama – težini povreda ili oboljenja, u ovom slučaju težina nastale posledice po stabilno funkcionisanje sistema (P).

Prema tome, rang rizika (R) se računa po formuli: $R = V \times U \times P$

Dobijeni proizvod se klasifikuje u odgovarajući rang, odnosno nivo rizika, kao što je prikazano u tabeli 13.

Tabela 13: Rang rizika u lancima snabdevanja po Kinney metodi

RANG	NIVO RIZIKA	OCENA	MERE KOJE TREBA PREDUZETI
I	Prihvatljiv	$R \leq 20$	Ne preduzimati dodatne mere
II	Mali	$20 < R \leq 70$	Potreban oprez, rešiti ga redovnom procedurom – radnim uputstvom
III	Umereni	$70 < R \leq 200$	Potrebne mere, moraju se utvrditi odgovornosti
IV	Visoki	$200 < R \leq 400$	Potrebna brza reakcija od strane višeg rukovodstva zahtevati poboljšanje od prvog pretpostavljenog
V	Ekstremni rizik	$R > 400$	Prekinuti aktivnost. Potrebna momentalna akcija od strane najvišeg rukovodstva

Izvor: Prilagođeno prema: Kinney, G.F., Wiruth, A.D. (1976), op. cit.

Polazeći od podataka iz tabele 3 u kojoj su prikazane kategorije i podkategorije identifikovanih rizika, odnosno opasnosti u lancu snabdevanja, primenom matematičke formule na kojoj se zasniva Kinney metoda, dobijeni su podaci interpretirani u tabeli 14.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Matematički model procene rizika u lancima snabdevanja

Tabela 14: Procena rizika u lancu snabdevanja primenom Kinney metode

RB	Prepoznavanje i utvrđivanje opasnosti	Izvršioči u riziku	Primenjivani zakoni i propisi	Procena rizika				
				Verova- noća	Posledice	Učestalost	V x P x U	Rang rizika
1	2	3	4	5			6	7
LJUDSKI RESURSI								
101	Dostupnost stručnog kadra			1.0	3.0	10.0	30.0	II
102	Ponašanje zaposlenih			6.0	3.0	10.0	180.0	III
103	Odnosi zajednica			3.0	1.0	2.0	6.0	I
104	Zdravlje i bezbednost			10.0	10.0	6.0	600.0	V
105	Outsourcing			6.0	3.0	2.0	36.0	II
106	Komunikacije			6.0	6.0	3.0	108.0	III
PROIZVODI I TRŽIŠTA								
201	Pitanja potrošača i tržišni trendovi			6.0	3.0	2.0	36.0	II
202	Spoljna sredina			6.0	6.0	2.0	72.0	III
203	Konkurentsko okruženje			6.0	3.0	1.0	18.0	I
204	Zlonamerni napadi na proizvod			3.0	3.0	3.0	27.0	II
205	Proizvodni proces :: Kvalitet i rizik			10.0	10.0	6.0	600.0	V
206	Trgovačke marke :: Brand name erozija			1.0	2.0	1.0	2.0	I
207	Upravljanje sa odnosima			3.0	2.0	2.0	12.0	I
208	Marketing i promocije			0.5	2.0	1.0	1.0	I
209	Komercijalizacija novih proizvoda			3.0	3.0	3.0	27.0	II
210	Zalihe			6.0	6.0	6.0	216.0	IV
INFRASTRUKTURA								
301	Akcije Vlade			3.0	6.0	1.0	18.0	I
302	Pravna odgovornost :: Pravni okviri			6.0	10.0	2.0	120.0	III
303	Skladišta			6.0	6.0	10.0	360.0	IV
INFORMACIJE								
401	Nedostatak informacija za donošenje odluka			1.0	3.0	2.0	6.0	I
402	Gubitak pristupa informacijama			0.5	6.0	1.0	3.0	I
403	Neovlašćen pristup informacijama			6.0	6.0	1.0	36.0	II
404	Dizajn informacione infrastrukture			1.0	3.0	1.0	3.0	I

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Matematički model procene rizika u lancima snabdevanja

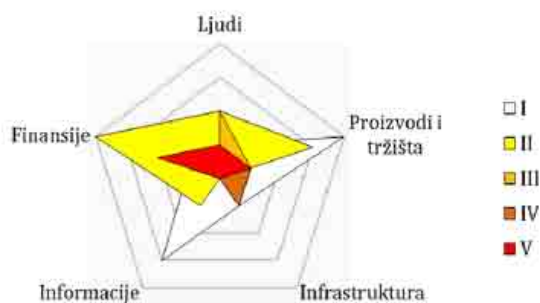
Tabela 14: Procena rizika u lancu snabdevanja primenom Kinney metode - nastavak

RB	Prepoznavanje i utvrđivanje opasnosti	Izvršioči u riziku	Primenjivani zakoni i propisi	Procena rizika				
				Verova- tnoća	Posledice	Učestalost	V x P x U	Rang pretnje
1	2	3	4	5			6	7
FINANSIJE								
501	Nestabilnost valute :: Devizno poslovanje :: Nestalnost kamatne stope			6.0	6.0	10.0	360.0	IV
502	Finansijske kontrole			3.0	6.0	2.0	36.0	II
503	Greške u finansijskim izveštajima			1.0	3.0	2.0	6.0	I
504	Predviđanje veličine budžeta kao upravljanje tokovima gotovine			3.0	6.0	2.0	36.0	II
505	Cena robe			10.0	6.0	10.0	600.0	V
506	Dostupnost kapitala			6.0	6.0	1.0	36.0	II
507	Krade inventara :: Prevare			10.0	6.0	10.0	600.0	V
508	Vrednovanje imovine			3.0	3.0	6.0	54.0	II

Izvor: autor

Na osnovu izvršene kvantifikacije rizika u lancima snabdevanja po Kinney metodi, zaključuje se da je nivo ekstremnog rizika identifikovan u sferi ljudskog faktora i oblasti finansija, dok su prihvatljivi rizici, za koje nije potrebna posebna intervencija, najčešći u oblasti informacija i proizvoda i tržišta (deo marketing i konkurencija) (slika 16.)

Slika 16: Grafički prikaz pojave identifikovanih rizika u lancima snabdevanja po nivoima I – V



Izvor: autor

3.1. Predlog mera za otklanjanje rizika u lancima snabdevanja

Efektivna bezbednost i zaštita lanca snabdevanja obuhvataju osnovne standarde za fizičku bezbednost, kontrolu pristupa, bezbednost osoblja, obrazovanje i obuku, proceduralnu sigurnost, bezbednost IT, poslovnih partnera, kao i bezbedan transfer iz tačke porekla do krajnje destinacije u okviru lanca snabdevanja. Polazeći od dobijenih podataka u tabeli 14. autor daje predlog mera za otklanjanje/ublažavanje svih identifikovanih rizika u lancima snabdevanja, bez obzira na rang rizika, odnosno i za one rizike koje nije potrebno tretirati, upravo zbog različitih specifičnosti kompanija koje bi, eventualno, mogle da iskoriste ovaj model u cilju efikasnog upravljanja rizicima u svom poslovanju.

Tabela 15: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji ljudski faktor

KATEGORIJA SUBKATEGORIJA	PREDLOŽENE MERE
Ljudski faktor	Dostupnost stručnog kadra
	uvodenje HR službe, interakcija sa NSZ, selekcija kadrova prilikom zapošljavanja kroz razne vidove testova, razgovora, intervjua, rešavanja konkretnog problema, probni rad
	Ponašanje zaposlenih
	uvodenje etičkog kodeksa zaposlenih, obuka zaposlenih, pojačana kontrola prilikom izlaza i ulaza u kompaniju, uvodenje ID kartica i sistema evidencije pristupa, pojačane disciplinske mere
	Odnosi zajednica
Ljudski faktor	podizanje ugleda kompanije kroz donacije, sponzorstva, kulturne manifestacije, davanje stipendija talentovanim učenicima
	Zdravlje i bezbednost na radu
	donošenje Akta o proceni rizika i Pravilnika o zaštiti od požara, obuka zaposlenih iz poznavanja propisa BZR 56 štite od požara, periodične provere znanja, lekarski pregledi zaposlenih koji rade na mestima sa povećanim rizikom, nabavka adekvatne opreme i korišćenje LZS
Ljudski faktor	Outsourcing
	usavršavanje zaposlenih, stimulisanje zaposlenih, davanje prvenstva svojim radnicima
Ljudski faktor	Komunikacije
	razmena informacija treba da postane norma, na taj način će biti mnogo lakše da se obezbedi efikasna komunikacija. Kreirati strategiju i plan komunikacije (npr. Power Point prezentacija). Organizovati nedeljne redovne sastanke projektnog tima sa ciljem razmene informacija, redovno ažuriranje e-pošte sa najnovijim vestima projekta, online diskusioni forum gde članovi projektnog tima mogu da postavljaju pitanja i dobijaju odgovore sa rezultatima, pretraživanje kataloga projektne dokumentacije radi lakšeg korišćenja, uključujući i proces upravljanja.

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Matematički model procene rizika u lancima snabdevanja

Tabela 16: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji proizvodi i tržišta

KATEGORIJA SUBKATEGORIJA	PREDLOŽENE MERE
Proizvodi i tržišta	Pitanja potrošača i tržišni trendovi
	Spoljna sredina, okruženje
	Konkurentsko okruženje
	Zlonamerni napadi na proizvod/uslugu
	Kvalitet proizvodnog procesa
	Trgovačke marke
	Brand name erozija
	Upravljanje sa odnosima (klijenti i konkurenti)
	Marketing i promocije
	Komercijalizacija novih proizvoda
	Zalihe

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Matematički model procene rizika u lancima snabdevanja

Tabela 17: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji infrastruktura

KATEGORIJA SUBKATEGORIJA	PREDLOŽENE MERE
Infrastruktura	Akcije Vlade
	donacije, krediti i subvencije, razmena informacija sa obe strane, smanjenje cena nacionalne proizvodnje, informisanost o kratkoročnim i dugoročnim planovima Vlade, usvajanje međunarodnim i nacionalnim standardima
	Pravna odgovornost Pravni okviri
	za svaki sistem u organizaciji treba eksplicitno definisati, dokumentovati i ažurno održavati sve odgovarajuće propise, statutarne i ugovorne zahteve, kao i pristup kompanije zadovoljenju ovih zahteva, projektovati i implementirati politiku zaštite i tajnosti podataka kompanije, redovna provera usklađenosti sistema sa standardima
	Skladišta
	ulaganja u infrastrukturu: investicije u transport, energetske infrastrukturu, IT infrastrukturu, skladišta, meteo stanice, itd.

Izvor: autor

Tabela 18: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji informacije

KATEGORIJA SUBKATEGORIJA	PREDLOŽENE MERE
Informacije	Nedostatak informacija za donošenje odluka
	keriranje jedinstvene baze podataka, organizovanje periodičnih sastanaka rukovodstva i odgovornih zaposlenih
	Gubitak pristupa informacijama
	istraživanje tržišta i načina poslovanja konkurenata
	Neovlašćen pristup informacijama
	fizička zaštita informacija od neovlašćenog pristupa, softverska zaštita prava pristupa, evidencija zapisa o pristupu i manipulacija informacijama, promena ključeva/brava, passworda, ukidanje prava pristupa
	Dizajn informacione infrastrukture
	izrada portfolia usluga, podizanje kvaliteta P/U, adekvatna implementacija IT usluga i servisa

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Matematički model procene rizika u lancima snabdevanja

Tabela 19: Predlog mera za ublažavanje/otklanjanje rizika u lancu snabdevanja u kategoriji finansije

KATEGORIJA SUBKATEGORIJA	PREDLOŽENE MERE
Finansije	Nestabilnost valute 75
	Devizno poslovanje
	Nestabilnost kamatne stope
	Finansijske kontrole
	Greške u finansijskim izveštajima
	Predviđanje veličine budžeta kao upravljanje tokovima gotovine
	Cena P/U
	Dostupnost kapitala
	Krade inventara
	Prezare
	Vrednovanje imovine

Izvor: autor

Navedene mere za ublažavanje i otklanjanje identifikovanih rizika u lancu snabdevanja, iskorištene su kao jedan od inputa – polaznih podataka koje je neophodno definisati pre sprovođenja procene rizika u lancima snabdevanja primenom softverskog alata Hestia.

3.2. Rezime poglavlja

Proces procene rizika je od vitalnog značaja i podrška procesu donošenja odluka u kompaniji. Različite kompanije koriste različite metode za procenu rizika, čiji nivoi sofisticiranosti u samom procesu variraju. Kinney metoda za procenu rizika uvedena je prvi put u upotrebu 1976. godine u okviru vojne industrije. Kao takav, metod je naišao na opšti uspeh širom Evrope. Većina relevantnih literaturnih izvora upravo ovu metodu kvalifikuje kao bazičnu metodu procene rizika.

Evaluacija i rangiranje rizika, po ovoj metodi, nastavlja da bude lider u oblasti širom država članica EU. Na primer, u Belgiji je Kinney metoda univerzalan alat, kako u velikim kompanijama, tako i u malim i srednjim preduzećima. Po Kinney metodi procena rizika se posmatra kroz tri parametra, i to: verovatnoća pojave opasnosti, učestalost izlaganja opasnostima i težina nastale posledice. Verovatnoća nastanka štete tokom izlaganja faktorima rizika je isključivo nenamernog, stohastičkog i neizvesnog karaktera. Procenjeni rizici se svrstavaju u jedan od pet definisanih nivoa: ekstreman rizik, visok rizik, umeren rizik, mali rizik i prihvatljiv rizik.

Polazeći od kategorija i podkategorija identifikovanih rizika, odnosno opasnosti u lancu snabdevanja, primenom matematičkog izraza na kojem se zasniva Kinney metoda, došlo se do zaključka da je ekstremni rizik evidentan u svim mapiranim procesima lanca snabdevanja u kojima ljudski faktor igra ključnu ulogu, od proizvodnog procesa, finansijskih obračuna, pa do neetičkog ponašanja u smislu krađe imovine i sl. Sa druge strane, prihvatljivi rizici su identifikovani na mestima u lancu snabdevanja gde uslove poslovanja diktira entitet iz okruženja, na čije odluke kompanija nema direktan uticaj (Vlada, zakonska regulativa, konkurentske kompanije, itd.).

