ФАКУЛТЕТ ЗА ИНДУСТРИЈСКИ МЕНАЏМЕНТ
АСОЦИЈАЦИЈА ЗА КВАЛИТЕТ И СТАНДАРДИЗАЦИЈУ СРБИЈЕ
УНИЈА ПОСЛОДАВАЦА СРБИЈЕ
XIII Научно стручни скуп "Систем квалитета услов за успешно пословање и конкурентност"
Врњачка Бања 24. - 26.11.2011. године, Хотел Бреза

OPERATIVNI RIZICI KAO TEMELJ SISTEMA UPRAVLJANJA

Zdenko Adelsberger, Buntak Krešimir, Dejan Adelsberger[1]

***Rezime**: Problem provođenja upravljanja rizicima u raznim aspektima poslovanja formalno je poprimio izuzetno veliki značaj u posljednjih nekoliko godina. Niz standarda koji su objavljeni u tom periodu su dokaz ozbiljnosti problema i potrebe njegovog rješavanja. Među raznim oblicima i područjima primjene upravljanja rizicima u svakom slučaju su operativni rizici jedni od najvažnijih i najznačajnijih. U radu se daje prikaz metodološkog pristupa upravljanju operativnim rizicima s posebnim naglaskom na procjeni rizika primjenom kvalitativne metode.*

***Ključne riječi:** rizici, upravljanje rizicima, procjena rizika, operativni rizici, kvalitativna procjena rizika*

1. UVOD

Sistemi upravljanja imaju osnovni zadatak da osiguraju funkcioniranje svih poslovnih procesa tako da ulazne zahtjeve svih zainteresiranih strana pretvore u njihovo zadovoljavanje unutar nekog poslovnog sistema. Teoretski bi to bio relativno mali problem da svaki poslovni sistema nema neki nivo entropije. To praktički znači da svaki poslovni sistem ima stohastičke karakteristike svih elemenata koji ga sačinjavaju i omogućavaju njegovo funkcioniranje. Kao posljedica se pojavljuje činjenica da za ni jedan aspekt funkcioniranja poslovnog sistema nema potpune sigurnosti u smislu da će se obaviti u potpunosti onako kako se očekuje i kako je planirano. Ta odstupanja postignute funkcionalnosti i ostvarenih ciljeva bilo kojeg poslovnog sistema od planiranih i očekivanih mogu biti toliko velika da dovode do ugrožavanja njihove održivosti i u konačnici mogu dovesti do uništenja poslovnog sistema. U cilju smanjenja entropije poslovnog sistema treba primijeniti proaktivno upravljanje čime se postiže viši nivo sigurnosti funkcioniranja sistema, a time i njegova održivost. Jedan od temelja proaktivnog upravljanja poslovnim sistemima je upravljanje rizicima kojemu je osnovna funkcija identifikacija svih mogućih situacija koje mogu ugroziti funkciju i/ili postojanje poslovnog sistema, te planiranje i provođenje akcija koje će smanjiti rizike, odnosno entropiju.

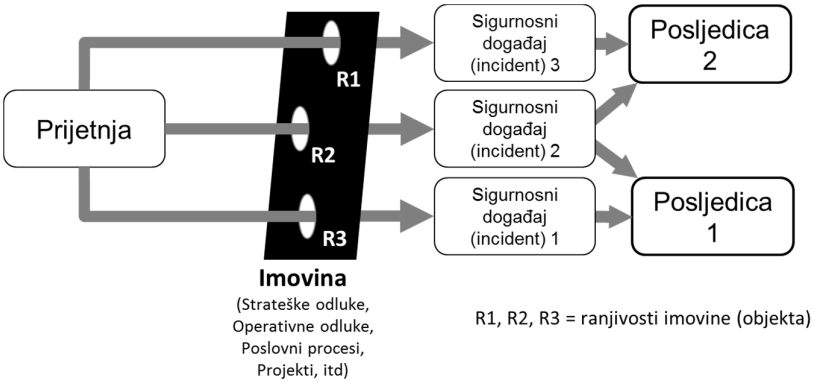
Ako se pođe od pojednostavljene definicije rizika, da je rizik vjerojatnost slučajnog događaja s posljedicama za poslovni sistem može se zaključiti da je nemoguće postići proaktivno upravljanje bez poznavanja svih potencijalnih uzroka i posljedica. Takvi slučajni događaji mogu izazvati negativne ali i pozitivne posljedice za poslovni sistem i njegovo funkcioniranje. Pojava slučajnih događaja sa pozitivnim posljedicama nije od značaja i ovdje se neće tretirati jer takvi događaji ne utječu na održivost poslovnog sistema u negativnom smislu. Međutim slučajni događaji koji imaju negativne posljedice za poslovni sistem su ključna tema problema proaktivnog upravljanja kao i problema upravljanja rizicima.

