FBIM Transactions
DOI 10.12709/fbim.04.04.01.11

AKTIVNI PRISTUP U OTKRIVANJU INTERNIH PREVARNIH RADNJI ANALIZOM PODATAKA IZ INFORMACIONOG SISTEMA

ACTIVE APPROACH IN DETECTION OF INTERNAL FRAUDULENT ACTS ANALYZING RAW DATA FROM INFORMATION SYSTEM

Predrag M. Simić
Komercijalna banka a.d. Beograd, Beograd, Srbija

Luka Milinković
Komercijalna banka a.d. Beograd, Beograd, Srbija

Milorad Jović
Komercijalna banka a.d. Beograd, Beograd, Srbija

JEL kategorija: **C51, C52, D82, D83**

Apstrakt

U radu su izneta iskustva autora u oblasti otkrivanja prevarnih radnji kroz rad u internoj i eksternoj reviziji. Na osnovu istraživanja u oblasti internih kontrola i bezbednosti informacija formiran je jedan model aktivnog pristupa u otkrivanju sumnjivih (internih prevarnih) radnji analizom podataka iz informacionog sistema, koji prezentujemo u ovom radu. U radu je ukazano na prednosti aktivnog pristupa zasnovanog na ukrštanju testova, koji ukazuju na sumnjive transkacije u odnosu na reaktivan pristup, koji se zasniva na žalbama klijenata, anonimnim dojavama i sl.

Ključne reči: *Finansijske zloupotrebe, IT revizija, indikatori prevare, sumnjive transakcije.*

Abstract

The paper contains authors' experience in detection of fraudulent activities by working with internal and external audit. Based on research in the area of internal controls and information security, authors established an active model approach in detection of internal fraudulent acts analyzing raw data from information system. The paper points out the advantages of an active approach based on

Adresa autora zaduženog za korespodenciju:
Predrag Simić
simicpredrag@yahoo.com

intersection tests that indicate suspicious transactions in relation to the reactive approach, which is based on customer complaints, anonymous tips, etc.

Key words: *Financial fraud, fraud indicators, IT audit, suspicious transactions.*

1 UVOD

Svaki dan se preko sredstava masovne komunikacije možemo informisati o brojnim internim prevarama u različitim kompanijama. One se mogu javiti u svakoj kompaniji i ne moraju podrazumevati samo krađu papirnog i elektronskog novca, već mogu biti vezane i za robu, ugovore, osiguranje, bankarske usluge itd. Prevare mogu počiniti zaposleni, dobavljači, osobe koje poznajemo ili ih nikada nismo i nećemo videti, kao što su prevare preko Interneta. Pojedine tehnike prevara su stare, i veoma poznate, ali postoje i nove sa kojima se po prvi put srećemo (Simon, Mitnick, & Wozniak, 2002), (Davis, Schiller, & Wheeler, 2011). Pojedine prevare, zbog reputacionog rizika, kompanije ne žele da objave.

Najveći broj internih prevara se dešava u marketingu, distribuciji i nabavci. Ove prevare, uglavnom, nisu velike, pa ih kompanije tolerišu. Sa druge strane, kod finansijskih institucija su česte prevare na šalterima ili bankomatima sa kreditnim karticama. Jedna uspešna prevara ovog tipa daleko je veća u obimu od drugih vidova internih prevara.

U internim prevarnim radnjama učestvuju osobe, koje dobro poznaju sistem internih kontrola i informacioni sistem koji podržava poslovanje što im omogućava da zaobiđu postojeće kontrole. U najvećem broju slučajeva zbog jednostavnosti i sprečavanja širenja informacija prevare osoba obavlja prevare sama. Pored klasičnih eksternih prevarnih radnji postoje i kombinovane interno-eksterne prevarne radnje, koje uključuju bitne insajdere unutar kompanija. Trend u prevarama je angažovanje insajdera od strane određene ekipe, koja istu tehniku prevarnih radnji ponavlja u više kompanija uglavnom u različitim državama (Rawsthorne, 2014).

