

# REVIZIJA INFORMACIJSKIH SISTEMOV, KOT PRISPEVEK K NJIHOVI USPEŠNOSTI IN UČINKOVITOSTI

Boža Javornik, CISA, Nova Ljubljanska banka d.d.

**V vedno hitreje se spreminjajočem okolju finančnih storitev ima informacijska tehnologija vedno večjo vlogo. Velika in pomembna tveganja povezana z njeno uporabo morajo iskati ravnotežje z izjemnimi priložnostmi.**

V sedanjem času sta pomembna ključna faktorja uspeha podjetij dostop do kapitala in trgov. Uspešnosti pri tem ni mogoče zagotavljati brez ustrezne izrabe informacijske tehnologije. Razpoložljivost in transparentnost informacij omogočata potencialnim investitorjem oceniti podjetje in ustrezno varno naložiti svoje viške sredstev, potencialnim poslovnim partnerjem transparentna informacija zagotavlja jamstvo dolgoročne uspešnosti poslovnih povezav. Vsako spreminjanje informacij in podatkov v smislu sprememb pričakovanih velikosti in odnosov, ki pomenijo osnovo vrednotenja podjetja za investitorje in poslovne partnerje, lahko pomeni vzrok za pomembno poslabšanje dostopnosti kapitala in stabilnosti odnosov z dobavitelji in kupci.

Upravljanje poslovnih sistemov postopoma postaja sistem spreminjajočega se okvira pravil, ki v določenem smislu pomeni načine obnašanja in reagiranja na spremembe v okolju in sistemu samem. Informacijski sistemi že dlje časa izgubljajo svojo zgolj evidenčno funkcijo in njihova vrednost postaja v sposobnosti zgodnjega odkrivanja indikatorjev neprijetnih dogodkov in njihove predstavitve. Tradicionalni mehanizmi kontroliranja aktivnosti v smislu preprečevanja "neprijetnih posledic" neustreznega ali celo nezakonitega delovanja niso več aktualni. Pritiski na zniževanje stroškov administriranja, kamor sodijo stroški kontroliranja, hoteli ali ne, so prisilili snovalce informacijskih sistemov, da kontrole avtomatizirajo, neprimerne za avtomatizacijo pa so lahko celo izginile. Avtomatizirane oblike kontrol so z integracijo posamičnih poslovnih aplikacij v "integrirane informacijske sisteme" izgubile prvotno obliko, njihova transformacija je bila povezana z (ne)združljivostjo z informacijsko tehnologijo in načinom njene izrabe. Redko je bilo pri transformaciji obravnavano tveganje, ki naj bi ga kontrola v osnovi preprečevala ali minimizirala posledice neprijetnih dogodkov v povezavi z njim. Razvoj družbenih odnosov je v upravljanje poslovnih sistemov prinesel še dejstvo, da ni potrebno poslovati zgolj uspešno in učinkovito. Upravljanje s poslovnimi sistemi zahteva, da so upoštevana etična načela nekega okolja ali celo širše skupnosti. Baselska načela varnega poslovanja bank v svoji osnovi ne pomenijo

drugega kot prisilo ali vsakodnevni opomin bančnikom, da ne pozabijo skrbno ravnati s prihranki posameznikov, ki so jih jim zaupali.

Upravljalci poslovnih sistemov se vedno bolj zavedajo odvisnosti uspešnosti in učinkovitosti od razpoložljivosti informacijskega sistema. Male nočne more postajajo zgodbe, ki so se zgodile drugim: požar v računskem centru, izguba podatkov zaradi tehnične okvare, nočni klici izsiljevanja povezani z izgubo podatkov ali razkritjem skrivnosti, milijoni dolarjev vloženi v razvojne projekte v povezavi z informacijsko tehnologijo brez pravega jamstva, da bodo pričakovani učinki prihrankov oz. zaslužkov ob novih priložnostih dejansko doseženi, ali pa vsa vlaganja morda pomenijo le preživetje. Ravnateljstva morajo prepričati delničarje in poslovne partnerje, da obvladujejo poslovanje in to ne le danes ampak tudi za prihodnost. Podjetje obvladuje informacijski sistem, če uspe iz podatkov pridobiti kvalitetnejša znanja hitreje kot konkurenca. Izvršni vodje morajo imeti na razpolago podatke za načrtovanje poslovanja in ukrepanja ob spremljajočih se pogojih v okolju.

