Zavod za informatičku djelatnost Hrvatske d.o.o.

UPRAVLJANJE RIZICIMA U POSLOVNOM SUSTAVU

Prof.dr.sc. Zdravko Krakar
Dr.sc. Silvana Tomić Rotim

1. MOTIVACIJA

1.1. Rizici kao nezaobilazni čimbenik svakog poslovanja

Rizici su nezaobilazni dio ljudskih aktivnosti i svakog posla. Uvijek su povezani s neizvjesnošću, što vrijedi za naš svakodnevni život, ali i svaki poslovni sustav. Oni su funkcija imovine, prijetnje, ranjivosti i mogućih posljedica. *Imovina* je sve što poslovni sustav posjeduje i što za njega ima neku poslovnu vrijednost. To može biti materijalna imovina, financijska imovina, informacije, procesi, ugled itd. *Prijetnje* su mogućnosti da dođe do ugrožavanja imovine, a njihovi izvori mogu biti unutarnji i vanjski. *Ranjivosti* su slabost uslijed nedostatka ili niske razine zaštitnih mjera imovine.

Rizici postoje u svakom poslovnom sustavu. Pojavljuju se od misije, vizije, određivanja i realizacije ciljeva poslovnih ciljeva, preko poslovnih procesa, do ostvarenja ili neostvarenja ovih odrednica. Uvijek postoji niz prijetnji sa svojim izvorima, koje mogu izazvati negativne događaje, a ovi rezultirati određenim, neželjenim posljedicama. Da se one ne dese, nužno je poduzimati adekvatne mjere postupanja s rizicima. Dakle, svrha upravljanja rizicima je povećati vjerojatnost da će se u slučaju pojave prijetnji, otkloniti ili umanjiti nepovoljne situacije. Rizici se ne mogu otkloniti u potpunosti i važno ih je svesti na prihvatljivu razinu.

Postoji više načina kategorizacije rizika, njihova najčešća podjela u nekom poslovnom sustavu, prikazana je na slici 1.

Slika .1. Vrste rizika u poslovnom sustavu

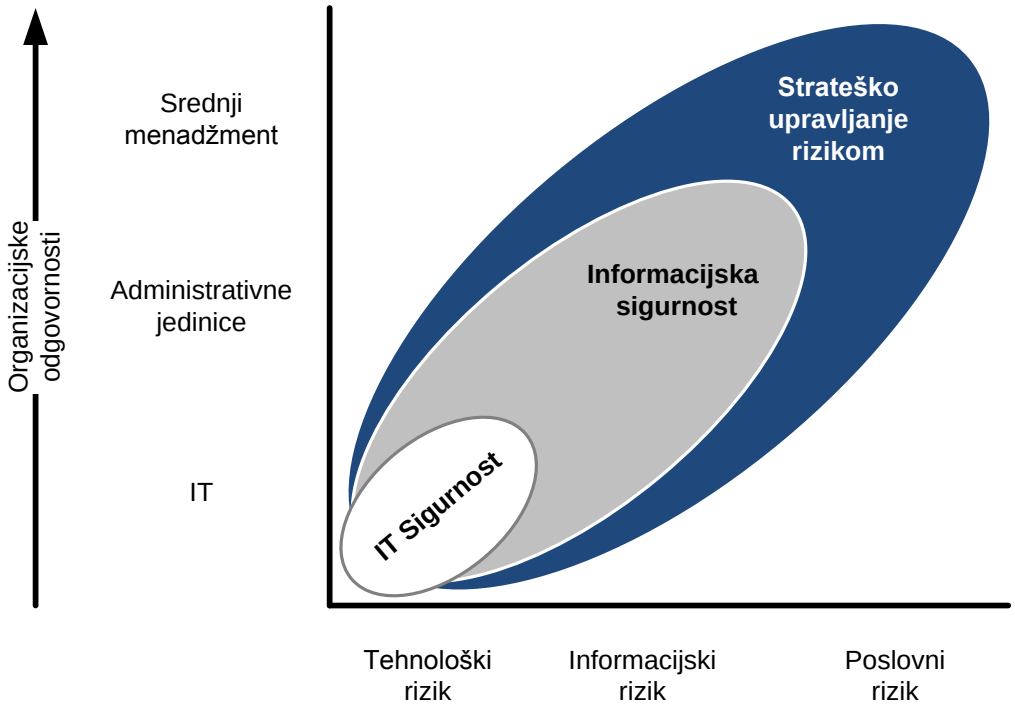
Može se uočiti da prema ovom pristupu postoje strateški rizici, rizici okoline, rizici tržišta, kreditni rizici, operativni rizici, rizici (ne)sukladnosti i rizici vezani za IT. Ukoliko neki poslovni sustav nema dobro strateško planiranje ili ga uopće ne provodi, nije definirao svoju viziju i misiju, nema svoje jasne ciljeve, evidentno je da se radi o strateškim rizicima. Ako ne percipira stalne promjene u svojoj okolini koje se dešavaju zbog razvoja tehnologije, uvjeta poslovanja, rastućih ekoloških zahtjeva, promjena kod konkurencije, to su rizici okoline. Ukoliko poslovni sustav ne prati dovoljno dobro neprestane promjene na tržištu, ne prilagođava mu svoje proizvode i usluge, loše je odredio svoje niše, ima lošu politiku cijena ili je loše odabrao svoje kupce, radi se o tržišnim rizicima. U slučaju da se koriste nepovoljni krediti, očito da je na sceni kreditni rizik. Ako neko svoje poslovanje nije prilagodio aktualnim zakonima, propisima ili normama, već ih netransparentno koristi ili čak krši, postoje rizici zbog nesukladnosti. Rizici se pojavljuju u vođenju projekata, kadrovskoj politici, vrlo su intenzivni i u području IT-a itd.

