Menadžment IT rizikom kao faktorom pouzdanosti poslovnih procesa

Momčilo Kokić
Katedra za industrijski menadžment i informatiku
Fakultet za menadžment
Sremski Kralovci, Srbija
momcilo.kokic@famns.edu.rs

Miljan Kokić
Bijeljina, Bosna i Hercegovina
kokicm@gmail.com

Sadržaj— **U svakodnevnim ljudskim aktivnostima, a posebno onima koje su vezane za poslovne procese neizbježna je primjena savremenih informaconih tehnologija (IT). Postalo je uobičajeno da se zahtjevi za ekonomičnijim poslovanjem, smanjenje gubitaka, porast dohotka, efektivnost i efikasnost djelumično zadovoljavaju povećanom primjenom IT resursa. Uvođenje novih tehnologija u poslovne procese utiče na rizik vezan za te procese, pozitivno ili negativno. IT se implementuraju u cilju smanjenja ukupnog poslovnog rizika. No, IT rizici u poslovnim procesima su u značajnoj korespodenciji sa ukupnim rizikom procesa, sa stalnom prijetnjom da negativno utiču na ukupni poslovni rizik. Da se ta prijetnja ne bi ostvarila IT rizik mora biti pod kontrolom. To podrazumijeva da se menadžmentu IT rizika mora posvetiti značajana pažnja u ukupnom menadžmentu poslovnim rizikom.**

Ključne riječi 1;Informacione tehnologije 2;IT rizik 3;poslovni proces ,4; pouzdanost.

I. UVOD

Poslovni procesi koji se odvijaju u cilju ostvarenja poslovnog cilja moraju biti pouzdani, znači moraju biti u stanju da sa velikom vjerovatnoćom zadovolje poslovne zahtjeve bez štetnog djelovanja na ljude i okolinu izvan dozvoljenih granica. U zadovoljenju ovih zahtjeva veliki udio, gotovo u svim poslovnim procesima koji se danas odvijaju u poslovnim sistemima, imaju savremene IT. Istraživanja potvrđuju da IT rizik može imati značajan uticaj na cjelokupne poslovne rezultate[1], taj uticaj može biti pozitivan i negativan. Nepouzdan rad, rad sa velikim rizikom primijenjenih IT-a u poslovnim procesima, za posledicu ima neadekvatne rezultate poslovnih procesa, odnosno poslovne procese sa visokim rizikom izazvane IT rizikom. Da bi se ukupni poslovni rizik sveo na prihvatljiv nivo neophodno je IT rizik staviti pod kontrolu, na njega primijeniti sve menadžerske procese, jer njegov nekontrolisani iznos može značajno doprinijeti porastu ukupnog poslovnog rizika. Rizici poslovanja proizilaze iz poslovanja preduzeća i odnose se na gubitke koji proističu iz neadekvatnih ili neuspješnih internih procesa, ljudi i sistema[2] Neadekvatan tretman IT rizika može izavati neke od sledećih problema:

- poslovanje sa gubicima zbog slabo realizovanih IT projekata
- slabo obavljanje poslovnih procesa zbog neadekvatnih IT resursa
- nedostupnost podataka i nformacija
- narušavanje integriteta poslovnih procesa i podataka
- krađa podataka i intelektualne svojine, znanja, ...
- nepotreban rast troškova izazvan težnjom za minimizacijom IT rizika, itd.

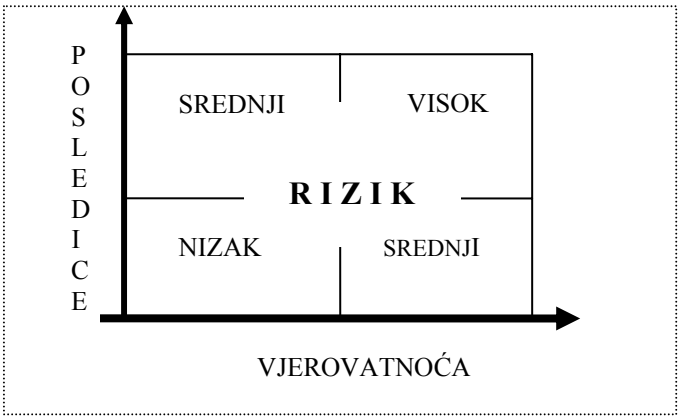
Da bi se efekti ovih i drugih problema, a koji su izazvani učešćem IT u poslovnim procesima sveli na prihvatljiv nivo potrebno je u procese menadžmenta poslovnog rizika inkorporirati i menadžment IT rizikom.

