ISSN 1846-6168
UDK 65.011.3

METODOLOGIJA IMPLEMENTACIJE UPRAVLJANJA RIZICIMA FMEA METODOM

IMPLEMENTATION METHODOLOGY OF RISK MANAGEMENT WITH FMEA METHOD

Krešimir Buntak, Ivana Drožđek, Marijana Košćak

Stručni članak

Sažetak: *Rizici su tema koja se ne smije zanemarivati, već s kojom se treba suočiti kako bi se povećali izgledi za opstanak i rast. Iako oni predstavljaju neizvjesnost i negativan utjecaj, ovim radom je prikazana metodologija implementacije upravljanja rizicima FMEA metodom, odnosno kako ih analizirati i suočiti se s njima. Rad ima za cilj ukazivanje na postojanje potrebe za pravilnim upravljanjem rizicima u organizaciji, te je u njemu prikazana primjena implementacije organizacije FMEA metodom općenito i na poduzeću XY.*

Ključne riječi: *rizici, implementacija, FMEA metoda, organizacija, ISO norma 31000:2009*

Professional paper

Abstract: *Risks are topic that should not be ignored, but with which to be faced in order to increase the likelihood of survival and growth. Although they represent the uncertainty and the negative impact, this work presents a implementation methodology of risk management with FMEA method, and how to analyze and deal with them. The work aims to point out the existence of the need for proper risk management in the organization, and it describes the application of the implementation of FMEA method in general and the company XY.*

Key words: *risks, implementation, FMEA method, organization, ISO standard 31000:2009*

1. UVOD

Životi ljudi prepuni su rizika od trenutka rođenja kao i životni vijek organizacije od trenutka postojanja. Može se reći da je cjelokupno upravljanje organizacijom ili poduzećem vezano za mogućnost rizika. Iako oni predstavljaju neizvjesnost i negativan utjecaj ovim radom je prikazana metodologija implementacije upravljanja rizicima FMEA metodom, odnosno kako ih analizirati i suočiti se s njima. Kroz rad će se opisati općenito vanjsko i unutarnje okruženje organizacije, definirati rizici i upravljanje rizicima sukladno normi ISO 31000:2009, primijeniti norma ISO 31000:2009 za implementaciju sustava upravljanja rizicima, primijeniti FMEA metoda kao alat za procjenu i upravljanje rizicima te na kraju prikazati primjenu implementacije organizacije FMEA analize na poduzeću XY. Rad ima za cilj ukazivanje na postojanje potrebe za pravilnim upravljanjem rizicima u organizaciji.

2. ORGANIZACIJA U NESIGURNOM OKRUŽENJU

Procesi svake organizacije se odvijaju u uvjetima manje ili veće neizvjesnosti stanja o budućnosti što dovodi do posljedice da se ciljevi poslovnih procesa, a time i poslovne politike organizacije ostvaruju u nesigurnom okruženju. Ako poslovne politike imaju za cilj zahtjeve koje treba osigurati, onda je upravljanje sa sigurnošću okruženja u kojem se odvijaju svi poslovni procesi sa svojim podprocesima jedan od ključnih zahtjeva opstanka i unapređenja poslovanja[1]. Organizacija ovisi o unutarnjem i vanjskom okruženju, a da bi se procijenila okruženja u ovom slučaju biti će iskorištena SWOT analiza.

SWOT analiza (*engl. Strenghts, Weaknesses, Opportunities, Threats*) se sastoji od četiri čimbenika: snage, slabosti, prilike i prijetnje (slika 1.)

	Pozitivno	**Negativno**
Unutarnje okruženje	Snaga (S)	Slabosti (W)
Vanjsko okruženje	Prilike (O)	Prijetnje (T)

Slika 1. Shema SWOT analize [2]

Najvažniji vanjski i unutarnji čimbenici za budućnost organizacije nazivaju se strateškim čimbenicima, te se sumiraju u SWOT analizi. U konačnici bi SWOT analiza trebala identificirati prilike koje se trenutno ne mogu iskoristiti zbog nedostatka potrebnih resursa i jedinstvene kompetencije koje organizacija posjeduje. Vanjsko okruženje sastoji se od varijabli (prilika i prijetnji) koje su izvan poduzeća i obično nisu unutar kratkoročne kontrole menadžmenta.

2.1. Unutarnje okruženje - slabosti i snage

Unutarnje snage i slabosti uvelike se razlikuju za različite subjekte, a mogu se kategorizirati na menadžment i organizaciju, operacije, financije i ostale čimbenike. Kod kategorizacije unutarnjih čimbenika za

potrebe SWOT analize čini se opravdanim koristiti se najvažnijim unutarnjim čimbenicima organizacije: ciljevi i strategije, tehnologija i zadaci, veličina, kadrovi, životni ciklus poduzeća, proizvodi, lokacija.

Kod utvrđivanja snaga određuju se jake točke i izuzetno je bitno da ih organizacija identificira kako bi mogla da ih iskoristi što je moguće više, a pritom se mogu postaviti sljedeća pitanja:

- Postoje li jedinstvene razlikovne prednosti koje čine ovu organizaciju različitom od konkurencije?
- Zašto potrošači odabiru ovu organizaciju umjesto konkurenata?
- Postoje li proizvodi i usluge koje konkurencija ne može imitirati (sada i u budućnosti)?