4. STUDIJA SLUČAJA PROCENE RIZIKA U LANCIMA SNABDEVANJA PRIMENOM SOFTVERSKOG ALATA HESTIA

U cilju dokazivanja istinitosti postavljene hipoteze, da je procenu identifikovanih rizika u lancima snabdevanja moguće automatizovati, ovim poglavljem je prikazan proces automatizovane obrade podataka (polazni parametri: resurs, ranjivost, pretnja, mera za otklanjanje) pri proceni rizika u lancima snabdevanja primenom softverskog alata Hestia. Način funkcionisanja osnovne verzije softverskog alata Hestia objašnjen je u drugom poglavlju. Da bi se softver efikasno i efektivno primenio na studiji slučaja procene rizika u lancima snabdevanja, izvršene su modifikacije uslova i kriterijuma kao što je prikazano tabelom 6. Na taj način je modifikovani softverski alat Hestia usklađen sa generisanim parametrima Kinney metode, kako bi se zaokružio ciklus procene rizika u lancima snabdevanja.

U predmetnoj studiji slučaja rizik, u stvari, predstavlja verovatnoću da će određena pretnja/izvor rizika iskoristiti ranjivost imovine/procesa, što se manifestuje kroz gubitak poverljivosti, integriteta ili raspoloživosti lanca snabdevanja. Matematički model procene rizika se zasniva na tzv. kvalitativnom modelu. Razlog za to je činjenica da parametri koji se koriste za vrednovanje rizika nemaju temelj u egzaktnim vrednostima, već su po pravilu subjektivni od strane lica koje procenjuje rizike. Inicijalnu fazu predstavlja generisanje liste unapred definisanih procesa, pretnji i ranjivosti u lancu snabdevanja. Zatim se za svaku ranjivost upisuje vrednosti za pretnju, te se na osnovu kalkulacije automatski izračunava rizik za tu ranjivost. Za svaku procenjenju ranjivost nudi se mogućnost obrade rizika. Obrada rizika je proces donošenja odluke.

4.1. Procesi u lancu snabdevanja

Prema definiciji resurs (u lancu snabdevanja) predstavljaju:

- ljudi, veštine, iskustvo i stručnost; sredstva potrebna za svaki korak u procesu upravljanja rizikom;
- procesi, metode i alati kompanije koji se koriste za upravljanje rizikom;
- dokumentovani procesi i procedure;
- informacije i sistemi za upravljanje znanjem i
- programe obuke (ISO 31000, 2009).

Na slici 17. prikazan je pregled 27 procesa u lancima snabdevanja, koji su grupisani u devet specifičnih grupa. Za svaki proces je pojedinačno analizirano koji bi uticaj na poverljivost, integritet i raspoloživost mogli da ostvare potencijalni rizici. Nakon analize, svakoj grupi procesa su pridružene određene grupe rizika (slika 18).

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 17: Lista procesa u lancu snabdevanja

Name	Serial	System ID	Version	Supplier	C	T	A	K	V	Z
<ul style="list-style-type: none"> <ul style="list-style-type: none"> PROCENA RIZIKA U LANCIMA SNABDEVANJA DIZAJN PROCESA DELEGIRANJE AUTORITETA DEPARTMANIZACIJA USPOSTAVLJANJE RASPODA KONTROLE UTVRĐIVANJE I PODELA POSLOVA KOMUNIKACIJA SA OKRUZENIEM I ZAKONSKA REGULATIVA KOMUNIKACIJA POSTOVANJE ZAKONSKIH PROCEDURA I STANDARDA MEHUŽNJE I PREDVIĐANJE POTRAŽNJE KONTROLA PROIZVODNJE KUPovina MATERIJALA PLANIRANJE MATERIJALA SKLADIŠTENJE PLANIRANJE I PREDVIĐANJE POTRAŽNJE PLANIRANJE BEZBEDNOSNIH ZALUHA PLANIRANJE DISTRIBUCIJE PLANIRANJE I PREDVIĐANJE TRAZNJE PLANIRANJE MREŽE SNABDEVANJA POVRATNI PROCESI POTVRDAJ ZAMENA PROIZVODNI PROCES IZVRŠENJE PROIZVODNJE PRIPREMI DEO PROIZVODNJE ZAVRSNI DEO PROIZVODNJE TRANSPORTNI PROCES ISTOVAR TRANSPORT UTOVAR UPRAVLJANJE FINANSIJAMA POSLOVI FINANSUSKOG UPRAVLJANJA POSLOVI PLATNOG PROMETA I LIKVIDACIJE POSLOVI PRIBAVLJANJA I PLASMANA SREDSTAVA UPRAVLJANJE INFORMACIJAMA KORISCENJE INFORMACIJA PRIPUJANJE I PROCESIRANJE INFORMACIJA 					0	0	0	0	0	0
					2	1	4	0	0	0
					2	1	2	0	0	0
					2	2	4	0	0	0
					1	2	3	0	0	0
					0	0	0	0	0	0
					2	2	3	0	0	0
					3	2	3	0	0	0
					0	0	0	0	0	0
					3	4	5	0	0	0
					1	2	3	0	0	0
					1	4	4	0	0	0
					1	3	4	0	0	0
					0	0	0	0	0	0
					3	2	1	0	0	0
					4	5	3	0	0	0
					4	4	2	0	0	0
					5	5	3	0	0	0
					0	0	0	0	0	0
					1	1	1	0	0	0
					1	2	1	0	0	0
					0	0	0	0	0	0
					3	4	5	0	0	0
					3	4	5	0	0	0
					3	4	4	0	0	0
					0	0	0	0	0	0
					2	1	4	0	0	0
					2	2	4	0	0	0
					2	2	4	0	0	0
					0	0	0	0	0	0
					5	4	3	0	0	0
					5	4	3	0	0	0
					3	5	3	0	0	0
					0	0	0	0	0	0
					5	4	5	0	0	0
					4	3	4	0	0	0

Izvor: autor

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

[illegible]

Izvor: autor

4.2. Ranjivosti i pretnje lanca snabdevanja

Ranjivost predstavlja slabost resursa (imovine, procesa...) i omogućava mu da bude eksploatisan/iskorišćen od strane jedne ili više pretnji (ISO 27005, 2011).

Pretnja ili izvor rizika može biti materijalne i nematerijalne prirode (ISO 31000, 2009) i predstavlja sve ono što može da iskoristi ranjivost resursa, namerno ili slučajno, pri čemu se narušava njegova stabilnost.

Nakon identifikacije ranjivosti vrši se njihovo pridruživanje pretnjama po pojedinim procesima, kao i po lancu snabdevanja u celini. U studiji je razmatrano 289 ranjivosti (slika 19) i 161 pretnja (slika 20) po poverljivost, integritet i raspoloživost u lancima snabdevanja.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/a: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum

Danićelova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	1
Classification	Interno
Version	1
Date	--
Page	1 / 9

Counter	Code	Name	Description
1	001	CMA - Lack of understanding / education of the requirements of the Computer Misuse Act	
2	002	Combustible material available	
3	003	Complicated user interface	
4	004	Compromise of assets	
5	005	Compromise of security	
6	006	Contractual obligations not identified and managed appropriately	
7	007	Client staff with access (physical and/or logical) not subject to same level of control as employees	
8	008	Designs & Patents Act)	
9	009	Default factory accounts and passwords are not disabled or changed	
10	010	Disgruntled or disruptive employee(s)	
11	011	DPA - Lack of understanding / education of the requirements of the Data Protection Act	
12	012	Environmental location	
13	013	Disposal or reuse of storage media without proper erasure	
14	014	Exposed cabling for network infrastructure (e.g. on outside of building)	
15	015	Extended working hours without adequate breaks	
16	016	Failure in change management	
17	017	Failure to adhere to company policies	
18	018	Failure to apply relevant patches to operating systems	
19	019	FoIA - Lack of understanding / education of the requirements of the Freedom of Information Act	
20	020	High profile target due to nature of business (e.g. Bank)	
21	021	High value of intellectual property held (e.g. attractive to competitors)	
22	022	High values of stock	
23	023	HRA - Lack of understanding / education of the requirements of the Human Rights Act	
24	024	Inadequate "Fail-over" capabilities for critical systems (e.g. routers, firewalls, etc.)	
25	025	Inadequate analysis of system/network/firewall logs for suspicious events	
26	026	Inadequate anti-malware software	
27	027	Inadequate anti-malware software updating	
28	028	Inadequate anti-virus and malicious code controls	
29	029	Inadequate application controls	
30	030	Inadequate arrangements for removal of access rights upon job termination	
31	031	Inadequate arrangements for review of user access rights	
32	032	Inadequate audit logs	
33	033	Inadequate authorisation requirements for changes to systems configurations (e.g. poor change control procedures)	

Hestia RISK - URL: <http://www.hestia-software.com>, Ver. 01.11.013

24.06.2014

09.24.15

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/b: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	1
Classification	Interni
Version	1
Date	...
Page	2 / 9

Counter	Code	Name	Description
34	034	Inadequate awareness of changing security issues	
35	035	Inadequate back-up facilities	
36	036	Inadequate back-up procedures	
37	037	Inadequate back-up testing	
38	038	Inadequate or non-existent Business Continuity Plans	
39	039	Inadequate change control management and procedures	
40	040	Inadequate classification and/or labelling of information	
41	041	Inadequate clear desk policy	
42	042	Inadequate clear screen policy	
43	043	Inadequate confidentiality agreements with third parties (e.g. partners)	
44	044	Inadequate configuration change control	
45	045	Inadequate configuration management (e.g. Inadequate records)	
46	046	Inadequate content monitoring of email (e.g. scanning for viruses)	
47	047	Inadequate control access to server / communications rooms	
48	048	Inadequate control copying	
49	049	Inadequate control copying of data/software	
50	050	Inadequate control downloading and using software	
51	051	Inadequate control / unsupervised access by contract staff	
52	052	Inadequate control of contractors & temporary staff	
53	053	Inadequate control of employee termination	
54	054	Inadequate control/policy over information storage on non-business systems (e.g. PDAs)	
55	055	Inadequate control of input or output data	
56	056	Inadequate control of internet usage	
57	057	Inadequate or careless use of physical access control to buildings	
58	058	Inadequate control of software distribution	
59	059	Inadequate control of use of shareware/freeware for corporate applications	
60	060	Inadequate control of use of system utilities	
61	061	Inadequate control over cabling	
62	062	Inadequate control over processes	
63	063	Inadequate control over software releases	
64	064	Inadequate control over system access	
65	065	Inadequate policy/control/management of cryptographic keys	
66	066	Inadequate controls and procedures over remote access to company systems	
67	067	Inadequate or lack of input	

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/c: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	I
Classification	Interno
Version	1
Date	2014
Page	3 / 9

Counter	Code	Name	Description
68	068	Inadequate controls for the removal of information from the premises	
69	069	Inadequate definite information classification policy and information marking (e.g. confidentiality ratings)	
70	070	Inadequate disciplinary action arrangements	
71	071	Inadequate documentation	
72	072	Inadequate emergency system access procedures (e.g. Administrator password availability in a crisis)	
73	073	Inadequate employment agreements	
74	074	Inadequate environmental monitoring (e.g. humidity)	
75	075	Inadequate environmental protection	
76	076	Inadequate equipment maintenance	
77	077	Inadequate exchange agreements	
78	078	Inadequate fire detection equipment	
79	079	Inadequate fire suppression equipment	
80	080	Inadequate firewall	
81	081	Inadequate firewall policy	
82	082	Inadequate handling or disposal of media	
83	083	Inadequate HR monitoring mechanisms (pre	
84	084	Inadequate HR policies	
85	085	Inadequate identification/authentication	
86	086	Inadequate incident handling	
87	087	Inadequate incident reporting arrangements and awareness	
88	088	Inadequate information security policy	
89	089	Inadequate internal / external audit	
90	090	Inadequate intruder alarms	
91	091	Inadequate Intrusion Detection System(s)	
92	092	Inadequate job definition (roles & responsibilities)	
93	093	Inadequate logical access security	
94	094	Inadequate maintenance of infrastructure / lack of planned maintenance	
95	095	Inadequate maintenance of security equipment (e.g. CCTV)	
96	096	Inadequate management direction / supervision	
97	097	Inadequate monitoring mechanisms	
98	098	Inadequate network capacity	
99	099	Inadequate network infrastructure	
100	100	Inadequate network management	
101	101	Inadequate or incomplete register of assets	
102	102	Inadequate or incorrect access control policy/procedures	
103	103	Inadequate or incorrect assignment of responsibilities	

Hestia RISK, URL <http://www.hestia-software.com>, Ver. 01.11.013

24.06.2014

09:24:15

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/d: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum

Danijeleova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	1
Classification	Interno
Version	1
Date	...
Page	4 / 9

Counter	Code	Name	Description
104	104	Inadequate or insufficient software testing	
105	105	Inadequate or incomplete specifications for developers	
106	106	Inadequate ownership for information assets	
107	107	Inadequate password management	
108	108	Inadequate periodic equipment replacement schemes	
109	109	Inadequate physical access controls (e.g. weak locks	
110	110	Inadequate physical protection for the building	
111	111	Inadequate physical security	
112	112	Inadequate planning/deployment of cabling	
113	113	Inadequate policies for the correct use of telecommunications media and messaging	
114	114	Inadequate policies relating to software licensing	
115	115	Inadequate policies relating to verbal communication	
116	116	Inadequate policy/procedure to ensure return of asset(s) upon job termination	
117	117	Inadequate or lack of procedures for handling and investigating security incidents (physical	
118	118	Inadequate proof of message receipt	
119	119	Inadequate proof of message sending	
120	120	Inadequate protection of mobile computing equipment	
121	121	Inadequate redundant/spare capacity (e.g. single points of failure potential)	
122	122	Inadequate delegation	
123	123	Inadequate secure disposal procedures for equipment (e.g. erasure of hard disks	
124	124	Inadequate security awareness/training for staff	
125	125	Inadequate security awareness/training for suppliers and other third parties	
126	126	Inadequate security staff	
127	127	Inadequate segregation of duties	
128	128	Inadequate segregation of networks	
129	129	Inadequate separation of test and operational facilities	
130	130	Inadequate service specifications	
131	131	Inadequate software change control	
132	132	Inadequate software development standards	
133	133	Inadequate software malfunction handling	
134	134	Inadequate software testing	
135	135	Inadequate software updating	
136	136	Inadequate specific job or specialist training	
137	137	Inadequate staff supervision	
138	138	Inadequate staff training	
139	139	Inadequate staff understanding of policies	

Hestia Risk, URL: <http://www.hestia-software.com>, Ver. 01.11.012

24.06.2014

09:24:15

Izvor: autor

• • •

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/e: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	1
Classification	Interno
Version	1
Date	...
Page	5 / 9