II. POJAM I VRSTE IT RIZIKA

Efekat neizvjesnosti u odnosu na ciljeve je rizik.[3] Rizik je višedimenziono zavisna veličina. On je mjera koja je povezana sa vjerovatnoćom nekog događaja i posledicama koje bi mogle biti izazvane tim događajem. Vjerovatnoća ili prijetnja od štete, povrede, odgovornosti, gubitka ili druge negativne pojave koja je uzrokovana od strane vanjskih ili unutrašnjih ranjivosti, i koja se može neutralisati kroz preventivne aktivnosti.[4] Rizik se ne može egzaktno odrediti jer varijable od kojih zavisi su varijable koje su generalno nemjerljive. Zato se rizik procjenjuje.

Rizik je moguće predstaviti u koordinatnom sistemu u ravni, gdje je jedna kordinata vjerovatnoća događaja, a druga posledice tog događaja Sl.1. Sa dijagrama se lako mogu izvesti značajni zaključci u pogledu veličine rizika u funkciji vjerovatnoće i mogućih posledica. Naime, vidljivo je da je najveći rizik koji ima visok nivo posledica a istovremeno je vrlo vjerovatan. Naravno, zbog nivoa posledica ne smije se zanemariti i rizik sa visokim posledicama, a i ako je malo vjerovatan. Na osnovu pozicije rizika u polju rizika može se suditi o potrebnim preventivnim ili korektivnim mjerama za smanjenje rizika.

Upravljanje rizikom se praktično realizuje smanjenjem obje koordinate rizika u polju rizika. U procesu upravljanja rizikom cilj je ona tačka rizika u kojoj su obje koordinate u koordinatnom početku. Naravno, to je praktično neizvodljivo, pa se u tom procesu zadovoljavamo nivom prihvatljivog rizika. To je onaj rizik čije posledice organizacija može podnijeti ili je to onaj nivo rizika koji je posledica mogućnosti (nemogućnosti) kompanije da investira u smanjenje rizika. Kako bilo da bilo, nivo prihvatljivog mrizika mora biti definisan, organizacije moraju biti svjesne njegovog postojanja i trebaju ga redovno preispitivati kao što se redovno moraju preispitivati sve komponente IT rizika.



Slika 1. Polje rizika

Kada je u pitanju IT rizik, osim specifičnosti koje su posledica specifičnosti IT-a, pojmovno određivanje rizika je u suštini isto. IT rizik je dio poslovnog rizika koji proističe iz primjene IT u poslovnim procesima. Naime, IT rizik je vjerovatnoća događaja sa posledicama koje mogu nastati ostvarenjem neke prijetnje usmjerene na IT resurse. Ostvarenje prijetnje je posledica slabosti, ranjivosti sistema zbog ranjivosti IT resursa. Znači IT rizik je vezan za realizaciju prijetnje ili prijetnji usmjerenih na ranjivost IT resursa. Nema IT rizika ako nema ostvarenja prijetnji, a nema ostvarenja prijetnji ako nema ranjivosti.

IT rizik se može klasifikovati po različitim kriterijumima. Jedan od kriterijuma može biti prema vrsti IT resursa. Po tom osnovu imamo rizike vezane za:

- Hardver
- Softver
- Baze podataka
- Organizacije IT resursa
- Mreže
- IT osoblje

Zbog složenosti IT resursa svaki od ovih rizika bi se mogao dalje razlagati na podvrste i po tom osnovu se može doći do zaključka da postoji veliki broj različitih vrsta IT rizika, čija se struktura može prikazati takozvanim matricama rizika. Ova taksomanija omogućava da se pri analizi rizika izbjegne nenamjerno zanemarenje nekog IT rizika. Insistiranje na klasifikaciji IT rizika po navedenom kriterijumu nije samo metodološkog karaktera, ono je duboko praktičnog karaktera, posebno u procesima koji su vezani za procjenu i menadžment IT rizika. Naime, poslovni rezultati mogu biti negativni kao posledica neidentifikovanih ili nepravilno klasifikovanih rizika.

