Synthesis
International Scientific Conference of IT and Business-Related Research

UPRAVLJANJE IT RIZICIMA

IT RISK MANAGEMENT

Mile Stanišić
Univerzitet Singidunum, Danijelova 32, Beograd, Srbija

Apstrakt:
Sve organizacije, kako male tako i velike, koriste informacione tehnologije u svom poslovanju. Informacione tehnologije su danas više neko ikada izložene najrazličitijim rizicima. Uzroci rizika mogu biti vrlo različiti, a njihove posledice izuzetno opasne za ostvarenje ciljeva organizacije. U većini organizacija nedostaju adekvanti formalni procesi upravljanja rizicima. Stoga je potrebno da sve organizacije ustanove efektivne i efikasne procese upravljana IT rizicima, bazirane na profesionalnim okvirima i ISO standardima.

Ključne reči:
upravljanje rizicima, IT rizici, ISO standardi, okvir upravljanja IT rizicima.

Abstract:
All organizations, either small or large, use information technologies in their business. Information technologies are today more than ever exposed to various types of risks. Such risks can be triggered by numerous factors, and their consequences can considerably hinder goal achievement of an organization. Most organizations lack adequate formal risk management processes. Therefore, all organizations should establish effective and efficient IT risk management processes, based on the professional frameworks and ISO standards.

Key words:
risk management, IT risk, ISO standards, IT risk management framework.

1. UVOD

Upravlajnje IT rizikom nije proizvod koji se kupuje ili politika koja se uvodi. To je proces upravljanja poslovnim rizikom koji se mora obavljati stalno. On je značajan za organizaciju zbog stalnog ispitivanja ciljeva koji se odnose na rizike i zaštitu u okviru poslovnog okruženja i zbog sistematskog ugrađivanja zaštite u način na koji posluje organizacija.

Upravljanje rizikom se primenjuje na čitav spektar aktivnosti u okviru organizacije, ne samo na IT aplikaciju. IT se ne može posmatrati izolovano, već mora biti tretirano kao integralni deo svih poslovnih procesa. Izbor IT kontrola nije jednostavno stvar primenjivanja onih koje su preporučene kao najbolje prakse. One moraju da ostvaruju dodatu vrednost za organizaciju smanjenjem rizika na efikasan način i povećanjem efektivnosti. Prilikom razmatranja adekvatnosti IT kontrola unutar okvira internih kontrola organizacije menadžment utvrđuje:

- Vrednost i značaj informacija.
- Prihvatljiv nivo i toleranciju rizika organizacije za svaku poslovnu funkciju i proces.
- IT rizike sa kojima se suočava organizacija i kvalitet usluga koje se pružaju korisnicima.
- Složenost infrastrukture IT.
- Odgovarajuće IT kontrole i koristi koje obezbeđuju.
- Štetne IT incidente u poslednja 24 meseca.

Cilj ovog rada je da se istraže prakse u svetu i u Republici Srbiji, koji standardi i okviri upravljanja IT rizicima se primenjuju u procesu upravljanja rizicima. Traži se odgovor na pitanje - koji nivo upravljanja IT rizicima je dostignut u Republici Srbiji, koje organizacije prednjače u tome, i šta treba uraditi da upravljanje ovim rizicima bude usklađeno sa Međunarodnim standardima za upravljanje rizikom informacione tehnologije.

2. DEFINISANJE IT RIZIKA, UPRAVLJANJA RIZIKOM, PRIHVATLJIVOG NIVOA RIZIKA I TOLERANCIJE RIZIKA

IT rizik je potencijalna mogućnost dešavanja neke pretnje koja može štetno delovati na organizaciju. IT rizici su rizici na poslovanje koji proizilaze iz korišćenja IT. Meri se u smislu kombinacije verovatnoće nastanka događaja i njegovom posledicom. Rizik informacione tehnologije ili IT rizik ili IT povezan rizik, je rizik povezan sa informacionim tehnologijama. Iako se informacije već dugo cene kao vredan i važan resurs, razvoj znanja o ekonomiji doprineo je da organizacije postanu sve zavisije od informacija, obrade podataka i posebno IT. Razni događaji ili incidenti koje prouzrokuju IT rizici mogu da izazovu negativne uticaje na poslovne procese ili misije te organizacije, u rasponu od nebitnih do katastrofalnih materijalnih posledica.[1]

U *Review Manual* 2006 je data sledeća definicija upravljanja rizikom: *"Upravljanje rizikom predstavlja proces utvrđivanja osetljivosti i opasnosti (ugroženosti) informacionih resursa koje koristi organizacija za postizanje poslovnih ciljeva, i odlučivanje koje kontramere, ako ih ima, da preduzme za smanjenje rizika na prihvatljiv nivo, na bazi vrednosti informacionih reursa za organizaciju."* ISACA (2006).