Svaka kompanija bi trebala da analizira i proračunava rizike u svom poslovanju kao i da implementira odgovarajuće mere zaštite kroz sistem internih kontrola (ISO 31000, 2009). Zajednički rizik za kompanije, nezavisno od tipa poslovanja, je upravo rizik od internih i eksternih prevarnih radnji. Ovaj rizik se teško može izračunati ili predvideti, ali menadžment svake kompanije treba da ga bude svestan. Kada se prevara dogodi potrebno je da rukovodstvo bude spremno na saniranje posledica da bi se obezbedilo uspešno prevazilaženje krizne situacije (Iyer & Samociuk, 2007).

Rizik od prevare spada u operativne rizike i kod banaka se mora uzeti u obzir prilikom proračuna adekvatnosti kapitala (NBS, 2014). Proračun se radi svake godine, pa tako svaka prevara, koja se desi u prethodnoj godini utiče na povećanje obaveznih rezervisanih sredstava za narednu, ali i za sledeće godine, jer se posmatra istorija operativnih rizika. Ako se pri tome desi da se prevara uoči kasno i da je teško povratiti izgubljena sredstva kompaniju mogu zadesiti i drugi mnogo ozbiljniji problemi, koji mogu u potpunosti ugroziti dalje poslovanje.

Istraživanja koja se periodično sprovode pokazuju da kompanije zbog internih prevara gube u proseku od 5% do 7% godišnje dobiti (Samociuk, Iyer, & Doody, 2010). Jedan deo izgubljenih sredstava najčešće uspeju da povrate, ali je to manji deo ukupnih gubitaka. Zato je veoma važno da svaka kompanija koja se suočava sa ovim problemom uspostavi aktivni pristup u sprečavanju i otkrivanju prevara.

Uvođenjem sistema internih kontrola menadžment pokušava da onemogući da se dogode prevare (ISO 27001, 2013), ali ne ulaže sredstva u njihovo otkrivanje. Kontrole se razlikuju među preduzećima i ne postoji jedinstven način zaštite. Najčešći problem, koji se desi jeste da kompanija misli da je sigurna i da u njoj nema prevare, jer je uspostavila veliki broj internih kontrola. Rano uočavanje prevare povećava verovatnoću da se povratiti veći deo gubitka. Zatim, sprečavaju se dalje zloupotrebe od strane istog radnika, kao i moguće nove prevare od strane drugih radnika, a zaposlenima se ukazuje na to da se svaka prevara može otkriti.

Zbog toga što većina kompanije nama aktivan pristup u otkrivanju prevarnih radnji one su prinuđene na reaktivan pristup, koji podrazumeva anonimne dojave, žalbe klijenata i dobavljača i sl.

Zato se prevarne radnje otkrivaju znatno kasnije pa nekada i prekasno. Prevare sa velikim obimom krađe su jedan od najstresnijih događaja po kompaniju, naročito ako menadžment na to nije pripremljen. Posledice su velike i mogu dovesti do trajnog gubitka sredstava, otpuštanja, tužbi, pa čak i do propadanja kompanije.

2 INDIKATORI SUMNJIVIH TRANSAKCIJA

Poslovne aplikacije u sebi uglavnom nemaju funkcionalnosti na osnovu kojih bi se otkrivale prevarne radnje. To je normalno, jer je osnovna namena tih aplikacija da podrže određeni poslovni proces. Međutim, u bazama podataka, koje koriste poslovne aplikacije ostaju zabeleženi podaci na osnovu kojih je moguće kreirati definisane opšte i specifične indikatore, koji bi preko sumnjivih transakcija ukazivali na prevarne radnje.