Da se IT riziku u poslovnom svijetu pridaje adekvatna pažanaja govore i sledeći podaci: više od 50 % svjetskih kompanija čija su sjedišta u razvijenim evropskim zemljama povećale su ulaganja u tretman IT rizika u 2013. godini u odnosu na 2008. godinu kao referentnu godinu., a 54% ispitanih planira porast investicija u narednih 12 mjeseci, ali ne više od 5% [1].

Pored navedene klasifikacije IT rizik se može klasifikovati prema izvoru prijetnje, na rizik koji je posledica unutrašnjih prijetnji i rizik kao posledica vanjskih prijetnji. Ostvarenje prijetnji bez obzira na izvor se može realizovati preko unutrašnjih ili slabosti izvan IT rasursa, pa i to može biti osnov za podjelu rizika. IT rizik se može klasifikovati i po vrijednosti štete na veliki, srednj i mali, ili prihvatljiv i ne prihvatljiv. Ovo je relativna klasifikacija, jer vrijednost rizika koji je neko okarakterisao kao mali rizik za nekog može predstavljati veliki rizik i obrnuto. Zato je potrebno rizike u ovoj podjeli jasno kvantifikovati.

Pošto su IT u poslovnim procesima prvenstveno u funkciji procesa koji se odvijaju nad podacima i informacijama značajnim za te i druge procese, bitno je napomenuti da je posebna vrsta IT rizika vezana za sigurnosti podataka i informacija, na što mogu uticati različiti faktori unutar i van ITa. U tom kontekstu, gubici, rizik odnosi se na narušavanje povjerljivosti, dostupnosti i integriteta informacija. U odnosu na informacije kao poslovni resurs, u IT se razmatraju rizici poverljivosti, dostupnosti i integriteta informacija.

Prema značaju procesa na koje utiče, IT rizik može biti strategijski ili operativni, itd. Naravno, ovo nije konačna lista mogućih podjela IT rizika, već je samo njihova naznaka usmjerena u pravcu ukazivanja složenosti IT rizika kao pojave sa kojom se suočavaju svi koji u svojim poslovnim procesima koriste IT. Zato je poznavanje izvora IT rizika preduslov za adekvatnu procjenu intenziteta rizika i odgovarajuće upravljačke procese da bi se on držao na prihvatljivom nivou, nivou koji neće ugroziti pouzdanost poslovnih procesa u kojima su IT implementirane.

III. PROCJENA IT RIZIKA

Zbog složenosti rizika kao pojave, mjerenje rizika nije moguće, ali je moguća procjena rizika sa velikim stepenom pouzdanosti, primjenom različitih metodologija procjene. Procjenom IT rizika se identifikuju prijetnje, izvori prijetnji i oblici ugrožavanja poslovnih procesa ili njihovih rezultata, a koji su posledica primjene IT u realizaciji tih procesa. Procjena IT rizika se vrši u cilju obezbjeđenja uslova za ostvarenje poslovnih ciljeva adekvatnom primjenom IT resursa.

U ovom procesu procjenjuju se moguće posledice, sagledavaju snaga, sredstava, preventivne i korektivne mjere, njihovi efekti kao odgovori na opasnosti izazvane ostvarenjem prijetnji. Procjena IT rizika se vrši po svim IT resursima.

Ne postoji jedinstven algoritam po kome se vrši procjena IT rizika. Ono čega se treba pridržavati jesu zahtjevi da se procjena mora uraditi sveobuhvatno, da se njome obuhvate sve potencijalne prijetnje, ranjivosti sistema i moguće posledice ostvarenja prijetnji. Potrebno je jasno identifikovati sve IT rizike. Ako se prepozna prijetnja mora se izvršiti procjena rizika, prijetnja se ne smije zanemariti.