Counter	Code	Name	Description
140	140	Inadequate storage environment	
141	141	Inadequate storage protection	
142	142	Inadequate system development procedures	
143	143	Inadequate system replacement policy	
144	144	Inadequate system security	
145	145	Inadequate systems documentation	
146	146	Inadequate technical maintenance	
147	147	Inadequate testing of new systems before release	
148	148	Inadequate updates for malicious code protection software	
149	149	Inadequate UPS	
150	150	Inadequate validation of processed data	
151	151	Inadequate vetting of staff	
152	152	Inadequate visitor control (e.g. lack of reception)	
153	153	Inadequate wireless network security controls	
154	154	Inadequate working environment (e.g. noisy)	
155	155	Inadequate workstation security	
156	156	Inadequately configured / maintained firewall	
157	157	Inadequately constructed contracts with third parties	
158	158	Inadequately documented software	
159	159	Inadequately maintained operating system	
160	160	Inadequately maintained security features	
161	161	Inappropriate use of cryptography (too much)	
162	162	Inappropriate/misuse of audit tools	
163	163	Inappropriate/misuse of information processing facilities	
164	164	Inappropriate/misuse of resources or assets	
165	165	Incompatible systems / poor integration	
166	166	Incorrect selection of test data	
167	167	Incorrectly configured operating system	
168	168	Incorrectly configured security controls/features	
169	169	Corruption of information due to systems failure (e.g. disk corruption)	
170	170	Insecure configuration of Remote Access Service clients	
171	171	Insufficient maintenance/faulty installation of storage media	
172	172	Insufficient or ineffective fire precautions (e.g. lack of sprinklers)	
173	173	Insufficient staff for vital security tasks (due to sickness)	
174	174	Job entails exposure to significant risk (e.g. visits to hazardous places)	
175	175	Known flaws in software	

Hestia Risk, URL: <http://www.hestia-software.com>, Ver. 01.11.012

24.06.2014

09:24:15

Izvor: autor

• • •

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/f: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	1
Classification	Interno
Version	1
Date	2014
Page	6 / 9

Counter	Code	Name	Description
176	176	Location in an area susceptible to flood	
177	177	Locked fire exits / fire doors wedged open	
178	178	Loss of key personnel	
179	179	Loss of telecoms	
180	180	Low staff morale	
181	181	Mixing of test - development and operational facilities	
182	182	Network topology diagrams/descriptions not held off-site	
183	183	No "logout" when leaving the work station policy	
184	184	No standard build for servers or workstations	
185	185	Non-compliance with legislation	
186	186	Number of software / application users exceeds valid licences	
187	187	Operating system vulnerabilities	
188	188	Output left unattended	
189	189	Output unmarked	
190	190	Over-reliance on key staff / lack of delegation	
191	191	Policy on monitoring in the workplace not issued (e.g. potential breach of Data Protection Act)	
192	192	Poor housekeeping	
193	193	Portable computer equipment not secured (e.g. laptops in public areas)	
194	194	Area susceptible to power fluctuations/outages	
195	195	Premises liable to damage from environment (Rain)	
196	196	Premises sited in high risk areas (e.g. near oil refineries)	
197	197	Premises situated in areas of high crime rates (e.g. danger of burglary)	
198	198	Computer equipment sited in areas of public access without constant supervision	
199	199	Public access to premises (either fully or partially)	
200	200	RIPA - Lack of understanding / education of the requirements of the Regulation of Investigatory Powers Act	
201	201	Security not included in job descriptions	
202	202	Single supplier / unreliable suppliers	
203	203	Software failure	
204	204	Special purpose systems used for other purposes (e.g. nothing else should run on a firewall)	
205	205	Staff approachable by the news media	
206	206	Storage of hazardous materials (e.g. paints)	
207	207	Susceptibility of equipment/systems to temperature variations	
208	208	Susceptibility of equipment/systems to voltage variations	
209	209	Susceptibility of equipment/systems to humidity	
210	210	Susceptible to approaches from competitors	

Hestia RS&C, URL <http://www.hestia-software.com>, Ver. 01.11.013

24.06.2014

06.24.15

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/g: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-V/UL
Level	1
Classification	interno
Version	1
Date	2014
Page	7 / 9

Counter	Code	Name	Description
211	211	Susceptible to corruption/fraud due to nature of work (e.g. handling money)	
212	212	System or component failures	
213	213	Transmission of confidential data	
214	214	Connection of unauthorised equipment to network (e.g. PDAs)	
215	215	Unauthorised software	
216	216	Unauthorised use/access to systems by family	
217	217	Unmotivated or disgruntled staff	
218	218	Unoccupied premises outside of working hours	
219	219	Unprotected public network connections	
220	220	Utilities entering premises via vulnerable points (e.g. exposed pipes/cables)	
221	221	Pogreš no kabliranje	
222	222		
223	223	LS-BANKROT	
224	224	LS-DODATNI TROSKOVI ZA VRACANJE OPREME U RADNO STANJE	
225	225	LS-DUPLOVANJE POSLOVA-PRODUZETAK PROIZVODNOG PROCES	
226	226	LS-FINANSIJSKI GUBICI	
227	227	LS-FUNKCIONALNA NEISPRAVNOST PROIZVODA	
228	228	LS-GUBITAK BRENDIA	
229	229	LS-GUBITAK POSTOJECIH I BUDUCIH KLJENATA	
230	230	LS-ISTOVARNA KONFUZIJA	
231	231	LS-KASNIJENJE SA ISPORUKOM	
232	232	LS-KONTAMINACIJA TOVARA	
233	233	LS-MAKSIMIZACIJA TROSKOVA TRANSPORTA	
234	234	LS-NEADEKVATNI PLANOWI KONTINUITETA POSLOVANJA	
235	235	LS-NEDOVOLJNA KOLICINA ZALIHA	
236	236	LS-NEEFEKTIVNO I NEEFIKASNO OBAVLJANJE SVAKOG POJEDINACNOG ZADATAKA	
237	237	LS-NEEFEKTIVNO I NEEFIKASNO OBAVLJANJE ZADATAKA	
238	238	LS-NEEFIKASNO FUNKCIONISANJE KOMPANJE	
239	239	LS-NEEKONOMICNA NABAVKA	
240	240	LS-NEISPUNJENJE NIVOA CILJNIH USLUGA	
241	241	LS-NEISPUNJENJE ROKOVA ISPORUKE	
242	242	LS-NEIZVRSENJE GRUPNIH ZADATAKA	
243	243	LS-NEKONKURETNOST KOMPANJE NA TRZISTU	
244	244	LS-NEMOGUCNOST NABAVKE OPREME	
245	245	LS-NEMOGUCNOST NAPLATE POTRAZIVANJA	

Hestia RISK, URL: <http://www.hestia-software.com>, Ver. 01.11.013

24.06.2014

09:24:15

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/h: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	1
Classification	Interno
Version	1
Date	2014
Page	8 / 9

Counter	Code	Name	Description
246	246	LS-NEMOGUCNOST OTPREMANJA ROBE	
247	247	LS-NEMOGUCNOST SKLAPANJA UGOVORA SA INOSTRANIM KOMPANIJAMA	
248	248	LS-NEMOGUCNOST UVOZA/IZVOZA	
249	249	LS-NEOPTIMALNA KOLICINA ZALIHA	
250	250	LS-NEPOSTOJANJE POVRATNE INFORMACIJE ZA DONOSENJE ODLUKA	
251	251	LS-NEPOSTOJANJE DOGVORENIH VREMENSKIH ROKOVA	
252	252	LS-NEPRENOSENJE INFORMACIJA	
253	253	LS-NEZADOVOLJSTVOA RADNIKA	
254	254	LS-NEZAVRSENI PROIZVODNI PROCESI	
255	255	LS-OBUSTAVLJANJE ISPORUKE SIROVINA	
256	256	LS-ODAVANJE POSLOVNE TAJNE	
257	257	LS-OSIPANJE/NEPOSTOJANJE KUPACA	
258	258	LS-OTPUSTANJE RADNIKA	
259	259	LS-PAD KONKURETNOSTI KOMPANIJE/SMANJENJE BROJA POSTOJEĆIH ILI NOVIH KLIJENATA	
260	260	LS-PAD REJTINGA KOMPANIJE	
261	261	LS-POGRESNA ODLUKA	
262	262	LS-POVEĆANJE FINANSIJSKIH TROSKOVA	
263	263	LS-POVEĆANJE SKARTA	
264	264	LS-POVEĆANJE TROSKOVA	
265	265	LS-POVEĆANJE TROSKOVA DIREKTNE PROIZVODNJE	
266	266	LS-POVEĆANJE TROSKOVA TRANSPORTA	
267	267	LS-POVRACAJ ROBE	
268	268	LS-POVREDA ZAPOSLENOG	
269	269	LS-PREVELIKO VEZIVANJE KAPITALA U ZALIHE MATERIJALA I GOTOVIH ROBA	
270	270	LS-PRODUZENJE PLANIRANOG PROIZVODNOG PROCESA	
271	271	LS-PRODUZETAK PROCESA RADA	
272	272	LS-PRODUZETAK TRAJANJA UTOVARNOG PROCESA	
273	273	LS-PROPUSTI U BIROKRATJI	
274	274	LS-PROPUSTI U INFORMACIONIM TOKOVIMA	
275	275	LS-PROPUSTI U POSLOVANJU	
276	276	LS-RASKID UGOVORA	
277	277	LS-RASKID UGOVORA SA DOBAVLJACIMA	
278	278	LS-SMANJEN KVALITET PROIZVODA	
279	279	LS-SMANJENJE BROJA POSTOJEĆIH I BUDUĆIH KLIJENATA	
280	280	LS-SMANJENJE STEPENA LIKVIDNOSTI PREDUZEĆA	

Hestia Risk, URL: <http://www.hestia-software.com>, Ver. 01.11.013

24.06.2014

00:24:15

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 19/i: Lista ranjivosti u lancu snabdevanja



Univerzitet Singidunum

Danijelevo 32, 11000, Beograd, Srbija

Lista ranjivosti u lancu snabdevanja

Reference	ISMS-VUL
Level	1
Classification	Interno
Version	1
Date	-
Page	9 / 9

Counter	Code	Name	Description
281	281	LS-SMANJENJE VEROVATNOCE POVRACAJA ULOZENIH SREDSTAVA	
282	282	LS-TRAJNO OSTECENJE ROBE	
283	283	LS-ULOGE U KOMPANIJU NISU JASNO DEFINISANE	
284	284	LS-UMANJEN KVALITET ZAVRSNOG PROIZVODA	
285	285	LS-ZAGUSENOST PROLAZA	
286	286	LS-ZASTOJ U PROIZVODNJI	
287	287	LS-KRADJA I NEISPORUKA	
288	288	LS-OSTECENJE ROBE PRILIKOM TRANSPORTA	
289	289	LS-NAMERNO POGRESNO OBELEZAVANJE PROIZVODA	

Document made by	Document controled by	Document approved by

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 20/a: Lista pretnji u lancu snabdevanja



Univerzitet Singidunum

Danišpolova 32, 11000, Beograd, Srbija

Lista pretnji u lancu snabdevanja

Reference:	ISMS-THR
Level:	1
Classification:	Interno
Version:	1
Date:	...
Page:	1 / 5

Counter	Code	Name	Description
1	001	Air conditioning failure	
2	002	Airborne pollution/particles	
3	003	Bomb blast	
4	004	Business disasters (e.g. market crashes)	
5	005	Casual oversight	
6	006	Contamination	
7	007	Covert channels	
8	008	Denial of service attack	
9	009	Disasters (natural or man-made)	
10	010	Duress to staff in key positions (e.g. administrators) / blackmail / entrapment	
11	011	Dust/dirt	
12	012	Earthquake	
13	013	Eavesdropping	
14	014	Electronic interference	
15	015	Environmental contamination (natural or man made)	
16	016	Environmental disasters	
17	017	Errors	
18	018	Espionage/spying	
19	019	Failure of equipment/services	
20	020	Falsification of records	
21	021	Fire	
22	022	Flood	
23	023	Fraud (incl. white-collar crime)	
24	024	Hacking	
25	025	Hardware failure	
26	026	Human error (accidental)	
27	027	Humidity extremes	
28	028	Hurricane	
29	029	Illegal import/export of software	
30	030	Illegal use of software	
31	031	Inaccurate input of information	
32	032	Inaccurate output of information	
33	033	Inappropriate employee selection	
34	034	Inappropriate/lack of action by third parties	
35	035	Industrial action (internal or external)	
36	036	Insufficient or untested back-ups	
37	037	Interception	

Hestia RISK, URL: <http://www.hestia-software.com>, Ver. 01.11.013

34.06.2014

06/21/20

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 20/b: Lista pretnji u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista pretnji u lancu snabdevanja

Reference	ISMS-THR
Level	1
Classification	Interno
Version	1
Date	-
Page	2 / 5

Counter	Code	Name	Description
38	038	Interference (incl. to or from the audit process)	
39	039	Introduction of unauthorized or untested code	
40	040	Key logging (soft or hard ware)	
41	041	Lack of staff / 3rd party awareness	
42	042	Lightning	
43	043	Maintenance error (poor maintenance etc)	
44	044	Malfunctions of supporting utilities	
45	045	Malicious code - Virus / Trojan Horse infection	
46	046	Malicious destruction	
47	047	Malware	
48	048	Masquerading	
49	049	Misdistalling (phone or fax)	
50	050	Misrouting or re-routing of messages	
51	051	Network intrusion	
52	052	Operational staff errors	
53	053	Overloading/lack of systems/network capacity	
54	054	Password cracking	
55	055	Physical interference	
56	056	Poorly constructed penetration tests	
57	057	Power supply disruption/fluctuations	
58	058	Private use of organisational information processing facilities	
59	059	Processing errors	
60	060	Publishing of incorrect/unapproved information	
61	061	Recovery of sensitive information from disposal of media (e.g. disks & tapes)	
62	062	Repudiation	
63	063	Sabotage - wilful damage / vandalism	
64	064	Sewerage problems	
65	065	Social engineering	
66	066	Software errors	
67	067	Software failure	
68	068	Spam	
69	069	Storm/storm damage	
70	070	System misuse (accidental or deliberate)	
71	071	Technical/mechanical failure	
72	072	Temperature extremes	
73	073	Terrorist attack/acts	
74	074	Theft of assets by employee/supplier/third party	

Hestia FileS, URL: <http://www.hestia-software.com>, Ver: 81.11.813

24.06.2014

88/21/26

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 20/c: Lista pretnji u lancu snabdevanja