Opšti indikatori su skup pravila, koja su primenjiva na veliki broj oblasti poslovanja. Oni su proizašli iz duha vremena i načina organizacije poslovanja u informatičkom dobu, koja je oslonjena na korišćenje aplikacija informacionog sistema, koje u presudnoj meri podražavaju razne poslovne procese. Oni proizilaze i iz relativno standardnog modela poslovnih aplikacija zasnovanog na relacionim bazama podataka, koje u sebi pored ostalog sadrže sistem personalizovanih korisničkih naloga i organizaciju koja podrazumeva glavne evidencije, pomoćne evidencije, istorije promena, razne šifarnike itd. Tako se u tabelama uglavnom prate razni podaci poput datuma i vremena kada je izvršena određena transakcija, informacija o korisniku, koji je obavio transakciju, iznos i opis transakcije, kao i razni drugi detalji.

Opšti indikatori, koji ukazuju na sumnjive transakcije mogu biti:

- Transakcije obavljene preko korisničkih naloga radnika, koji tog dana nisu bili na poslu;
- Transakcija koja je obavljena van radnog vremena, vikendom ili praznikom;
- Transakcija od strane osobe, koje uobičajeno ne obavljaju tu vrstu posla;
- Transakcija bez opisa ili sa ključnim rečima, koje ukazuju na sumnju;
- Transakcije ispod određenog limita za koji je potrebna dodatna kontrola ili dozvola;
- Transakcije sa specifičnim iznosom (na primer 1.000.000,00; 5.000.000,00 RSD);
- Transakcija kod kojih se datum unosa i datum na koji se odnosi transakcija značajno razlikuju;
- Iznosi koji se veoma često ponavljaju i sl.

Specifični indikatori, koji ukazuju na sumnjive transakcije zavise od konkretnih oblasti poslovanja. U svakoj oblasti poslovanja postoje odgovarajuće radne procedure i poslovne aplikacije u kojima je manje ili više ugrađen sistem internih kontrola, koji pored ostalog služi i za sprečavanje prevarnih radnji. Jedan primer takve kontrole u bankarskom poslovanju može biti i kontrola, koja onemogućava šalterskom radniku da sam sebi lično isplati novac ili uruči čekove. U sistem internih kontrola je nemoguće ugraditi sve kontrolne mehanizme, koji bi sprečavali prevarne radnje. Često se određena radna procedura sprovodi i istovremenim korišćenjem više poslovnih aplikacija između kojih je teško implementirati kontrolne mehanizme u realnom vremenu. Prevarne radnje su nuspojava, koju treba sprečiti, ali ne prekomernom ugradnjom kontrolnih mehanizama, jer su oni direktno suprotstavljeni efikasnosti rada, što je bitno za čitav niz pitanja od odnosa prema klijentima do profitabilnosti. Specifični indikatori treba da ukazuju na transakcije, koje su prošle kroz sistem internih kontrola. Ovi indikatori posmatraju normalne transakcije, koje su odrađene uz pomoć poslovnih aplikacija, ali iz određenog, za tu vrstu posla specifičnog pogleda, tako oblikovanog da razdvajaju sumnjivo od uobičajenog. Prevarna radnja se u stvari vrši simulacijom regularne, normalne transakcije kroz informacioni sistem i obavlja se uz poštovanje značajnog dela propisanih radnih procedura uz eksploataciju „rupe“ u sistemu internih kontrola. To se često radi na papirnoj dokumentaciji (falsifikovanjem ili nedostatkom), koja naravno nije svima dostupna, već stoji sklonjena u nekom registratoru ili arhivi.

Tako, u bankarskom poslovanju kod poslova štednje specifični indikator, koji ukazuje na prevarnu radnju može biti neuobičajeno veliki broj razoročenja štednih uloga u određenom periodu, koji je obavljen od strane istog radnika. Veliki broj transakcija preko platnih kartica, koji je urađen u kratkom vremenskom periodu ukazuje na

mogućnost krađe kartice. Sa druge strane, u oblasti mobilne telefonije to može biti aktivnost korisnika, koja statistički značajno odudara od uobičajenog načina potrošnje, što ukazuje na eventualnu krađu telefona ili dupliciranje i zloupotrebu kartice korisnika.

