

# FRAUD PREVENTION IN ACCOUNTING INFORMATION SYSTEMS

## SPRJEČAVANJE PRIJEVARA U RAČUNOVODSTVENIM INFORMACIJSKIM SUSTAVIMA

OLUIC, Ana

**Abstract:** *This paper introduces the role of internal control systems in fraud prevention in accounting information systems and offers prevention as the most cost-effective means to reduce the fraud impact on business. The most effective tool in fraud prevention is a strong system of internal control. Preventing fraud consists of actions taken to discourage the perpetration of fraud and limit the exposure it fraud does occur.*

**Key words:** *frauds, internal controls, accounting information systems, information technology*

**Sažetak:** *U radu se prikazuje uloga internih kontrola u sprječavanju prijevara u računovodstvenim informacijskim sustavima te se prevencija prijevara prikazuje kao troškovno najisplativija u reduciranju utjecaja prijevara na poslovanje poduzeća. Najučinkovitija mjera u sprječavanju prijevara je uspostava adekvatnog sustava internih kontrola. Sprječavanje prijevara podrazumijeva poduzimanje potrebnih radnji kako bi se obeshrabrilo počinjenje prijevara i ograničila izloženost poduzeća ako do prijevara dođe.*

**Ključne riječi:** *prijevara, interne kontrole, računovodstveni informacijski sustavi, informacijske tehnologije*



## 1. Uvod

Nakon nedavnih velikih korporativnih skandala i medijske pažnje koja im je posvećena, primarni cilj poduzeća je upravljanje rizicima kako bi se mogućnost pojave pogrešaka i prijevarena svela na najmanju moguću mjeru. Ocjenjivanje rizika prijevare sve je teže provoditi u današnjoj modernoj poslovnoj praksi, posebice tamo gdje su transakcije i procesi međusobno povezani. Podaci o prijevarama gotovo su pa uvijek sadržani u računovodstvenim informacijskim sustavima stoga je presudno njegovo odgovarajuće razumijevanje za uspješno sprječavanje i pravovremeno otkrivanje prijevarena. Najisplativiji način borbe protiv prijevarena je uspostava odgovarajućeg sustava internih kontrola. Cilj ovoga rada je definiranje pojma i oblika prijevarena te identificiranje najčešćih mjera za sprječavanje prijevarena.

## 2. Prijevare i pojavni oblici prijevarena

Prijevarena je svaki namjeran čin počinjen da bi se osigurala nepoštena i nezakonita osobna ili poslovna korist. Obuhvaća raspon nepravilnosti i nezakonitih radnji koje karakterizira namjerno obmanjivanje ili lažno prikazivanje za koje osoba zna da su lažne ili ne vjeruje da su istinite. [1] Počinitelji prijevarena se uobičajeno mogu klasificirati u tri temeljne skupine: menadžeri, ostali zaposlenici u poduzeću i osobe izvan poduzeća (dobavljači, kupci, hakeri). Prijevare su uglavnom povezane sa osobama visokih vještina, znanja i mogućnosti pristupa. Većina prijevarena je počinjena od strane osoba zaposlenih u poduzeću koja su žrtva prijevare [2]. Razlog tome je što pristup lakše stječu osobe zaposlene u poduzeću nego osobe izvan poduzeća (uljezi, hakeri), stoga zaposlenici predstavljaju veću potencijalnu opasnost od počinjenja prijevarena. Uobičajeno, tri su faktora prisutna kad nastane prijevarena: motiv, opravdanje (opravdanost pojedinaca za prijevarene radnje) i prilika (često funkcija slabih internih kontrola) [3]. Sa počinjenim prijevarama u pravilu su povezani i veliki gubici. A da postoji i velika korelacija između profila počinitelja prijevarena i iznosa gubitka pokazuje istraživanje ACFE-a (Association of Certified Fraud Examiners) [4] prema kojemu gubici zbog prijevarena koju su počinili počinitelji prijevarena starije dobi su 27 puta veći od gubitaka koje su uzrokovali mlađi počinitelji. Razlog tome je što stariji počinitelji zbog svoje viskokopozicioniranosti imaju veće dozvole pristupanja računovodstvenom informacijskom sustavu poduzeća. Povezano s tim, osobe na višoj poziciji imaju i viši stupanj obrazovanja. Većina prijevarena se ne objavljuje zbog straha od gubitka ugleda i povjerenja poslovnih partnera. Neizvještavanje je razlog što je teško utvrditi iznose gubitka uzrokovanog prijevarama. Procjenjuje se da u Velikoj Britaniji gubitak uzrokovan prijevarama svake godine iznosi nekoliko stotina milijuna funti [5], dok je procjena da u tipičnoj američkoj organizaciji iznosi oko 7% godišnjeg prihoda (prema tome u 2008. godini je iznosio 944 milijarde dolara) [6]. Podaci ukazuju na značajno prijevorno ponašanje u poslovanju poduzeća. Riziku prijevare su izložena sva poduzeća, bez obzira na njihovu veličinu ili djelatnost kojom se bave. Prema prethodno spomenutom istraživanju ACFE-a industrije koje su najviše izložene riziku prijevare, po učestalosti pojavljivanja prijevare, su u prvom redu bankarstvo i financijske usluge, vlada i javna poduzeća, zdravstvo, proizvodnja,

