UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

POSLOVNI POMEN NOTRANJIH KONTROL Z VIDIKA INFORMATIKE

LJUBLJANA, JUNIJ 2007 MILAN OSTERMAN

IZJAVA

Študent Milan Osterman izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom docenta dr. Aleša Groznika in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 4.6.2007 Podpis:

Kazalo

Seznam slik

Seznam tabel

1. Uvod

1.1. Opredelitev področja in namen magistrskega dela

Področje notranjih kontrol je v svoji zgodovini doživelo že mnogo prelomnic. Začetki sovpadajo s prvimi resnejšimi poskusi uvajanja konsistentnosti pravil v organizacijo, hiter razvoj pa se je začel v drugi polovici dvajsetega stoletja, in sicer s pojavom novih poslovnih oblik, ki so bile posledica tehnološkega napredka in vsesplošne globalizacije. Nov mejnik se je pojavil v devetdesetih letih prejšnjega stoletja, ko je COSO[1] izdal publikacijo z natančnimi definicijami vseh pomembnih elementov povezanih z notranjimi kontrolami, v tem obdobju pa se je že v veliki meri kazal vpliv informacijske tehnologije.

Da samo teoretična podlaga ne zadošča, se je pokazalo že zelo kmalu. Po dogodkih izpred nekaj let je postalo jasno, da je nadzor nad poslovanjem podjetja mnogo bolj kompleksna stvar, kot pa je videti na prvi pogled. Govor se nanaša predvsem na nepravilnosti v podjetjih Enron, Parmalat, Worldcom in podobnih, ki so omajali zaupanje vlagateljev ter povzročili pretrese na kapitalskih trgih. Slednje je prizadelo gospodarstva razvitih držav, ki so nemudoma odgovorile s strožjo zakonodajo. Med prvimi so se odzvale Združene države Amerike, kjer so v letu 2002 sprejeli Sarbanes-Oxleyev zakon, katerega namen je bil urediti in zaostriti področje računovodstva v podjetjih, in sicer predvsem z vidika dokumentiranja in notranjega nadzora (Carpenter, 2004, str. 3). Ostale države, tudi Evropska skupnost, sledijo ameriškemu zgledu in pripravljajo oziroma že uporabljajo podobne predpise.

Da tovrstna problematika ni nova, dokazuje škandal povezan z zavarovalno družbo Equity Funding, ki je že pred več kot tridesetimi leti korenito vplival na pristop k revidiranju organizacij. Prevara, kjer je sodelovalo blizu sto zaposlenih in je temeljila na ponarejanju zavarovalnih polic, je povzročila spremembo revizijskega dela (Investor Confidence Index Summary, 2006). Slednje sedaj večjo pozornost namenja odkrivanju tovrstnih dejanj, poleg tega pa je odgovornost revizorja večja, saj je v primeru Equity Fundinga dobršno mero krivde nosil posredno vpleteni revizor. Equity Funding, Enron in podobni primeri kažejo, da je bil učinkovit nadzor nad poslovanjem podjetja vedno svojevrsten izziv, takšen pa bo ostal tudi v prihodnje. V veliko pomoč pri tem so nam lahko notranje kontrole, seveda je predpogoj, da so učinkovite. Glede na neprestan razvoj je nesporno dejstvo, da tudi na tem področju vse večjo vlogo prevzema informacijska tehnologija.

V današnjem času je informacijska tehnologija vpletena v vse vidike poslovanja, kar je potrebno upoštevati pri snovanju in izvajanju nadzorske funkcije. Tako notranje kontrole, ki so neposredno ali posredno povezane z računalniškimi programi in informacijsko infrastrukturo, že prevladujejo nad ročnimi. Tega se nekatera poslovodstva ne zavedajo in ne izkoriščajo možnosti, ki jih ponujajo avtomatske kontrole, posledično pa ne morejo izrabljati koristi, ki so na voljo pri uporabi sodobnih tehnologij. S tem je povezano tudi to magistrsko delo, katerega namen je razjasniti problematiko na področju IT notranjih kontrol in prispevati