Nivoom prihvatljivog rizika za organizaciju definiše se stepen rizika koji je određena kompanija ili neka druga organizacija spremna da prihvati u postizanju svojih ciljeva, kako odredi izvršni menadžment i upravno telo. Nivoom prihvatljivog rizika može da se utvrdi, na primer, da li će organizacija imati agresivniju ulogu u raspoređivanju novih tehnologija i onih tehnologija koje se tek pojavljuju. Na nivo prihvatljivog rizika u organizaciji

1 Različite definicije IT rizika date su u dokumentu IT risk, http://en.wikipedia.org/wiki/IT_risk#Standards_organizations_and_standards

E-mail: mile.stanisic@singidunum.ac.rs
DOI: 10.15308/Synthesis-2015-723-728

može da utiče njeno industrijsko i regulatorno okruženje. U bliskoj vezi sa nivoom prihvatljivog rizika je tolerisanje rizika u organizaciji kojim se meri koliko daleko je organizacija spremna da odstupi od svoje navedene mere prihvatljivog rizika.

Prihvatljiv nivo rizika organizacije COSO (2004) je definisao kao:

"… stepen rizika, na širem nivou, koji je kompanija ili neka druga organizacija spremna da prihvati u postizanju svojih ciljeva. Menadžment razmatra prihvatljiv nivo rizika organizacije prvo prilikom ocenjivanja strateških alternativa, zatim prilikom postavljanja ciljeva u skladu sa odabranom strategeijom, i prilikom razvoja mehanizama za upravljanje odgovarajućim rizicima."

Takođe, COSO definiše toleranciju rizika kao:

"… prihvatljiv nivo odstupanja u odnosu na postizanje ciljeva. Prilikom postavljanja određenih tolerancija rizika menadžment razmatra relativan značaj odgovarajućih ciljeva i usaglašava toleranciju rizika sa prihvatljivim nivoom rizika."

Cilj upravljanja rizikom u preduzeću je da obezbedi da svako radi sa istim nivoom i poznavanjem rizika i da odluke donesene na svim nivoima upravljanja budu konzistentne sa prihvatljivim nivoom rizika organizacije.

Upravljanje rizikom je proces koji omogućava IT menadžerima da uspostave balans operativnih i ekonomskih troškova zaštitnih mera i postignu dobre rezultate što se tiče sposobnosti (kapaciteta) i za ispunjavanje misije (glavnog zadatka) zaštitom IT sistema i podataka koji podržavaju misije (zadatke) njihovih organizacija. Ovaj proces nije jedinstven za sva IT okruženja; ali je zaista proces koji je široko zastupljen kod odlučivanja u svim oblastima našeg svakodnevnog života.[2]

3. ZAKONODAVNI OKVIR UPRAVLJANJA RIZIKOM INFORMACIONOG SISTEMA

Narodna banka Srbije (2013) je donela Odluku o minimalnim standardima upravljanja Informacionim sistemom finansijske institucije. Prema ovom propisu sve banke su obavezne da u okviru sveobuhvatnog sistema upravljanja rizicima, uspostave proces upravljanja rizikom informacionog sistema koji obuhvata identifikovanje i merenje, odnosno procenu tog rizika, kao i njegovo ublažavanje, praćenje i kontrolu. Banka je dužna da rizikom informacionog sistema upravlja tako da omogući nesmetano upravljanje bezbednošću ovog sistema i upravljanje kontinuitetom poslovanja banke. Ova obaveza banke proizilazi iz primene zahteva Bazela II, koji je posvećen operativnom riziku, a time i IT rizicima kao integralnom delu operativnih rizika.

Upravljanje rizikom informacionog sistema mora da obuhvati celokupan informacioni sistem banke i da bude integrisano u sve faze razvoja tog sistema. Pored toga, banka je dužna da adekvatno upravlja rizicima koji proizlaze iz ugovornih odnosa sa pravnim i fizičkim licima čije se aktivnosti odnose na njen informacioni sistem, kao i da kontinuirano nadzire način i kvalitet ugovorenih aktivnosti.

Menadžment banke treba da primenjuje zadovoljavajuće kontrolne prakse kao deo svoje sveobuhvatne strategije za ublažavanje rizika. Ove prakse treba da uključuju:

- Interne kontrole koje na efikasan način ublažuju utvrđene rizike koji se odnose na IT procese kao što su upravljanje sistemima i zaštitom, razvoj sistema, IT poslovanje, funkcije spoljnih provajdera, upravljanje prodajom, i druge oblasti IT rizika;
- Obezbeđenje kontrola nad MIS (*Management Information System*) da bi se obezbedile menadžmentu tačne i pravovremene informacije radi donošenja pravilnih odluka;
- Usvajanje i jačanje IT politika i standarda;
- Standarde za angažovanje, menjanje dužnosti i otpuštanje IT osoblja, uključujući interno osoblje, konsultante, privremeno zaposlene, i druge spoljne strane;
- Programi obuke i ocenjivanja radi održavanja nivoa IT ekspertize;
- Godišnji pregled IT pokrića osiguranja i potrebe za osiguranjem;
- Formalni planovi nastavka poslovanja za svaku značajnu oblast poslovanja;
- Nadzor i upravljanje odnosima sa trećim stranama (spoljnim stranama).