Da bi se lakše pratio nastavak pokazat će se osnovni mehanizam funkcioniranja rizika. U tom smislu definirat će se neki pojmovi,kao što su prijetnja, ranjivost i posljedica.

[1]Mr.sc. Zdenko Adelsberger, Bluefield d.o.o., Zagreb, HR, zadelsbe@zg.t-com.hr
[2]Dr.sc. Krešimir Buntak, DZM RH, Zagreb, RH, kresimir.buntak@dzm.hr
[3]Dejan Adelsberger, Bluefield d.o.o., Zagreb, RH, dejan@bluefield.hr

Pod pojmom prijetnja se podrazumijeva mogući uzrok neželjenog događaja (incidenta) koji može uzrokovati štetu sistemu ili organizaciji. Ranjivost je slabost imovine ili grupe imovina (elemenata poslovnog sistema, organizacije, procesa, projekta, itd.) koju jedna ili više prijetnji mogu iskoristiti. Posljedice su rezultat ili ishod nekog događaja. Pri tome je važno uočiti da jedan događaj može imati jednu ili više posljedica. Kao što je rečeno posljedice mogu biti pozitivne ili negativne, a mogu se izražavati kvantitativno (numerički u financijskim iznosima) ili kvalitativno (opisno).

Mehanizam pojave rizika se može opisati na slijedeći način: ako jedna ili više prijetnji iskoristi jednu ili više ranjivosti objekta (imovine) može doći do neželjenih posljedica. U koliko se to desi govori se da je došlo do sigurnosnog događaja, odnosno incidenta. Grafički prikaz fizikalnog procesa rizika prikazan je slici 1.



Slika 1. Fizikalni princip pojave rizika

Na slici se može vidjeti da je problem pojave rizika u pravilu vrlo složen i višedimenzionalni problem, odnosno da zavisi od niza faktora koji se dijelom mogu kontrolirati u određenim granicama, ali i niz faktora su van domašaja i utjecaja poslovnog sistema, odnosno organizacije.

2. POJAM I ZNAČAJ OPERATIVNOG RIZIKA

Prema svom mjestu gdje se rizici mogu pojaviti, njihovom znanju i potencijalnim posljedicama realizacije događaja sa negativnim učinkom (incidentima) može se razlikovati niz vrsta. Neke od takvih vrsta rizika su: strateški, operativni, procesni, projektni, aspekata okoliša, itd. Na slici 2. Je prikazana shema integralnog rizika organizacije s kratkim opisom gdje je usmjeren i kako nastaje neki od tih rizika.

Slika 2. Integracija rizika u organizaciji

Za daljnje razmatranje neće se ulaziti u diskusije vezane za kreditne, poslovne i tržišne rizike. Pažnja će biti usmjerena samo na operativne rizike.

Operativni rizik se definira kao rizik od gubitka koji nastaje zbog neadekvatnih ilipogrešnih internih procesa, pogrešaka koje su uzrokovaliljudi i sistemi ili kao rezultatvanjskih događaja. Ova definicija obuhvaća pravni rizik, ali isključuje strateški rizik irizik reputacije[4]. Definicija je uzeta iz područja bankarstva i njihovog dokumenta Basel II u kojem je praktički precizno i sveobuhvatno dana definicija koja je primjenljiva u svim vrstama organizacije. U tabeli 1 su dani primjeri uzroka operativnog rizika s nekim od vrsta događaja koje mogu biti izazvani od strane nekog uzroka.

Iz tabele 1 se može vidjeti da postoji niz događaja koje mogu izazvati prikazani uzroci. Naravno da je tu prikazan samo manji dio potencijalno mogućih i to onih najčešćih događaja. Praktički nema organizacije koja se ne susreće sa navedenim događajima u svom poslovanje, ili

barem dijelom njih. Postavlja se pitanje, zar je moguće provesti upravljanje organizacijom i osigurati viši nivo njene sigurnosti, a ne voditi računa o operativnim rizicima i pripremiti određene aktivnosti i radnje kojima bi se smanjili efekti pojave događaja?