[1] Committee of Sponsoring Organizations of the Treadway Commission – COSO je ameriška iniciativa v zasebnem sektorju, ustanovljena leta 1985, ki si je za svoj cilj zastavila zmanjšati prevare povezane s finančnim poročanjem in ima izredno pomembno vlogo na področju notranjih kontrol.

k boljšemu razumevanju, kako uspešno zasnovati in pravilno uporabljati kontrolne mehanizme in s tem prispevati k poslovnim uspehom. Obenem je njegov namen spodbuditi in upravičiti vlaganja v notranje kontrole, in sicer prek predstavitve koristi, ki se jih podjetje ob pravilnem postopanju lahko nadeja.

1.2. Cilji magistrskega dela

Glavni cilj magistrskega dela je poiskati odgovor na vprašanje, kakšen pomen imajo notranje kontrole v povezavi z informacijsko tehnologijo za podjetje. Pri tem ne moremo iti mimo številnih dejavnikov, ki oblikujejo to področje. Mednje spadajo tako zakonodaja kot različni standardi in tehnologija, za vse pa je značilno, da niso statični. Slednje pomeni, da je potrebno opredeliti stanje in silnice, ki imajo pomemben vpliv, zato med cilje magistrskega dela spada tudi predstavitev zakonodaje, ki je trenutno aktualna oziroma je v pripravi, prikaz standardov in priporočil, ki se uporabljajo, ter oris ugotovitev, kako in v kakšnem obsegu na to področje vpliva tehnološki razvoj.

Na splošno želim prek vsebine magistrskega dela pojasniti vlogo IT notranjih kontrol v poslovanju podjetja in primerjati koristi, ki jih prinašajo, s potrebnimi napori in porabo virov za njihovo vpeljavo in uporabo. S tem namenom bodo predstavljeni tudi koraki, ki jih je potrebno izvesti za uspešno uvedbo in uporabo kontrolnih mehanizmov. V povezavi z zgoraj omenjenimi elementi – zakonodajo, standardi in tehnologijo – ter dokumentiranjem in poročanjem o IT notranjih kontrolah bom skušal celovito zaokrožiti to tematiko in potrditi svojo hipotezo, da ustrezna obravnava tega področja pomeni pomembne koristi pri poslovanju podjetja in upravičuje vlaganja.

1.3. Struktura magistrskega dela

Vsebina prvega dela se nanaša na predstavitev notranjih kontrol, pozornost je usmerjena predvsem na kontrole, ki so vzpostavljene s pomočjo informacijske tehnologije in so od nje tudi odvisne. Pri tem je pomembno razlikovati med izključno računalniškimi in tistimi, pri katerih je za uspešno delovanje še vedno potrebna prisotnost človeškega dejavnika. V praksi se pri tej tematiki pojavlja dosti nejasnosti, zato je ta tematika obdelana bolj podrobno. Ta del vključuje tudi razdelitev IT notranjih kontrol. Pri opredelitvi posameznih vrst kontrol je poudarek na razlikah med njimi ter na njihovih posebnostih in prednostih na določenem področju.

V drugem delu so prizadevanja usmerjana k predstavitvi zunanjih elementov, na katere podjetja nima vpliva, vendar morajo v skladu z njimi oblikovati kontrole. Področje, ki je tu najbolj izpostavljeno, je zakonodaja, saj ta predpisuje obvezujoče smernice za razliko od tehnologije in standardov, kjer je mogoče izbirati načine, kako se prilagajati vedno novim zahtevam. V tem delu so prikazane predvsem spremembe v zadnjih letih, še bolj pomemben del pa predstavlja obravnava trenutnih oziroma prihodnjih potreb in odgovorov nanje. Zakonodaji sledi opis tehnoloških dejavnikov in opredelitev standardov, ki podrobneje opredeljujejo pristop k obravnavi področja notranjih kontrol v povezavi z informacijsko tehnologijo. Z drugimi besedami, COSO, COBIT in ostali standardi predstavljajo ogrodja oziroma okvire (frameworks), z uporabo katerih lahko vzpostavimo celosten sistem kontrol