Specifični indikatori za pojedine oblasti poslovanja su u osnovi isti, ali se mogu u brojnim detaljima međusobno razlikovati od banke do banke, od jedne do druge osiguravajuće kuće (Mihajlović, 2014), proizvodnog preduzeća ili telekomunikacionog operatera. Razlog za to je razlika u unutrašnjoj organizaciji, proizvodima, radnim procedurama, sistemu internih kontrola, aplikacijama informacionog sistema i njihovoj konfiguraciji.

3 TESTOVI ZA OTKRIVANJE SUMNJIVIH TRANSAKCIJA

Ovi testovi se uglavnom grade na osnovu definisanog opšteg ili specifičnog indikatora sumnjivih transakcija ili na osnovu njihove kombinacije. Test predstavlja konkretnu realizaciju okruženja u kome će se određeni indikator ispoljiti.

Testovi mogu biti osmišljeni i sprovedeni jedino na osnovu raspoloživih podataka, koji se prate preko poslovnih i drugih aplikacija. Ukoliko se pojedini bitni elementi na koje indikator ukazuje ne prate u odgovarajućim tabelama kroz aplikacije informacionog sistema ili ih je nemoguće jednoznačno odrediti onda taj test neće biti moguće realizovati.

3.1 Izvori podataka i načini realizacije testova

Pojedine testove je nemoguće realizovati korišćenjem podataka iz jedne aplikacije, već samo ukrštanjem i povezivanjem podataka iz više aplikacija i sistema. Na primer, opšti indikator, koji se tiče transakcija, koje su obavljene od strane korisničkog naloga radnika, koji tog dana nije bio na poslu je nemoguće realizovati bez povezivanja podataka iz konkretne poslovne aplikacije sa sistemom za evidenciju radnog vremena. Izrada testova podrazumeva visok stepen znanja o funkcionisanju poslovnih aplikacija, načinima kako su međusobno povezani i strukturi njihovih baza podataka. To znači da je potrebno znatno angažovanje programera, projektanata, sistemskih i poslovnih analitičara i eventualno dobavljača, koji su isporučili određene poslovne aplikacije ukoliko je stepen njihovog poznavanja u organizaciji mali.

Testovi se mogu realizovati na dva načina. Prvi je u formi uskladištenih procedura na produkcionim bazama podataka. To može predstavljati problem zbog opterećenja i usporenja redovnog rada korisnika sistema, pa zato testove treba obavljati van radnog vremena. Drugi način podrazumeva angažovanje specijalizovanih IT sistema za prikupljanje i analizu podataka, koji ne opterećuje produkciono okruženje. S obzirom da se podaci za testove prikupljaju i povezuju sa više različitih poslovnih aplikacija i drugih sistema najprirodnije mesto za objedinjavanje podataka i realizaciju testova je *Datawarehouse* sistem. Od velike koristi mogu biti i tzv. *Database audit* softverski alati, koji u realnom vremenu mogu preuzimati i dalje analizirati podatke sa produkcionih sistema bez njegovog opterećivanja obzirom da podatke prikupljaju sa mreže filtrirajući saobraćaj, koji se odnosi na baze podataka. SIEM (*Security Information and Event Management*) sistemi se, takođe, mogu koristiti za izradu ovakvih testova, jer su pored ostalog namenjeni prikupljanju i analizi log fajlova. To čak podrazumeva i proaktivni pristup u izradi poslovnih aplikacija, tj. ugrađivanje kontrolnog mehanizma, koji bi komunicirao preko aplikativnog log-a. Na ovaj način bi se u njega upisivali svi bitni događaji čijom bi se analizom kroz SIEM sistem mogli realizovati testovi. Preko ovakvog sistema bi se gotovo u realnom vremenu mogli beležiti sumnjive transakcije na šalterima raznih kompanija, gde se rade gotovinske uplate u slučajevima kada se ona stornira. Ukoliko se nakon određenog vremena uplata ne ponovi to ukazuje na sumnjivu transakciju. Na taj način bi se mogle razdvojiti normalno stornirane transakcije, čiji je uzrok greška u kucanju ili greška u odabiru računa od sumnjive transakcije, koja je mogla rezultirati prevarnom radnjom otkazivanjem transakcije i prisvajanjem novca klijenta.