Tabela 1. MATRICA DOGADJAJA KOJI SU IZVOR OPERATIVNOG RIZIKA PO VRSTAMA UZROKA

Uzrok	Kategorija događaja
Ljudski faktor	Neovlašćene aktivnosti Krađe i prevare zaposlenih Unutrašnji sistem sigurnosti Odnosi prema zaposlenima Različitost i diskriminacija Ne odgovarajuća poslovna ili tržišna praksa
Procesi	Sigurnost radnog okruženja Prikladnost, transparentnost i povjerljivost Greške u proizvodima i uslugama Selekcija, sponzorstvo i izloženost prema klijentu Savjetodavne aktivnosti Nezgode i opća sigurnost Upravljanje procesima, obuhvaćanje i izvršenje transakcija Nadzor i izvještavanje Prijem klijenata i adekvatnost dokumentacije
Sistemi	Neadekvatnost, neefikasnost, loše funkcioniranje ili pad IT sistema
Eksterni faktor	Krađe i prijevare (od strane trećih lica) Vanjski sistem Sigurnosti Druge namjerne aktivnosti Prirodne nepogode Katastrofe prouzrokovane ljudskim faktorom Politički i zakonski rizik (Javne usluge/informacije) neraspoloživost dobavljača Poslovni partneri Prodavači i dobavljači

Vjerojatno nema organizacije koja barem po nekim potencijalnim događajima iz tabele 1 ne vodi računa. No, to je najčešće na niskom nivou organiziranosti bez sistemskog pristupa. Koliki i kakav nivo pripreme i borbe protiv incidenata ï sigurnosnih događaja neka organizacija primjenjuje vezano za operativne rizike zavisi u prvom redu od svijesti vrhovne uprave, ali i znanja i vještinaljudi koji bi se trebali baviti tim aktivnostima. Na slici 3 je prikazana shema nivoa zrelosti upravljanja operativnim rizicima. Može se vidjeti da viši nivo zrelosti upravljanja operativnim rizicima zahtjeva i viši nivo sofisticiranosti ljudi uključenih u proces upravljanja rizicima. Opća mjera sposobnosti zaposlenika da dođu na viši nivo sofisticiranosti borbe protiv operativnih rizika se može prepoznati iz poticanja vrhovne uprave za edukacijom i treningom timova koji su zaduženi za te poslove. U koliko je količina edukacije malena ili nikakva, direktna posljedica je i vrlo niski nivo sposobnosti borbe protiv operativnih rizika.

Slika 3. Stupnjevanje zrelosti upravljanja operativnim rizikom

3. EVIDENCIJA SIGURNOSNIH DOGAĐAJA VEZANIH ZA OPERATIVNE RIZIKE

Najjednostavniji nalin dokazivanja i uvjeravanja vrhovne uprave (ili bilo koga drugog) unutar neke organizacije je prvo napraviti evidenciju sigurnosnih dogaLaja vezanih za operativne rizike. Ta evidencija koja ima u biti ulogu stvaranja statistilke povijesti vezane za operativne rizike unutar organizacije predstavlja u organiziranom sistemu upravljanja rizicima trajnu obavezu. Podaci iz takve evidencije se mogu koristiti za procjenu operativnog rizika i optimalnog odreLivanja nalina borbe unutar organizacije za viši nivo sigurnosti. U tu svrhu se može primijeniti predložak evidencije incidenata prikazan u tabeli 2. Svaka organizacija treba razviti svoj nalin evidencije, ali prikazani primjer dobro ilustrira što se obilno registrira za svaki incident.

Tabela 2. Primjer evidencije incidenata operativnih rizika

Red Br	Datum početka događaja	Org. jed.	Vrsta događaja ID	Status ID	Uzrok ID	Tip ID	Opis događaja	Predložena mjera

Podaci koji se upisuju u kolone oznale sa ID parametrom za statuse, uzroke i tip gubitka/dobiti prikazani su u tabeli 3.

Tabela 3. Primjer šifriranja statusa, uzroka i tipa gubitaka/dobiti operativnih rizika

Status	ID
Otvoren	1
Istražuje se	2
Kompletiran	3
Odobren	4
Zatvoren	5

Uzrok	ID
Ljudski faktor	1
Procesi	2
Sistemi	3
Vanjski faktor	4

Tip gubitka/dobiti	ID
Gubitak	1
Operativna dobit	2
Izbjegnuti gubitak	3
Propuštena dobit	4

U tabeli 4. se nalaze podaci i pripadne šifre za klasifikaciju dogaLaja na dva nivoa (kategorija i podkategorija). U praksi se koristi daljnja razrada u još niže podkategorije što doprinosi boljoj analizi dogaLaja i njihovog pozicioniranja unutar poslovnog sistema organizacije.