(COBIT, 1998, str. 17). Njihova predstavitev temelji predvsem na pomembnejših razlikah med njimi - na primer COSO se osredotoča na finančne procese, COBIT pa na informacijsko tehnologijo (Brand K., Boonen H., 2005, str. 69).
Predstavitvi zakonodaje, vpliva tehnologije in standardov sledi bolj praktičen del. Nanaša se na sistematičen pregled faz običajno potrebnih za vzpostavitev učinkovitega sistema notranjih kontrol in obsega vse od priprave projekta do končnega analiziranja pomanjkljivosti notranjih kontrol ter poročanja o rezultatih. Za lažjo ponazoritev so tu podani konkretni primeri, ki sem jih pripravil za podjetje X. Slednje je družba s sedežem v Sloveniji, ki se glede na določila Zakona o gospodarskih družbah uvršča med srednje velike družbe, po dejavnosti sodi med trgovsko-storitvena podjetja in se ukvarja s prodajo blaga ter storitev predvsem na domačem trgu.
Pred samim zaključkom so predstavljene prednosti, ki jih nudijo učinkovite IT notranje kontrole. Med pridobitvami lahko najdemo tako neposredne kot posredne koristi, ki se kažejo v različnih oblikah in jih je posledično težko nedvoumno ovrednotiti, za vse pa sem skušal oceniti njihov vpliv na podjetje, pri čemer sem se zanašal na priporočila strokovnjakov s tega področja ter svoje izkušnje. Podjetja se običajno ne zavedajo vseh prednosti, ki jih nudijo IT notranje kontrole, zato sem opozoril tudi na to problematiko in jo dopolnil s svojim mnenjem.

1.4. Metode dela

Magistrsko delo temelji v veliki meri na teoretični podlagi, ki je pridobljena prek proučevanja dostopne domače in tuje literature. V okviru tega sem izpostavil stvari, za katere menim, da so bistvenega pomena za razumevanje problematike. Pri tem so mi bile v veliko pomoč praktične izkušnje, ki sem jih pridobil pri svojem delu revidiranja informacijskih sistemov.
Nezanemarljiv prispevek temelji na znanju pridobljenim v okviru magistrskega študija Informacijsko-upravljalskih ved, saj sem pridobljeno znanje smiselno apliciral na obravnavano tematiko.
Kot sem že omenil, del magistrskega dela temelji na teoretičnih spoznanjih – sem spadajo predvsem temeljne razlage, zakonodaja, standardi in razlage posameznih pojmov. Ravno nasprotno pa sem predstavitev koristi IT notranjih kontrol obravnaval predvsem skozi praktični pristop, in sicer tudi s pomočjo zgledov. Mnogi med njimi temeljijo na mojih lastnih izkušnjah, vendar so predstavljeni v takšni obliki, da niso sporni s stališča zaupnosti med revizorjem in stranko. Podobno velja za predstavitev vzpostavitve IT notranjih kontrol, ki v veliki meri sloni na praktičnem pristopu.
Področje je sicer metodološko dobro podprto, kar predstavlja osnovo, ki sem ji pri svojem delu sledil. Upoštevanje standardov in strukturiranega pristopa je zagotovilo, da je subjektivna komponenta posameznika v kar največji meri izključena, poleg tega se zmanjša možnost izpustitve katerega od pomembnih elementov. Kjer obstaja več različnih pristopov, sem po svoji presoji izbral tistega, ki naj bi predstavljal najbolj zanesljivo in učinkovito pot do zastavljenega cilja. Obenem pa sem omenil in opisal vsaj osnovne značilnosti ostalih najpogosteje uporabljenih ali omembe vrednih z drugih vidikov.
Poseben izziv na obravnavanem področju predstavlja slovenska terminologija. Notranje kontrole v organizacijah z vidika informacijske tehnologije v slovenski literaturi niso tako

pogosta tema, da bi bilo izrazoslovje nedvoumno določeno, še dodatno zmedo pa povzroča dosledna uporaba angleških izrazov pri vsakodnevnem delu. Kljub temu sem v magistrskem delu navajal predvsem slovensko terminologijo, ki je ustrezno predstavljena z angleškimi sopomenkami.