Osnovni ISO internacionalni standardi koji se odnose na upravljanje rizicima su sledeći:[3]

- IEC 31010:2009, Risk management - Risk assessment techniques
- ISO 31000:2009, Risk management - Principles and guidelines
- ISO Guide 73:2009, Risk management - Vocabulary
- ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management

Najpoznatiji okviri i metodologija za upravljanje rizicima su (Uremović, 2009):

- CRAMM - Velika Britanija, za velike organizacije
- BS 7799-3:2006 - Velika Britanija, za sve organizacije
- ISO/IEC 27005:2008 - Velika Britanija, za sve organizacije
- IT-Grundschutz – Nemačka, za sve organizacije
- Mehari 2007 – Francuska, besplatno za sve organizacije
- Octave – SAD, za srednje i male organizacije
- SP800-30 (NIST) – SAD, za sve organizacije

Ocenjivanja rizika u skladu sa nacionalnim okvirom treba da obuhvataju sve funkcije upravljanja IT rizikom uključujući bezbednost, korišćenje usluga spoljnih provajdera, i poslovni kontinuitet. Viši menadžment treba da obezbedi da utvrđivanje i ocenjivanje IT rizika na nivou preduzeća bude koordinisano i konzistentno u okviru cele organizacije. Snažan i visokog nivoa proces ocenjivanja rizika obezbeđuje osnovu za detaljnije ocenjivanje u okviru funkcionalnih oblasti upravljanja rizikom. Efikasan proces ocenjivanja IT rizika će unaprediti odluke koje se odnose na politiku i interne kontrole u organizaciji.

Viši menadžment može da koristi podatke ocenjivanja rizika za donošenje pravilnih odluka o upravljanju rizikom na bazi potpunog upoznavanja sa poslovnim rizicima. Male organizacije sa manje složenim sistemima mogu imati jednostavniji proces ocenjivanja rizika. Bez obzira na složenost proces treba da bude formalan i treba da se prilagodi promenama u IT okruženju. Ispitivači treba da ocenjuju efikasnost procesa ocenjivanjem poznavanja i svesnosti menadžmenta o riziku, adekvatnosti formalnih ocenjivanja rizika, i efikasnosti odgovarajućih politika i internih kontrola.

4. UTVRĐIVANJE I OCENJIVANJE RIZIKA

Analiziranje i ocenjivanje rizika koji se odnosi na IT može biti kompleksano. IT infrastruktura se sastoji od hardvera, softvera, komunikacija, aplikacija, protokola, i podataka, i njihove primene u fizičkom prostoru, organizacionoj strukturi, i između organizacije i njenog eksternog okruženja. Infrastruktura

2 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

3 www.iso.org

DOI: 10.15308/Synthesis-2015-723-228

takođe obuhvata ljude koji imaju inetraktivnu vezu sa fizičkim i logičkim elementima sistema.

Popis komponenata IT infrastrukture otkriva osnovne informacije o osetljivosti okruženja. Na primer, poslovni sistemi i mreže povezane sa Internetom su izloženi opasnostima koje ne postoje za samostalne sisteme i mreže. Pošto povezanost sa Internetom predstavlja bitan element većine poslovnih sistema i mreža, organizacije moraju da obezbede da arhitektura njihovih sistema i mreža obuhvata osnovne kontrole koje obezbeđuju osnovnu zaštitu.

Organizacije treba da obavljaju proces ocenjivanja kojim se usmerava izbor tehnologije i primena kontrola. Proces ocenjivanja rizika treba da obuhvata specifična ocenjivanja koja se obavljaju za funkcionalne odgovornosti kao što su bezbednost, kontinuitet poslovanja, i upravljanje komitentima (*vendor managament*). Ocenjivanje rizika obuhvata četiri značajne etape:

- Stalno prikupljanje podataka iz novih inicijativa ili monitoring postojećih aktivnosti;
- Analiza rizika u vezi sa potencijalnim uticajem tih rizika;
- Utvrđivanje pioriteta kontrola i aktivnosti za ublažavanje rizika; i
- Stalni monitoring aktivnosti za ublažavanje rizika.