3.2 Vremenski okvir za testiranje

U zavisnosti od situacije i potrebe vremenski okvir u kome se posmatraju i analiziraju prevarne radnje može biti različit. Prevarne radnje je veoma teško otkrivati u realnom vremenu, tj. relativno brzo

nakon što su počinjene. Razlog za to je kumulativna i agregatna priroda većine indikatora i odgovarajućih testova što zahteva određeno vreme. Pravilniji pristup za otkrivanje prevarnih radnji je periodična, ciklična provera, koja bi obuhvatala testiranje i analizu podataka unazad. Ciklus provere bi mogao biti na mesec dana, ali po potrebi i duži ili kraći. Otkrivanje prevarnih radnji je efikasnije ukoliko se posmatra što duži vremenski period upravo zbog agregatne i kumulativne prirode najvećeg broja indikatora. Tako, ukoliko je testiranje započeto u januaru i obavlja se jednom mesečno vremenski okvir za testiranje bi bio početak i kraj januara, januar – februar, januar – mart i tako redom. Moguće je ostvariti i drugačiji pristup kada bi se testiranje vršilo strogo na nivou definisanog perioda, ali da se rezultati poslednjih testova pridružuju rezultatima testova iz prethodnih perioda. Na taj način bi se istakla kumulativna i agregatna priroda indikatora.

Vremenski okvir ne bi smeo da bude previše veliki, jer to može praviti probleme u performansama ukoliko se testiranje vrši na produkcionom sistemu.

3.3 Potvrda testova

Mnogi specifični indikatori i odgovarajući testovi su kreirani nakon analize ranije otkrivenih slučajeva prevarnih radnji, a koji su otkriveni na drugačiji način. Zato je veoma važno da se ti testovi retroaktivno provere neposredno na podacima u periodu kada je načinjena prevarna radnja kako bi se sama ideja i koncept testa mogli potvrditi. Ukoliko takav test ne daje pozitivne rezultate očigledno je da nisu obuhvaćeni svi elementi specifičnog indikatora, pa je potrebna njegova dorada ili odbacivanje.

3.4 Parametri testova

Da bi se konkretan indikator ispoljio potrebno je kroz test realizovati i određene parametre, kojima će se razdvojiti sumnjive transakcije od onih koje nisu sumnjive.

Tako, na primer, da bi se kroz test realizovao opšti indikator, koji posmatra transakcije, koje su obavljene van radnog vremena, vikendom i praznikom potrebno je definisati ulazne parametre kao što su vreme dolaska i vreme odlaska sa posla radnim danima i subotom. Potrebno je definisati i listu praznika za određeni period, jer su neki praznici uvek istog datuma, a drugi, poput verskih pokretni.

Dalje, kada se definišu indikatori, koji su vezani za konkretne iznose limita najčešće se koristi formula, koja ima sledeći oblik:

$$x \cdot \left(1 - \frac{y}{100}\right) < I < x\,. \qquad (1)$$

Parametar *I* predstavlja vrednost koju treba da zadovolji transakcija da bi se smatrala sumnjivom. Parametar *x* predstavlja gornji limit, a *y* procentualno odstupanje ispod limita.

Konačno, svaki test mora imati određene parametre ne bi li se ispoljio indikator na osnovu koga se razdvaja sumnjivo od normalnog.