Jasno je, da kontroliranje informacijskih sistemov že dolgo ne pomeni več zagotavljanje varnosti procesiranja in zaščite pred razkritjem, vedno večji del kontrol je usmerjen k razpoložljivosti sistema, njegovi učinkovitosti in uspešnosti. Način poslovanja v smislu odvisnosti od uporabe informacijske tehnologije vedno bolj zahteva, da se informacijski sistem obravnava kot osnovna in ne podporna dejavnost. Cilji poslovanja so vedno pogostejše lahko doseženi le, če so podprti z uspešnim in učinkovitim informacijskim sistemom. Avtomatizacija poslovnih procesov in elektronsko izmenjavanje podatkov imata za posledico, da je analiziranje poslovnih procesov vedno težje, vedno manj je možnosti, da bi brez informacijskega znanja bilo mogoče razumeti, kako so oblikovane kontrole, še težje pa je preverjati, ali delujejo. Tveganja povezana s poslovanjem morajo biti jasno opredeljena v smislu materializiranih posledic neprijetnih dogodkov, da je mogoče pri oblikovanju rešitev informacijskega sistema oceniti, katere kontrole so potrebne in zadostne, da so tveganja minimizirana na še sprejemljivi nivo. Poslovni

sistemi si preprosto ne morejo privoščiti preveč oz. prekrivajočih se kontrol.

Odgovornosti nadzornih svetov, uprav, izvršnih direktorjev so se zaostriale, zato so njihove zahteve do revizorjev računovodskih izkazov in notranjih revizorjev bolj določene v smislu večje zanesljivosti trditev, zahtevajo visok nivo profesionalnega ocenjevanja. Zaradi kompleksnosti vprašanja varnega ravnanja z informacijskim sistemom, njegovo uspešnostjo in učinkovitostjo, zagotavljanjem zakonitosti in preprečevanjem prevar, je potreba po profesionalni oceni kontrolnih sistemov in rešitev informacijskega sistema na sploh, vedno bolj izoblikovala vlogo revizorja informacijskih sistemov pri tem. Omenjeni proces je na drugi strani izoblikoval širino znanj, ki jih revizor informacijskih sistemov potrebuje, kot tudi potrebo po izdelavi primerjalnega okvira dobrega obvladovanja informacijskega sistema.

Mednarodna organizacija revizorjev informacijskih sistemov (Information System Audit and Control Association - ISACA) se tega že dlje časa zaveda. V sredini 90-tih let je raziskovalna organizacija tega združenja pričela z izdelavo okvira kontroliranja informacijskih sistemov. V letu 1996 je bila tako izdana prva, v letu 1998 pa že druga izpopolnjena izdaja COBIT-a (Governance, Control and Audit for Information and Related Technology). Namen izdelave serije petih priročnikov Cobit-a je bil raziskati, razviti, dokumentirati in promovirati mednarodno priznan, kvaliteten, z zadnjimi dosežki izpopolnjen in široko sprejemljiv okvir kontroliranja informacijske tehnologije, namenjen tako upravljalcem poslovnih procesov kot profesionalcem s področja informatike in revizorjem. Pristopi kontroliranja so v priročnikih predstavljeni nivojsko, glede na ciljno skupino bralcev: od ravnateljev do odgovornih za varno ravnanje s posameznimi elementi informacijskih sistemov. Na osnovi tveganj, ki so povezana z uporabo informacijske tehnologije, je grobo predstavljena dobra praksa varnega ravnanja in pa napotki, kako naj revizor to preveri.

Revizorji informacijskih sistemov, kot odgovorni za informacijske sisteme v velikih poslovnih sistemih, so priročnike ugodno sprejeli in tako z njihovimi prizadevanji nastajajo še podrobnejši in bolj praktični okviri obvladovanja posameznih tehnologij (strežnik - odjemalec, obvladovanje reševanja skladnosti za leto 2000 za menedžerje, Y2K - načrtovanje dela brez prekinitev ..).