Kod slabosti se određuju nedostaci sa stajališta organizacije i sa stajališta potrošača. Slabosti su ograničenja ili nedostatak resursa, vještina i znanja. Slabe strane nekad mogu utjecati na produktivnost, na proizvodnost ili nedostatak resursa, sposobnosti i mogućnosti. Najbolje ih je priznati bez suzdržavanja i pritom se mogu postaviti sljedeća pitanja:

- Postoje li operacije ili procedure koje mogu biti naglašenije?
- Što i kako konkurencija radi bolje?
- Postoji li neko izbjegavanje kojeg bi organizacija trebala biti svjesna?
- Je li konkurencija osvojila određeni tržišni segment [3]?

2.2. Vanjsko okruženje - prilike i prijetnje

U analizi vanjskog okruženja moraju se uzeti u obzir mnogi različiti čimbenici. Ti se čimbenici, koji mogu biti ili prijetnje ili prilike, mogu grupirati u sljedeće kategorije: ekonomski, društveni, političko-pravni, tehnološki, ekološki, etički i ostali. Ili se može koristiti neki drugi pristup analizi okruženja za koji se autori opredijele. Najvažniji dio vanjskog okruženja je industrijsko okruženje (kupci, dobavljači, konkurencija).

Važno je odrediti kako organizacija može nastaviti rast na tržištu. Prilike su svuda, kao što su promjene u tehnologiji, vladina politika, tržišni segmenti, itd. Neka od pitanja koja se mogu postaviti kod određivanja prilika su:

- Koje su atraktivne prilike na tržištu?
- Javljaju li se novi trendovi?
- Koje se nove prilike mogu predvidjeti u budućnosti?

Prijetnje su vanjski čimbenici izvan kratkoročne kontrole menadžmenta poduzeća. Organizacija mora biti spremna suočiti se s prijetnjama, čak i tijekom turbulentnih situacija. Većina prijetnji se može kontrolirati do neke granice. Cilj SWOT analize jest da identificira kritične točke u svakoj situaciji i organizira ih u pravac koji ce se uklopiti sa strategijom poduzeća.

Neka od pitanja koja se pritom mogu postaviti su:

- Koji potezi konkurencije potiskuju razvoj organizacije?
- Postoje li promjene u potražnji potrošača zbog kojih su potrebne nove karakteristike proizvoda i usluga?
- Štete li promjene (primjerice tehnologije) položaju organizacije na tržištu?

2.3. Uzroci nesigurnosti

U svakoj organizaciji postoje odstupanja od postignute funkcionalnosti i ostvarenih ciljeva bilo kojeg poslovnog sistema od planiranih i očekivanih koja mogu biti toliko velika da dovode do ugrožavanja njihove održivosti i u konačnici mogu dovesti do uništenja poslovnog sistema. Do tih odstupanja dolazi zbog nesigurnosti ili prijetnje koje postoje u organizaciji. Pojednostavljeni fizikalni princip pojave rizika prikazan je na slika 2., a značenje pojedinih veličina u tabela 1.

Slika 2. Blok shema pojednostavljenog fizikalnog principa pojave rizika [4]

Tabela 1. Značenje pojedinih veličina na slika 2. [4]

Prijetnja	- mogući uzrok neželjenog incidenta koji može uzrokovati štetu organizaciji.
Ranjivost	- slabost organizacije koju jedna ili više prijetnji mogu iskoristiti.
Posljedica	- rezultat ili učinak nekog događaja.
Sigurnosna mjera (Kontrola)	- sredstvo upravljanja rizikom, uključujući politike, procedure, smjernice, praksu ili organizacijske strukture, koje mogu biti administrativne, tehničke, upravne ili zakonodavne naravi.
Sigurnosni događaj (Incident)	- prepoznatljiv slučaj stanja sustava koji upućuje na moguću povredu sigurnosne politike ili neuspjeh zaštite ili do tada nepoznate okolnosti koje mogu biti važne za sigurnost.

3. RIZICI I UPRAVLJANJE RIZICIMA SUKLADNO NORMI ISO 31000:2009

Mnoge organizacije se susreću u svojem poslovanju s golemim rizicima različitog porijekla (vanjskog i unutarnjeg). Područje analize i upravljanja rizicima neraskidivo je vezano za strategiju organizacije koja je, kako je već spomenuto, u stalnoj interakciji i međusobnoj ovisnosti s vanjskim i unutarnjim okruženjem.

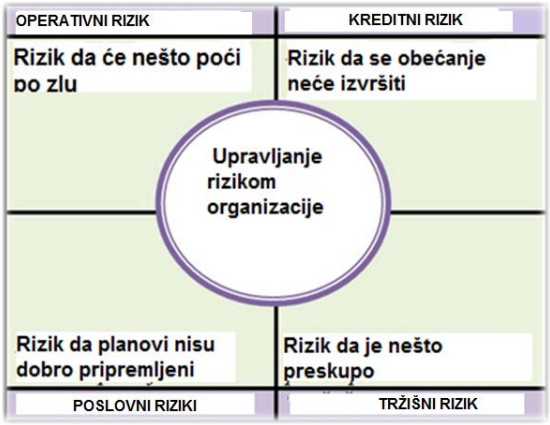
3.1. Definiranje i strukturiranje rizika

U literaturi se mogu pronaći različite definicije i objašnjena rizika. Robert L. Simons definira rizik kao: "Neočekivani događaj ili niz okolnosti koji u značajnoj mjeri reducira sposobnost menadžera da implementiraju svoju namjeravanu poslovnu strategiju" [5]. U knjizi Jonesa i Ashendena rizik je definiran kao funkcija razine prijetnje, ranjivosti i vrijednosti informacijske imovine [6]. Točnije rečeno rizik je vjerojatnost prijetnje da iskoristi neku ranjivost imovine te time ugrozi imovinu. Matematički, rizik možemo izraziti sljedećom formulom (1):

$$\text{Rizik} = \text{prijetnja} * \text{ranjivost} * \text{vrijednost imovine} \quad (1)$$

S aspekta poslovnih rizika, rizik se definira kao vjerojatnost nastupanja događaja koji će imati negativne učinke na vrijednost očekivanih zarada, novčanih tokova i vrijednosti organizacije, odnosno koji će ugroziti njezine poslovne ciljeve [7].