Operativnim IT planiranjem treba utvrditi i oceniti izloženost riziku da bi se obezbedilo da politike, procedure i kontrole budu efikasne. Ocenjivanja rizika bezbednosti (zaštite) informacija se zahtevaju u skladu sa nacionalnim okvirom. Ovim ocenjivanjima treba utvrditi lokaciju svih poverljivih podataka o komitentima i korporativnih podataka, sve predvidive interne i eksterne opasnosti za te informacije, verovatnoću opasnosti (ugroženosti) i adekvatnost politika i procedura za ublažavanje tih opasnosti. Menadžment treba da razmotri rezultate tih ocenjivanja kada vrši nadzor IT poslovanja.

4.1. STALNO SAKUPLJANJE PODATAKA

Upoznavanje sa okruženjem organizacije predstavlja prvi korak (etapu) u procesu ocenjivanja rizika. Viši menadžment treba da obuhvati informacije o pitanjima (problemima) iz oblasti IT kao što su ograničenja resursa, opasnosti, prioriteti i ključne kontrole, iz nekoliko izvora. Prilikom obavljanja formalnog ocenjivanja rizika menadžment treba da sakupi informacije koje se odnose na IT okruženje organizacije iz nekoliko lokacija uključujući sledeće:

- Popisi IT sistema su značajni za upoznavanje i monitoring taktičkog poslovanja IT u organizaciji kao i za utvrđivanje punktova (mesta) pristupa i čuvanja poverljivih informacija komitentima i korporativnih podataka.
- IT strateški planovi obezbeđuju uvid u proces planiranja organizacije. Pregled i analiza strateških planova kao deo procesa ocenjivanja rizika može da ukaže na razvoj izloženisti riziku ili druge nedostatke koji ograničavaju mogućnost organizacije da primeni strateške prioritete.
- U planovima za oporavak i kontinuitet (nastavak) poslovanja se daje prednost raspoloživosti raznih poslovnih linija u organizaciji i oni često obuhvataju ozdravljenje i obezbeđenje kontrole, usluge komitentima, i podršku. Ti planovi mogu da obezbede uvid u značajne operativne sisteme i kontrolno okruženje u organizaciji.
- Dužna pažnja (posvećenost) i monitoring provajdera usluga mogu da predstavljaju dragocene informacije o kontrolnom okruženju provajdera. Te informacije su potrebne za potpuno ocenjivanje rizika IT okruženja u organizaciji.
- Izveštaji call centra o praćenju u vezi sa ovim pitanjima mogu često da ukažu na potencijalne probleme u poslovanju i kontroli ukoliko su ti izveštaji o raznim pitanjima (problemima) udruženi i analizirani zbog problema koji se ponavljaju ili su uobičajeni.
- Samoocenjivanje IT kontrola od strane odeljenja može da obezbedi rano identifikovanje neusaglašenosti sa politikama ili slabosti u kontroli.
- Nalazi IT revizije obezbeđuju uvid u verodostojnost (istinitost) i pristupačnost (stepen reagovanja, odziva) osoblja i menadžmenta, posvećenost primeni politika (usaglašenosti sa politikama) i internim kontrolama.

Izvesni indikatori mogu da upozore na visok nivo rizika u IT procesima. Njih treba razmotriti prilikom ocenjivanja rizika:[4]

- Koliko i koje ključne kontrole su imale propuste u testiranju prethodnog perioda ili za vreme internih revizija?
- Koja je starost aplikacije i koliko često se modifikuje?
- Da li postoje poznati problemi kod obrade ili podataka?
- Da li ima poznatih problema kod funkcionalnosti važnih aplikacija?
- Koliko široko je menjana kupljena aplikacija, prilagođena klijentima, ili menjana njena konfiguracija?
- Koji su bili zahtevi za promenama visokog prioriteta?
- Koliko se često dešavaju problemi u obradi?
- Koliko često se vrše hitne promene?
- Koji je nivo fluktuacije osoblja na ključnim pozicijama?
- Koliko je iskusno osoblje i da li je prošlo kroz dovoljnu obuku?

Kod razumevanja rizika kod aplikacije sledeće stavke su tipične stavke koje su dobijene da bi se shvatili i ocenili rizici na svakom nivou seta aplikacija:[5]