osiguranje, građevinarstvo itd. Udruženje ovlaštenih istraživača prijevare (ACFE) klasificira prijevare u tri glavne kategorije [7]:

- *Zloupotreba imovine* su prijevare u kojima počinitelj krađe ili zloupotrebljava imovinu poduzeća odnosno organizacije. Uobičajeni primjeri zloupotrebljavanja imovine uključuju lažno fakturiranje, prijevare prilikom obračunavanja plaća, krađa zaliha itd.
- *Korupcija* podrazumijeva pojave kod kojih počinitelji prijevare iskorištavaju svoj poslovni utjecaj u poslovnim transakcijama kršenjem svojih dužnosti prema poslodavcima s namjerom stjecanja osobne koristi ili koristi za druge. Npr. zaposlenici mogu primiti ili ponuditi mito, iznuditi sredstva od trećih strana ili sudjelovati u sukobu interesa.
- *Prijevarno izvještavanje* podrazumijeva krivotvorenje financijskih izvještaja poduzeća. Npr. namjerno pogrešno ili nepotpuno prikazivanje značajnih informacija kao što je prikazivanje fiktivnih prihoda ili skrivanje troškova ili obveza s namjerom prikazivanja boljeg rezultata.

Zloupotreba imovine predstavlja najčešći slučaj prijevare, a uobičajena imovina koja je na meti počinitelja je novac [8]. Porast primjene informacijske tehnologije i njezin brzi napredak povećava rizik nastanka novih oblika prijevare. Računalne prijevare su problem s kojim se suočavaju poduzeća u kojima sigurnosna politika nije dobro implementirana i u kojima se sigurnosti računalnih sustava ne posvećuje dovoljna pažnja. Izuzetno je bitno voditi računa o informacijskoj sigurnosti, budući da su informacije zapravo najznačajniji resurs poduzeća. Ocjenjivanje rizika prijevare u današnjoj modernoj polovnoj praksi sve je teže, posebice tamo gdje su transakcije i procesi međusobno povezani. Efikasan pristup za poslovno upravljanje rizikom prijevare je onaj koji je fokusiran na tri cilja: *preventivne kontrole* dizajnirane najprije za sprječavanje prijevare, *detektivne kontrole* dizajnirane za otkrivanje prijevare kad su već nastale, te *korektivne kontrole* dizajnirane s namjerom poduzimanja korektivnih mjera i popravljivanja šteta uzrokovanih prijevarama [9]. U novije vrijeme sve se veći naglasak stavlja na preventivne kontrole budući da one predstavljaju troškovno najefikasnije mjere za sprječavanje prijevare.