Da bi se mogli odrediti načini mjerenja te instrumenti i strategije upravljanja rizicima u organizaciji, potrebno je odrediti vrste rizika. U ovom radu biti će prikazana jedna vrsta kategorizacije rizika i to rizika koji se razlikuju prema događaju koji ih je uzrokovao. Tu se ubrajaju tržišni rizici, rizici likvidnosti, kreditni rizici, operativni rizici, te ostali. Na slika 3. prikazana je shema integralnog rizika organizacije s kratkim opisom gdje je usmjeren i kako nastaje neki od tih rizika.



Slika 3. Integracija rizika u organizaciji [8]

Tržišni rizici mogu nastati zbog nepovoljnog kretanja svojih faktora poput tržišnih kamatnih stopa, cijena dobara na robnim burzama te tržišne vrijednosti glavnice.

Rizici likvidnosti predstavljaju rizike da novčani primici organizacije neće biti dovoljni za pokrivanje novčanih izdataka, a to često rezultira u likvidaciji imovine organizacije manjim vrijednostima od realnih kako bi se nadomjestio manjak novčanih sredstava.

Kreditni rizici predstavljanju postojeće ili potencijalne nesposobnosti poslovnih partnera da podmire dospjele obveze ili izvrše dogovorenu poslovnu transakciju.

"Operativni rizik je rizik gubitaka koji nastaju zbog neadekvatnih procedura i neuspjelih internih procesa, ljudskog faktora, sistemskih ili eksternih događaja." Ova definicija operativnih rizika ugrađena je u Novi okvir kapitalne adekvatnosti - Bazelski sporazum [9].

3.2. Procjena rizika

Svaka organizacija treba identificirati izvore rizika, područja utjecaja, događaje (uključujući i promjenjive okolnosti) i njihove uzroke te moguće posljedica. Cilj ovog koraka je generirati sveobuhvatnu listu rizika, koji mogu stvarati, promijeniti, spriječiti, degradirati ili odgoditi postizanje cilja organizacije. Važno je identificirati rizike koji osporavaju neku priliku organizacije. Sveobuhvatna identifikacija je kritična, jer postoji mogućnost da se pojedini uzrok rizika ili rizik izostavi, te on neće biti uključen u daljnju analizu. Dakle, u ovoj fazi je potrebno utvrditi koji rizici mogu imati utjecaj na tok odnosno na ostvarenje planiranih aktivnosti. Nakon što je rizik identificiran procjenjuje se vjerojatnost njegove pojave, stupanj utjecaja na planirani raspored, opseg, troškove i kvalitetu aktivnosti, a zatim se određuju prioriteti.

Zahvaljujući analizi rizika dolazimo do rangiranja svih evidentiranih potencijalnih rizika do čega možemo doći koristeći [10]:

- kvalitativne analize koje se daju opisnu skalu za opisivanje vjerojatnosti i posljedica rizika,
- polu – kvantitativne analize koje određuje numeričke vrijednosti za opisivanje skale, brojevi su korišteni kako bi se kvantificirali faktori rizika,
- kvantitativne analize koje koriste numeričke skale za mogućnosti i posljedice rizika.

Svaki rizik koji je rangiran tijekom analize mora biti nadziran. Svi prepoznatljivi rizici bi trebali biti uneseni u registar rizika, koji sadrži sve informacije o riziku kao i tretmane koji su povezani s njima i dokumentirani kao rizici gubitaka.

Procjena rizika (*engl. Risk assessment*) je dio jednog većeg procesa kojeg nazivamo upravljanje rizikom (*engl. Risk management*). Procjena rizika je proces prepoznavanja, kvantificiranja i razvrstavanja rizika po prioritetima prema kriterijima za prihvaćanje rizika i ciljevima važnim za organizaciju. Procjena rizika sastoji se od dva potprocesa, a to su analiza rizika i vrednovanje rizika [11].

Postoje mnogi načini i metode koji se koriste za prepoznavanje opasnosti i procjenu rizika, a svaki od njih ima svoje prednosti i nedostatke. Kod izbora adekvatne metode treba uzeti u obzir određene podatke. Oni uključuju svrhu procjene, aktualno stanje u organizaciji, dostupne podatke ili financijske mogućnosti i osobnu sklonost ocjenitelja. Svaka metoda treba omogućiti jasan uvid u pojedine korake postupka procjene, kako korisnicima rezultata procjene tako i svim zaposlenicima koji mogu biti izloženi riziku.

3.3. Upravljanje rizicima

Minimiziranjem, praćenjem i kontrolom vjerojatnosti i utjecaja nepoželjnih događaja, nakon prepoznavanja, procjenjivanja i klasificiranja rizika po važnosti definira se upravljanje rizicima ili *risk management*.

Upravljanje rizicima kao najvažniji instrument anticipativnog upravljanja krizom, jedna je od najsloženijih poslovnih aktivnosti u kojoj se traži istraživanje i stručno prosuđivanje koje zahtijeva poznavanje metoda i načina adekvatnog izračunavanja različitih vrsta rizika uz praktično primjenjivanje na aktualne probleme.