Tabela 4. Matrica za klasifikaciju vrsta događaja koji mogu prouzrokovati operativne rizike i gubitke

Kategorija operativnih rizika	ID	Potkategorija
Interne prevare i aktivnosti Gubici uslijed namjernih aktivnosti ili propusta koji uklju uju najmanje jednu osobu koja radi za organizaciju ili u organizaciji. Bitno je da postoji "namjera" da se stekne lina korist.	11	**Neovlaštene aktivnosti** Gubici prouzrokovani krenjem zakona,ugovora, internih pravila i procedura.
	12	**Krađa i prevara** Gubici prouzrokovani postupcima ji je cilj lina ekonomska dobit/korist
	13	**Unutrašnji sistem sigurnosti** Gubici prouzrokovani nedozvoljenim pristupom i korištenjem informacija iz bankarskog IT sistema, zlonamjerna manipulacija, i oštelenje ili brisanje podataka, neovlaštena upotreba IT sistema, od strane zaposlenih
Eksterne prevare i aktivnosti Gubici uslijed namjernih postupaka uinjenih od strane trelih lica. Preovladava "namjeran" i "zlonamjeran" koncept, i stoga su ovdje uklju eni postupci podvale i zloupotrebe ili izbjegavanje zakona i regulativa, propisa i politike organizacije.	21	**Krađe i prevare** Gubici prouzrokovani postupcima ji je cilj osobna ekonomska dobit
	22	**Vanjski sistem sigurnosti** Gubici prouzrokovani nedozvoljenim pristupom ili pokušajem pristupa bankarskom IT sistemu od strane treleg lica sa ciljem da se manipuliraju/prisvoje/oštete podaci odnosno resursi banke
	23	**Druge namjerne aktivnosti** Gubici uslijed namjerno prouzrokovane štete organizaciji ali bez line koristi za poinioca štete
Odnos prema zaposlenima i sigurnost na radnom mjestu Gubici uslijed ne primjenjivanja zakona o redu i drugih regulativa vezanih za rad,	31	**Odnosi prema zaposlenima** Gubici zbog krenja odredbi zakona o radu.
	32	**Sigurnost radnog okruženja** Gubici zbog neprimjenjivanja zakona i regulativa vezanih za zdravstvenu i socijalnu zaštitu i sigurnost na radnom mjestu