Univerzitet Singidunum

Danijelova 32, 11000, Beograd, Srbija

Lista pretnji u lancu snabdevanja

Reference	ISMS-THR
Level	1
Classification	Interno
Version	1
Date	- -
Page	3 / 5

Counter	Code	Name	Description
75	075	Transmission errors	
76	076	Unavailability/loss of personnel	
77	077	Uncontrolled (unapproved/untested) changes to information systems and/or operating environment	
78	078	Unsuccessful changes	
79	079	Use of inappropriate identification and authentication mechanisms	
80	080	Use of network facilities in an unauthorized way	
81	081	Use of pirated software	
82	082	Vandalism	
83	083	Vermis	
84	084	Violation of intellectual property rights	
85	085	Willful damage	
86	086	Workplace violence	
87	087	Nedozvoljen upad na web stranicu	
88	088		
89	089	LS-AUTOKRATIJA	
90	090	LS-BANKROT DUZNIKA	
91	091	LS-CARINSKE BARIJERE	
92	092	LS-FLUKTUACIJA POTRAZNJE	
93	093	LS-ISPORUCENA ROBA NIJE SAOBRAZNA UGOVORU	
94	094	LS-ISTOVARNA KONFUZIJA	
95	095	LS-KOMPETNTNOST RADNE SNAGE	
96	096	LS-KONFUZNI PLANOVI	
97	097	LS-KORISCENJE JAVNIH DRUSTVENIH MREZA	
98	098	LS-KREDITNA NESPOSOBNOST	
99	099	LS-LOKACIJE NA PREVELIKOJ UDALJENOSTI	
100	100	LS-LOSA INTERNA KOMUNIKACIJA	
101	101	LS-LOSE PLANIRANJE BEZBEDNOSNIH ZALIHA	
102	102	LS-NAMERNO POGRESNO OBEZAVANJE PROIZVODA	
103	103	LS-NAPLACIVANJE SERVISA U GARANTNOM ROKU	
104	104	LS-NEADEKVATAN KAPACITET	
105	105	LS-NEADEKVATNA LOGISTICKA INFRASTRUKTURA	
106	106	LS-NEADEKVATNA POLITIKA KVALITETA	
107	107	LS-NEADEKVATNA ZASTITA PODATAKA	
108	108	LS-NEADEKVATNO UPRAVLJANJE LOGISTICKOM TEHNIKOM I INFRASTRUKTUROM	
109	109	LS-NEAUTORIZOVAN PRISTUP PODACIMA	
110	110	LS-NEDOSTATAK KOORDINACIJE	

Hestia RISK - URL: <http://www.hestia-software.com/>, Ver. 01.11.013

24.06.2014

09:21:28

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 20/d: Lista pretnji u lancu snabdevanja



Univerzitet Singidunum

Danijelova 32, 11000, Beograd, Srbija

Lista pretnji u lancu snabdevanja

Reference	ISMS-THR
Level	1
Classification	Interno
Version	1
Date	-
Page	4 / 5

Counter	Code	Name	Description
111	111	LS-NEDOSTATAK SOFISTICIRANIH TEHNIKA I METODA U PROCESU	
112	112	LS-NEIDENTIFIKOVANJE SNABDEVACA	
113	113	LS-NEKOMPETENTNOST PODREDJENIH	
114	114	LS-NEKOORDINISANA SARADNJA SA DOBAVLJACIMA	
115	115	LS-NEPLACANJE NABAVLJENIH SIROVINA	
116	116	LS-NEPOSTAJANJE DEPARTMANA	
117	117	LS-NEPOSTOJANJE ISTORIJSKIH PODATAKA	
118	118	LS-NEPOSTOJANJE OBJEDINJENOG INFORM. SIS. NA NIVOU DRZAVNE UPRAVE	
119	119	LS-NEPRECIZAN FINANSUSKI PLAN	
120	120	LS-NERASCLANJIVANJE UKUPNIH ZADATAKA KOMPANIJE	
121	121	LS-NERASPOLOZIVOST MATERIJALA	
122	122	LS-NEREALNI GARANTNI ROK	
123	123	LS-NEREDOVNO PLACANJE NABAVLJENIH SIROVINA	
124	124	LS-NESPROVODJENJE TENDERSKIH PROCEDURA	
125	125	LS-NESTABILNOST TRZISTA SNABDEVANJA	
126	126	LS-NESTABILNOST VLADE	
127	127	LS-NESTANDARDIZOVANE PROCEDURE	
128	128	LS-NESTRUČNOST MENADZERA	
129	129	LS-NETACNOST UNOSA I PRENOSA PODATAKA	
130	130	LS-NEUSAGLASENOST UGOVORNIH OBAVEZA	
131	131	LS-NEUSKLADJENOST SPECIFIKACIJA NARUDZBINE I KVALITETA	
132	132	LS-NAZADOVOLJSTVO ZAPOSLENIH	
133	133	LS-OBIM PROIZVODNJE NIJE PLANIRAN	
134	134	LS-OPREMA NIJE OSIGURANA	
135	135	LS-ORGANIZACIONE JEDINICE NISU UMREZENE	
136	136	LS-OSTECENJE AMBALAZE	
137	137	LS-OTPOR PREMA NOVIM IKT	
138	138	LS-PLANOWI PROIZVODNIH KAPACITETA NISU IZRADJENI	
139	139	LS-POGRESAN IZBOR GEOGRAFSKIH LOKACIJA OBJEKATA	
140	140	LS-POGRESNO GRUPISANI POSLOVI	
141	141	LS-POJEDINACNI RADNI ZADACI NISU DEFINISANI	
142	142	LS-POVEĆANJE DUZINE LANACA SNABDEVANJA	
143	143	LS-PROBLEMI PREDVIĐANJA	
144	144	LS-PROBLEMI U INFORMACIONIM TOKOVIMA	
145	145	LS-PRODAJNO TRZISTE NIJE ISPITANO	

Hestia RISK, URL: <http://www.hestia-software.com>, Ver. 01.11.013

24.06.2014

09:21:28

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 20/e: Lista pretnji u lancu snabdevanja



Univerzitet Singidunum
Danijelova 32, 11000, Beograd, Srbija

Lista pretnji u lancu snabdevanja

Reference	ISMS-THR
Level	1
Classification	Interno
Version	1
Date	-
Page	5 / 5

Counter	Code	Name	Description
146	146	LS-PROMENA DEVIZNOG KURSA	
147	147	LS-PROMENA PONASANJA POTROSACA	
148	148	LS-PROMENA PLANA PRODAJA	
149	149	LS-PROMENA PLANA PROIZVODNJE	
150	150	LS-PROTIVREDNE POLITIKE UPRAVLJANJA LOGISTICKIM RESURSIMA	
151	151	LS-SAOBRACAJNE NEZGODE	
152	152	LS-SLOZENOST PROIZVODA	
153	153	LS-SPEDITER BEZ CERTIFIKATA	
154	154	LS-TAKTIKA PRITISKA	
155	155	LS-TEHNICKO-TEHNOLOSKE PROMENE	
156	156	LS-TIMSKI RAD IZMEDJU NABAVKE U RACUNOVODSTVA NIJE KOORDINIRAN	
157	157	LS-TOK INFORMACIJA NE PRATI TOK MATERIJALA	
158	158	LS-TRZISNA ANALIZA SE NE ZASNIVA I NA ISTORUSKIM PODACIMA	
159	159	LS-ZASTARELA TEHNOLOGIJE	
160	160	LS-ZAVISNOST OD PARTNERA U LANCU	
161	161	LS-SPEDITER BEZ CERTIFIKAT	

Document made by	Document controlled by	Document approved by

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Na slici 21. prikazana je lista pretnji/izvora rizika koji su nakon analize pridruženi konkretnim ranjivostima pojedinih procesa, kao i lanca snabdevanja u celini.

Nakon analize, pretnje su podeljene u četiri grupe rizika (ljudski faktor, procesi, sistem i eksterni faktori). Svakoj grupi procesa, pridružene su jedna ili više grupa rizika. U fazi procene rizika analiziraju se rizici za svaki pojedinačni proces od strane svake pojedinačne pretnje koja im je pridružena kroz grupe rizika.

U studiji je definisano 76 kontrola – mera koje treba primeniti da bi se nivo rizika, nakon faze tretiranja rizika, smanjio na prihvatljiv nivo (slika 22). Kontrole – mere mogu biti organizacione, proceduralne i tehničke, a u ovom slučaju se prenose iz zaključaka nakon sprovedene procene rizika primenom metode Kinney.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 22/a: Lista predloženih mera za ublažavanje/uklanjanje rizika u lancu snabdevanja

Univerzitet Singidunum

Danjlova 32, Beograd, Srbija

Lista korišćenih mera
za uklanjanje/ublažavanje rizika

Referenca	ISMS-USEDC
Nivo	1
Klasifikacija	Interni
Verzija	1
Stranica	- -
Datum	1 / 3

Rbr	Tocka	Kontrola	Broj korišćenja
1	16.1.1.	ANGAZOVANJE AGENCIJE KOJA SE BAVI OTKUPOM POTRAZIVANJA	8
2	16.1.3.	EDUKACIJA ZAPOSLENIH	849
3	16.1.4.	FORMIRANJE CENA PROIZVODA KOJE IZVESNO OMOGUĆAVAJU REALIZACIJU POSLOVNIH PLANOVA	9
4	16.1.5.	FORMIRANJE OBLJEĐENOG INTERNOG REGISTRA ZA ČUVANJE ORIGINALNIH PRIMERAKA UGOVORA, ANEKSA, REŠENJA, IZVODA I DR.	9
5	16.1.6.	FORMIRANJE RAZNIH JEDINICA	18
6	16.1.7.	INFORMACIJE U SMISLU POSLOVNE TAJNE NEKORISTITI U CILJU REKLAME PUTEJEM JAVNIH DRUŠTVENIH MREŽA	27
7	16.1.8.	INOVIRANJE PUI I VRACANJE TRENTOVA	12
8	16.1.9.	INTERNA KONTROLA	92
9	16.1.10.	ISTRAŽITI TRŽISTE I POTREBE POTROŠACA	20
10	16.1.11.	ISTRAŽIVANJE I PRILAGOĐAVANJE POTREBAMA TRŽISTA	67
11	16.1.12.	ISTRAŽIVANJE TRŽISTA	13
12	16.1.13.	ISTRAŽIVANJE TRŽISTA I POTREBA POTROŠACA	20
13	16.1.14.	IZrada STRATEGSKOG PLANA ZA MEDUINSTITUCIONALNU SARADNJU	3
14	16.1.15.	IZrada, USVAJANJE I PRIDRŽ AVANJE FINANSIJSKOG PLANA ZA SVAKU KALENDARNU GODINU/KVARTAL	8
15	16.1.17.	JASNO DEFINISATI OPIS RAČNOG MESTA, PRAVA I OBAVEZE ZAPOSLENIH	17
16	16.1.19.	JASNO DEFINISATI PRIORITETE	8
17	16.1.20.	KONTROLA USKLADENOSTI ROBE I OTPREMNICA	9
18	16.1.21.	KORIŠĆENJE PRIZNATIH METODA I ALATA ZA IZRAČUN FINANSIJSKIH PLANOVA	4
19	16.1.22.	KREIRANJE BAZE PODATAKA INFORMACIJA IZ PRETHODNIH PERIODA POSLOVANJA, KAKO BI SE DONOSILE ISPRAVNE ODLUKE	35
20	16.1.24.	OBEZBEDITI FINANSIJSKA SREDSTVA PUTEJEM PROJEKATA I PREKOGRANICNE SARADNJE	8
21	16.1.25.	ODRŽ AVANJE OPTIMALNOG NIVOA ZALIH SA POSEBNOM PAŽNJOM NA SIGNALNE ZALIBE	12
22	16.1.26.	ODSTRAŽIVANJE ELEMENATA LANCA SNABDEVANJA KOJI NE STVARAJU VREDNOST	12
23	16.1.27.	OPTIMIZOVANJE KORIŠĆENJA ZAPREMINSKOG PROSTORA SKLADIŠTA	67
24	16.1.28.	OSIGURANJE OD ODGOVORNOSTI Š PEDITERA	1
25	16.1.29.	OSIGURATI ROBU U TRANSPORTU	9
26	16.1.30.	PERIODICNO PREVENTIVNO I KOREKTIVNO ODRŽ AVANJE MAŠINA I OPREME	19
27	16.1.31.	PLANIRANJE OPTIMALNOG ISKORIŠĆENJA CENJA OPREME I RAČNE SNAGE ZA RUKOVANJE MATERIJALIMA	67

Date: 16.04.22

Time: 10:54:22

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 22/b: Lista predloženih mera za ublažavanje/uklanjanje rizika u lancu snabdevanja

Univerzitet Singidunum		Lista korišćenih mera za uklanjanje/ublažavanje rizika		Referenca	ISMS-ISEDC
Danijeleova 32, Beograd, Srbija				Nivo	1
				Klasifikacija	Interno
				Versija	1
				Stranica	1
				Datum	2 / 3
Rbr	Činjenica	Ublažavanje	Uklanjanje	Broj korišćenja	
28	16.1.33.	Kontrola	POLISA OSIGURANJA	9	9
29	16.1.34.	POS TOVANJE	ZAKONA O JAVNIM NABAVKAMA	17	17
30	16.1.35.	PRACENJE	TRENDOVA	20	20
31	16.1.36.	PRAVOVREMENO	OSMIŠLJAVANJE ALTERNATIVNIH REŠENJA	67	67
32	16.1.37.	PREFORMULISATI	PROIZVOD KAKO BI SE SMANJILA IZLOŽENOST OGRANIČENOJ ROBI	18	18
33	16.1.38.	PRILAGODJAVANJE	RAZNOGODNOG OKRUŽENJA PROIZVODNOM PROCESU	67	67
34	16.1.39.	PRIMENA	ALATA ZA RUTINIZACIJU	3	3
35	16.1.40.	PRIMENA	GISA	4	4
36	16.1.41.	PROVERA	BONITETA POSLOVNOG PARTNERA PRE SKLAPANJA POSLA	9	9
37	16.1.42.	PROVERITI	NA KOJI NAČIN SE OBELEŽAVA, PAKUJE, ROBA I KOJE MAŠINE KORISTE ZA UTOVAR I ISTOVAR SPECIJALNIH TERETA	6	6
38	16.1.43.	RASPIŠIVANJE	TENDERA ZA USLUGE TRANSPORTA	67	67
39	16.1.44.	RAZMATRANJE	ALTERNATIVNIH TRŽIŠTA ZA IZVOZ	9	9
40	16.1.45.	RAZMENA	STECENIH ZNANJA I UNAPREĐENJE PRAKSE	4	4
41	16.1.46.	REDOVNO	AŽURIRATI I ADEKVATNO ZAŠTITI REZERVNE KOPIJE PODATAKA	46	46
42	16.1.49.	REDOVNO	USAVRŠAVANJE ZAPOSLENIH	57	57
43	16.1.50.	SELEKCIJA	KADROVA PRILIKOM ZAPOSLLAVANJA KROZ RAZNE VIDOVE TESTOVA, RAZGOVORA, INTERVJUA, REŠAVANJA KONKRETNOG PROBLEMA, PROBNI RAD	9	9
44	16.1.51.	SERVIS	SPROVODITI U GARANTNOM ROKU PREMA ZAKONU O ZAŠTITI POTROŠAČA	4	4
45	16.1.52.	SISTEMATIZACIJA	RAZNOGODNOG MESTA U SKLADU SA ZAKONOM I POTREBAMA KOMPANIJE	19	19
46	16.1.53.	SKRACENJE	VREMENA OBRTA ZALIHA	4	4
47	16.1.55.	STALNO	USAVRŠAVANJE Ljudskih MENADŽERA I MENADŽERA SREDNJEG NIVOA	4	4
48	16.1.56.	STANDARDIZOVANJE	METODA RUKOVANJA MATERIJALIMA	19	19
49	16.1.57.	STIMULACIJE	ZAPOSLENIH	38	38
50	16.1.58.	STROGO	PRIDRŽAVANJE UGOVORNIH OBAVEZA	9	9
51	16.1.59.	STUPANJE	U JAVNO - PRIVATNA PARTNERSTVA	3	3
52	16.1.60.	UDRUŽIVANJE	U KLASTERE	9	9
53	16.1.61.	ULAGANJE	U SAVREMENU PROIZVODNU OPREMU	27	27
54	16.1.62.	UMREŽAVANJE	SVIH SEKTORA KOMPANIJE	13	13