3.5 Težina testova i njihovo međusobno ukrštanje

Rezultat svakog testa su sumnjive transakcije, koje su pronađene na osnovu određenih podataka iz informacionih sistema za posmatrani vremenski okvir. Svaka transakcija, koja je dobijena kao rezultat nekog testa može, ali u većini slučajeva i ne mora, da bude sumnjiva. Malobrojne sumnjive transakcije prolaze istim putem kroz aplikacije kao što to rade i daleko brojnije, regularne transakcije. One prolaze i razne logičke, sigurnosne kontrole kao i kontrole toka operacija. Paralelno sa tim obavljaju se i brojne druge manuelne kontrole, koje zahtevaju određene radne procedure. Činjenica da je konkretna transakcija pronađena određenim testom ne mora ništa da znači. Isto tako pojedini testovi manje ili više od drugih ukazuju na određene prevarne radnje. Testovi, kojima se realizuju određeni dobro definisani specifični indikatori, sigurno više ukazuju na prevarne radnje ili su „teži“ od nekih opštih testova. Ono što je veoma bitno je da se povećava stepen sumnje ukoliko je jedna transakcija pronađena od strane više testova. Dakle, potrebno je međusobno ukrstiti testove nad istim podacima kako bi se anulirala sumnja na određenim transakcijama i radnicima, koji su ih obavili. Da bi pravilno odredili stepen sumnje pojedine transakcije, moramo ukrstiti rezultate svih testova na pravilan način, tj. pravilno sabrati veću ili manju sumnju, koju sa sobom nosi određeni test.

U tabeli 1 je dat primer spiska testova sa njihovim šiframa i težinama. Veoma je važno da se odredi težina, w_i, svakog testa ponaosob i to relativno u odnosu na sve ostale testove. Parametar *i* predstavlja redni broj testa. Preporučuje se da težina, w_i, uzima vrednosti od 1 do 5 (ili 10) radi lakšeg ponderisanja. U tabeli 1 vrednosti su od 1 do 5. Međutim, mnogo su važniji relativni odnosi težina, koje je potrebno na početku odrediti na osnovu procene, a kasnije usklađivati na osnovu efikasnosti testiranja i iskustva u otkrivanju prevarnih radnji.

Grupisanje se obavlja iz zajedničke tabele u kojoj su prikazani svi rezultati testiranja. Svaku transakciju, koja je pronađena od strane određenog testa, mora pratiti i odgovarajuća šifra ili naziv testa kao i određena težina kako bi se moglo izvršiti grupisanje. U ovoj zajedničkoj tabeli je prirodno da se određena transakcija pojavi više puta, ali isključivo na osnovu toga što je prepoznata od strane više testova, tabela 2. Ponavljamo da se jedna transakcija na osnovu jednog testa može ponoviti samo jednom.

3.6 Grupisanje rezultata testiranja

Tabela 1: Spisak testova sa njihovim šiframa i težinama

Šifra testa	Težina	Opis testa
Test_01	3	Transakcije ispod određenog limita, 3.000 €, za koji je potrebna dodatna kontrola ili dozvola
Test_02	3	Transakcija koja je obavljena van radnog vremena, vikendom ili praznikom
Test_03	2	Transakcija od strane osobe, koje uobičajeno ne obavljaju tu vrstu posla
Test_04	1	Transakcija bez opisa ili sa ključnim rečima, koje ukazuju na sumnju
Test_05	4	Retko korišćeni računi

Tabela 2: Transakcije koje su prepoznate od strane testova

Broj testa	Težina	Transakcija	Vreme	Radnik	Iznos	Ostali podaci
Test_01	3	TR001045	28.05.2014.	RB103	2.900 €	…
Test_03	2	TR001045	28.05.2014.	RB103	2.900 €	…
Test_05	4	TR001045	28.05.2014.	RB103	2.900 €	…
Test_01	3	TR007752	21.06.2014.	RB553	2.850 €	…
Test_03	2	TR007752	21.06.2014.	RB553	2.850 €	…
Test_01	3	TR004277	16.06.2014.	RB072	2.950 €	…
Test_05	4	TR004277	16.06.2014.	RB072	2.950 €	…
Test_04	1	TR200024	23.07.2014.	RB005	23.000 €	…
Test_02	3	TR012345	03.07.2014.	RB553	7.000 €	…

U tabeli 2 su prikazani rezultati testova sa osnovnim kolonama. Mogu postojati i neke druge kolone, a to zavisi od tipa testa i same kompanije u kojoj se oni sprovode.