Poduzeća su ranije upravljala rizicima na tradicionalan način [12]:

- upravljanje rizicima kada menadžment reagira nakon spoznaje i nastanka rizika,
- upravljanje rizicima je usmjereno prema unutra, u žarištu su rizici računovodstva i plaćanja – tradicionalna područja interne revizije; neučinkovito osoblje je primarni izvor poslovnih rizika,
- u žarištu upravljanja su financijsko-ekonomski rizici (kamatni, valutni i sl.) i time je njihovo praćenje zadatak određenog odjela,
- upravljanje rizicima se promatra fragmentarno, tj. svaka funkcija i svako područje analizira se odvojeno s obzirom na rizike,
- upravljanje rizicima nije bio sastavni dio aktivnosti vrhovnog menadžmenta poduzeća;
- menadžeri su imali averziju prema riziku,
- rizici su promatrani individualno, svaki za sebe.

Takvo upravljanje rizicima nije davalo zadovoljavajuće rezultate. Suvremen pristup upravljanja rizicima uključuje proaktivni pristup, rizik proučava kao priliku, a ne samo kao prijetnju te obilježava sljedeće:

- vrednovanje rizika je kontinuiran proces,
- u upravljanju rizicima sudjeluju svi,
- menadžment preuzima odgovornost za vrednovanje i upravljanje rizicima, te se definira plan upravljanja rizicima,
- neprekidno se promatraju i vrednuju stvarni izvori rizika, i to preventivno.

Sustav upravljanja rizicima (*engl. Enterprise risk management*, ERM) prema standardu za upravljanje rizicima proces je kojim organizacije metodički vode računa o rizicima povezanim s njihovim aktivnostima s ciljem postizanja kontinuiranog probitka, kako unutar svake pojedine aktivnosti, tako i u cjelokupnom portfelju aktivnosti. Upravljanje rizikom sve se češće prepoznaje kao sustav koji uključuje pozitivne (*engl. upside risk*) i negativne aspekte rizika (*engl. downside risk*) [13].

Sustav upravljanja rizicima u poduzeću sastoji se od sljedećih komponenti:

- proces upravljanja rizicima
- elementi organizacijske strukture
- instrumenti, metodologije i sustavi i
- znanje i vještine u upravljanju rizicima.

3.4. Norma ISO 31000:2009 za implementaciju sustava upravljanja rizicima

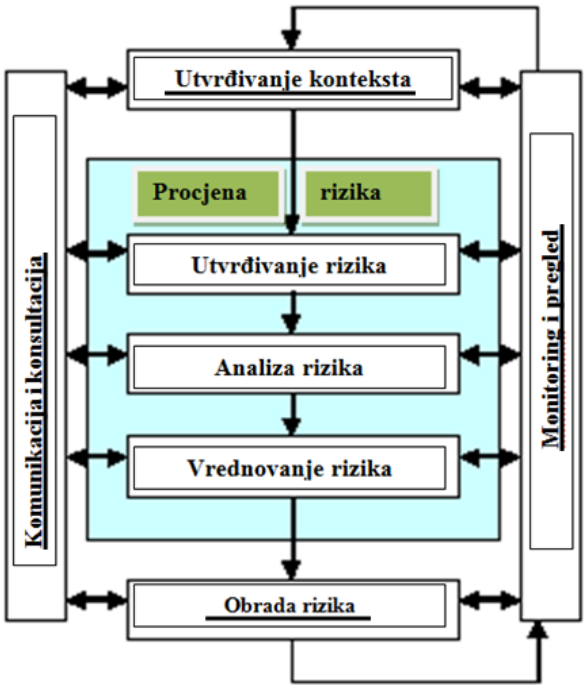
Generički pristup upravljanju rizicima koji promovira norma ISO 31000:2009 ne zavisi od područja primjene, a koncepcijski pruža kvalitetnu osnovu za analizu, procjenu te obradu rizika. U okviru te norme procjena rizika ne tretira se u metodološkom smislu, pa generički pristup omogućava da se proces upravljanja rizicima bez teškoća primjeni u bilo kojem području, bilo da se radi o procesima sigurnosti nekom drugom poslovnom procesu ili društvenim procesima. ISO 31000:2009 navodi da je upravljanje rizicima treba sadržavati sljedeće principe:

- učešće u stvaranju viška vrijednosti,
- sastavni dio ostalih poslovnih procesa,
- učešće u donošenja odluka,
- izričito adresira nesigurnosti,
- sustavnost, strukturiranost i pravovremenost,
- organizira i provodi na temelju najbolje dostupne informacije,
- prilagođen potrebama organizacije i djelatnosti gdje se koristi,
- uzimanje ljudskih i kulturnih elemenata u obzir,
- transparentnost i inkluzivnost,
- dinamičnost, iterativnost i odgovore na promjene,
- omogućavanje stalnog unapređenja i poboljšanja organizacije.

Norma ISO 31000:2009 Upravljanje rizicima – Principi i smjernice, detaljno opisuje sistematičan i logičan proces upravljanja rizicima.

Norma ustanovljava brojne principe koje treba primijeniti kako bi upravljanje rizikom bilo učinkovito. ISO 31000:2009 preporuča da organizacije razviju, primjene i kontinuirano poboljšavaju okvir rada čija je svrha integrirati proces upravljanja rizikom u sveopćem upravljanju organizacije, njezinoj strategiji i planiranju, menadžmentu, procesima izvješćivanja, politici, vrijednostima i kulturi.

Blok shema procesa za upravljanje rizicima kako se predlaže u normi ISO 31000:2009 prikazana je na slika 4., a osnovni opisi elemenata prikazanih na slika 4., nalaze se u tabela 2.