Drugo dejstvo, ki kaže na to, da potreba po reviziji informacijskih sistemov narašča, je, da se pomembno spreminjajo vsebine znanj, ki bi jih morali obvladati revizorji računovodskih izkazov in računovodski ter finančni strokovnjaki na sploh. Podobno velja za interne revizorje. Da se je obseg revidiranja informacijskih sistemov močno povečal, kaže tudi dejstvo, da je iniciativa za prenovo standardov revidiranja informa-

cijskih sistemov pokazala ne le, da je potrebno standarde prenoviti, temveč, da je potrebno izdelati nekatere nove standarde, kot tudi, da je za posamične segmente tehnologij potrebno izdelati smernice revidiranja. Da spremembe standardov niso le kozmetične narave, kaže tudi dejstvo, da je npr. besedilo smernice Vplivi revizorjevega vključevanja v pridobivanje in uvajanje po prvi objavi za obravnavo pri članstvu narastlo za 6 krat. Trenutno je dokončanih, v javni obravnavi ali pa so še v strokovni dodelavi več kot 30 smernic.

Revizija informacijskih sistemov obsega tako revizijo splošnih kontrol varnega ravnanja s podatki, kot tudi revizijo uspešnosti in učinkovitosti posameznih rešitev podpor poslovnih sistemov. V sklopu preverjanja delovanja splošnih kontrol je mogoče kot primerjalni okvir upoštevati Slovenski standard varnega ravnanja s podatki (prevod angleškega standarda BS 7799) ali COBIT. Preverjanje varnih, uspešnih in učinkovitih uporab informacijske tehnologije v poslovnih procesih pa zahteva ustrezno razumevanje in poznavanje tveganj poslovanja, metod prepoznavanja in zgodnjega odkrivanja indikatorjev prisotnosti tveganj in v povezavi s tem sposobnosti presojanja, kaj je priporočljiva dobra praksa pri uporabi informacijske tehnologije in kako so oblikovane uspešne in učinkovite kontrole za omejevanje posledic tveganj pri poslovanju.

Rešitve v posameznih poslovnih procesih niso enake, za nekatere velja, da je ključno, da so sistemi na razpolago brez časovnih zakasnitev, drugje je spet pomembno, da je zagotovljeno vse, da ni mogoče nepooblaščno pridobiti podatkov in jih razkriti, pri nekaterih sistemih je pomembno, da so postavljeni tako, da omejujejo prevare. Od računovodskih sistemov zahtevamo njihovo preglednost, sledljivost sprememb, popolnost in točnost podatkov in pa zagotavljanje varnosti pred izgubo podatkov; uporaba prekrivanja vrednosti podatkov je najstrožje prepovedana.

Revizija informacijskih sistemov ni oblika kontrole kakovosti v smislu ocenjevanja dobrih računalniških rešitev (certificiranja). Posamezno rešitev obravnava v okolju poslovanja, zato je isto programsko rešitev mogoče neke oceniti kot ne tvegano, v drugem okolju pa kot izjemno tvegano, pač odvisno kolikšen vpliv na poslovanje (zagotavljanja finančnega rezultata ali zakonitosti poslovanja) ima del poslovanja, ki jo rešitev podpira. Pristopi pri revidiranju se razlikujejo tudi od okolja: manjši poslovni sistemi imajo lahko enostavnejše rešitve, ki jih obvladuje peščica posameznikov in je seveda lahko ekonomsko neopravičljivo vztrajanje na določenih standardih dobre prakse; drugačne so rešitve povezane z varnim ravnanjem s podatki v primerih servisnih storitev; najzahtevnejši in najkompleksnejši pa so sistemi kontrol obvladovanja tveganj pri velikih

poslovnih sistemih z najraznovrstnejšo uporabljenjo informacijsko tehnologijo in visokimi zahtevami razpoložljivosti informacijskega sistema.

Kako lahko ravnateljstvom pomaga revizija informacijskih sistemov?