Grupisanje rezultata testova se može raditi po transakciji ili po radniku. Grupisanje po transakciji treba da sabere sve težine testova po kojim je pala određena transakcija, tabela 3. Rezultati ovakvog grupisanja treba da budu prikazani od najveće zajedničke težine ka najmanjoj, jer ukupna težina reprezentuje stepen sumnje.

Grupisanje po radniku kao rezultat daje ukupnu težinu sumnjivih transakcija, koje je obavio određeni radnik, tabela 4. Grupisanje je moguće obaviti na različite načine, a vrlo jednostavno putem pivot tabela u Excel-u. Ovakvo grupisanje ukazuje na konkretne radnike i njihove konkretne transakcije na kojima postoji najveća sumnja.

Tabela 3: Grupisanje po transakciji

Transakcija	Ukupna težina
TR001045	9
TR004277	7
TR007752	5
TR012345	3
TR200024	1

Tabela 4: Grupisanje po radniku

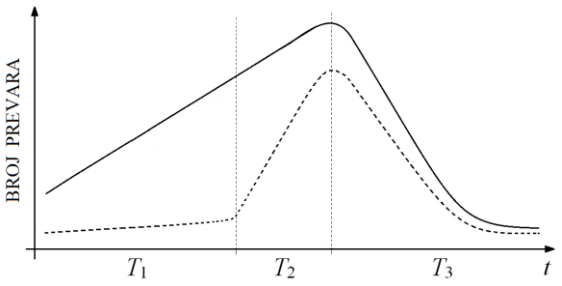
Radnik	Ukupna težina
RB103	9
RB553	8
RB072	7
RB005	1

Izveštaji u vezi sumnjivih transakcija se dalje prosleđuju nadležnom organizacionom delu kompanije. Oni treba da ispitaju uočene transakcije, kao i zaposlene da bi utvrdili da li je došlo do prevarnih radnji. Prilikom detaljne analize može se naići i na lažno sumnjive transakcije. Ove transakcije su predmet izuzetka od pravila i ne treba ih dalje razmatrati. Zbog toga svaki test da bi bio efikasan mora da bude jasan i jednostavan u ideji, ali i do kraja zaokružen u smislu konkretne realizacije.

4 ZAKLJUČAK

Primenom aktivnog pristupa prikazanom u ovom radu povećava se efikasnost u otkrivanju internih prevarnih radnji, jer se ciljano sužava skup transakcija, koje se analiziraju. Koliki je ovo doprinos za kompaniju najbolje se može videti preko grafika na slici 1.

Isprekidana linija predstavlja otkrivene prevare, a puna sve prevare u kompaniji. Vremenski period T_1 je period u kome postoje implementirane samo interne sistemske kontrole. Tada je onemogućeno da se dogode pojedine prevare. Ako se nađe način da se zaobiđu kontrole, što zaposleni, koji su dobro upoznati sa radom sistema mogu da urade, broj prevara će se povećavati i to sve do uvođenja aktivnog pristupa u otkrivanju prevarnih radnji.



Slika 1: Promene u broju načinjenih i otkrivenih internih prevarnih radnji

Postojanje internih kontrola i aktivnog pristupa obuhvata period T_2. Tada se znatno povećava broj otkrivenih prevara i približava se ukupnom broju prevara u posmatranoj kompaniji. Ipak, cilj menadžmenta je da se ukupan broj prevara smanji. To se postiže informisanjem zaposlenih o postojanju modela aktivnog pristupa i rešenosti rukovodstva da prati rizik od prevare. Ovakav metod odvraćanja treba da podstakne neku vrstu autocenzure kod zaposlenih kada su pitanju prevarne radnje. Ta aktivnost je prikazana u vremenskom periodu T_3. Broj otkrivenih prevara u odnosu na sve prevare u kompaniji je približno isti, ali je ukupan broj prevara smanjen.