Slika 4. Proces upravljanja rizicima prema ISO 31 000 [14]

Tabela 2. Osnovni opisi elemenata prikazanih na slici 4. [14]

Komunikacija i konzultacija	- s internim i eksternim ulagačima - zainteresiranim stranama, kako je primjereno (tehnološki), na svakom stupnju procesa upravljanja rizikom i razmatranje procesa kao cjeline.
Utvrđivanje konteksta	- utvrđivanje eksternog, internog i konteksta upravljanja rizikom u kojem će se odvijati ostatak procesa, - utvrditi kriterije prema kojima će se procjenjivati rizik i definirati struktura analize.
Identifikacija rizika	- gdje, kada, zašto i kako bi događaji mogli spriječiti, umanjiti, odložiti ili povećati postizanje ciljeva.
Analiza rizika	- ova analiza treba razmotriti područje potencijalnih posljedica i kako bi se one mogle pojaviti.
Procjena rizika	- usporedba procijenjenih razina rizika s prethodno utvrđenim kriterijima i razmatranje ravnoteže između potencijalnih koristi i nepovoljnih rezultata, - omogućuje donošenje odluka o opsegu i prirodi potrebnih obrada i o prioritetima.
Obrada rizika	- izrada i primjena specifičnih troškovno učinkovitih strategija i akcijskih planova za povećanje potencijalnih koristi i smanjenje potencijalnih troškova.
Praćenje i preispitivanje	- neophodno je pratiti učinkovitost svih koraka procesa upravljanja rizikom, - važno je za neprekidno poboljšavanje, - potrebno je pratiti rizike i učinkovitost mjera obrade kako bi se osiguralo da promjena uvjeta ne mijenja prioritete.

4. FMEA METODA - ALAT ZA PROCJENU I UPRAVLJANJE RIZICIMA

Analiza utjecaja i posljedica pogrešaka (*engl. Failure Mode and Effect Analysis*) sustavna je metoda kojom se identificiraju i sprečavaju problemi na proizvodu ili procesu prije njihova nastanka. FMEA metoda fokusirana je na prevenciju pogrešaka i smanjivanje mogućnosti da se pogreška dogodi te povećanje zadovoljstva korisnika [15]. Za popularnost ove metode najviše je zaslužna njezina jednostavnost i mogućnost prilagodbe svim područjima promatranja nekog problema te činjenica da su potrebu primjene analize utjecaja i posljedica pogrešaka prepoznale i strukturne međunarodne organizacije koje predlažu i usvajaju standarde kvalitete. Prilagodba FMEA metode rješavanju različite problematike očituje se prije svega u mogućnosti kreiranja tablica za procjenu važnosti, vjerojatnosti pojavljivanja i vjerojatnosti otkrivanja, gdje se i opisno mogu karakterizirati intervali rizičnosti pojedine potencijalne pogreške i pripadajućih posljedica.

Učinkovitost FMEA se očituje u identificiranju korektivnih mjera potrebnih kako bi se spriječilo da dođe do propusta, a kako bi se osiguralo što više profita, kvalitete i pouzdanosti.

4.1. Definiranje i povijest FMEA metode

Po definiciji, FMEA je sustavna metoda potencijalnog propusta u načinu rada koja ima za cilj spriječiti i korigirati te propuste. Kako bi se ovo moglo ostvariti, FMEA metodu je potrebno početi primjenjivati što je prije moguće, bez obzira što u danom trenutku svi podaci ili informacije nisu u potpunosti poznati. Stoga je i moto FMEA metode: "učini najbolje što možeš, s onim što sada imaš" [16]. U idealnom slučaju, FMEA se provodi u dizajnu proizvoda ili procesu razvojnog stadija te na bilo koji željeni nivo detaljnosti - sustav, podsustav, sklop ili komponentu.

FMEA se koristi već više od četrdesetak godina. Počeci razvijanja i primjenjivanja vezani su najprije za NASA-in svemirski program. Ubrzo metoda postaje formalizirana i bolje definirana te se primjena širi kroz vojnu i avionsku industriju. Osamdesetih godina FMEA postaje alat za Total Quality Management a devedesetih Six Sigma alat. Industrija motornih vozila (AIAG - *Automotive Industry Action Group*) i američko društvo za kontrolu kvalitete (ASQC - *American Society for Quality Control)* u veljači 1993. godine su zaštitili autorska prava na FMEA standarde koji su bili široko rasprostranjeni u industriji [17].

FMEA je postala dio zahtjeva za dobivanje certifikata ISO QS 9000, a također je razmatrana i unutar ISO serije standarda ISO 9001 i ISO 14 000. Kratkoročno, FMEA daje popis potencijalnih otkaza i identificira ozbiljnost njihovih efekata i određuje prioritet akcija korekcije. Dugoročno, FMEA razvija kriterij za planiranje testiranja sustava, osigurava dokumentaciju za buduće analize pouzdanosti u slučaju izmjene dizajna sustava, osigurava osnovu za planiranje održavanja, osigurava osnovu za kvalitativnu i kvantitativnu analizu pouzdanosti sustava.

Postoje nekoliko vrsta analiza utjecaja i posljedica pogrešaka :

- FMEA sustava
- FMEA dizajna
- FMEA procesa
- FMEA usluge
- FMEA softvera

4.2. Primjena FMEA metode

Kod primjene razlikujemo FMEA za projektiranje i za proizvodni proces. Postupak je gotovo identičan, ali su razlike u ciljevima i mogućnostima korištenja rezultata FMEA. Kod projektiranja naglasak je na identificiranje potencijalno problematičnih područja koja mogu zahtijevati detaljnije razmatranje glede projekta, analize ili testiranja. Postupak može otkriti i doprinijeti projektiranju nalazima koje je inače moguće propustiti.