Hestia RSE - LSC, <http://www.hestia-rse.com>, Ver. 01.11.2013

Date: 24.06.2014 Time: 10:56:22

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 22/c: Lista predloženih mera za ublažavanje/uklanjanje rizika u lancu snabdevanja

 University of Singapur Danaselova 32, Beograd, Srbija		Lista korišćenih mera za uklanjanje/ublažavanje rizika				Referenca Nivo Klasifikacija Verzija Stranica Datum	ISMS-USEDC 1 Interni 1 1 3 / 3
Rbr	Točka	Kontrola	Broj korišćenja				
55	16.1.63.	USAVRŠ AVANJE I SERTEFIKACIJA ZAPOSLENIH U OBLASTI IKT, POZNAVANJE IT NAVESTI KAO PREDUSOV PRI ZAPOS LIAVANJU	76				
56	16.1.64.	USPOSTAVLJANJE ADEKVATNOG SISTEMA KONTROLE KORIŠ CENJA DOCELJENOG OVLAS CENJA	76				
57	16.1.65.	USPOSTAVLJANJE FUNKCIONALNOG IS	8				
58	16.1.66.	UVODENJE CENTRALNOG RACUNARA IJ BAZE PODATAKA	8				
59	16.1.67.	UVODENJE DEMOKRATSKOG TIPIA RUKOVOĐENJA	4				
60	16.1.68.	UVODENJE I PRIMENA STANDARDA	13				
61	16.1.69.	UVODENJE JIT KONCEPTA	18				
62	16.1.70.	UVODENJE MEDUFAZNE KONTROLE	40				
63	16.1.71.	UVODENJE PRAKSE UGOVORNIH SKLADIS TA	67				
64	16.1.72.	UVODENJE SISTEMA DISTRIBUTION REQUIREMENTS PLANING	26				
65	16.1.73.	UVODENJE SISTEMA KOJI OMOGUĆUJU AUTORIZOVANO UPRAVLJANJE TOKOVIMA INFORMACIJA	38				
66	16.1.75.	UVODENJE SISTEMA ZA PODIRS KU ODLUCIVANJU	27				
67	16.1.76.		19				

Izvor: autor

4.3. Evaluacija rizika u lancu snabdevanja

Korišćenjem aplikacije izvršena je automatska evaluacija rizika (slika 23), a kao rezultat su dobijene 2393 pojedinačne procene rizika. Procene rizika su klasifikovane po nivoima rizika, i to:

- nivo "5" 1084 rizika;
- nivo "4" 709 rizika;
- nivo "3" 537 rizika;
- nivo "2" 50 rizika i
- nivo "1" 13 rizika.

Metodologijom za upravljanje rizicima u lancima snabdevanja definisano je da će biti tretirani samo rizici nivoa "4" i "5", što je u predmetnoj studiji ukupno 1793 različitih rizika, a da se u fazi tretiranja rizika iskoriste sve kontrole – mere za umanjenje rizika, po principu primena svake pojedinačne kontrole – mere umanjuje nivo pojedinačne pretnje za vrednost 1.

Na slikama 24 – 28 je prikazan deo svih identifikovanih rizika nivoa "5" do "1" pre tretiranja rizika, kao i vrednosti tretiranih rizika (nivoa "5" i "4") nakon primene kontrole – mera, tj. smanjivanja nivoa pretnji za vrednost 1 (slika 29 – 31).

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 23: Evaluacija rizika u lancu snabdevanja

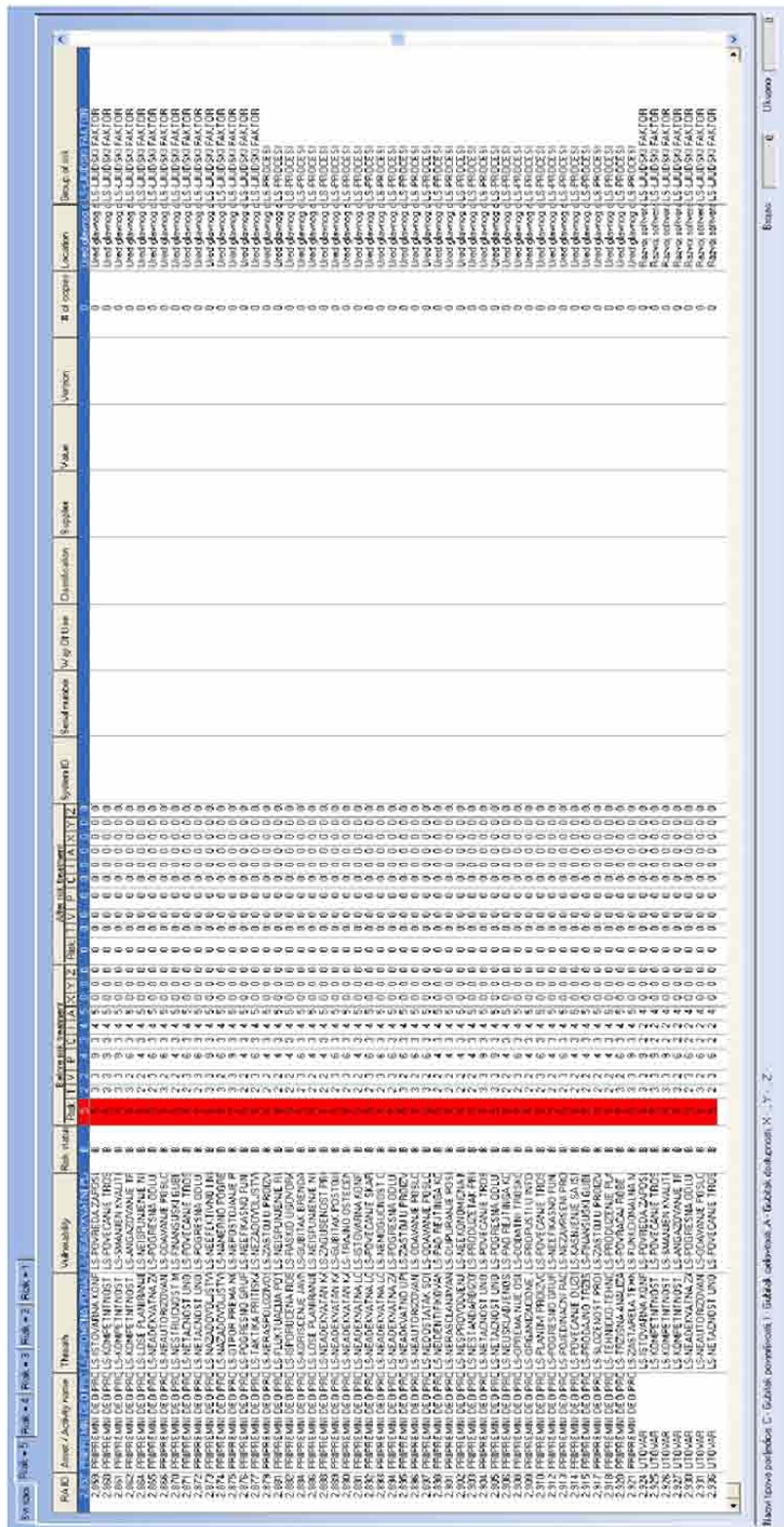


Izvor: autor

Kvantifikacija rizika u lancima snabdevanja

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 24: Rizici nivoa 5 pre tretiranja



Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 25: Rizici nivoa 4 pre tretiranja

[illegible]

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 27: Rizici nivoa 2

[illegible]

Izvor: autor

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 29: Preostali rizici nivoa 5 nakon prve iteracije tretiranja predloženim merama

Univerzitet Srijem

Danijele 32, Božjard, Srijem

Preostali rizik nivoa "5"

Rbr	ID rizika	Naziv imovint	Prethnja	Ranjivost	Prin nhrade rizika										Nakon obrade rizika						
					P	R	V	C	I	A	Rizik	P	R	V	C	I	A	Rizik			
1	3.011	IZVRŠNI DEO PROIZVODNE	LS-ISTOVARNA KONFUZIJA	LS-POVREDA ZAPOSLENOG	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
2	3.012	IZVRŠNI DEO PROIZVODNE	LS-KOMPETITIVNOST RADNE SNAGE	LS-POVEĆANJE TROSKOVA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
3	3.013	IZVRŠNI DEO PROIZVODNE	LS-KOMPETITIVNOST RADNE SNAGE	LS-SMANJEN KVALITET PROIZVODA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
4	3.025	IZVRŠNI DEO PROIZVODNE	LS-NAZADOVOLJSTVO ZAPOSLENIH	LS-NEEFKATIVNO I NEEFKASNO OBAVLJANJE SVAKOG POSLOVNOG ZADATAKA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
5	3.057	IZVRŠNI DEO PROIZVODNE	LS-OSTATNA UNOSNA I PRENOŠIVA PODATAKA	LS-POGREŠNA ODLUKA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
6	3.058	IZVRŠNI DEO PROIZVODNE	LS-OSTATNA UNOSNA I PRENOŠIVA PODATAKA	LS-POVEĆANJE TROSKOVA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
7	3.027	IZVRŠNI DEO PROIZVODNE	LS-OTPOR PREMA NOVIM IKT	LS-NEPOSTUPANJE POVRATNE INFORMACIJE ZA DOKAZIVANJE ODLUKA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
8	3.073	IZVRŠNI DEO PROIZVODNE	LS-ZASTARELA TEHNOLOGIJE	LS-FUNKCIONALNA NEISPRAVNOST PROIZVODA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
9	3.817	KONTROLA PROIZVODNE	LS-CARINSKE BARIJERE	LS-NEPOGOĐENOST UNOŠAČI	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
10	3.839	KONTROLA PROIZVODNE	LS-ISTOVARNA KONFUZIJA	LS-POVREDA ZAPOSLENOG	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
11	3.840	KONTROLA PROIZVODNE	LS-KOMPETITIVNOST RADNE SNAGE	LS-POVEĆANJE TROSKOVA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
12	3.841	KONTROLA PROIZVODNE	LS-KOMPETITIVNOST RADNE SNAGE	LS-SMANJEN KVALITET PROIZVODA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
13	3.863	KONTROLA PROIZVODNE	LS-KREDITNA NESPOSOBNOST ZAPOSLENIH	LS-NEEFKATIVNO I NEEFKASNO OBAVLJANJE SVAKOG POSLOVNOG ZADATAKA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
14	3.853	KONTROLA PROIZVODNE	LS-NAZADOVOLJSTVO ZAPOSLENIH	LS-NEEFKATIVNO I NEEFKASNO OBAVLJANJE SVAKOG POSLOVNOG ZADATAKA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
15	3.873	KONTROLA PROIZVODNE	LS-NEADEKVATNA ZAŠTITA PODATAKA	LS-POGREŠNA ODLUKA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5
16	3.882	KONTROLA PROIZVODNE	LS-NEPOSTUPANJE IZOSTRUKIH PODATAKA	LS-OTPUŠTANJE RADNIKA	3	3	9	3	4	5	5	5	5	5	2	2	4	3	4	5	5

File name: RIS-RIBASOLUTERSRISNEWVAL = 5

Page: 38/394 Date: 20.09.2017

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 30: Preostali rizici nivoa 4 nakon prve iteracije tretiranja predloženim merama

Univerzitet Singidunum

Danaslova 32, Beograd, Srbija

Preostali rizik nivoa "4"

Rbr	ID rizika	Naziv imovini	Pretnja	Ranjivost	Prele nhrade rizika					Nakon obrade rizika									
					P	R	V	C	I	A	Rizik	P	R	V	C	I	A	Rizik	
1	4.821	DELEGRANJE AUTORITETA	LS-KOMPETITIVNOST RAONE SNAGE	LS-ANGAZOVANJE TREGIM LICAPOVECANJE TROSKOVA	3	2	6	2	1	4	5	2	1	2	2	1	4	3	
2	4.778	DELEGRANJE AUTORITETA	LS-KORISCENJE JAVNIH DRUSTVENIH MREZA	LS-GUBITAK BRENDA	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
3	4.833	DELEGRANJE AUTORITETA	LS-NAZADVOLISTVO ZAPOLSENH	LS-HAMENKO POGRESNO ODLEZANJE PROZVOA	3	2	6	2	1	4	5	2	1	2	2	1	4	3	
4	4.783	DELEGRANJE AUTORITETA	LS-NEADEKVATAN KAPACITET	LS-KORISAK PROZVOH BUDUJSH KULERATA	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
5	4.784	DELEGRANJE AUTORITETA	LS-NEADEKVATAN KAPACITET	LS-TRAJNO OSTECENJE ROBE	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
6	4.787	DELEGRANJE AUTORITETA	LS-NEADEKVATNA LOGISTICKA INFRASTRUKTURA	LS-NEADUGUCNOST OTPREMANJA ROBE	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
7	4.786	DELEGRANJE AUTORITETA	LS-NEADEKVATNA LOGISTICKA INFRASTRUKTURA	LS-POVECANJE SKARTA	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
8	4.824	DELEGRANJE AUTORITETA	LS-NEADEKVATNA ZASTITA PODATAKA	LS-POGRESNA ODLIKA	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
9	4.788	DELEGRANJE AUTORITETA	LS-NEADEKVATNA ZASTITA PODATAKA	LS-POGRESNA ODLIKA	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
10	4.789	DELEGRANJE AUTORITETA	LS-NEADKVATNO UPRAVLJANJE LOGISTICKOM TEHNIKOM I INFRASTRUKTUROM	LS-ZASTOU U PROZVOVANJE	3	2	6	2	1	4	5	2	1	2	2	1	4	3	
11	4.790	DELEGRANJE AUTORITETA	LS-NEAUTORIZOVAN PRISTUP PODACIMA	LS-ODAVANJE POSLOVNE TAJNE	3	2	6	2	1	4	5	2	1	2	2	1	4	3	
12	4.825	DELEGRANJE AUTORITETA	LS-NEAUTORIZOVAN PRISTUP PODACIMA	LS-ODAVANJE POSLOVNE TAJNE	3	2	6	2	1	4	5	2	1	2	2	1	4	3	
13	4.791	DELEGRANJE AUTORITETA	LS-NEODSTATAK SOPSTVENIH TEHNICKA I METODA U PROCESU	LS-ODAVANJE POSLOVNE TAJNE	3	2	6	2	1	4	5	2	1	2	2	1	4	3	
14	4.831	DELEGRANJE AUTORITETA	LS-NETACNOST UNOSA I PRENOSA PODATAKA	LS-POGRESNA ODLIKA	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
15	4.830	DELEGRANJE AUTORITETA	LS-NETACNOST UNOSA I PRENOSA PODATAKA	LS-POVECANJE TROSKOVA	2	3	6	2	1	4	5	1	2	2	2	1	4	3	
16	4.801	DELEGRANJE AUTORITETA	LS-OBIM PROZVOOVANJE NIJE PLANIRAN	LS-NEOPTIMALNA KOLICINA ZALHA	1	3	3	2	1	4	4	A	1	2	2	2	1	4	3