1.2. IT kao izvor poslovnih rizika

IT rizici sastavni su dio svake od kategorija poslovnih rizika. Niti jedna poslovna odluka ne može se donijeti bez odgovarajućih informacija. Izvori ovih informacija u poslovnom sustavu su njegov informacijski sustav s pripadajućim bazama strukturiranih podataka, ali i obilje informacijskih izvora u kojima one najčešće nisu strukturirane. I internet je danas nezaobilazno vrelo najraznovrsnijih informacija. Budući su informacijski sustavi temeljeni na IT potpori, a ona se koristi za dobivanje i drugih izvora informacija, područje IT-a je potencijalno veliki rizik za poslovni sustav. Neki primjeri ovih rizika su: rizici nedovoljno dobro povezanog poslovanja i IT potpore, rizici nepostojanja strateškog plana IT-a, rizici loše provedenih IT investicija, rizici prekida IT potpore poslovnim procesima, rizici nedovoljne kvalitete IT potpore, rizici u vođenju informatičkih projekata, rizici niske razine usluga koje IT pruža itd.

Dakle, IT rizici su uzrokovani opasnostima i prijetnjama uslijed neadekvatnog odlučivanja o ovom području, nepoduzimanja potrebnih mjera ili svega onog što

može dovesti do neželjenih ili neočekivanih posljedica i financijskih i drugih šteta unutar organizacije i njezinog neposrednog i šireg okruženja. Šteta može biti materijalna i financijska, izravna ili neizravna, a svaku od njih mora se u procjeni rizika uzeti u obzir. Položaj IT rizika u ukupnom upravljanju rizicima poslovnog sustava prikazan je na slici 2.



Slika 2. Položaj IT rizika u ukupnom upravljanju rizicima poslovnog sustava

Istraživanja relevantnih svjetskih institucija i organizacija (World Bank, Gartner, Forrester, SEI – Software Engineering Institute Pitsbourgh, Disaster Recovery Institute, IBM-a itd.) pokazuju da je područje IT-a visoki poslovni rizik. Neki pokazatelji IT rizika iz prakse navode se u nastavku:

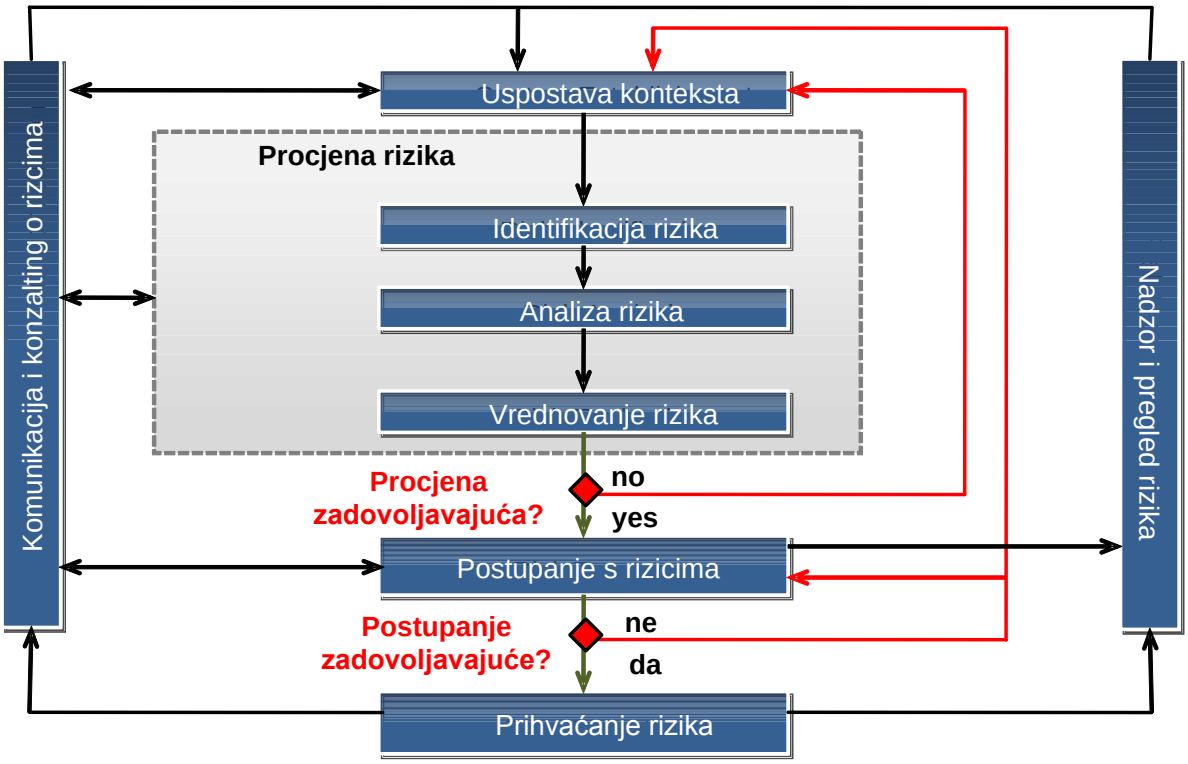
- Vjerojatnost da će neki IT projekt ostvariti poslovnu vrijednost nije veća od 15 % (Standish Report). IBM istraživanje pokazuje da je to max 30 % (IBM Fortune 1000 survay).
- Godišnje se samo u SAD na neuspješne IT projekte nepotrebno utroši preko 600 mld $ (Gartner).
- Vjerojatnost da će neki IT projekt završiti u planiranom terminu je samo 20 %, da ne će probiti planirani budžet, manja je od 18 % (Project Management Institute).
- Godišnji troškovi održavanja aplikacija u poslovnim sustavima (ljudi + licence) kreću se od 70 – 90 % IT budžeta zbog nedovoljno izgrađene strategije upravljanja aplikacijama (Forrester, Gartner, Cambridge University).
- U novoj programskoj opremi u trenutku isporuke ima još oko 60 pogrešaka / 1.000 linija koda, što uzrokuje visoke troškove njenog održavanja.

- Više od 80 % poslovnih sustava uopće ne optimizira svoje IT troškove.
- Preko 75 % poslovnih sustava nema razrađene postupke za slučajeve većeg prekida IT potpore (Business Continuity Institute i dr.).
- Cjelovite sustave informacijske sigurnosti nema niti 15 % poslovnih sustava.
- Preko 80 % poslovnih sustava ima zastarjele interne organizacije svojih IT funkcija (Info Tech Research Group)
- Itd.

2. KAKO UPRAVLJATI RIZICIMA?

Upravljanje rizicima osnova je svakog upravljanja poslovnim sustavima. Svodi se na pronalaženje razumnog odnosa između različitih aspekata opasnosti, mogućih posljedica i mjera kojima se rizici svode na razumnu razinu. U nekom poslovnom sustavu nije moguće identificirati i otkloniti sve rizike, već je nužno neprihvatljive rizike svesti na prihvatljivu razinu. Kako to učiniti?

Postoji više načina upravljanja rizicima. Opće prihvaćena norma za ovo područje je ISO/IEC 31000. Njene faze su prikazane na slici 3.



Slika 3. Proces upravljanja rizicima prema normi ISO/IEC 31000

Postavljanje konteksta

Na početku procesa upravljanja rizicima nužno je postaviti kontekst u kojem organizacija posluje. To znači da je potrebno jasno iskazati njene ciljeve, definirati vanjske i unutarnje parametre o kojima treba voditi računa u upravljanju rizicima te postaviti opseg i kriterije za procjenu rizika.

U prepoznavanju vanjskih parametara može se koristiti poznata PESTLE[1] analiza, koja u razmatranje uzima političke, ekonomske, sociološke, tehnološke, pravne te čimbenike okoliša te njihov utjecaj na ciljeve organizacije. Također, treba uzeti u obzir odnos i potrebe vanjskih dionika organizacije.
Za definiranje unutarnjih parametara od značaja za poslovni sustav, može se provesti SWOT[2] analiza te na taj način odrediti njene slabije dijelove. Pri tome se analiziraju IT resursi, ljudski resursi, organizacijska kultura, politike, prihvaćeni standardi, ciljevi, potrebe unutarnjih dionika itd. Također, na taj način prepoznaju se i sve prilike koje organizacija može postaviti kao svoje ciljeve i ostvariti ih u budućem razdoblju.