2. IT notranje kontrole

2.1. Opredelitev notranjih kontrol

Skozi izkušnje so podjetja prišla do spoznanja, da tveganje, ki je predstavljeno kot kombinacija verjetnosti dogodka in njegovih posledic, lahko bistveno zmanjša vrednost njihovi organizaciji (The Institute of Risk Management, 2002, str. 6), čemur pa se je moč z ustrezno pripravljenimi in izvedenimi kontrolnimi mehanizmi izogniti oziroma vsaj ublažiti posledice. Posledično so kontrole potrebne povsod tam, kjer obstaja možnost napak, ki bi imele pomemben vpliv na poslovanje. Tako moramo za vsako pomembnejšo skupino transakcij znotraj pomembnih procesov, kjer zaznamo povečano tveganje, predvideti napake, ki bi se lahko pojavile, in hkrati postaviti ustrezne kontrole, da bi bile takšne nepravilnosti pravočasno odkrite oziroma naj bi bil celo preprečen njihov nastanek.

Notranje kontrole lahko razumemo kot procese, vzpostavljene s strani vodstva ali drugih odgovornih zaposlenih, z uporabo katerih si lahko do določene, primerno visoke stopnje zagotovimo doseganje ciljev na področju učinkovitosti in uspešnosti, zanesljivosti (na primer finančnega poročanja) ter skladnosti s predpisanimi pravili (Ecora, 2004, s. 6). Osnovna načela, ki tu veljajo so (COSO Definition of Control, 2006):

- notranje kontrole so procesi;
- najpomembnejši vpliv imajo ljudje, ne politike, navodila ali obrazci, temveč zaposleni na različnih nivojih;
- kontrole zagotavljajo le zmerno stopnjo varnosti, ne popolne;
- čeprav so kontrole praviloma ločene po skupinah glede na značilnosti, je potrebno upoštevati, da se prekrivajo in so v nekaterih primerih soodvisne.

Zelo pomembna je stopnja učinkovitosti notranje kontrole. Pri presojanju tega kriterija je potrebno upoštevati naslednje dejavnike (Meigs at al, 1996, s. 306):

- jasna določitev odgovornosti;
- vsaka pomembna transakcija mora iti skozi postopek avtorizacije, potrjevanja, izvedbe in beleženja;
- delitev dolžnosti in odgovornosti;
- ločitev računovodske funkcije od tiste, ki skrbi za upravljanje s sredstvi.

Za celovito razumevanje celotnega sistema praviloma najprej preučimo kontrole na ravni organizacije. Pri tem so pomembne predvsem stvari, kot so na primer velikost organizacije, sektor, njena kompleksnost in lastništvo, kajti te komponente imajo vpliv na vse ostale elemente na aplikacijskem nivoju.

Praviloma se s kontrolami srečamo najprej pri upravljanju s tveganji. Pri tem nam je v veliko pomoč poznavanje poslovnih procesov, saj na ta način lahko določimo kritične točke z

največjim tveganjem in na podlagi tega postavimo kontrole, na katere se bomo zanašali. Pri predvidevanju tveganja si pomagamo z določitvijo dogodkov, ki bi se lahko zgodili in imeli nasproten vpliv od pričakovanega oziroma želenega. Na podlagi tega se potem določijo kontrole, ki nam ponujajo določeno zagotovilo, da stvari ne bodo ušle izpod nadzora, temveč bodo potekale po predvidenem scenariju. Kontrol poznamo več vrst, vse pa morajo imeti skupne sledeče lastnosti, da se nanje lahko zanesemo:

- biti morajo dokumentirane;
- izvajati se morajo pravočasno;
- ves čas se morajo izvajati na primerljivi in zadovoljivi ravni (konsistentno) ter
- upravičiti morajo rezultat glede na svojo ceno.