### 3. Mjere za sprječavanje prijevare

Prijevare ne uzrokuju samo novčane gubitke već i lošu atmosferu u poduzeću. Najbolji način njihova sprječavanja je razumijevanje zašto se one uopće dešavaju te poduzimanje potrebnih radnji kako bi se spriječile [10]. Glavni mehanizam za sprječavanje prijevare je uspostava efikasnog sustava internih kontrola. Sustav internih kontrola sastoji se od svih politika i postupaka (internih kontrola), koje je usvojio menadžment kako bi osigurao, koliko je to svrsishodno, postizanje redovitog i uspješnog poslovanja, uključujući privrženost svojoj politici, zaštitu imovine, sprječavanje i otkrivanje prijevare i pogrešaka, točnost i pouzdanost računovodstvenih evidencija, kao i pravodobno pripremanje pouzdanih financijskih informacija [11]. Prevencija prijevare uključuje radnje koje obeshrabruju počinjenje prijevare i ograničavaju izloženost prijevare kad do nje dođe [12]. U nastavku su prikazani neki od kontrolnih elemenata programa za sprječavanje prijevare koji su

predstavljani unutar kontrolnog okvira COSO (Internal Control – Integrated Framework; the COSO Framework) [13]:

- Kontrolno okruženje.* Mnogi faktori utječu na uvjete u kojima se provodi kontrola, neki od njih su: organizacijska struktura, poštenje, etičke vrijednosti i stručnost zaposlenih, načini na koje uprava daje ovlasti i odgovornosti, sudjelovanje uprave, kadrovska politika. Poduzeća moraju utemeljiti primjereno kontrolno okruženje koje uključuje: pravila postupanja, politiku etike ili politiku protiv prijevара koja određuju odgovarajući ton na samom vrhu, programe besplatnih telefonskih linija za etička pitanja i zviždače gdje mogu prijaviti sumnje, smjernice i praksu za zapošljavanje i promaknuća, nadzor odbora za reviziju, uprave ili drugog nadzornog tijela, istraživanje prijavljenih problema i popravne mjere za potvrđena kršenja. Budući da je 90% prijevара počinjeno na rukovodećim nivoima uspostava jakih antiprijevernih programa i kontrola je osnovna komponenta zdravog kontrolnog okruženja.
- Procjena rizika od prijevара.* Organizacije moraju utvrditi i procijeniti rizike od prijevара uključujući procjenu potencijalnog netočnog financijskog izvještavanja, nezakonita prisvajanja imovine, nepravilnih računa i troškova ili financijsko kršenje dužnosti rukovodstva i ostalih.
- Kontrolne aktivnosti.* Nakon što je procijenjen rizik od prijevара poduzeća moraju uspostaviti i provoditi učinkovitu kontrolu, uključujući radnje koje poduzima rukovodstvo za utvrđivanje, sprječavanje i ublažavanje lažnog financijskog izvještavanja ili zlouporaba imovine organizacije, te sprječavanje rukovodstva da zaobilazi kontrole. Osim toga, poduzeća trebaju uspostaviti postupak potvrđivanja ili certifikacije u svrhu potvrđivanja da je zaposlenik pročitao i razumio politiku poduzeća i da je se pridržava. Kontrolne aktivnosti uključuju mnoštvo postupaka od kojih se izdvajaju podjela dužnosti, ovlasti i odgovornosti, autorizacija, provjera transakcija, osiguranje imovine itd. Zbog važnosti informacijske tehnologije u poslovanju poduzeća nužno je voditi računa i o uvođenju odgovarajućih općih i aplikacijskih kontrola.
- Informiranje i priopćavanje.* Zbog uspješnog provođenja antiprijevernih programa i politika poduzeća moraju uspostaviti djelotvornu praksu informiranja i priopćavanja o prijevarama, uključujući dokumentiranje i distribuciju politika, smjernica i rezultata, prilike za raspravu o etičkim dvojabama, komunikacijske kanale, izobrazbu osoblja i razmatranje utjecaja i korištenja tehnologije za sprječavanje prijevара, kao što je trajno korištenje softvera za praćenje.
- Nadzor (praćenje).* Organizacije trebaju provoditi trajno i povremeno ocjenjivanje sustava internih kontrola. Iako antiprijevernih programi i kontrole trebaju uključivati svih pet komponenti COSO-a, poseban je naglasak na kontrolnom okruženju jer uvjeti u kojima se obavlja interna kontrola direktno utječu na djelotvornost određenih kontrolnih postupaka. Učinkovitost interne kontrole zapravo je funkcija poštenja i etičkih vrijednost pojedinaca koji kreiraju, provode i nadziru provedbu postavljenih kontrolnih postupaka [14]. Iz svega navedenog može se zaključiti da mjere za sprječavanje prijevара trebaju osigurati tri realna i mjerljiva cilja [15]: 1. smanjenje gubitka uzrokovanog prijevaram, 2. obmanjivanje prijevара kroz proaktivne politike te 3. jačanje okruženja za rano otkrivanje prijevара.