Identifikacija rizika

Identifikacija rizika provodi se prepoznavanjem svih mogućih rizika i njihovih izvora. Cilj ove faze je doći do liste onih događaja koji bi u negativnom smislu mogli utjecati na ostvarivanje poslovnih ciljeva. Važno je identificirati sve potencijalne rizike, jer oni koji se ne prepoznaju u ovoj fazi, biti će u narednim koracima isključeni iz daljnjeg postupka upravljanja rizicima.
Poslovni sustav može primijeniti razne alate i tehnike prilagođene svojim ciljevima i uvjetima te koristiti ranije iskustvo o rizicima koji su se već desili. Za identifikaciju rizika od presudne je važnosti da su prikupljene informacije relevantne i ažurne. U ovaj postupak potrebno je uključiti ljude s adekvatnim poznavanjem područja za koje se on provodi.

Analiza rizika

Analiza rizika uključuje razumijevanje identificiranih rizika. Razmatraju se uzroci i izvori rizika, njihove pozitivne i negativne posljedica te vjerojatnosti pojave. Također, potrebno je identificirati i čimbenike koji utječu na posljedice i vjerojatnost. U analizi rizika nužno je prepoznati i sve druge atributa rizika, jer neki događaj može imati više posljedica i može utjecati na više ciljeva. Pri analizi rizika potrebno je uzeti u obzir i postojeće mjere postupanja s rizicima (kontrole), ako one postoje, te odrediti njihovu efikasnost i učinkovitost.

Vrednovanje rizika

U fazi vrednovanja rizika donose se odluke o izboru onih rizika koji zahtijevaju obradu te prioritete implementacije predviđenih kontrola. Odluke se donose na osnovi rezultata analize rizika. Vrednovanje rizika uključuje uspoređivanje razine određenog rizika ustanovljenog tijekom faze analize, s kriterijima ustanovljenim tijekom utvrđivanja konteksta u kojem se promatra pojava rizika. U određenim okolnostima, vrednovanje rizika može rezultirati pokretanjem daljnje analize rizika. Također, vrednovanje rizika može dovesti i do odluke o nepoduzimanju nikakvih daljnjih aktivnosti, osim održavanja postojećih kontrola. Naravno, ove odluke prvenstveno ovise o postavljenim kriterijima rizika i razini rizika koju poslovni sustav smatra prihvatljivom.

[1] PESTLE model analizira vanjske činitelje: Političke, Ekonomske, Socijalno-kulturološke, Tehnološke, Legalne, Ekološke. PESTLE je skraćenica od početnih slova svakog pojedinog činitelja okoline.
[2] SWOT –kvalitativna analitička metoda koja kroz 4 čimbenika nastoji prikazati snage, slabosti, prilike i prijetnje određene pojave ili situacije.

Postupanje s rizicima

Postupanje s rizicima uključuje izbor i implementaciju jedne ili više mogućnosti utjecanja na rizik. Uobičajene strategije su:

- smanjenje rizika – to je pristup koji podrazumijeva implementaciju odgovarajućih novih kontrola kojima se umanjuje identificirani rizik;
- prenošenje rizika – to je pristup u kojem se rizik se prenosi na treću stranu, npr. osiguravajuću kuću ili dobavljača;
- prihvaćanje rizika – jest pristup kojim se identificirani rizik prihvaća bez implementacije novih kontrola. Primjenjuje se ukoliko analiza pokaže da je trošak nove kontrole veći od potencijalnog gubitka. Odluka o prihvaćanju rizika predstavlja veliku odgovornost njenog donositelja i zahtijeva pismeno izvješće s detaljnim obrazloženjem zašto ne implementirati dodatne kontrole.
- izbjegavanje rizika – jest postupak koji podrazumijeva prekidanje ili nepokretanje aktivnosti unutar poslovnog sustava koje mogu izazvati određeni rizik. To se može primijeniti u slučaju kad se ukidanjem takvih aktivnosti ne utječe značajnije na poslovne procese organizacije ili kad postoji neki drugi način realizacije ovih aktivnosti.