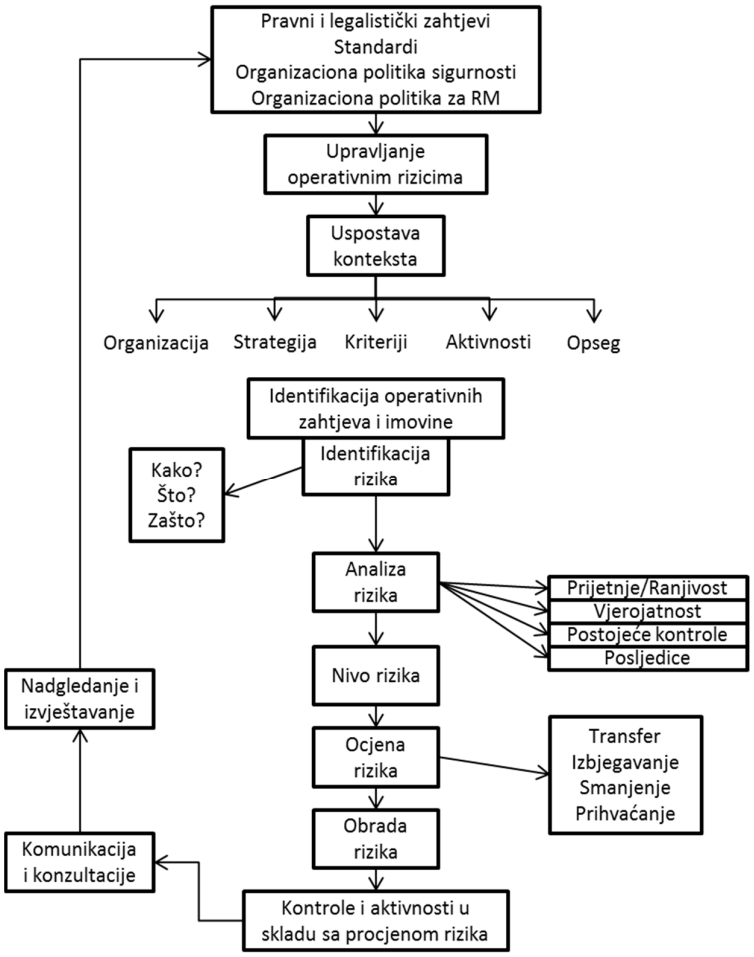
zapoġljavanje. zdravstvenu i socijalnu zaġtitu i sigurnost na radnom mjestu.	33	**Različitost i diskriminacija** Gubici zbog bilo kog oblika diskriminacije zaposlenih.
Klijenti, proizvodi i poslovna praksa Gubici proistekli iz nenamjernih ili nemarnih propusta u ispunjavanju profesionalnih obaveza prema klijentima, ili zbog prirode ili konstrukcije proizvoda	41	**Prikladnost, transparentnost i povjerljivost**
	42	**Ne odgovarajuća poslovna ili tržišna praksa**
	43	**Greške u proizvodima i uslugama** Gubici zbog greġaka u proizvodima/uslugama/modelima ili greġke u ugovorima
	44	**Selekcija, sponzorstvo i izloženost prema klijentu** Gubici zbog greġaka u selekciji klijenata, u analizi potreba klijenata ili prekoraļenja limita izloġenost
	45	**Savjetodavne aktivnosti** Gubici zbog sporova sa klijentima u vezi savjetodavnih aktivnosti, ako je aktivnost regulirana ugovorom
	46	**Nezgode i opća sigurnost** Gubici uslijed nezgoda koje prouzrokuju ġtetu ili povrede treĆim licima
Štete na fiksnoj imovini OġteĆenja fiksne imovine zbog prirodnih katastrofa i drugih dogaĽaja	51	**Prirodne nepogode** OġteĆenja fiksne imovine (zgrade, infrastrukture,...) i ljudski gubici zbog prirodnih katastrofa
	52	**Katastrofe prouzrokovane ljudskim faktorom** OġteĆenja fiksne imovine (zgrade, infrastrukture,...) i ljudski gubici zbog prirodnih katastrofa
	53	**Politički i zakonski rizik** Gubici zbog politiļkih ili zakonskih promjena
Prekid u poslovanju i pad sistema Gubici zbog neraspoloġivosti/ nedostataka/neefikasnosti IT sistema/dobavljaļa komunalnih i informacijskih usluga. Gubici zbog loġeg funkcioniranja hardvera i softvera, strukturne neadekvatnosti, telekomunikacijskih nedostataka itd.	61	**Neadekvatnost, neefikasnost, loše funkcioniranje ili pad IT sistema** Gubici vezani za tehniļke probleme sistema: neraspoloġivost, neefikasnost, pad ili poremeĆaj u IT sistemu (hardver, softver, telekomunikacije)
	62	**(Javne usluge/informacija) neraspoloživost dobavljača** Gubici zbog vanjskih usluga i koriġtenja dobavljaļa

U koliko u organizaciji ne postoji takva evidencija sama procjena rizika za pojedine dogaĽaje se temelji na iskustvu drugih organizacija i pretpostavkama kakva je situacija u vlastitoj organizaciji. Na temelju tako pretpostavljenih podataka i sama procjena rizika po kvalitativnoj metodi moġe biti relativno netoļna.

4. PROCES UPRAVLJANJA OPERATIVNIM RIZICIMA U ORGANIZACIJI

Problem identifikacije uzroka, mjesta, frekvencije, posljedica itd. vezanih za incidente operativnih rizika predstavlja proces koji tokom vremena treba razviti poboljġanjima na prihvatljivi nivo zrelosti. Nezgodna stvar je u tome ġto se do te zrelosti moġe doĆi prvenstveno vlastitim zaposlenicima, kao najboljim poznavaocima stanja i moguĆnostima po pitanjima prijetnji i ranjivosti svakog dijela organizacije s toļke gledigta operativnog rizika. Tu su vanjski konzultanti u biti nemoĆni bez suradnje zaposlenika. Odnosno vanjski konzultanti su za pitanje uspostave i poboljġanja procesa za upravljanje (operativnim) rizicima pogodni da interni tim uspostavljen u organizaciji u struļnom smislu pomaġu, a praktiļni postupci i rezultati rada tog procesa trebaju biti od strane internih ljudi, prvenstveno ļlanova tima za upravljanje rizicima, ali i ostalih zainteresiranih strana. Zbog toga je od presudnog znaļaja edukacija i trening tima za upravljanje rizicima koji predstavljaju profesionalnu jezgru u organizaciji. U velikim organizacijama, bankama i drugim financijskim institucijama obiļno se formira posebni odjel za rizike sastavljen od kompetentnih struļnjaka.