File: risk04 - (RIS-RBASOLUTERISKNEVVAL u 3)

File: RIS04 - URL: http://www.risbasol.com, Ver: 31.1.2013

Date: 26.09.2014 Time: 09:23:44

Filter izdat: (ROS-RRABSOLUTIONSNEWVAL = 3)
Hestia 1024 - LUM, <http://www.hestia-software.com>, Ver. 31.11.2013

Date: 26.06.2014 Time: 09:23:44

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Slika 31: Preostali rizici nivoa 3 nakon prve iteracije tretiranja predloženim merama

Univerzitet Singidunum

Danilova 32, Beograd, Srbija

Preostali rizik nivoa "3"

Referenca	ISMG-RESIO
Nivo	1
Klasifikacija	Interno
Verzija	1
Datum	
Stranica	1 / 87

Rbr	ID rizika	Naziv inoviranih	Pretnja	Ranjivost	Preostali rizik										Nakon obrade rizika											
					P	R	V	C	I	A	R	i	z	i	k	P	R	V	C	I	A	R	i	z	i	k
1	4.821	DELEGIRANJE AUTORITETA	LS-KOMPETENTNOSTI RADNE SNAGE	LS-ANGAZOVANJE TREĆIH LICA-POVEĆANJE TROŠKOVA	3	2	6	2	1	4	5	●	B			2	1	2	2	1	4	3	●			
2	4.778	DELEGIRANJE AUTORITETA	LS-KORISCENJE JAVNIH DRUSTVENIH MREŽA	LS-GUBITAK BRENDA	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
3	4.833	DELEGIRANJE AUTORITETA	LS-NAZADOVOLJSTVO ZAPOSLENIH	LS-NAJAMNO POGREŠNO OBLIKOVANJE PROJEKTA	3	2	6	2	1	4	5	●	B			2	1	2	2	1	4	3	●			
4	4.783	DELEGIRANJE AUTORITETA	LS-NEADEKVATAN KAPACITET	LS-GUBITAK POSTOJEĆIH BUDUĆI KLIJENATA	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
5	4.784	DELEGIRANJE AUTORITETA	LS-NEADEKVATAN KAPACITET	LS-TRAJNO OSTEĆENJE ROBE	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
6	4.787	DELEGIRANJE AUTORITETA	LS-NEADEKVATNA LOGISTIKA INFRASTRUKTURA	LS-NEPOUGODNOST OTPREMANJA ROBE	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
7	4.786	DELEGIRANJE AUTORITETA	LS-NEADEKVATNA LOGISTIKA INFRASTRUKTURA	LS-POVEĆANJE SKARTA	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
8	4.824	DELEGIRANJE AUTORITETA	LS-NEADEKVATNA ZASTITA PODATAKA	LS-POGREŠNA ODLUKA	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
9	4.788	DELEGIRANJE AUTORITETA	LS-NEADEKVATNA ZASTITA PODATAKA	LS-POGREŠNA ODLUKA	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
10	4.789	DELEGIRANJE AUTORITETA	LS-NEADEKVATNO UPRAVLJANJE LOGISTIKOM I TEHNIKOM I	LS-ZASTOJ U PROJEKTOVANJU	3	2	6	2	1	4	5	●	B			2	1	2	2	1	4	3	●			
11	4.790	DELEGIRANJE AUTORITETA	LS-NEAUSLOJIVAN PRISTUP PODACIMA	LS-ODAVANJE POSLOVNE TAJNE	3	2	6	2	1	4	5	●	B			2	1	2	2	1	4	3	●			
12	4.825	DELEGIRANJE AUTORITETA	LS-NEAUSLOJIVAN PRISTUP PODACIMA	LS-ODAVANJE POSLOVNE TAJNE	3	2	6	2	1	4	5	●	B			2	1	2	2	1	4	3	●			
13	4.791	DELEGIRANJE AUTORITETA	LS-NEDOSTATAK SOFISTICIRANIH TEHNIKA I METODA U PROCESU	LS-ODAVANJE POSLOVNE TAJNE	3	2	6	2	1	4	5	●	B			2	1	2	2	1	4	3	●			
14	4.831	DELEGIRANJE AUTORITETA	LS-NETACNOST UNOSA I PRENOSA PODATAKA	LS-POGREŠNA ODLUKA	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
15	4.830	DELEGIRANJE AUTORITETA	LS-NETACNOST UNOSA I PRENOSA PODATAKA	LS-POVEĆANJE TROŠKOVA	2	3	6	2	1	4	5	●	B			1	2	2	2	1	4	3	●			
16	4.801	DELEGIRANJE AUTORITETA	LS-OBIM PROJEKTOVANJE I PLANIRAN	LS-NEOPTIMALNA KOLIČINA ZALIH	1	3	3	2	1	4	4	●	A			1	2	2	2	1	4	3	●			

Fajl izlazi: (RIS-ROBASOLITERISKNEVAL-3)

Dokument: RIS-ROBASOLITERISKNEVAL-3
Datum: 08.03.2018
Stranica: 08.03.2018

Izvor: autor

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Studija slučaja procene rizika u lancima snabdevanja primenom softverskog alata Hestia

Nakon završetka faze tretiranja rizika preostalo je 85 rizika nivoa "5" (umanjeno za 999 rizika) i 203 rizika nivoa "4" (umanjeno za 506 rizika).

Analizom rezultata rizika nivoa "5", a nakon završetka faze evaluacije rizika, kao najkritičniji u lancima snabdevanja identifikovani su sledeći procesi:

- planiranje distribucije, kontrola proizvodnje i planiranje mreže snabdevanja – po 15 rizika;
- korišćenje informacija 13 rizika;
- izvršenje proizvodnje, poslovi akvizicije i plasmana sredstava, priprema proizvodnje – po 9 rizika nivoa "5".

Slika 32: Statistika procene rizika u lancu snabdevanja



Univerzitet Singidunum
Danjelska 32, Beograd, Srbija

Statistika procene rizika

Referenca	ISMS-STAT
Nivo	1
Klasifikacija	Interno
Verzija	1
Datum	02.04.2014
Stranica	1 / 1

Broj grupa imovine	10
Broj imovine	26
Broj procena rizika	2,395
Broj procena rizika 5	1,084
Broj procena rizika 4	710
Broj procena rizika 3	537
Broj procena rizika 2	50
Broj procena rizika 1	13
Broj procena rizika 0	1
Sveukupni broj kontrola	209
Broj koriscenih kontrola	23

Dokument napravio	Dokument kontrolirao	Dokument odobrio

Izvor: autor

Sledeći korak je donošenje odluke da li se prihvataju procenjeni nivoi rizika ili se odlučuje sa primenu novih kontrola/mera, nakon čega je neophodno da se opet izvrši faza evaluacije rizika. U predmetnoj studiji su prihvaćeni nivoi rizika dobijenih evaluacijom rizika.

4.4. Rezime poglavlja

U cilju dokazivanja istinitosti postavljene hipoteze, da je procenu identifikovanih rizika u lancima snabdevanja moguće automatizovati, u ovom poglavlju je prikazan proces automatizovane obrade podataka (polazni parametri: resurs, ranjivost, pretnja, mera za otklanjanje) pri proceni rizika u lancima snabdevanja primenom softverskog alata Hestia. Da bi se softver efikasno i efektivno primenio na studiji slučaja procene rizika u lancima snabdevanja, izvršene su modifikacije uslova i kriterijuma, u odnosu na osnovnu verziju softvera koja se oslanja na standard ISO 27005 (upravljanje rizicima i informaciona bezbednost). Modifikovani softverski alat Hestia usklađen je sa generisanim parametrima Kinney metode, kako bi se zaokružio ciklus procene rizika u lancima snabdevanja.

Poređenja radi, Kinney metoda za procenu rizika se bazira na parametrima: verovatnoća pojave događaja, učestalost pojavljivanja događaja i težina posledice; dok se primenjeni softver bazira na inputima ranjivost resursa i pretnja po njegovo stabilno funkcionisanje. Ranjivost predstavlja slabost resursa (imovine, procesa...) i omogućava mu da bude eksploatisan/iskorišćen od strane jedne ili više pretnji, odnosno izvora rizika koji može biti materijalne ili nematerijalne prirode.

Nakon identifikacije ranjivosti izvršeno je njihovo pridruživanje pretnjama po pojedinim procesima, kao i po lancu snabdevanja u celini. U studiji je razmatrano 289 ranjivosti i 161 pretnja po poverljivost, integritet i raspoloživost u lancima snabdevanja. Osim unapred definisanih ranjivosti i pretnji u lancu snabdevanja, specifično je što se unapred mora dati predlog mera za ublažavanje rizika, kako bi se obezbedili svi ulazni parametri za procenu rizika. Iskorišćene su mere za ublažavanje rizika koje su predložene nakon procene rizika primenom Kinney metode, čime se praktično nadograđuje "tradicionalni" način procene rizika.

Korišćenjem aplikacije izvršena je automatska evaluacija rizika, a kao rezultat su dobijene 2393 pojedinačne procene rizika. Došlo se do zaključka da je ekstremni rizik evidentan u segmentima proizvodnje, planiranja i korišćenja informacija, posebno na mestima gde se pretnja usko vezuje za ljudski faktor (kompetentnost radne snage, otpor prema usvajanju novih informaciono komunikacionih tehnologija, netačnost unosa podataka, itd.). Sa druge strane, prihvatljivi rizici su identifikovani u procesima zamene (proizvoda) usled propusta u poslovanju partnera, osipanja broja klijenata, itd., dakle u segmentima na čije funkcionisanje kompanija – članica lanca snabdevanja kao samostalni entitet nema direktnog uticaja.

5. ZAKLJUČNA RAZMATRANJA

Savremeni poslovni trendovi često uslovljavaju kompanije da implicitno uključe u proces upravljanja i kontrolu rizika u cilju smanjenja efekata poremećaja koji ugrožavaju kontinuitet poslovanja. Sa aspekta kompleksnog okruženja u kojem danas egzistiraju kompanije, ovaj rad podvlači potrebu za uvođenje metodologije kojom bi se identifikovali, klasifikovali i upravljali rizici u lancu snabdevanja, i izvršila procena i izbor radnji u cilju poboljšanja otpornosti kako svake pojedinačne kompanije (članice lanca snabdevanja), tako i čitavog lanca snabdevanja.

Logistika predstavlja novu paradigmu za postizanje konkurentnosti kompanije u različitim proizvodnim i uslužnim sektorima. Pokretačka snaga logistike transformiše se od projektovane minimizacije troškova i maksimizacije kvaliteta usluge i/ili finalnog proizvoda, do sistemskog pristupa izučavanju složenih logističkih fenomena. Složenost, kompromisi, efikasna koordinacija, konflikti i potreba da se vodi računa o odnosima van logističkog sistema, kao implikacije sistemskog pristupa izučavanju logističkog sistema i logističkih podсистема ukazuju na važnost logistike u cilju kreiranja pozitivnog privrednog okruženja.

Pred svakom međunarodno orijentisanom kompanijom dominantan značaj, u odnosu na ostale faktore poslovnog uspeha, ima upravljanje lancima snabdevanja, jer je obezbeđivanje raspoloživosti zahtevanog proizvoda u pravo vreme, na pravom mestu i po prihvatljivim troškovima daleko teže ostvariti u planetarnim nego u nacionalnim okvirima.

Primarna svrha lanca snabdevanja je povezivanje glavnih poslovnih funkcija i procesa ²⁸ između kompanija u konzistentan poslovni model sa maksimalnim učinkom. Iako još uvek ne postoji opšte prihvaćena definicija lanca snabdevanja, niti model njegovog upravljanja, može se okvirno reći da lanac snabdevanja predstavlja složen proces koordinacije tačno određenih aktivnosti različitih kompanija u cilju zadovoljenja potreba krajnjeg korisnika.

Funkcija upravljanja lancem snabdevanja suočava se sa izazovima koje pred nju postavljaju rizici iz internog i eksternog okruženja svih članova lanca snabdevanja. Posledice izazvane rizicima mogu biti različitog intenziteta, od neprimetnih do katastrofalnih. Prema usvojenoj definiciji, rizik u lancu snabdevanja predstavlja proizvod pozitivne verovatnoće pojave smetnje koja će uticati na funkcionisanje sistema i evidentnih ili neevidentnih posledica po stabilnost sistema.

Efikasno upravljanje rizicima u lancima snabdevanja direktno implicira njihovu kategorizaciju. Analizom relevantne i dostupne literature koja se bavi problematikom kategorizacije rizika u lancima snabdevanja, došlo se do zaključka da postoji više od 70 vrsta strukturno različitih rizika u lancima snabdevanja.

Dakle, upravljanje rizikom je važno sredstvo u obezbeđivanju ekonomskog integriteta kompanije, posebno ukoliko se jasno postave granice kompanije. U okruženju, upravljanje lancem snabdevanja postaje zamagljeno, što ne znači da ono zakonski više

ne postoji, ali proces identifikovanja linije razdvajanja između dve kompanije postaje veoma težak. Paralelno sa proširenjem obima upravljanja lancem snabdevanja, upravljanje rizikom treba da postane odgovornije.