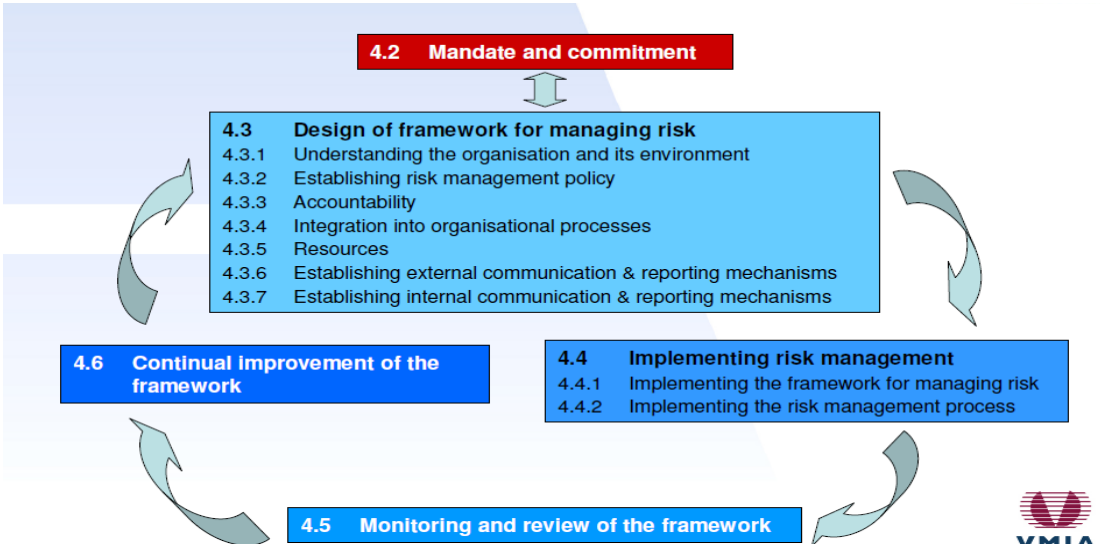
Nakon implementacije poduzetih mjera, ostaje rizik kojeg nazivamo rezidualnim rizikom. To je rizik koji podrazumijeva sve one prijetnje i ranjivosti za koje se smatra da ne zahtijevaju dodatni tretman u pogledu njegovog smanjenja. Također, rezidualni rizik može nastati kao posljedica „cost-benefit“ analize kojom je ustanovljeno da bi troškovi implementacije eventualnih mjera nisu isplativi.

Smanjivanje rizika obuhvaća slijedeće aktivnosti:

- određivanje prioriteta potrebnih mjera,
- evaluaciju preporučenih mjera,
- analizu isplativosti (dobiveno/uloženo),
- odabir mjera postupanja,
- dodjeljivanje odgovornosti,
- razradu plana za implementaciju mjera postupanja i njegovu realizaciju.

Rezultati ovih aktivnosti se obično objedinjavaju u planu postupanja s rizicima. Taj plan mora biti integriran u upravljačke dokumente organizacije i iskomuniciran sa svim zainteresiranim dionicima.

Upravljanje rizicima jedna je od temeljnih obveza menadžmenta. One su prikazane na slici 4, u skladu s točkama norme ISO 31000.