Za procjenu rizika se koriste različite metodologije, a u principu su sve zasnovane na statističkim pokazteljima i statističkim metodama ili su zasnovane na ocjeni usaglašenosti sa definisanim skupom zahtjeva i preporuka izraženih kroz

različite normativne akte. Procjena IT rizika na osnovu procjene stepena usaglašenosti sa određenim standardima ili preporukama se realizuje poređenjem relevantnih parametara sa preporučenim ili očekivanim. Relevantni standardi koji se mogu koristiti u cilju procene IT rizika su:

- ISO standardi serije 27000, prvenstveno ISO 27005.
- ISO 17799
- CobiT5 - zbirka preporuka na osnovu dobre prakse koju je kreiralo međunarodno udruženje za reviziju i kontrolu IT resursa (ISACA) u saradnji sa Institutom za upravljanje IT (ITGI),
- NIST-800 Preporuke nacionalnog instituta za standardizaciju i tehnologiju SAD-a (National Institute of Standards and Technology), itd.

Po istraživanjima 50% kompanija koristi ISO 27005:2008 (Information security risk management), 39% ISACA – risk IT framework [1], itd

Procjena rizika, primjenom statističkih pokazatelja o visini (vrijednosti) posledica nastalih realizaciom neke ili nekih prijetnji i vjerovatnoće njihovog nastanka, je povezana sa izračunavanjem sume matematičkih očekivanja odgovarajućih proizvoda šteta i vjerovatnoća. [4]

$$R=\sum_{i=1}^{n} P(u_i)\, L(u_i) \qquad (1)$$

Gdje su :
P(ui) – vjerovatnoća događaja i
L(ui) – veličina gubitaka događaja.

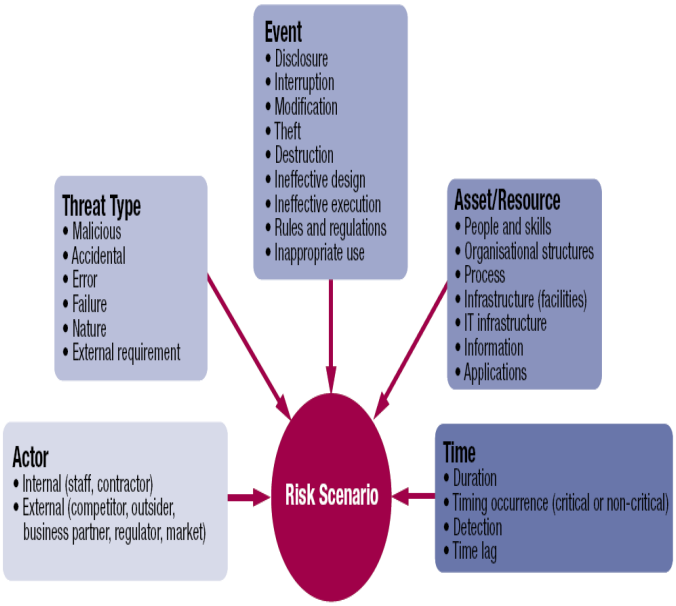
Po ovoj metodologiji suština problema se svodi na pravilnu procjenu prethodne dvije veličine. Posebno treba obratiti pažnju na procjenu baš tog gubitka koji je vezan za tačno određeni događaj, to zato što na visinu određenog gubitka uticaj može imati više različitih događaja sa različitim vjerovatnoća i tada može doći do kumulacije veličine gubitka. Posledica toga može biti precijenjena vrijednost rizika, što za posledicu može imati zahtjev za prevelika ulaganja za svođenje rizika na prihvatljiv nivo.