FMEA je moguće vrlo uspješno primjenjivati za više različitih svrha. Glavne primjene su:

- Kreiranje tablica za jednostavnije pronalaženje kvarova.
- Primjena zahtjeva za preventivno održavanje, vjerojatnost i kritičnost nekog kvara određuju potrebu za preventivnim ili korektivnim pristupom održavanju.
- Dodatna pomoć kod ugrađenih testiranja, indikacija kvarova i redundantnosti.
- Za analizu korištenje automatskih ili manualnih rješenja.
- Kod kreiranja, održavanja i spremanja dokumentacije o analizi pouzdanosti i sigurnosti postrojenja.

- Optimiranje proizvodnog procesa, te ispitivanje potencijala za pojavljivanje problema kod proizvodnje.

4.3. Faze uvođenja FMEA metode

Uvođenje FMEA metode u organizaciji se odvija kroz nekoliko faza, u ovom slučaju su to dizajn FMEA i postupke FMEA. Dizajn FMEA metode se priprema prije nego sustav počne djelovati u poduzeću. Osiguran je kroz djelovanje tima koji je odgovoran za razvoj proizvoda te koji surađuje s uredom za osiguranje kvalitete, planiranje proizvodnje, tehnološkim i proizvodnim odjelima i po potrebi s potrošačima. Kod dizajna se u obzir uzimaju postojeći podaci o kvaliteti i probni rezultati sličnih elemenata. Tokom dizajniranja FMEA primjenjuju se sljedeći koraci:

- pripremiti listu karakteristika elemenata ili sustava koja sadrži dijelove sustava i njihove moguće defekte,
- prikazati i opisati sve moguće zasebne defekte na funkcijama sustava te navesti detalje oko mogućnosti otkrivanja defekata.

Dizajnom FMEA se osigurava baza za provedbu postupka FMEA metode. Bez obzira na mjesto utvrđivanja nepravilnosti funkcioniranja procesa kao rezultata specifične greške, FMEA postupci određuju tu nepravilnu funkciju kao moguću grešku te ju analiziraju. Postupci FMEA pripremaju se u odjelu za planiranje proizvodnje, uredu za osiguranje kvalitete ili proizvodnom odjelu sa sudjelovanjem specijalista iz određenog područja i po potrebi u suradnji s potrošačem.

4.4. Priprema dizajna FMEA metode

S ciljem osiguranja usklađenosti rada s FMEA u dizajnu i procesu organizacije preporuča se korištenje jednoobraznih i standardnih obrazaca. U daljnjem tekstu su opisani podaci potrebni za kreiranje obrasca FMEA te aktivnosti koje se provode u sklopu analize grešaka i efekata u nekom procesu, a to su:

- osnovni podaci
- naziv/karakteristike sustava
- potencijalne greške
- potencijalne posljedice pogreške
- potencijalni uzroci greški
- planirana ispitivanja
- vjerojatnost događaja
- utjecaj na kupca
- RPR - razina potencijalnog rizika
- preporučene preventivne mjere
- odgovornost
- usvojene mjere
- ponovna procjena
- novi finalni RPR .

5. IMPLEMENTACIJA SUSTAVA UPRAVLJANJA RIZICIMA U ORGANIZACIJI PRIMJENOM FMEA METODE

Primjena FMEA metode u upravljanju rizicima u organizaciji posebice se odnosi na fazu definiranja i predviđanja svih mogućih rizika te izračuna RPR faktora razine potencijalnih rizika. Za efikasnu procjenu rizika i provođenje mjera njihovog smanjivanja treba provesti FMEA u timu čiji članovi imaju osnovna znanja iz područja generiranja ideja. Kod korištenja FMEA metode treba rangirati određene pokazatelje, a to su pokazatelj procjene značenja odstupanja (P), vjerojatnosti nastanka odstupanja (V) te vjerojatnosti otkrivanja odstupanja, tzv. detekcija (D). Tabela rangova kao prilog izvještaju FMEA metode prikazana je u tabela 3.

Tabela 3. Tabela rangova [18]

P rang	Zapažanje korisnika	Značenje odstupanja za korisnika je:		
1	Vjerojatno neće primijetiti odstupanje	neznatno		
od 9-10	Ugrožena je sigurnost korisnika, proizvod je neupotrebljiv	vrlo veliko		
V rang	Intenzitet odstupanja	Rasipanje	Cpk	Vjerojatnost nastanka odstupanja je
1	1< 1*10^6	< > -5s	≥1,67	Gotovo nikakva
10	1 u 2			Vrlo velika
D rang	Vjerojatnost otkrivanja odstupanja pomoću SPC je			Vjerojatnost otkrivanja odstupanja je
1	Gotovo sigurna			Vrlo velika
10	Odstupanje neće biti otkriveno			Nikakva

Bez obzira o kakvim se rizicima radi, FMEA metoda može pouzdano procijeniti mogućnost njihove realizacije kroz izračun RPR faktora, čije su prihvatljive vrijednosti unaprijed zadane.. Računanje pokazatelja veličine rizika prikazano je u tabela 4. Kao prilog izvještaju FMEA analize prilaže se i tabela za FMEA analizu prikazana u tabela 5.

Tabela 4. Računanje pokazatelja veličine rizika [19]

RPR	Komentar rizika	Rizik
< 50	V neznatna, D velika, odstupanje se otkriva na mjestu nastanka	Neznatan
>50 <100	V neznatna, P mala, D mala, odstupanje može doći do korisnika, V umjerena, P mala, D velika	Značajan
>100	V velika, P velik, D mala	Velik
1000	Kritično, odstupanje može imati posljedice za korisnika	Vrlo velik

Tabela 5. Tabela za FMEA analizu [20]

Područje	Zahtjev	Odstupanje	Posljedica	Uzrok	Značenje greške (P)	Vjerojatnost nastanka (V)	Detekcija(D)	Veličina rizika (RPR)	Preventivne/ popravne radnje
1	2	3	4	5	6	7	8	9	10
					od 1-10	od 1-10	od 1-10	1000	
	RPR <50 neznatan RPR >50<100 značajan				RPR >100 velik RPR =1000 vrlo velik				

Nakon provođenja FMEA metode vrše se preventivne ili popravne radnje.