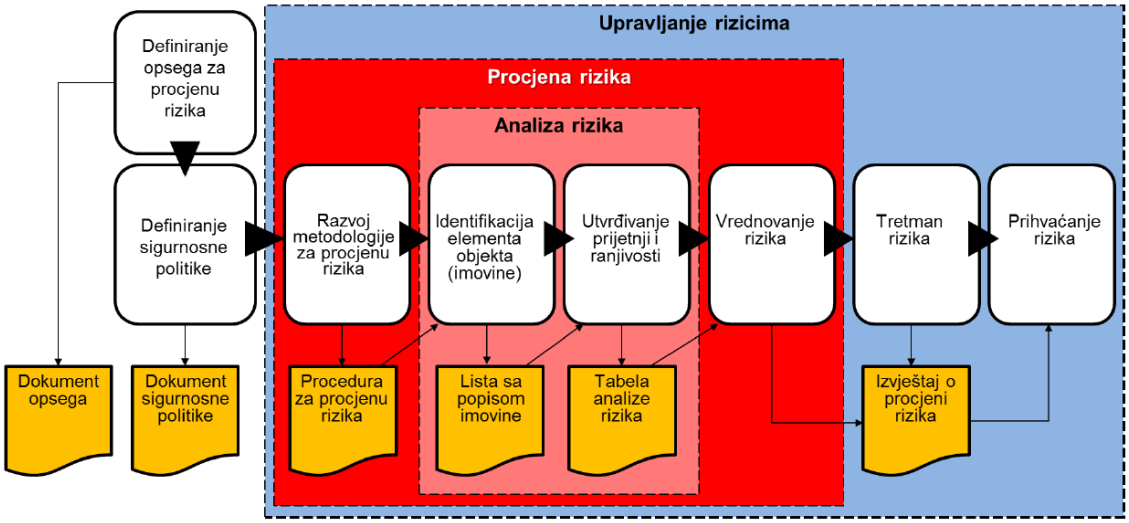


Slika 4. Obveze menadžmenta u upravljanju s rizicima prema normi ISO 31000

3. USLUGE ZIH-a

3.1. Konzultantski poslovi

Za poslovni sustav koji to želi, ZIH može razraditi cjelokupni proces upravljanja poslovnim rizicima, načiniti analize i procjene rizika, te izraditi prijedloge postupanja s rizicima. Ovaj proces slijedi opće smjernice određene normom ISO 31000, slika 5.



Slika 5. Smjernice za proces upravljanja rizicima prema normi ISO 31000

Razrada politike upravljanja rizicima i izrada procedure

Za konkretnog korisnika ZIH može izraditi politiku postupanja s rizicima i razraditi proceduru kojom se čini upravljanje poslovnim rizicima.

Identifikaciju rizika ZIH obavlja na slijedeći način*:*

Po svim relevantnim područjima poslovnog sustava, ZIH identificira prisutne prijetnje i ranjivosti koje iz njih proizlaze. U tablici 1 vidi se dio takvih razmatranja na primjeru IT-a.

Tablica 1. Identifikacija poslovnih rizika zbog IT-a

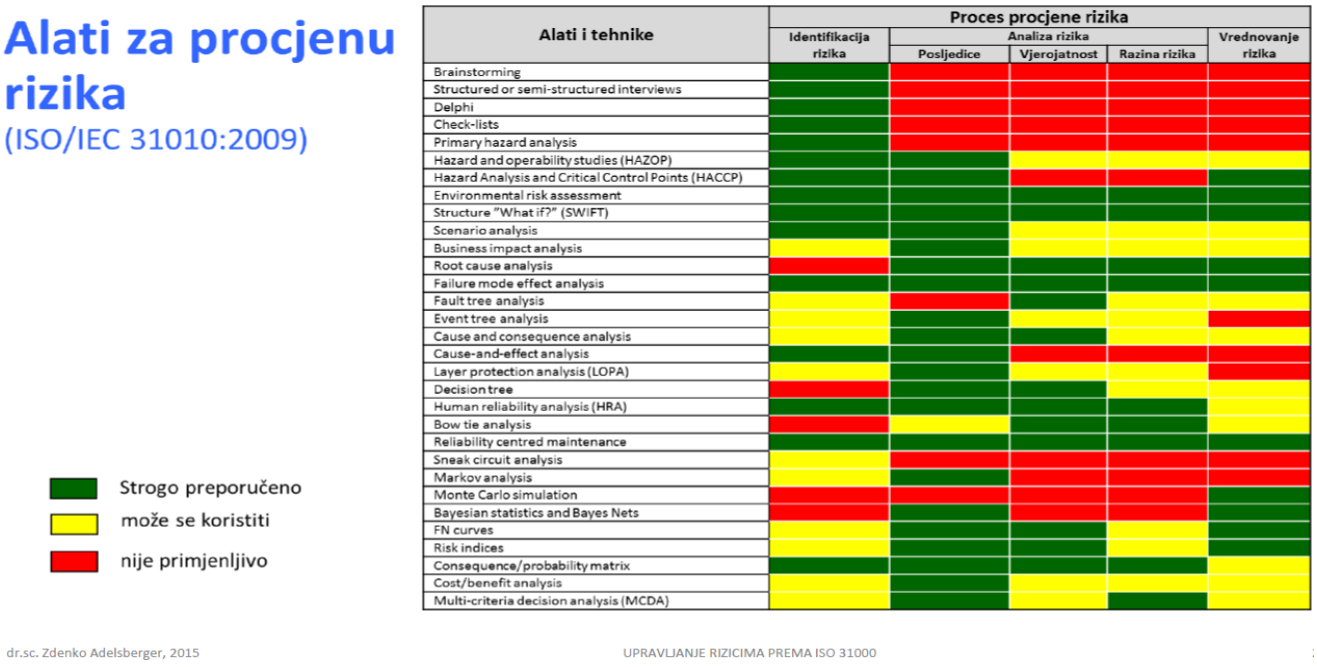
Područje	Prijetnja	Ranjivost
Upravljanje	• Ciljevi poslovnog sustava i IT-a nisu dovoljno povezani • Ne postoji strategija daljnje informatizacije • Ne upravlja se poslovnim rizicima zbog IT-a • IT se ne koristi za inoviranje poslovnih procesa • Kontrola i evaluacija IT-a je nedovoljna • itd	Uloga ICT-a u poslovnom sustavu je reaktivna i njen doprinos je biti „tehnološki sluga“, ne koristi se za digitalnu transformaciju poslovanja, njegovu agilnost, učinkovitost i djelotvornost i inovativnost.
Ekonomika informatizacije	• Ne procjenjuje se poslovna vrijednost doprinosa IT-a • Nije razrađen konzistentan način upravljanja IT budžetom i troškovima • Ne čini se optimizacija IT troškova • itd	IT je trošak, a ne pokretač poslovnih inovacija. Dominantni dio IT budžeta jesu troškovi održavanja i licenci, razvoj novih rješenja je minimalan.
Ljudi i resursi	• IT organizacija nije suvremeno oblikovana • Nije razrađeno upravljanje ljudskim potencijalima • Ne mjeri se osobna uspješnost IT djelatnika	Prisutne su sve boljke klasične IT organizacije, njena uspješnost je ograničena, HRM je orijentiran na tehnologije, a ne nove metode rada, osobna motivacija ne postoji.
IT usluge, IT arhitektura, IT infrastruktura i operativa	• IT arhitektura je fokusirana na tehnologiju, a ne poslovanje • Razina upravljanja IT uslugama je niska • Kvaliteta IT usluga je niska • Operativni IT postupci nisu dovoljno razrađeni	Razvoj IT arhitekture ne temelji se na poslovnim prioritetima, nisu razrađene IT usluge niti njihovi postupci.