- Elementi infrastrukture koji podržavaju aplikacije (na primer: baze podataka, operativni sistemi, mreže i centri podataka).
- Stepen do kojeg automatizovane kontrole predstavljaju rezultat postavljene konfiguracije pre nego aplikacionog koda.
- Tehnologija baze podataka u upotrebi. Upoznati se sa prirodom i dinamikom događanja promena kod elemenata baze podataka, kao što su šematski prikazi, koje su bitne za ključne automatizovane kontrole.
- Operativni sistem (na primer: koji se koristi za koju aplikaciju i koliko često se vrše promene).
- Značajni interfejsi i njihove manulne kontrole. Možda je potrebno da ove kontrole dodate listi ključnih automatizovanih kontrola ukoliko nisu uključene kao ključne kontrole, njihovi propusti ne bi bili otkriveni uobičajenom primenom utvrđenih ključnih kontrola, i one bi mogle dovesti do materijalne greške.
- Infrastruktura mreže i njene potencijalne tačke propusta (na primer: aplikacija i njene ključne automatizovane kontrole se možda oslanjaju na prenos kroz mrežu gde propust u mreži ili kršenje zaštite mreže bi mogli da imaju za rezultat neotkrivene materijalne greške u finansijskim izveštajima).
- Da li je aplikacija kreirana interno, ili je kupljena?
- Da li se aplikacija održava interno ili se održava uslugama iz spoljnih izvora?
- Kako su aplikacije i infrastruktura podržavane: centralizovano kroz zajedničke usluge, geografski, ili pojedinačno po poslovnim jedinicama?

4 GAIT Methodology: A risk-based approach to assessing the scope of IT general controls, The Institute of Internal Auditors, 2007. p.18.

5 GAIT Methodology: A risk-based approach to assessing the scope of IT general controls, The Institute of Internal Auditors, 2007. pp. 17-18.

DOI: 10.15308/Synthesis-2015-723-728

- Da li centri podataka funkcionišu interno ili uz pomoć usluga iz spoljnih izvora?
- Koje primene mreže i tehničke infrastrukture se obavljaju interno, a koje uz pomoć trećih lica?
- Kako je IT organizovan? Da li postoji podela važnih funkcija?

4.2. ANALIZA RIZIKA

CRO (*chief risk officer*) zajedno sa predstavnicima iz IT (*chief information officer* - CIO, *chief information security officer* - CISO, *chief security officer* – CSO, *information system security officer* - ISSO) i poslovnih oblasti obavlja procenu rizika. Postoji osam osnovnih pitanja u vezi sa procesom ocenjivanja rizika. Prvih pet su:

- Koja su sredstva rizična i vrednost njihove poverljivosti, integriteta i raspoloživosti?
- Šta bi se moglo dogoditi što bi negativno uticalo na vrednost tih informacionih sredstava (događaj)? Ono što podrazumeva ovo pitanje je analiza ugroženosti i planiranje osetljivosti na opasnosti i potencijalni uticaj na informaciona sredstva.
- Ukoliko bi se taj događaj (opasnost) dogodio koliko loš bi njegov uticaj bio?
- Kolikočesto se može očekivati da se dogodi taj događaj (učestalost događanja)?
- Koliko su sigurni odgovori na prva četiri pitanja (analiza neizvesnosti)?

Sledeća tri pitanja se odnose na analizu ublažavanja rizika:

- Šta se može uraditi da se smanji rizik?
- Koliko će to koštati?
- Da li je to ekonomično/efikasno?

Menadžment treba da koristi sakupljene podatke o IT sredstvima i rizicima da bi analizirao potencijalni uticaj rizika na organizaciju. Analizom treba da se utvrde razni događaji ili opasnosti koji bi mogli da negativno utiču na organizaciju u strateškom ili operativnom pogledu. Menadžment treba da oceni verovatnoću raznih događaja i rangira mogući uticaj. Neki primeri događaja koji bi mogli da utiču na organizaciju uključuju sledeće:

- *Prekršaji koji se odnose na bezbednost* - Prekršaji koji se odnose na bezbednost koji mogu da utiču na organizaciju obuhvataju eksterne i interne prekršaje koji se odnose na bezbednost, prevare u programiranju, viruse u računarima, ili poricanje (odbijanje) kritika koje se odnose na pružanje usluga.
- *Ispadi sistema (System failures)* - Uobičajeni uzroci ispada sistema obuhvataju prekid (ispad) u mreži, rizik međuzavisnih odnosa (interdependency risk), prekid u interfejsu (interface failure), hardware failure (propust u hardveru), propust u softveru (software failure), ili nefunkcionisanje internih telekomunikacija.
- *Spoljni događaji* – Organizacije su takođe izložene spoljnim opasnostima uključujući vremenske prilike, zemljotrese, terorizam, cyber upade, prekid linija javnih usluga ili zastarelost električnih instalacija koji dovode do ispada sistema i drugih uređaja.
- *Greške kod ulaganja u tehnologiju* - Greške kod ulaganja u tehnologiju obuhvataju rizik koji se odnosi na strateško platformu ili dobavljače, neodgovarajuću definiciju poslovnih zahteva, nekompatibilnost sa postojećim sistemima, ili zastarelost softvera mogu ograničavati profitabilnost ili rast.
- *Problemi u razvoju i primeni sistema* - Uobičajeni problemi u razvoju i primeni sistema obuhvataju neadekvatno upravljanje projektom, prekoračenja u troškovima/vremenu (rokovima), greške u programiranju (interno/eksterno), propust da se uspešno integrišu i/ili pokrenu (odmaknu, migriraju) od postojećih sistema, ili propust sistema da ispuni poslovne zahteve.
- *Nedostatak (manjak) kapaciteta* - Manjak kapaciteta je rezultat neadekvatnog planiranja kapaciteta uključujući precizna prognoziranja (predviđanja) rasta.