IV. MENADŽMENT IT RIZIKA

O IT riziku se mora voditi računa pri projektovanju informacionog sistema (IS), u procesima nabavke, održavanja i eksploatacije, znači u svim životnim fazama IT rasursa kao komponentama IS-a. IT rizik se manifestuje kroz razvoj i podržavanje poslovnih procesa koji stvraju prihode, ispunjavaju ciljeve organizacije i obavljaju poslovanje na efikasan i efektivan način. Menadžment IT rizikom mora biti dio strateškog opredjeljenja u pogledu upravljanja cjelokupnim poslovnim rizikom. Menadžment IT rizikom mora postati dio poslovne kulture organizacija, pošto je iplementacija IT resursa to već postala odavno. Gdje to nije, odvijanje poslovnih procesa i ostvarenje poslovnih ciljeva je znatno neizvjesnije.

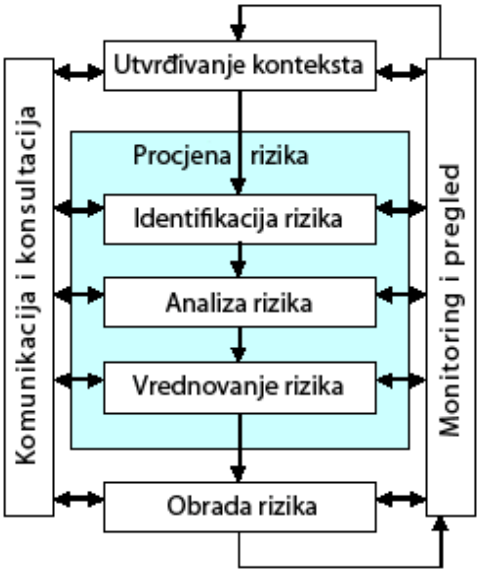
Da bi IT dale očekivani doprinos pouzdanosti poslovnih procesa u koje su implementirane neophodno je poslovni rizik, a koji je posledica IT-a svesti na odgovarajući, za poslovne procese, prihvatljiv nivo. Da bi se u tome uspjelo u organizacijama treba uspostaviti skup aktivnosti koje su usmjerene na upravljanje i kontrolu rizika. Ove aktivnosti moraju biti satavni dio menadžerskih procesa usmjerenih na rizik organizacije kao cjeline, sa posebnim akcentom na IT rizik kao dio cjelokupnog rizika organizacije. Integrisani pristup upravljanju rizikom 52% kompanija navode kao presudni faktor za napredak menadžmenta IT rizikom.[1] Za kvalitetan menadžment IT rizikom potrebno je uspostaviti upravljački okvir sa jasnim planovima, procesima, resursima usklađen sa strateškim i operativnim politikama i zadacima organizacije.

Istraživanja pokazuju da 82% organizacija imaju formalni okvir za upravljanje rizikom, a 72% ih ima formalni okvir za upravljanje IT rizikom. Međutim, samo u 23% organizacija su sadržaji tih okvira međusobno u potpunosti usklađeni.[1] Svaki od IT okvira definiše relevantne procese menadžmenta IT rizika. Na primjer, CobiT5 sugeriše ključne procese upravljanja rizicima *(EDM03 Ensure risk optimisation i APO12 Manage risk*), scenario rizika (*Risk Scenarija*) - ključne informacije neophodne za identifikaciju, analizu i odgovor na rizik (CobiT ima 111 scenarija rizika razvrstanih u 12 kategorija Sl.2.); i konkretne, procjenjive ocjene rizika, sa odgovorima na neprihvatljive scenarije rizika [6].



Slika 2. Scenario rizika[6]

Na Sl.3. su prikazani relevantni procesi menadžmenta rizika u skladu sa zahtjevima ISO 31000, kao baznog standarda u domenu menadžmenta rizikom bez obzira na vrstu djelatnosti, veličinu, itd. organizacije.



Slika 3. Procesi menadžmenta rizika [2]

Važan proces u sistemu menadžmentom rizika jeste obavezna periodična procjena stanja rizika. Ovaj proces je neophodan zato što IT rizik nije statična vrijednost, jer kako smo konstatovali nisu statični parametri od kojih on zavisi. Kroz ovaj proces se prvenstveno dolazi do podataka da li je došlo do promjene rizika i koji su uzroci doveli do te promjene. Periodičnu procjenu IT rizika najčešće sprovode interni ocjenjivači rizika, IT menadžment, menadžment organizacije, mendžeri rizika ili ocjenjivači izvan organizacije.