Prednost u odnosu na proces upravljanja rizicima je njegova univerzalnost. To znaļi da sam proces po svojoj strukturi i aktivnostima ne zavisi od veliļine i djelatnosti organizacije. Zbog toga za proces upravljanja rizicima postoji poseban standard odnosni niz standarda iz serije ISO 31000 [1,2,3]. Standard ISO 31000 opisuje generiļki proces za upravljanje rizicima i pogodan je za sve vrste rizika u svim podruļjima, ġto znaļi i i za upravljanje operativnim rizicima. Modificirana blok shema procesa za upravljanje rizicima prema ISO 31000 prikazana je na slici 4.



Slika 4. Blok shema procesa za upravljanje rizicima (na temelju ISO 31000:2009)

Iz priloģene blok sheme na slici 4 moģe se vidjeti da proces upravljanja rizicima relativno sloģen i da ima niz podprocesa koji se u pojedinim sluļajevi podruļja primjene mogu drugaļije realizirati. Npr. identifikacija operativnih zahtjeva i imovine, kao i identifikacija rizika moģe se razlikovati za podruļje informacijske sigurnosti (ISMS), procesne rizike, upravljanje zaģtitom ģivotne sredine (EMS), operativnih rizika, itd. MeĽutim, proces je u potpunosti jednak u svakom sluļaju i jedinstven za sve vidove rizika u organizaciji. Detaljni opis procesa se nalazi u okviru standarda ISO 31000.

5. ZAKLJUČAK

Iz gore iznesenog moģe pokazati da problem operativnog rizika je sastavni dio bilo kakvih aktivnosti u organizaciji i nemoguĹe je njih isključiti. Utjecaj realizacije operativnih rizika kroz posljedice incidenata moģe biti izuzetno ģtetan za organizaciju pa se u normalnom poslovanju treba oļekivati angaģman vrhovne uprave na poduzimanju aktivnosti za spreļavanje pojave incidenata, odnosno, na smanjenju vjerojatnosti njihovih pojava. To ima za posljedicu da Ĺe borba protiv incidenata operativnih rizika imati direktan utjecaj na poveĹanje viģka vrijednosti u organizaciji. To poveĹanje viģka vrijednosti se moģe promatrati u svjetlu ne troģenja sredstava na sanacijama posljedica incidenata.

Uspjeģno provoĽenje borbe protiv operativnih rizika podrazumijeva u prvom redu uļinkovitu i efikasnu implementaciju procesa za upravljanje rizicima sa potrebnim resursima i kompetentnim timom.

LITERATURA

1. ISO 31000:2009, Riskmanagement -- Principlesandguidelines
2. ISO 31010:2009, Riskmanagement -- Riskassessmenttechniques
3. ISO Guide 73:2009, Riskmanagementï Vocabulary
4. Basel II, *InternationalConvergenceof Capital Measurementand Capital Standards*, Bank for InternationalSettlements, 2004
5. CarolAlexander, *OperationalRisk*, Financial TimesPrenticeHall, 2003
6. ChernobaiAnna S., *OperationalRisk: A Guide To BaselII Capital Requirements, Models, AndAnalysis (Frank J. FabozziSeries)*, Wiley, 2007
7. Da Costa Lewis, Nigel, *OperationalRiskWith Excel AndVba: Applied StatisticalMethods For Risk Management*, Wiley, 2004
8. Dickstein, Dennis I.,*No Excuses*, Wiley, 2009
9. MoosaImad A., *OperationalRisk Management (FinanceAnd Capital Markets)*, Palgrave Macmillan, 2007
10. ReuvidJonathan, ManagingBusinessRisk: A PracticalGuide To ProtectingYourBusiness, Kogan Page, 2008
11. ChorafasDimitris N., *OperationalRiskControlWithBaselII: BasicPrinciplesAnd Capital Requirements*, Butterworth-Heinemann, 2003
12. Tarantino Anthony, *Manager's Guide To Compliance: Sarbanes-Oxley, Coso, Erm, Cobit, Ifrs, BaselII, Omb's A-123, Asx 10, OecdPrinciples, TurnbullGuidance, Best Practices, AndCaseStudies (Manager's GuideSeries)*, Wiley, 2006