Kada organizacija utvrdi delokrug rizika menadžment treba da oceni verovatnoću nastajanja kao i finansijski uticaj, uticaj na reputaciju i druge uticaje na organizaciju. Uticaji na organizaciju su veoma različiti i nije ih uvek lako kvantifikovati, ali takođe obuhvataju takva razmatranja kao što su izgubljeni prihodi, pogrešne poslovne odluke, troškovi oko rehabilitacije i rekonstrukcije podataka, troškovi sporova i potencijalnih sudskih odluka (presuda), gubitak udela (učešća) na tržištu, i povećanje premija ili odricanja od osiguranja. Po pravilu se analizom rizika rangiraju rezultati na bazi odnosa između troškova i verovatnoće (The Open Group, 2010, str. 26-38).

Dinamika analize rizika je važna i na nju u velikoj meri utiče tehnološka promena. U statičnom okruženju poslovne i tehničke infrastrukture proces ocenjivanja bi mogao biti na godišnjem nivou ili bi se mogao obavljati zajedno sa nekim značajnim implementacionim projektom.

4.3. UTVRĐIVANJE PRIORITETA

Kada se menadžment upozna sa IT okruženjem organizacije i analizira rizik treba da rangira rizik i utvrdi prioritete za reagovanje na njih. Verovatnoća nastajanja i stepen uticaja obezbeđuju osnovu za smanjenje izloženosti rizku ili utvrđivanje kontrola za ublažavanje sa ciljem da se obezbedi sigurno, zdravo i efikasno IT poslovanje koje odgovara složenosti organizacije. Ukupni rezultati ocenjivanja rizika treba da predstavljaju važniji faktor u odlučivanju u većini oblasti odgovornosti IT upravljanja uključujući:

- Planiranje budžeta za tehnologiju, investiranje i odluke o raspoređivanju;
- Planiranje eventualnih događaja (nepredviđenih izdataka, obaveza);
- Politike i procedure;
- Interne kontrole;
- Angažovanje osoblja i ekspertize;
- Osiguranje;
- Repere (nivoe) za IT poslovanje;
- Nivoe usluga za interne IT usluge i IT usluge spoljnih provajdera; i
- Jačanje politika i usaglašenost sa politikama.

4.4. MONITORING

Mnoge aktivnosti služe za praćenje efikasnosti upravljanja rizikom preduzeća u normalnom toku poslovanja. Iz ovoga proističu aktivnosti upravljanja koje mogu da uključuju analizu odstupanja, upoređivanje informacija iz različitih izvora, i da se bave neočekivanim događajima.

Aktivnosti kontinuiranog monitoringa uglavnom obavljaju menadžeri za linijsku poslovnu ili funkcionalnu podršku razmatrajući implikacije informacija koje primaju. Fokusiranjem na odnose, nedoslednosti ili relevantne implikacije oni pokreću pitanja i prate ih sa ostalim osobljem da bi utvrdili da li su potrebne korektivne ili druge mere.

DOI: 10.15308/Synthesis-2015-723-728

Menadžment i Bord treba da prate aktivnosti za ublažavanje rizika da bi obezbedili da su utvrđeni ciljevi postignuti ili su u toku. Monitorng treba da bude stalan, odeljenja treba da dostavljaju menadžmentu periodične izveštaje o napretku ostvarivanja ciljeva i implementaciji korektivnih planova. Stalni monitoring dalje obezbeđuje da proces ocenjivanja rizika bude kontinuiran a ne jednokratan ili godišnji događaj. Ključni elementi efikasnog programa monitoringa uključuju:

- Planove aktivnosti za ublažavanje ili korekciju;
- Jasno određivanje odgovornosti; i
- Izveštavanje menadžmenta.

5. STRATEGIJE ZA SMANJENE RIZIKA

Pošto je procenio relevantne IT rizike menadžment odlučuje kako će na to odgovoriti. Odgovori obuhvataju izbegavanje rizika, smanjenje, podelu odgovornosti za rizike i prihvatanje rizika. Prilikom razmatranja svojih akcija koje će preduzeti menadžment ocenjuje efekat na verovatnoću i uticaj rizika, kao i na troškove i dobiti, tako što odabira odgovor koji svodi rezidualni rizik u okvire željenog nivoa rizika. Generalno, postoji nekoliko načina da se ublaže potencijalni uticaji rizika, koji u stvari predstavljanju odgovore na rizike (The Open Group, 2010, str. 31):