#### 4. Zaključak

Prijevare ne uzrokuju samo velike gubitke već stvaraju i moralne probleme u radnom okruženju. Najefikasniji način za sprječavanje prijevara je uspostava učinkovitog sustava internih kontrola. Zbog postojanja inherentnog rizika čak ni efikasan sustav internih kontrola ne može dati ništa više od razumnog uvjerenja da će se prijevare spriječiti. Međutim, poticanjem adekvatnih internih kontrola od strane menadžmenta te dobrom praksom zapošljavanje, poduzeća mogu poduzeti proaktivni stav u suzbijanju, tj. zaštiti od prijevara i pogrešaka te na taj način minimizirati poslovne gubitke.

#### 5. Literatura

- [1] Fondacija za istraživanje Instituta internih revizora (2007). *Okvir profesionalnog djelovanja*, Hrvatski institut internih revizora
- [2] Seetharaman, A.; Senthivelmurugan, M. & Periynayagam, R. (2004). Anatomy of computer accounting frauds. *Managerial Auditing Journal*, 19(8), str. 1055-1072.
- [3] KPMG (2009) *Fraud Survey 2008*, New York
- [4] Seetharaman, A.; Senthivelmurugan, M. & Periynayagam, R. (2004). Anatomy of computer accounting frauds. *Managerial Auditing Journal*, 19(8), str. 1055-1072.
- [5] Commercial Angles' Newsletter (2001). Fraud prevention. *Dostupno na:* [www.tradeangles.fsbusiness.co.uk/articles/fraud\\_prevention.htm](http://www.tradeangles.fsbusiness.co.uk/articles/fraud_prevention.htm) *Pristup:*20-4-2010
- [6] Association of Certified Fraud Examiners (2008) 2008 Report to the Nation on Occupational Fraud & Abuse. *Dostupno na:* <http://www.intercedeservices.com/downloads/2008-rttn.pdf> *Pristup:* 15-04-2010
- [7] Seetharaman, A.; Senthivelmurugan, M. & Periynayagam, R. (2004) Anatomy of computer accounting frauds. *Managerial Auditing Journal*, 19(8), str. 1055-1072.
- [8] Seetharaman, A.; Senthivelmurugan, M. & Periynayagam, R. (2004) Anatomy of computer accounting frauds. *Managerial Auditing Journal*, 19(8), str. 1055-1072.
- [9] KPMG (2009) *Fraud Survey 2008*, New York
- [10] Commercial Angles' Newsletter (2001). Fraud prevention. *Dostupno na:* [www.tradeangles.fsbusiness.co.uk/articles/fraud\\_prevention.htm](http://www.tradeangles.fsbusiness.co.uk/articles/fraud_prevention.htm) *Pristup:* 20-4-2010
- [11] <http://www.revizorska-komora.hr/pdf/Medjunarodni-Rev-Standardi.pdf>
- [12] Fondacija za istraživanje Instituta internih revizora (2007) *Okvir profesionalnog djelovanja*, Hrvatski institut internih revizora
- [13] PricewaterhouseCoopers, *Key Elements of Antifraud Programs and Controls*. *Dostupno na:* <http://www.tdot.state.tn.us/internalaudit/documents/PwCantifraudWP.pdf> te Fondacija za istraživanje Instituta internih revizora (2007) *Okvir profesionalnog djelovanja*, Hrvatski institut internih revizora
- [14] Messier, W. F.(2000). *Revizija; Priručnik za revizore i studente s rješenjima zadataka*, II. dopunjeno izdanje, prijevod s engleskog jezika, Faber & Zgombić Plus, Hrvatsko udruženje revizora
- [15] Seetharaman, A.; Senthivelmurugan, M. & Periynayagam, R. (2004) Anatomy of computer accounting frauds. *Managerial Auditing Journal*, 19(8), str. 1055-1072.



Photo 128. Moto cross in Emovci / Moto kros utrke u Emovcima