Analiza kontrole nam pokaže, da je običajno sestavljena iz šestih elementov (Wilkinson, Cerullo, 1997, s. 248), in sicer iz:

- dejavnika kontroliranja;
- poslovnega procesa, v katerega je umeščena kontrola;
- indikatorja, ki zaznava stanje poslovnega procesa v danem trenutku;
- merila, s katerim je trenutno stanje primerjano;
- nadzornika, ki postavlja merila in
- mehanizma, ki primerja želeno in dejansko stanje ter proži ustrezne akcije.

Po namembnosti se notranje kontrole običajno delijo v tri skupine (Kramer, 2003, s. 9): preprečevalne, zaznavalne in popravljalne. Tu je še dodatna skupina notranjih kontrol, in sicer predvidevalne, ki bo z naraščajočo kompleksnostjo poslovnega okolja in razvojem inteligentnih sistemov zavzemala vedno večjo vlogo, ter sčasoma prerasla v enakovredno ostalim.

Preprečevalne kontrole so vse tiste, ki so vzpostavljene z namenom, da preprečijo nastanek dogodka, ki pomeni tveganje za poslovanje organizacije in so običajno že del poslovnih procesov, tipičen primer je razmejitev dolžnosti. Zamišljene so, da učinkujejo še preden se karkoli, kar bi imelo negativne posledice, zgodi in iz tega vidika imajo bistveno prednost pred ostalim kontrolami. Slednje pa pomeni, da moramo dogodke predvideti, še preden se pojavijo, kar predstavlja druge težave. Dostikrat je to zelo težko oziroma celo nemogoče storiti, zato jih pogosto zamenjujejo zaznavalne ali popravljalne. Preprečevalne kontrole se v največ primerih nanašajo na izvedbo nekega postopka po predpisanih fazah, kar pomeni, da je za njegovo izpeljavo potrebno slediti določenim korakom ter potek nadzorovati (Vangemi, 2003, s. 28). Njihova uporaba je dokaj pogosta, vendar imajo v določenih primerih prevelik vpliv na poslovni proces (na primer, potrebne so bistvene prilagoditve poslovnega procesa), da bi jih lahko uporabljali v kakršnihkoli razmerah. Zato je v vsakem konkretnem primeru potrebno presoditi, če je njihova uporaba res upravičena, nadalje pa je potreben stalen nadzor.

Naslednja vrsta kontrol, zaznavalna, nezaželen dogodek samo zazna in ga ne skuša preprečiti ali popraviti stanja. Značilen primer so različna beleženja, ki se pregledujejo periodično oziroma se na njihovi podlagi ustvarjajo poročila ali obvestila glede odstopanj in podobno. Marsikdo se verjetno sprašuje, zakaj preprečevalne kontrole v celoti ne nadomestijo zaznavalnih, saj bi s tem v večini primerov korenito zmanjšali potrebo po človeških virih.