6. PRIMJENA IMPLEMENTACIJE SUSTAVA UPRAVLJANJA RIZICIMA U ORGANIZACIJI **PRIMJENOM FMEA METODE U PODUZEĆU XY**

Prije prikaza implementacije u poduzeću XY u ovom radu biti će prikazan postupak upravljanja nabave i skladištenja robe i materijala u tom poduzeću, a koji se primjenjuje sukladno zahtjevima norme HRN EN ISO 9001:2009.

Postupak upravljanja nabavom i skladištenjem primjenjuje se u odjelu nabave i skladišta, a odgovornost snosi Voditelj nabave i skladištenjem.

6.1. Postupak upravljanja nabavom i **skladištenjem robe i materijala u poduzeću** XY primjenom norme ISO 9001:2009

Postupak upravljanja nabavom i skladištenjem robe i materijala se sastoji od:

- inventure
- plana zaliha
- nabave robe
- zaprimanja
- izdavanja robe
- kupovanja robe na terenu
- povrata robe u skladište
- povrata robe dobavljaču
- obračuna troškova
- skladište gotovih proizvoda.

6.2. Opis FMEA postupka

Kao što je već i spomenuto u radu, FMEA metoda je sustavna metodologija za relativno međusobno rangiranje rizika, a pomaže organizaciji da se fokusira i razumije utjecaj potencijalnih rizika. Rizik se računa za svaku vrstu opasnosti i njegove posljedice.

Razina potencijalnog rizika (RPR) funkcija je koja se sastoji od triju čimbenika: posljedice (P), vjerojatnosti pojavljivanja uzroka (V) i mogućnosti detekcije uzroka (D).

FMEA metoda se koristi kao temelj za Planove kontrole, a oni su broj prevencije grešaka i reakcijskih detekcijskih tehnika. U oba tipa FMEA provodi se deset koraka prikazanih u tabela 6.

Tabela 6. 10 koraka FMEA postupka

1.	Pregled procesa
2.	Oluja mozgova o potencijalnim vrstama opasnosti
3.	Popis potencijalnih posljedica opasnosti
4.	Pridruživanje razina vjerojatnosti
5.	Pridruživanje razina posljedici
6.	Pridruživanje razina detekcije
7.	Računanje rizika
8.	Izrada akcijskog plana
9.	Provedba akcija
10.	Računanje novih rizika

Za provedbu FMEA metode treba biti zadužen tim, a ne pojedinac. Ono što je potrebno izbalansiranom timu za uspješnu provedbu FMEA su vještine i iskustvo. Rezultat postupka FMEA je procjena razine rizika (RPR) za svaku potencijalnu opasnost. Redoslijed poduzimanja mjera slijedi RPR od najveće vrijednosti prema manjoj.

6.3. Primjena FMEA u postupku skladištenja robe i materijala u poduzeću XY

Postupak FMEA metode u skladištenju robe i materijala se započinje tako da se odrede izvori opasnosti, uzroci te njihove posljedice. Kod skladištenja robe neki od mogućih izvora opasnosti su :

- temperatura,
- vlaga,
- poplava,
- mehanička oštećenja,
- krađa, itd.

Kod postupka FMEA bitne su sljedeće napomene:

- Napomena 1: U svakom se koraku može dogoditi više grešaka i svaka greška može imati više uzroka i posljedica.
- Napomena 2: Razina potencijalnog rizika se računa formulom (3):
  $$RPR = P * V * D \quad (3)$$
  a računa se prije i poslije provedenog Plana aktivnosti.
- Napomena 3: FMEA se mora koristiti i za izradu Plana aktivnosti.
- Napomena 4: Politikom upravljanja rizicima definiraju se mjerne skale koje se ne smiju mijenjati, odnosno definiraju se ponderi za određene parametre. Politikom upravljanja rizicima definiraju se boje semafora (zelena, žuta, crvena).
- Napomena 5: Izvori koji u sustav unose rizik su obično: čovjek, stroj (mjerilo i pribor), metoda, mjerenje, materijal, okoliš i organizacija.

Najprije se definiraju ponderi za parametre, odnosno pondere za vjerojatnost, detekciju te posljedicu. U ovom slučaju su to:

- Vjerojatnost nastanka uzroka posljedice:
  5 – jednom u godini
  3 – jednom od jedne do pet godina
  1 - jednom u pet godina

- Detekcija opasnosti ili uzroka:
  5 – nemoguća detekcija
  3 - moguća detekcija
  1 - sigurna detekcija
- Posljedica realizacije opasnosti:
  5 – trošak otklanjanja posljedice veći od 50 000 kn
  3 – trošak otklanjanja posljedice od 5 000 do 50 000 kn
  1 - trošak otklanjanja posljedice do 5 000 kn

Nakon određivanja pondera za parametre, vjerojatnosti, posljedice i detekcije, kreće se na provedbu FMEA. Provedba FMEA postupka je prikazana u tabela 7., iz koje je izdvojen i napravljen semafor koji prikazuje rezultat FMEA postupka a tumači se politiko upravljanja rizicima prikazan na slika 5.