	• Itd.	
Sigurnost	• Razina informacijske sigurnosti je nedovoljna • Razina upravljanja kontinuitetom poslovanja je niska • Nisu razrađeni postupci u slučaju katastrofa • Ne postoji program cyber sigurnosti s potrebnim procedurama • Itd.	Sigurnost informacijske imovine je nedovoljna i postoje mnogobrojne opasnosti njenog ugrožavanja, a time i ugroze poslovanja i reputacijskih rizika.
Aplikacije	• Ne postoji upravljanje portfeljem aplikacija • Verifikacija, validacija i testiranje aplikacija gotovo se ne primjenjuju • Ljudski resursi su koncentrirani na održavanje aplikacija • Itd.	Kriza daljnjeg razvoja. IT funkcija je fokusirana na održavanje i operativu. Postojeće stanje je ozbiljna barijera bilo kakvih inovacijskih promjena. Relacija uprava – IT – korisnici je niska i nije održiva.
Programi, projekti	• Razina upravljanja IT projektima je nedovoljna • Portfelj novih projekata nije (dovoljno) povezan s portfeljem IT investicija	Rizik uspješne realizacije novih projekata izrazito visok (probijanje budžeta, vremena, nedovoljna kvaliteta rješanja).

Na osnovi detaljno identificiranih prijetnji, ranjivosti i vjerojatnosti pojavljivanja, radi se registar svih rizika, kao osnova analize rizika.

Analiza rizika:

U ovoj fazi, u uskoj suradnji s korisnicima, istražuju se uzroci i izvori rizika, određuju vjerojatnosti pojavljivanja i procjenjuju moguće posljedice. Kao rezultati ove faze nastaje registar imovine za koju se čini procjena rizika, te izvješće o provedenoj analizi rizika. U analizi rizika moguće je koristiti različite metode, tehnike i alate u skladu s preporukama norme ISO 31010, kao što se vidi na slici 6.



Alati i tehnike	Proces procjene rizika				
	Identifikacija rizika	Analiza rizika			Vrednovanje rizika
		Posljedice	Vjerojatnost	Razina rizika	
Brainstorming					
Structured or semi-structured interviews					
Delphi					
Check-lists					
Primary hazard analysis					
Hazard and operability studies (HAZOP)					
Hazard Analysis and Critical Control Points (HACCP)					
Environmental risk assessment					
Structure "What if?" (SWIFT)					
Scenario analysis					
Business impact analysis					
Root cause analysis					
Failure mode effect analysis					
Fault tree analysis					
Event tree analysis					
Cause and consequence analysis					
Cause-and-effect analysis					
Layer protection analysis (LOPA)					
Decision tree					
Human reliability analysis (HRA)					
Bow tie analysis					
Reliability centred maintenance					
Sneak circuit analysis					
Markov analysis					
Monte Carlo simulation					
Bayesian statistics and Bayes Nets					
FN curves					
Risk indices					
Consequence/probability matrix					
Cost/benefit analysis					
Multi-criteria decision analysis (MCDA)					

Slika 6. Metode, tehnike i alati za procjenu rizika prema preporukama norme ISO 31010.