- *Izbegavanje rizika* – Napuštanje tehnologije koja doprinosi riziku. Moguće je rizik da bude povezan sa upotrebom određene tehnologije, dobavljača ili proizvođača. Rizik se može eliminisati zamenom sa drugom tehnologijom.
- *Smanjenje rizika* – Preduzima se akcija da se smanji verovatnoća ili uticaj rizika, ili oba. Pod ovom tehnikom se podrazumeva osmišljavanje i implementacija kontrolnih aktivnosti čime se minimiziraju efekti na rizik.
- *Podela odgovornosti za rizik* – Smanjenje verovatnoće ili uticaja rizika prenošenjem dela rizika ili podelom odgovornosti za rizik sa partnerima i provajderima. Uobičajene tehnike obuhvataju kupovinu proizvoda osiguranja, angažovanjem u transakcijama hedžinga, ili angažovanjem spoljnih izvora za neku aktivnost. Dobar primer je outsourcing upravljanja infrastrukturom. U tom slučaju, partner ublažava rizike povezane sa upravljanjem IT infrastrukturom time što je partner sposobniji i ima više visoko stručnog kadra nego primarna organizacija. Rizik se može ublažiti i prenošenjem troškova ostvarenog rizika na neko osiguravajuće društvo.
- *Prihvatanje rizika* – Ne preduzimaju se akcije (mere) za uticanje na verovatnoću ili uticaj rizika. Neki rizici su mali, jer je njihov uticaj i verovatnoća pojave je niska. U ovom slučaju, svesno se prihvata rizik kao trošak poslovanja kada je to odgovarajuće. Takav rizik se periodično razmatra, kako bi se osiguralo da njegov uticaj i dalje ostane mali.

Prilikom utvrđivanja reagovanja na rizik menadžment treba da razmotri stvari kao što su:

- Efekti potencijalnih odgovora na verovatnoću i uticaj rizika – i koji odgovori su u skladu sa tolerancijom rizika entiteta.
- Troškovi nasuprot koristi potencijalnih odgovora.
- Moguće prilike da se postignu ciljevi koji idu dalje od bavljenja specifičnim rizikom.

Za značajne rizike entitet po pravilu razmatra potencijalne odgovore iz niza opcija odgovora. Na ovaj način se doprinosi da izbor odgovora bude temeljan i stvaraju se izazovi za *status quo*.

6. ZAKLJUČAK

Opšti zaključak je da u većini organizacijama ne postoje adekvatni i efikasni procesi upravljanja IT rizicima. Nedostaju formalni okviri upravljana rizicima ustanovljeni na ISO standardima, na prvom mestu ISO 27005 standardom, koji bi obuhvatali identifikovanje i merenje, odnosno procenu rizika, kao i njegovo ublažavanje, praćenje i kontrolu. Ogranizacije koje su najdalje odmakle u upravljanju IT rizicima su banke i telekomunikacione kompanije, posebno one čiji su vlasnici iz inostranstva. Prepreka boljem upravljanju je nedostatak kulture upravljanja IT rizicima i nedovoljna primena COBIT okvira. Za IT stručnjake to nije atraktivan posao, što dakazuje neznatan broj profesionalnih sertifakata za upravljanje IT rizicima i CISA revizora.

Sve organizacije treba da izgrade i uspostave procese upravljanja IT rizicima, respektujući njihovu veličnu i kompleksnost poslovanja i primene informacione tehnologije. Upravljanje rizicima u Republici Srbiji je još u razvoju. Pomake u ovoj disciplini treba obezbediti donošenjem odgovarajućih zakona i regulative, koja respektuje relevantne međunarodne standarde za upravljanje rizicima. Na ovaj način organizacije bi se naterale na donošnje okvira za upravljanje IT rizicima na metodološki ispravan način. Adekvatno upravljanje IT rizicima bi rezultiralo smanjenjem gubitaka. Organizacije koje nemaju dovoljno resursa i osposobljene kadrove za ustanovljavanje procesa upraljanja IT rizicima treba da koriste spoljne usluge specijalizovanih provajdera.

Proces upravljanja rizikom je stalni iterativni proces. Mora se neograničeno ponavljati. Poslovno okruženje se stalno menja i nove opasnosti i osetljivosti se dešavaju svakog dana.

Mogućnost ublažavanja rizika u oblasti IT zavisi od ocenjivanja rizika. Viši menadžment treba da identifikuje, oceni, kontroliše i prati tehnologiju da bi izbegao rizike koji predstavljaju opasnost (ugrožavaju) bezbednost i pouzdanost određene organizacije. Organizacija treba (1) da planira korišćenje tehnologije, (2) oceni rizik povezan sa tehnologijom, (3) da utvrdi kako da primeni tu tehnologiju, i (4) da ustanovi proces za ocenjivanje i monitoring rizika koji se preuzima. Sve organizacije treba da imaju:

- Efikasan proces planiranja koji je u skladu sa IT ciljevima i poslovnim ciljevima;
- Stalni proces ocenjivanja rizika kojim se procenjuje okruženje i potencijalne promene;
- Procedure za primenu tehnologije koje obuhvataju odgovarajuće kontrole; i
- Ocenjivanje i monitoring kojima se efikasno utvrđuju načini za upravljanje izloženosti riziku.