Tabela 7. FMEA skladištenja robe i materijala u skladištu

Analiza rizika – FMEA skladištenja robe i materijala						
Izvor	**Uzorak**	**Posljedica**	**P**	**V**	**D**	**RPR**
Temperatura	Loša izolacija	Nemogućnost neadekvatne regulacije temperature	3	1	5	15
	Previsoke/ preniske temperature u skladištu	Pokvarljivost robe	3	5	3	45
Vlaga	Neprikladna ambalaža	Kalo robe ili materijala	1	5	3	15
	Prodiranje vode izvana	Oštećenje	5	3	5	75
	Neadekvatno skladištenje	Smanjuje se ili čak gubi uporabna vrijednost	5	3	3	45
Poplava	Prirodna nepogoda	Oštećenje ili uništenje robe i materijala	5	5	3	75
Krađa	Od strane radnika	Nestanak/ manjak robe ili materijala	3	5	3	45
	Provala	Manjak robe ili materijala	3	5	5	75
Mehanička oštećenja	Neadekvatno rukovođenje kod skladištenja	Roba ili materijal više nisu iskoristivi	3	5	3	45
	Oštećenje kod transporta	Povrat robe ili materijala	3	5	3	45

RPR	1	3	5	15	45	75	125

Slika 5. Prikaz semafora koji se definira politikom upravljanja rizicima

7. ZAKLJUČNE NAPOMENE

Svaka organizacija se nalazi pod utjecajem vanjskog i unutarnjeg okruženja, što joj može donijeti različiti prilike, ali i prijetnje. a to su uglavnom rizici s kojima se organizacije svakodnevno susreću.

Norma ISO 31 000:2009 preporuča da organizacije razviju, primjene i kontinuirano poboljšavaju okvir rada čija je svrha integrirati proces upravljanja rizikom u sveopće upravljanje organizacijom, a upravljanje rizikom prema zahtjevima ove norme može se primijeniti na cjelokupnu organizaciju.

FMEA metoda odgovara na dva osnovna pitanja: koje se sve potencijalne pogreške mogu pojaviti te koja je vjerojatnost njihova pojavljivanja i važnost posljedica koje sa sobom nosi njihova realizacija. Korištenje FMEA metode daje veće povjerenje u donošenje ispravnih odluka na temelju činjenica razvijanje timskog rada i razmjene znanja, aktivnosti dokumentirane u Izvještaju o FMEA postupku, koji se provodi u posebnom FMEA obrascu. Ukoliko se želi smanjiti mogućnost nastanka pogreške, potrebno je u potpunosti ili djelomično eliminirati uzrok njezina nastanka, jer pogreška koja je kasnije prepoznata, donosi veće posljedice, a time i veće troškove za organizaciju.

8. LITERATURA

[1] http://www.kvalis.com/component/k2/itemlist/tag/ISO9001
[2] http://hr.wikipedia.org/wiki/SWOT_analiza
[3] http://www.besplatniseminarskiradovi.com/PROIZVODNI%20I%20USLUZNI%20MENADZMENT/PrimenaSwotAnalize-.htm
[4] http://www.kvalis.com/component/k2/itemlist/tag/rizik
[5] Gilad, B.: Rano upozoravanje, HESPERIJAedu, Beograd, 2009.
[6] Jones, A., Ashenden, D.,: Risk Management for Computer Security, ELSEVIER,Amsterdam, 2005.
[7] Sprčić, D. M.: Upravljanje rizicima, Sinergija, Zagreb, 2013.
[8] http://www.kvalis.com/component/k2/item/688-operativni-rizici-kao-temelj-sustava-upravljanja
[9] Basel II, International Convergence of Capital Measurement and Capital Standards, Bank for International Settlements, 2004.
[10] Cooper, D.; Grey, S.; Raymong, G.; Walker, P.: Project risk management guidelines: managing riks in large projects and complex procurements, John Wiley & Sons Ltd., West Sussex, 2005.
[11] http://security.foi.hr/wiki/index.php/Procjena_rizika
[12] http://www.amazon.com/Corporate-Risk-Management-Value-Creation/dp/1904339832
[13] Jakaša, T.; Osmanagić Bedenik, N.; Iliopoulos, F.: Određivanje učinkovitosti sustava, Energija, god.57(2008), br.2,str.156-177
[14] http://www.kvalis.com/component/k2/item/165-iso-31000-upravljanje-rizicima
[15] McDermont, R.E.; Mikulak, R.J.; Beauregard, M.R.: The basic of FMEA, Productivity INC., New York, USA, 1996.
[16] http://issuu.com/kvaliteta.net/docs/pi_v2_no2
[17] http://www.laboi.fon.rs/data/OI/FMEA.pdf
[18] http://www.hgk.hr/wpcontent/files_mf/FMEA%20analiza%20kao%20mo%C4%87an%20alat%20u%20svijetu%20rizika%20%20%20prezentacija35.pdf

[19] http://www.hgk.hr/wpcontent/files_mf/FMEA%20analiza%20kao%20mo%C4%87an%20alat%20u%20svijetu%20rizika%20%20%20prezentacija35.pdf
[20] http://www.hgk.hr/wpcontent/files_mf/FMEA%20analiza%20kao%20mo%C4%87an%20alat%20u%20svijetu%20rizika%20%20%20prezentacija35.pdf

Kontakt autora:

Dr.sc. Krešmir Buntak, docent
Veleučilište u Varaždinu
J.Križanića 33, 42000 Varaždin
kresimir.buntak@inet.hr

Ivana Drožđek, univ.spec.oec.
Veleučilište u Varaždinu
J.Križanića 33, 42000 Varaždin
ivana.drozdek@velv.hr

Marijana Košćak, bacc.ing.log
marijanakoscak@hotmail.com