Vrednovanje rizika:

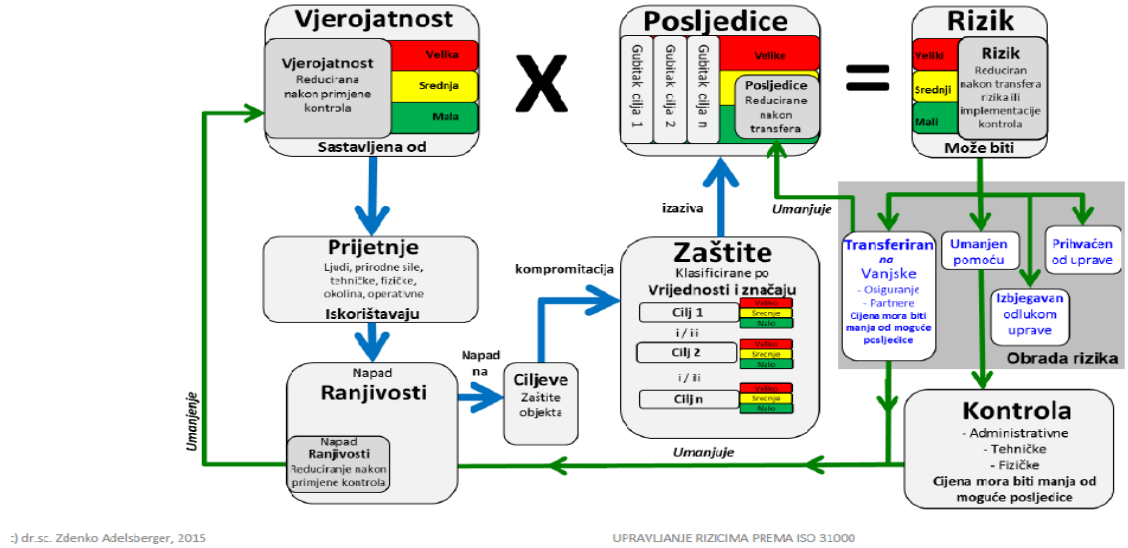
Nakon završene analize rizika, čini se njihovo vrednovanje. U obzir se uzimaju vjerojatnost nastanka neželjenih događaja, posljedice rizika i određuje izloženost organizacije riziku. Ona se najčešće izloženost izražava kao umnožak vjerojatnosti i posljedice rizika, no moguće su i neke druge formule, ovisno u primijenjenoj metodi procjene rizika. Na osnovi izračunatih rizika, čini se njihovo rangiranje, najčešće to se obavlja njihovim pozicioniranjem u zelenu, žutu i crvenu zonu. Na slici 7 naveden je jedan pojednostavljeni primjer vrednovanja rizika.

Significance						
	Extreme	Significant 5	Major 10	High 15	Severe 20	Severe 25
	Very High	Moderate 4	Significant 8	Major 12	High 16	Severe 20
	Medium	Low 3	Moderate 6	Significant 9	Major 12	High 15
	Low	Trivial 2	Low 4	Moderate 6	Significant 8	Major 10
	Negligible	Trivial 1	Trivial 2	Low 3	Moderate 4	Significant 5
		Rare	Unlikely	Moderate	Likely	Almost Certain
		Likelihood				

Slika 7. Primjer vrednovanja rizika

Postupanje s rizicima:

Nakon obavljenog vrednovanja rizika, izrađuju se prijedlozi postupanja s rizicima. Na slici 8 na pojednostavljen način, prikazan je krug Identifikacija – Analiza – Vrednovanje – Postupanje s rizicima, s aspektom na ovu posljednju fazu. U predlaganju mjera za svaki rizik, strogo se vodi računa o odnosu između ulaganja u poduzimanje potrebnih kontrola i potencijalnih posljedica, ukoliko se kontrole ne bi poduzele.



Slika 8. Krug Identifikacija – Analiza – Vrednovanje – Postupanje s rizikom

3.2. Seminari, treninzi

ZIH nudi održavanje slijedećih treninga i radionica:

- Motivacijsku prezentaciju članovima uprava / poslovodstva poslovnih sustava na temu *Zašto i kako upravljati poslovnim rizicima*
- Seminare iz primjene norme ISO 31000
  - ISO 31000 Foundation
  - Seminar ISO 31000 Lead Risk Manager
- Seminare iz rizika informacijske sigurnosti
  - Seminar ISO 27005 Foundation
  - Seminar ISO 27005 Risk Manager