LITERATURA

Blokdijk, G., Engle, C., & Brewster, J. (2008). *IT risk management guide: Risk management implementation guide, presentations, blueprints, templates : complete risk management toolkit guide for information technology processes and systems*. Brisbane, Australia: Art of Service.

Boyce, J.G., & Jennings, D.W. (2002). *Information assurance: Managing organizational IT security risks*. Amsterdam: Butterworth-Heinemann.

COSO. (2004). *Enterprise Risk Management: Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission. Preuzeto sa http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

DOI: 10.15308/Synthesis-2015-723-728

Hahn, U., Askelson, K.D., & Stiles, R. (2006). *Managing and auditing privacy risks*. Altamonte Springs, Fla: Institute of Internal Auditors.

ISACA. (2006). *CISA Review Manual 2006*. Information Systems Audit and Control Association, www.isaca.org

ISACA. (2009). *The Risk IT Framework*. Preuzeto sa http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf

ISACA. (2012). COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, USA: Information Systems Audit and Control Association.

ISO. (2005). ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems – Requirements. Preuzeto sa http://www.iso.org/iso/catalogue_detail?csnumber=42103

ISO. (2009a). ISO 31000:2009 - Risk management - Principles and guidelines. Preuzeto sa http://www.iso.org/iso/catalogue_detail?csnumber=43170

ISO. (2009b). ISO Guide 73:2009 - Risk management – Vocabulary. Preuzeto sa http://www.iso.org/iso/catalogue_detail?csnumber=44651

ISO. (2009c). IEC 31010:2009 - Risk management - Risk assessment techniques. Preuzeto sa http://www.iso.org/iso/catalogue_detail?csnumber=51073

ISO. (2011). ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management. Preuzeto sa http://www.iso.org/iso/catalogue_detail?csnumber=56742

Lientz, B. P., & Larssen, L. (2006). *Risk management for IT projects: How to deal with over 150 issues and risks*. Amsterdam: Elsevier/Butterworth-Heinemann.

Narodna banka Srbije. (2013). Odluka o minimalnim standardima upravljanja Informacionim sistemom finansijske institucije, „Službeni glasnik RS", br. 23/2013 i 113/2013. Preuzeto sa http://www.nbs.rs/export/sites/default/internet/latinica/20/sis/min_standardi_upravljanja_IT_sistemom.pdf

Quarterman, J.S. (2006). *Risk management solutions for Sarbanes-Oxley section 404 IT compliance*. Indianapolis: Wiley.

The Institute of Internal Auditors. (2007). *GAIT Methodology, A risk-based approach to assessing the scope of IT general controls*.

The Institute of Internal Auditors. (2008a). *GAIT for Business and IT Risk (GAIT-R)*. Preuzeto sa http://www.iia.nl/SiteFiles/IIA_leden/Praktijkgidsen/GAIT_ForBusiness.pdf

The Institute of Internal Auditors. (2008b). *GAIT for IT General Control, Deficiency Assessment, An approach for evaluating ITGC deficiencies in Sarbanes-Oxley Section 404 assessments of internal controls over financial reporting*. Preuzeto sa http://www.iia.nl/SiteFiles/IIA_leden/Praktijkgidsen/GAIT_ForBusiness.pdf

The Institute of Internal Auditors. (2010). GTAG 15: Information Security Governance. Preuzeto sa https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG15.aspx

The Open Group. (2010). *Technical Guide:* FAIR – ISO/IEC 27005 Cookbook. Preuzeto sa http://www.businessofsecurity.com/docs/FAIR%20-%20ISO_IEC_27005%20Cookbook.pdf

Tho, I. (2005). *Managing the risks of IT outsourcing*. Amsterdam: Elsevier Butterworth-Heinemann.

Uremović, D. (2009). *Upravljanje rizicima: Metodologije procesa upravljanja rizicima.* InfoTrend. Preuzeto sa http://www.alterinfo.hr/userfiles/Media/Upravljanje_rizicima.pdf

Wieczorek, M., Naujoks, U., & Bartlett, R. (2002). *Business continuity: IT risk management for international corporations*. Berlin: Springer.

Wiles, J., Rogers, R., & Withers, D. (2007). *Techno Security's guide to managing risks: For IT managers, auditors, and investigators*. Burlington, Mass: Elsevier.

DOI: 10.15308/Synthesis-2015-723-728