Istraživanja koja se odnose na ove procese pokazuju da: 55% ispitanika se izjasnilo da peridičnu procjenu IT rizika vrše interni revizori u saradnji sa zaposlenim na radnim mjestima čije su aktivnosti u značajnoj sprezi sa IT rizikom, u 56% kompanija to vrše kvartalno ili češće, preko 80% organizacija ima utvrđen period provere IT rizika. Samo 2% ispitanika u svojim organizacijama nema procjenu IT rizika[1].

V. ZAKLJUČAK

Rizik koji je posledica implementacije IT u poslovne procese ima značajan uticaj na pouzdanost poslovnih procesa. Ako se IT rizik kao dio poslovnog rizika, najčešće operativnog poslovnog rizika, drži pod kontrolom, onda sa velikom sigurnošću možemo tvrditi da će se poslovni procesi, a koji imaju veliku zavisnost od IT, pouzdano odvijati, odnosno da će se ukupni rizk poslovanja implementaciom IT smanjiti. Organizacije moraju biti svjesne sledećih činjenica koje su u vezi sa IT rizikom:

- IT rizici utiču na rizike cijelog poslovnog sistema
- Organizacije treba da budu svjesne prednosti koje su posledica usklađenosti menadžmenta IT rizikom sa menadžmentom ukupnog rizika organizacije i da u takvim okolnostima mogu efektivno i efikasno ostvariti IT i poslovne ciljeve
- Dobra komunikacija i usklađene funkcije unutar preduzeća preduslov su za izgradnju konzistentnog okvira IT rizika.
- Optimizacija potencijanih troškova, koji su u vezi sa optimizaciom IT rizika je neophodna, u protivnom bi efekti optimizacije IT rizika mogli biti manji od ulaganja u njegovu optimizaciju, a što samo po sebi predstavlja svojevrstan finansijski rizik.
- Mora se koristiti jedinstveno značenje rizika, sprovodi integralni menadžment rizikom u cijeloj kompaniji jer, 65% ispitanih kompanija smatra da govore jedinstvenim jezikom kada je rizik u pitanju.[1]
- Poslovima menadžmenta rizikom se moraju baviti profesionalci, menadžeri rizika, u saradnji sa profesionalcima , vlasnicima procesa.

LITERATURA

[1] Ernst & Young „Managing IT risk in a fast-changing environment", EMEIA FSO IT Risk Management Survey 2013, http://www.ey.com

[2] T.Raska**, "**Enterprise Risk Management", Univerzitet u Tuzli - Ekonomski Fakultet, Tuzla, 2011. http://www.upravljanjerizicima.com

[3] Međunarodni standard ISO 31000: 2013.

[4] S. Stevan, Udruženje e-Razvoj, S. Konstantin , ETŠ Zemun, "Analiza i ocena rizika u informacionoj bezbednosti", Konferencija o bezbednosti informacija BICES 2012,Fakultet informacionih tehnologija,Beograd 2012.

[5] Međunarodni standard ISO 27005:2011.

[6] http://www.isaca.org/COBIT

ABSTRACT

Abstract - In everyday human activities, especially those related to business processes, the application of modern information technology (IT) is inevitable. It has become customary that demands for more economical operations, reducing losses, increasing incomes, effectiveness and efficiency partially fulfill by increased use of IT resources. The introduction of new technologies into business processes affects the risk which is associated with these processes, positively or negatively. IT is implemented in order to reduce the overall business risk. However, IT risks in business processes are in the significantly correspondence with the overall risk process, with the constant threat that adversely affect on the overall business risk. In order to avoid this threat, IT risk must be controlled. This implies that IT risk management must get significant attention in the overall management of business risk.

Keywords: Information Technology, IT risk, business processes, reliability.

IT risk management as a factor of reliability of business processes

Momčilo Kokić
Miljan Kokić