Proces procene rizika je od vitalnog značaja i podrška procesu donošenja odluka u kompaniji. Različite kompanije koriste različite metode za procenu rizika, čiji nivoi sofisticiranosti u samom procesu variraju. Kinney metoda za procenu rizika uvedena je prvi put u upotrebu 1976. godine u cilju prevencije rizika od eksplozija u vojnoj industriji. Kao takav, metod je naišao na opšti uspeh širom Evrope. Većina relevantnih literaturnih izvora upravo ovu metodu kvalifikuje kao bazičnu metodu procene rizika.

Za potrebe ovog istraživanja parametri dobijeni korišćenjem Kinney metode uneti su u modifikovani softverski alat Hestia, pa je sačinjen novi model za upravljanje rizicima, koji je testiran na studiji slučaja zamišljenog poslovnog sistema uz poštovanje aktuelnih ograničenja realnih poslovnih sistema. Time je potvrđena opšta hipoteza: *"Moguće je automatizovati procenu rizika u lancima snabdevanja"*. Prikazan je proces automatizovane obrade podataka (polazni parametri: resurs, ranjivost, pretnja, mera za otklanjanje) pri proceni rizika u lancima snabdevanja primenom softverskog alata Hestia.

Posebna hipoteza 1: *"Moguće je generisati efikasan model za upravljanje rizicima u lancima snabdevanja, koji će biti kompatibilan sa generalnom strategijom upravljanja rizicima"* je takođe dokazana ovim istraživanjem, tako što je konstruisan model za upravljanje rizicima u lancima snabdevanja koji u sebi sadrži sinergiju Kinney metode i modifikovanog softverskog alata Hestia, uz poštovanje osnovnih postulata teorije verovatnoće i teorije rizika. Primenjeni model je komplementaran sa ISO standardima (27000 – bezbednost informacija, 28000 – bezbednost u lancu snabdevanja i 31000 – menadžment rizikom) i ovim istraživanjem je dobio potvrdu svoje primenljivosti u studiji slučaja zamišljenog poslovnog sistema, odnosno entiteta u lancu snabdevanja.

Poređenja radi, Kinney metoda za procenu rizika se bazira na parametrima: verovatnoća pojave događaja, učestalost pojavljivanja događaja i težina posledice; dok se primenjeni softver bazira na inputima ranjivost resursa, pretnja po njegovo stabilno funkcionisanje i predložena mera za ublažavanje pretnje. Ranjivost predstavlja slabost resursa (imovine, procesa...) i omogućava mu da bude eksploatisan/iskorišćen od strane jedne ili više pretnji, odnosno izvora rizika koji može biti materijalne ili nematerijalne prirode.

U studiji je razmatrano 289 ranjivosti i 161 pretnja po poverljivost, integritet i raspoloživost u lancima snabdevanja. Osim unapred definisanih ranjivosti i pretnji u lancu snabdevanja, specifično je što se unapred mora dati predlog mera za ublažavanje rizika, kako bi se obezbedili svi ulazni parametri za procenu rizika. Iskorišćene su mere za ublažavanje rizika koje su predložene nakon procene rizika primenom Kinney metode, čime se praktično nadograđuje "tradicionalni" način procene rizika. Korišćenjem aplikacije izvršena je automatska evaluacija rizika, a kao rezultat su dobijene 2393 pojedinačne procene rizika.

Posebna hipoteza 2: *"Definisani model za upravljanje rizicima u lancima snabdevanja, koji će poštovati osnovne teorijske postulate risk menadžmenta imaće potvrdu svoje aplikativnosti u realnim poslovnim sistemima"* u ovom istraživanju je potvrđena

testiranjem modela za procenu rizika u lancu snabdevanja, koji je sačinjen od Kinney metode i modifikovanog softverskog alata Hestia uz poštovanje strategije risk menadžmenta na zamišljenom modelu poslovnog sistema. Rezultati testiranja ovog modela ukazuju na postojanje prihvatljivih i ekstremnih rizika u lancima snabdevanja. Dok su prvi izazvani takozvanim okolinskim faktorima, drugi su evidentirani u svim unutrašnjim dimenzijama funkcionisanja preduzeća.

1. Okolinski faktori koji izazivaju prihvatljive rizike identifikovane u segmentima na čije funkcionisanje kompanija – članica lanca snabdevanja kao samostalni entitet nema direktnog uticaja su:

a) politički:

- terorizam,
- političke pretnje koje se odnose na donošenje poslovnih odluka,
- česte promene ekonomske politike i zaustavljanje reformi zbog izbora,
- nepostojanje političke stabilnosti i kontinuiteta u vođenju ekonomske politike,
- previsok nivo javnih rashoda,
- glomazna i skupa državna administracija,
- religijske i etničke tenzije,
- nepostojanje demokratske odgovornosti lokalne samouprave prema kompanijama na teritoriji njene nadležnosti;

b) ekonomski:

- globalna finansijska kriza,
- visina deviznog kursa,
- česte promene ekonomske politike i zaustavljanje reformi zbog izbora,
- loš kreditni rejting zemlje,
- skupi eksterni izvori finansija,
- postojanje monopola ili oligopola,
- nepovezivanje kompanija u izvozne klastere,
- pojava supstituta/zamenskih P/U,
- erozija brenda zbog povećanja konkurencije,
- Vlada ne interveniše na tržištu u cilju stabilizacije kursa,
- ne pruža se podrška posrnutim kompanijama posebnim olakšicama ili smanjenjem poreza,
- ne štite se domaće kompanije, tehnologije i sl. kako bi se regulisali makroekonomski uslovi,
- konvertibilnost valute,
- prekid u određenom trendu navika krajnjeg korisnika,
- prekid rasta pozitivnog trenda rasta neto dobitka;

c) pravni:

- nepostojanje elektronskih servisa u domenu javnih registara,
- diskriminišuća regulativa,
- rizik eksproprijacije,
- kršenje ugovora,
- masovna nacionalizacija,
- regulatorne promene,

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Zaključna razmatranja

- kvalitet birokratije i administracije,
 - pronevere i kriminalne radnje u poslovanju partnera.
2. Ekstremni rizik je evidentan u svim segmentima rada poslovnog sistema, gde je dominantan ljudski faktor. Radi se o sledećim unutrašnjim dimenzijama funkcionisanja preduzeća:
- a) pravna regulativa poslovanja:
 - nepoštovanje sistematizacije radnih mesta i ostalih pravnih akata na nivou organizacije/države,
 - istek ugovora kojim se regulišu odnosi sa poslovnim partnerima;
 - b) upravljanje ljudskim resursima:
 - neusklađenost potreba radnog mesta sa obrazovnim sistemom,
 - neadekvatno obrazovanje/veštine/sposobnosti,
 - nizak nivo znanja i odgovornosti,
 - nepostojanje prethodnog radnog iskustva,
 - rad pod pritiskom,
 - otpuštanje kadrova,
 - angažovanje kadrova (prethodno otpuštenih) posredstvom agencije za privremeno zapošljavanje,
 - neizvesnost među radnicima u pogledu stabilnosti radnog mesta,
 - neadekvatna (ili nepostojanje) komunikacija,
 - neodgovarajuća reputacija kompanije u javnosti zbog poremećenih međuljudskih odnosa;
 - c) bezbednost i zdravlje na radu:
 - neuspešno kreiranje bezbednog radnog okruženja,
 - nepoštovanje propisanih akata iz domena bezbednosti i zdravlja na radnom mestu i zaštite od požara,
 - korišćenje neispravne opreme i sredstava za rad;
 - d) poslovni moral:
 - nemoralno ponašanje zaposlenih,
 - odavanje poslovnih tajni,
 - mito i korupcija,
 - krađa informacija/materijalnih dobara,
 - mobing,
 - nepotizam;
 - e) otpori prema tehnološkim i organizacionim promenama:
 - pružanje otpora ka usvajanju novih tehnologija/procesa poslovanja,
 - otpor prema novim tehnologijama (EDI, RFID, SAP, e-mail...);
 - f) menadžment:
 - nemogućnost obezbeđivanja potrebnih investicija,
 - nedostatak kvalitetne kontrole i upravljanja,
 - nedostatak ideja i inovacija,
 - neracionalni i šablonski rad,
 - neuklanjanje uzroka lošeg kvaliteta P/U,
 - nepostojanje kontrole kvaliteta P/U,
 - nepreduzimanje korektivnih mera, itd.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Zaključna razmatranja

Za ublažavanje identifikovanih rizika u segmentima rada poslovnog sistema, gde je ljudski faktor prepoznat kao primarna pretnja po stabilno funkcionisanje kompanije predlažemo sledeće:

- a) U cilju poštovanja i obezbeđivanja pravne regulative poslovanja potrebno je ustanoviti rad disciplinske komisije i/ili nadzornog tela, ali i pristupati redovnim revizijama ugovora kojima se regulišu odnosi sa poslovnim partnerima;
- b) Za ublažavanje rizika prouzrokovanih neadekvatnim upravljanjem ljudskim resursima, smatramo značajnim formiranje i razvijanje Službe za upravljanje ljudskim resursima koja bi obezbedila kvalitetnu interakciju sa NSZ, obavljala aktivnosti regrutacije i selekcije, ocenjivala performance rada zaposlenih i adekvatno upravljala fluktuacijom kadrova;
- c) Podizanje nivoa bezbednosti i zdravlja na radu moguće je postići: kreiranjem bezbednog radnog okruženja, donošenjem Akta o proceni rizika i Pravilnika o zaštiti od požara, obukom zaposlenih ⁵⁶ poznavanja propisa BZR i zaštite od požara kao i lekarskim pregledima zaposlenih koji rade na mestima sa povećanim rizikom;
- d) Afirmisanje korporativne kulture koja bi bila zasnovana na moralnim obrascima ponašanja može biti postignuto uvođenjem etičkog kodeksa za zaposlene i pooštavanjem disciplinskih mera za nepoštovanje radne discipline i etičkog kodeksa;
- e) Otpori prema tehnološkim i organizacionim promenama mogu biti smanjeni obukom i usavršavanjem zaposlenih kao i formiranjem skale nagrađivanja zaposlenih što je u nadležnosti Službe za upravljanje ljudskim resursima;
- f) Za ublažavanje rizika prouzrokovanih neefikasnim menadžmentom predlažemo sledeće: redovno praćenje poslovnih trendova, racionalizacija proizvodnih procesa, sprovođenje kontrole kvaliteta P/U, preduzimanje preventivnih mera, podizanje ugleda kompanije kroz donacije, sponzorstva, kulturne manifestacije, davanje stipendija talentovanim učenicima, kreiranje strategije i plana komunikacije kako vertikalne, tako i horizontalne unutar organizacije, organizovanje redovnih sastanaka projektnog tima sa ciljem razmene informacija, online diskusioni forum gde članovi tima mogu da postavljaju pitanja i dobijaju odgovore sa rezultatima ali i kreiranje baze podataka poslovne dokumentacije i njeno pretraživanje radi lakšeg korišćenja, uključujući i proces upravljanja.

Rezultati do kojih se došlo tokom istraživanja klasifikovani su na sledeći način:

- Kreiran je registar rizika u lancima snabdevanja;
- Kreiran je registar ranjivosti i pretnji u lancima snabdevanja;
- Kreiran je registar predloženih mera za mitigaciju rizika u lancima snabdevanja;
- Kreiran je model za procenu rizika u lancima snabdevanja kojim se povezuje Kinney metoda sa modifikovanim softverskim alatom Hestia.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

Zaključna razmatranja

Ograničenje primenjene metode za procenu rizika u lancu snabdevanja ogleda se u činjenici da postoji izvesna doza subjektivnosti analitičara. U cilju proveravanja predloženog modela i obezbeđivanja objektivnosti neophodno je da model verifikuje više analitičara u različitim realnim poslovnim sistemima, kako bi se poređenjem njihovih rezultata došlo do objektivnije procene koja je ključna faza u upravljanju rizicima u lancima snabdevanja.

6. LITERATURA

- Adamović, Ž., Jovanov, G., Radojević, M. & Meza, S., 2008. *Upravljanje rizikom*. 1st ed. Zrenjanin: Tehnički fakultet "Mihajlo Pupin".
- Adelsberger, D., 2010. *Hestia Risk*. Beograd: Univerzitet Singidunum.
- Adelsberger, Z., 2014. *Hestia Risk Manager – Upute*. Zagreb: Bluefield.
- Antić, V. et al., 2004. *Hrvatski enciklopedijski rječnik*. Zagreb: Novi Liber.
- Arsovski, S., 2014. *Mapiranje poslovnih procesa*. Kragujevac: Mašinski fakultet u Kragujevcu.
- Beamon, B.M., 1998. Supply chain design and analysis: Models and methods. *International Journal of Production Economics*, 55, p.281.
- Bek, U. 2001. *Rizično društvo*. Beograd: Filip Višnjić.
- Brindley, C., 2004. *Supply Chain Risk*: Ashgate, Aldershot.
- Bulatović, M., 2013. *Logistika*. Podgorica: Inženjerska komora Crne Gore.
- Cavinato, J.L., 1982. *The traffic service corporation*. Washington DC: The traffic service corporation.
- Černiček, I. & Molnar, R., 2012. *Teorija sistema*. 1st ed. Zrenjanin: Visoka tehnička škola strukovnih studija u Zrenjaninu.
- Christopher, M., 1998. *Logistics and Supply Chain Management*. 2nd ed. Harlow: Financial Times Prentice Hall.
- Chopra, S. & Meindl, P., 2014. *Supply Chain Management: Strategy, Planning, and Operation*. 6th ed. New York: Prentice Hall.
- Christopher, M., 2005. *Logistics and Supply Chain Management*. Great Britany: Pretince Hall Co.
- Covello, V.T. & Mumpower, J., 1985. Risk Analysis and Risk Management: An Historical Perspective. *Risk Analysis*, 5(2), p.103.
- Cox, J.F. & Blackstone, J.H., 1998. *Apics Dictionary*. 9th ed. Falls Church: The APICS Educational and Research Foundation.
- CSCMP, 2015. *Council of Supply Chain Management Professionals*. <https://cscmp.org>
- ELA, 2015. *European Logistics Association*. <http://www.elalog.eu>
- Goh, M., Lim, J. & Meng, F., 2007. A stochastic model for risk management in global supply chain networks. *European Journal of Operational Research*, 182(1), p.164.