Nezadostno razumevanje možnosti in načinov uporabe informacijske tehnologije ne omogoča enostavnega odgovora, ali se naložbe v informacijsko tehnologijo vračajo z rezultati poslovanja. Ravnateljstva si zastavljajo vprašanja, ali morda ni nevarnosti, da nekega lepega jutra sistem preprosto ne bo deloval in ga ne bo mogoče vzpostaviti dlje časa in ali sploh podjetje

zmore poslovati brez informacijske podpore, oz. so posledice tega lahko omejene. Na podobna vprašanja jim lahko pomagajo najti odgovor revizorji informacijskih sistemov. Res je, lahko bi jim dali odgovor tudi odgovorni sodelavci v organizacijskih enotah informatike - računskih centrih, obstajata le vprašanja: ali se more in ali se je modro zanesti na tak odgovor. V primeru računovodskih izkazov bi bila dilema lahko podobna - mnenje o računovodskih izkazih bi podali računovodje, vendar sta se lastnik in v določenem smislu tudi država odločila drugače. ■

## EVROPSKI IN DOMAČI VIDIKI ELEKTRONSKEGA POSLOVANJA

Aljoša Domijan

Okrogle mize na temo elektronskega poslovanja na DSI 99 so se udeležili Aaron Marko, direktor Microsoft d.o.o., kot predstavnik ponudnika programske opreme za izvedbo elektronske trgovine, Zoran Thaler, direktor EON d.o.o., kot predstavnik ponudnika varnega poslovanja na Internetu, dr. Dušan Caf kot predstavnik GZS ter Aljoša Domijan, direktor Gambit trade d.o.o., kot vodja okrogle mize in predstavnik sistemske hiše, ki ponuja izdelavo zasnov, izvedbo in vzdrževanje elektronskih trgovin.

Letos smo med publiko prvič zasledili tudi predstavnike podjetij, ki so z odprtjem elektronskih trgovin razširila svojo ponudbo in se približala tudi kupcem na svetovnem spletu. V razpravi smo se osredotočili predvsem na izvedbeni del in delitev nalog med ponudniki komunikacijske infrastrukture, ponudniki varnih transakcij, bankami, trgovci in nenazadnje kupci. Ugotovili smo, da je Slovenija tik pred tem, da elektronsko trgovanje postane del našega vsakdana, saj smo bili v primerjavi z DSI 98, ko so referenti govorili predvsem o varnosti in teoriji elektronskega poslovanja, letos zelo konkretni. Na DSI 2000 pa bomo zagotovo že govorili o izkušnjah in razlogih za uspeh najuspešnejših domačih e-trgovcev.

### 1. UVOD

Pred leti se je Jeff Bezos, ustanovitelj podjetja Amazon.com uprl takratni splošni prodajni logiki, ki je govorila, da je pot do uspešne elektronske prodaje v ponujanju kvalitetnih produktov z visoko vrednostjo, in pričel s prodajo knjig na internetu. Takrat je bila večina ljudi mnenja, da je cena edino, kar je pomembno. A Buzon je menil drugače. Razmišljal je v smeri, da je uspeh prodaje preko interneta v informiranosti potencialnih kupcev. Najrevolucionarnejši vidik pro-

daje preko interneta je bil in je še vedno ta, da potencialni kupec, ki se "oglasil" v virtualni trgovini, najde nekaj zase. Le tako bo ponudnik produkt oz. storitev tudi prodal.

Jeff Bezos je danes lastnik najbolj znane trgovine na internetu s ponudbo več kot 3 milijone naslovov knjig in pol milijarde dolarjev prometa, s podružnico v Evropi in z izredno hitro rastjo vrednosti delnic. Jeff Bezos je seveda Američan. Zdi se, da v Evropi ne bi mel nobenih možnosti, da Slovenije niti ne omenjamo. In vendarle, Bezos ni odkril ničesar novega! Ista tehnologija je na voljo tudi v Sloveniji in Evropi. In čeprav Evropejci preko svetovnega spleta kupujejo vse več in večino denarja potrošijo na spletnih straneh ameriških podjetij, se zdi, da Evropa še vedno ni našla pravega odgovora. Ali ga sploh lahko?

### 2. EVROPSKE ZAVORE

Ko primerjamo trgovanje preko interneta v Ameriki in Evropi, ne moremo mimo dejstva, da je ameriški trg večji. Izreden uspeh Amazon.com, kateremu nikakor ne gre oporekati, je v veliki meri tudi posledica velikega trga. Dosežki drugih dveh uspešnih ameriških podjetij s svojima elektronskima trgovinama Gap.com (oblačila) in Dell.com (računalniki) kažejo, da gre kljub