Koliki je značaj uvođenja aktivnog pristupa u otkrivanju internih prevarnih radnji najbolje se vidi ako uporedimo vremenske periode T_1 i T_3. Najčešće je broj otkrivenih prevara isti ili približan, ali je broj nastalih prevara daleko manji nakon uvođenja i informisanja zaposlenih o postojanju naprednih metoda za otkrivanje prevarnih radnji.

CITIRANI RADOVI

Davis, C., Schiller, M., & Wheeler, K. (2011). *IT Auditing Using Controls to Protect Information Assets* (2nd ed.). The McGraw-Hill Companies.

ISO 27001. (2013). *ISO/IEC 27001 - Information security management.* Retrieved from International Organization for Standardization: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO 31000. (2009). *ISO 31000 – Risk Management Standard.* Retrieved from International Organization for Standardization: http://www.iso.org/iso/home/standards/iso31000.htm

Iyer, N., & Samociuk, M. (2007). *Fraud And Corruption: Prevention And Detection.* Gower.

Mihajlović, N. (2014). Primjena sigurnih i pravovremenih informacija i informacijskih tehnologija u otkrivanju prijevara u osiguranju. *Konferencija BISEC.* Beograd, Srbija: Univerzitet Metopolitan.

NBS. (2014). Odluka o adekvatnosti kapitala banke. *Službeni glasnik RS*(51), 1-243. Retrieved from http://www.nbs.rs/export/sites/default/internet/latinica/20/kpb/adekvatnost_kapitala.pdf

Rawsthorne, L. (2014). Global Fraud Trends in the Credit Industry. *16th Finance tech forum.* Sofia, BG.

Samociuk, M., Iyer, N., & Doody, H. (2010). *A Short Guide to Fraud Risk (Short Guides to Business Risk).* Gower.

Simon, W., Mitnick, K., & Wozniak, S. (2002). *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons. Retrieved from https://books.google.rs/books?id=OIy4F-8b_uEC

Datum prve prijave: 30.11.2014.
Datum prijema korigovanog članka: 04.12.2014.
Datum prihvatanja članka: 11.09.2015.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*
Simić, P. M., Milinković, L., & Jović, M. (2016, januar 15). Aktivni pristup u otkrivanju internih prevarnih radnji analizom podataka iz informacionog sistema. (Z. Čekerevac, Ur.) *FBIM Transactions, 4*(1), 91-98. doi:10.12709/fbim.04.04.01.11

*Style – **Chicago** Sixteenth Edition:*
Simić, Predrag M, Luka Milinković, i Milorad Jović. 2016. „Aktivni pristup u otkrivanju internih prevarnih radnji analizom podataka iz informacionog sistema.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 4 (1): 91-98. doi:10.12709/fbim.04.04.01.11.

*Style – **GOST** Name Sort:*
Simić Predrag M, Milinković Luka i Jović Milorad Aktivni pristup u otkrivanju internih prevarnih radnji analizom podataka iz informacionog sistema [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 januar 2016. - 1 : T. 4. - str. 91-98.

*Style – **Harvard** Anglia:*
Simić, P. M., Milinković, L. & Jović, M., 2016. Aktivni pristup u otkrivanju internih prevarnih radnji analizom podataka iz informacionog sistema. *FBIM Transactions,* 15 januar, 4(1), pp. 91-98.

Style – **ISO 690** Numerical Reference:
Aktivni pristup u otkrivanju internih prevarnih radnji analizom podataka iz informacionog sistema. **Simić, Predrag M, Milinković, Luka i Jović, Milorad.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 januar 2016, FBIM Transactions, T. 4, str. 91-98.