- 12
Grubić – Nešić, L., 2005. *Razvoj ljudskih resursa*. Novi Sad: AB print.
- 38
Giunipero, L. & Eltantawy, R., 2004. Securing the upstream supply chain: a risk management approach. *International Journal of Physical Distribution & Logistics Management*, 34(9), p.698.
- Hadžiselimović, E., 2006. Mapiranje poslovnih procesa. *Kvalitet*, 5-6, p.44.
- 52
Hopkin, P., 2012. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. Kogan Page Publishers.
- 51
Hunt, D., 1996. *Process Mapping – How to Reengineer Your Business Processes*. New York: John Wiley & Sons Inc.
- 57
ISO 27005, 2011. *ISO/IEC 27005 - Information technology - Security techniques - Information security risk management*. International Organization for Standardization.
- 35
ISO 31000, 2009. *ISO 31000 - Risk management - Principles and guidelines*. International Organization for Standardization.
- ISO, 2009. *ISO Guide 73:2009 - Risk Management - Vocabulary*. Geneva: International Organization for Standardization.
- 37
Jomini, A.H., 1838. *Précis de l'Art de la Guerre: Des Principales Combinaisons de la Stratégie, de la Grande Tactique et de la Politique Militaire*. Paris: Anselin.
- 84
Jomini, A.H., 1862. *Art of War*. Philadelphia: J.B. Lippincott & Co.
- 6
Jüttner, U., Peck, H. & Christopher, M., 2003. Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, 6(4), p.197.
- 34
Kersten, W., Hohrath, P. & Boger, M., 2007. An empirical approach to supply chain risk management: development of a strategic framework. In *Proceedings of the 18th Annual POMS (Production & Operations Management Society) Conference*. Dallas, USA, 2007.
- 54
Kight, F.H., 1921. *Risk, Uncertainty and Profit*. 1st ed. Boston and New York: Houghton Mifflin Company.
- 48
Kinney, G.F. & Wiruth, A.D., 1976. Practical risk analysis for safety management. In *NWC Technical publication 5865*. China Lake California, USA: Naval Weapons Centre.
- Klimov, R.A. & Merkurjev, Y.A., 2006. Simulation-based risk measurement in supply chains. In *Proceedings 20th European Conference on Modelling and Simulation*, 2006.
- Kleiman, F.H., 1999. Risk Management Agonistes. *Risk Analysis Journal*, 10(2), p.201.
- 30
Koob, J.P. & Malchaire, J., 2003. *Fiabilité de la méthode Kinney d'analyse des risques*. Brussels: Université catholique de Louvain.
- 17
Lavastre, O., Gunasekaran, A. & Spalanzani, A., 2012. Supply chain risk management in French companies. *Decision Support Systems*, 54(4), p.828.

Lukić, S.M., Vujnović Gligorić, B. & Lukić, S., 2009. *Menadžment rizika*. Banja Luka: Panevropski univerzitet Apeiron.

Lummus, R. & Alber, K., 1997. *SupplyChain Management: Balancing the SupplyChain with Customer Demand*. Falls Church, Virginia: The Educational and Resource Foundation of APICS.

Maslarić, M., 2014. *Razvoj modela upravljanja logističkim rizicima u lancima snabdevanja*. Doktorska disertacija. Novi Sad: Fakultet tehničkih nauka.

Matotek, M. & Regodić, D., 2015. Gestión del riesgo de los recursos humanos en la cadena de suministro. *Dyna Management*, 3, pp.1-8. <http://dx.doi.org/10.6036/MN7478>.

Mentzer, J.T. et al., 2001. Defining Supply Chain Management. *Journal of Business Logistics*, 22(2), p.1.

Milovanović, G., Barac, N. & Anđelković, A., 2011. Logistika, menadžment lanca snabdevanja i konceptualne perspektive njihovog odnosa. *Ekonomске teme*, 3, p.339.

Molnar, R. & Matotek, M., 2014. *Strategijski menadžment - Praktikum*. 1st ed. Zrenjanin: Visoka tehnička škola strukovnih studija u Zrenjaninu.

Nadrljanski, Đ. & Nadrljanski, M., 2014. *Menadžment rizika*. Split: Visoka škola za inspeksijski i kadrovski menadžment.

Norrman, A & Lindroth, R., 2002. Supply Chain Risk Management: Purchasers' vs. Planners' Views on Sharing Capacity Investment Risks in the Telecom Industry. In *11th International IPSERA Conference*. Enschede, Netherlands.

Norrman, A. & Jansson, U., 2004. Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management*, 34(5), p.434.

Ostojić, S., 2007. *Osiguranje i upravljanje rizicima*. Beograd: Data Status.

Park, A., Nayyar, G. & Low, P., 2013. *Supply Chain Perspective and Issues. A Literature Review*. Geneva and Hong Kong: Fung Global Institute and World Trade Organization.

Pfohl, H.C., Kohler, H. & Thomas, D., 2010. State of the art in supply chain risk management research: empirical and conceptual findings and a roadmap for the implementation in practice. *Logistics Research*, 2(1), p.33.

Post, T., Van den Assem, M.B.G. & Thaler, R., 2008. Deal or No Deal? Decision Making under Risk in a Large Payoff Game Show. *American Economic Review*, 98(1), pp.38-71.

Procter, P., 2001. *Cambridge International Dictionary of English*. London: Cambridge University Press.

Ravindran, R.A. & Warsing, D.P.J., 2012. *Supply Chain Engineering: Models and Applications*. Boca Raton - London - New York: CRC Press.

- Regodić, D., 2014. *Logistika - Lanci snabdevanja*. 4th ed. Beograd: Univerzitet Singidunum. 81
- Rejda, G.E. & McNamara, M., 2014. *Principles of Risk Management and Insurance*. 12th ed. Edinburg: Prentice Hall. 42
- Reniersa, G., Sörensen, K. & Dullaert, W., 2012. A multiattribute Systemic Risk Index for comparing and prioritizing chemical industrial areas. *Reliability Engineering & System Safety*, 98(1), p.32. 49
- Robinson, P.J., Faris, C.W. & Wind, Y., 1967. *Industrial Buying and Creative Marketin*. Boston: Allyn and Bacon. 47
- Rogers, D. & Tibben-Lembke, R., 2005. *Going Backwards: Reverse Logistics Trends and Practices*. Pittsburgh: Reverse Logistics Executive Council. 24
- Santos Ceryno, P., Scavarda, L.F., Klingebiel, K., Yüzgülec, G., 2013. Supply Chain Risk Management: A Content Analysis Approach. *International Journal of Industrial Engineering and Management*, 4(3), pp. 141-150. 60
- SCOR: *Supply Chain Operations Reference Model. Version 9.0.*, 2008, Supply Chain Council.
- Sizemore, B., 2003. Determining System Boundaries for Federal IT Systems. In *GIAC Security Essentials Certification Practical Assignment*. Swansea, Wales: SANS Institute. 6
- Taleb, N.N., 2007. *The Black Swan: The Impact of the Highly Improbable*. 1st ed. London: Penguin. 6
- Tang, C. S., 2006. Perspectives in supply chain risk management. *International Journal of Production Economics*, 103(20), p.451. 8
- The Chartered Institute of Logistics and Transport, 1998. *Glossary of Inventory and Materials Management Definitions*. London. 17
- Tummala, R. & Schoenherr, T., 2011. Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management: An International Journal*, 16(6), p.474. 36
- Vaughan, E.J. & Vaughan, T.M., 2000. *Essentials of Insurance : a risk management perspective*. 10th ed. Zagreb: Mate. 67
- Vukaklija, M., 1980. *Leksikon stranih reči i izraza*. Beograd: Prosveta. 59
- Waters, D., 2007. *Supply chain risk management: vulnerability and resilience in logistics*. United Kingdom and USA: Kogan Page. 64
- Zakon o tehničkim zahtevima za proizvode i ocenjivanju usaglašenosti, 2009. Službeni glasnik RS 36/2009.
- Zelenika, R. & Pupovac, D., 2001. Suvremeno promišljanje osnovnih fenomena logističkih sustava. *Ekonomski pregled*, 52(3-4), pp.354-78.

KVANTIFIKACIJA RIZIKA U LANCIMA SNABDEVANJA

ORIGINALITY REPORT

17%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.cqm.rs Internet	879 words — 3%
2	upravljanjerizicima.com Internet	764 words — 3%
3	www.ef.uns.ac.rs Internet	230 words — 1%
4	www.pepogledi.org Internet	225 words — 1%
5	www.srdjansimic.com Internet	146 words — 1%
6	doku.b.tu-harburg.de Internet	103 words — < 1%
7	kvalitet.telefonija.rs Internet	98 words — < 1%
8	webserver.rcub.bg.ac.rs Internet	90 words — < 1%
9	instifdt.bg.ac.rs Internet	81 words — < 1%
10	www.caruk.rs Internet	69 words — < 1%
11	www.mfin.hr Internet	67 words — < 1%

12	147.91.175.145 Internet	65 words — < 1%
13	www.kvalis.com Internet	63 words — < 1%
14	Idriz, Ćosić. "LOGISTIKA TRGOVAČKIH CENTARA", Business Consultant / Poslovni Konsultant, 2015. Publications	56 words — < 1%
15	www.lib.umd.edu Internet	49 words — < 1%
16	www.singipedia.com Internet	49 words — < 1%
17	www.amfiteatruconomic.ro Internet	44 words — < 1%
18	Dragosavac, Milos. "Operational risks", Skola biznisa, 2012. CrossCheck	43 words — < 1%
19	www.overa.rs Internet	39 words — < 1%
20	www.seminarski-diplomski.rs Internet	37 words — < 1%
21	www.singipedia.singidunum.ac.rs Internet	36 words — < 1%
22	www.mif.gov.me Internet	35 words — < 1%
23	archive.org Internet	35 words — < 1%
24	Levner, Eugene, and Alexander Ptuskin. "An entropy-based approach to identifying vulnerable	33 words — < 1%

25 "e - Marketing. Svaka tvrtka nastoji razvijati nove proizvode, to zbog zadovoljavanja elja i potreba kupaca, to zbog natjecanja s konkurencijom ili odr anja i povećanja prodaje. ", International Baccalaureate/Languages, 2011-07-05
Publications

32 words — < 1%

26 0353-8648, 2002
Publications

32 words — < 1%

27 www.oxera.com
Internet

31 words — < 1%

28 1451-107X, 2005
Publications

30 words — < 1%

29 S. M. Wagner. "A case study-based analysis of spare parts management in the engineering industry", Production Planning & Control, 06/2008
CrossCheck

30 words — < 1%

30 cdn.intechopen.com
Internet

28 words — < 1%

31 www.tadbir.ca
Internet

27 words — < 1%

32 www.cps.org.rs
Internet

26 words — < 1%

33 www.paragraf.rs
Internet

26 words — < 1%

34 web.logu.tu-harburg.de
Internet

25 words — < 1%

35 library.tisi.go.th
Internet

24 words — < 1%

36	Budimir &#352;o&#353;ko, Gabrijela and Volarevi&#263;; Aurora. "ULOGA RA&#268;UNOVODSTVA U PROCESU UPRAVLJANJA RIZICIMA", Business Consultant / Poslovni Konsultant, 2014. Publications	24 words — < 1%
37	www.perspectivia.net Internet	23 words — < 1%
38	www.drkresearch.org Internet	23 words — < 1%
39	sr.wikipedia.org Internet	23 words — < 1%
40	Sica, Emanuele. "June 1940: The Italian Army and the Battle of the Alps", Canadian Journal of History, 2012. Publications	23 words — < 1%
41	www.tdmarvel.com Internet	22 words — < 1%
42	www.hubrussel.net Internet	21 words — < 1%
43	www.vaspitacka.edu.rs Internet	21 words — < 1%
44	www.qucosa.de Internet	20 words — < 1%
45	www.ekapija.com Internet	20 words — < 1%
46	www10.iadb.org Internet	19 words — < 1%
47	www.mzlu.cz Internet	

18 words — < 1%

48 www.databankarbo.nl
Internet

18 words — < 1%

49 lrd.yahooapis.com
Internet

17 words — < 1%

50 etd.auburn.edu
Internet

17 words — < 1%

51 spa.synisys.com
Internet

17 words — < 1%

52 customwritingtips.com
Internet

17 words — < 1%

53 www.inf.ed.ac.uk
Internet

16 words — < 1%

54 www.bmibourse.org
Internet

16 words — < 1%

55 www.kopija.co.rs
Internet

16 words — < 1%

56 belmedic.rs
Internet

16 words — < 1%

57 comum.rcaap.pt
Internet

15 words — < 1%

58 eprints.hud.ac.uk
Internet

14 words — < 1%

59 veronica186.blogspot.com
Internet

13 words — < 1%

60	Schneider, Christian O., Philipp Bremen, Paul Schäfers, and Robert Alard. "Transaction cost economics in global sourcing: Assessing regional differences and implications for performance", <i>International Journal of Production Economics</i> , 2013. CrossCheck	13 words — < 1%
61	<i>Industrial Management & Data Systems</i> , Volume 101, Issue 8 (2006-09-19) Publications	13 words — < 1%
62	<i>Journal of Manufacturing Technology Management</i> , Volume 24, Issue 4 (2013-05-27) Publications	13 words — < 1%
63	cebralog.com Internet	13 words — < 1%
64	serbia-energy.eu Internet	12 words — < 1%
65	1452-0680, 2008 Publications	12 words — < 1%
66	Kuzmanovic, Srecko. "Simulation model for solving tactical situations and ethical challenges during marching of military units", <i>Vojnotehnicki glasnik</i> , 2009. CrossCheck	11 words — < 1%
67	www.iaus.ac.rs Internet	10 words — < 1%
68	Adamović, Mirjana. "Tijelo, identitet i tjelesne modifikacije", <i>Sociologija i prostor / Sociology & Space</i> 18465226, 20110101 Publications	10 words — < 1%
69	www.carinskatarifa.rs Internet	10 words — < 1%
70	caruk.rs Internet	10 words — < 1%

71	www.ru.ac.za Internet	9 words — < 1%
72	www.kontrolnaja.ru Internet	9 words — < 1%
73	www.ifacts.se Internet	9 words — < 1%
74	Radovanovic, Lj., Z. Adamovic, and J. G. Speight. "Risk Analysis for Increasing Safety in Power Plants", Energy Sources Part B Economics Planning and Policy, 2015. CrossCheck	9 words — < 1%
75	www.akroasis.org Internet	9 words — < 1%
76	www3.ptt.rs Internet	9 words — < 1%
77	rs.isede-net.eu Internet	9 words — < 1%
78	www.paragraf.co.rs Internet	9 words — < 1%
79	www.omnis.rs Internet	9 words — < 1%
80	www.golfklub.rs Internet	9 words — < 1%
81	yedion.afeka.ac.il Internet	8 words — < 1%
82	biotaxa.org Internet	8 words — < 1%
83	novedadesenred.com Internet	8 words — < 1%

84	onlinebooks.library.upenn.edu Internet	8 words — < 1%
85	www.doria.fi Internet	8 words — < 1%
86	www.socioloskaluca.ac.me Internet	8 words — < 1%
87	www.centarzaregionalizam.org.rs Internet	8 words — < 1%
88	www.kontekst.org.yu Internet	8 words — < 1%

EXCLUDE QUOTES OFF
EXCLUDE BIBLIOGRAPHY OFF

EXCLUDE MATCHES OFF