Prav v tem pa se skriva bistvo prednosti zaznavalnih kontrol pred ostalimi, in sicer mnogokrat je razlikovanje med pravilnim in nepravilnim delovanjem tako zapleteno, da računalnik kljub vgrajenim zapletenim mehanizmom ni kos nalogi in ne more ugotoviti nepravilnosti ali pa prepogosto sproža lažne alarme. V tem primeru je boljše, da se dogajanje ob določenih predpostavkah samo beleži in se potem ročno preverja vsakokratno stanje. Druga prednost zaznavalne kontrole je, da nas lahko obvesti, da proces poteka po pričakovanjih. Ni torej potrebno, da gre nekaj narobe, dovolj je, da hočemo biti seznanjeni s stanjem ali potekom.
Popravljalne kontrole so nadgradnja zaznavalnih, saj moramo biti prepričani o zanesljivosti kontrole. Slednja poseže v dogajanje nekje vmes med časom, ko se pojavi napaka in obdobjem, v katerem bi se pojavili negativni učinki napake. V nekem procesu bi popravljalno napako prepoznali po tem, da zaustavi nadaljnje postopke in jih popravi v tolikšni meri, da še vedno lahko pričakujemo želeni rezultat. Te kontrole so dobrodošle pri vnosu podatkov, eden od preprostih primerov so tudi samodejni popravki v urejevalnikih besedil. Seveda kontrola v tem primeru in še v mnogih drugih deluje le z določeno stopnjo zanesljivosti, kar je potrebno upoštevati pri njeni uporabi. Tovrstne kontrole se izkažejo predvsem pri rutinskih operacijah, kjer so nezaželena stanja odkrita hitro in z veliko verjetnostjo, da ne gre le za napako pri zaznavi, poleg tega mora biti popravek vnaprej predviden in vgrajen v kontrolo.
Predvidevalne kontrole se uporabljajo zelo redko, saj je potrebno vložiti precejšna sredstva, da jih razvijemo do stopnje, ko so primerne za uporabo v kontrolnem sistemu. Težava se skriva v dejstvu, da je težko predpostavljati, kakšne napake se lahko pojavijo, še težje pa vzroke, ki povzročijo te napake. Tako so potrebni zapleteni algoritmi ali pa prisotnost človeškega dejavnika, in sicer v takšni meri, da potem kontrole ne prištevamo več k aplikacijskim temveč ročnim. Vendar razvoj tehnologije zagotavlja, da se bo uporaba tovrstnih kontrol povečala, cena njihove vpeljave pa se bo zmanjšala z dveh vidikov. Prvič, zaradi lažje dostopnosti potrebne tehnologije, in drugič, napaka, ki bo ugotovljena, še preden bo vplivala na samo izvajanje poslovnih procesov, bo odpravljena z manjšimi stroški oziroma teh stroškov sploh ne bo. Primer predvidevalnih kontrol, ki se ne nanaša neposredno na osnovne procese podjetja, temveč na podporne, je analiziranje prometa na vratih (portih), saj prek tega lahko zaznamo računalniški napad na informacijski sistem podjetja iz zunanjega omrežja. Tako lahko pravočasno sprejmemo zaščitne ukrepe, ki nam poleg preprečevalnih kontrol, ki so v tem primeru povezane s požarnim zidom, pomagajo zaščititi sredstva podjetja.
Druga razlika med kontrolami se nanaša na nivo, na katerem se izvajajo. Visokonivojske, kot je na primer pregled dosežene mesečne marže izveden s strani vodstva – to je zaznavalna kontrola kot večina tovrstnih – so določene s tem, da jih običajno izvajajo vodstvene strukture zaposlenih in pokrivajo večji obseg transakcij. Čeprav so dokaj učinkovite, se občasno ni mogoče povsem zanesti nanje. To velja za primer, ko jih izvaja oseba, ki nima dovolj dobrega razumevanja oziroma, ko obstaja nevarnost, da kontrola ne zazna dovolj dobro nivoja podrobnosti, ki je zahtevan za odkrivanje pomembnih napak. Primer tovrstnih kontrol so kazalniki poslovanja (key performance indicators). Vodstvo jih uporablja za spremljanje, merjenje in nadziranje poslovnih procesov. Kazalniki so merila, ki primerjajo različne podatke med seboj in kažejo dosežen rezultat v primerjavi s ciljem. Tukaj je potrebna previdnost pri uporabi kazalnikov kot kontrol, saj nekateri ne premorejo dovolj občutljivosti,

da bi lahko zaznali neko nepravilnost. Drugi pogoj je, da se spremljajo konstantno in ne le po potrebi, tretji pa da predhodno ustvarimo neka pričakovanja, na podlagi katerih potem analiziramo kazalnike.

Na drugi strani je primer nizkonivojske kontrole primerjava in uskladitev računa in dobavnice glede količine. Če so visokonivojske predvsem zaznavalne, so nizkonivojske večinoma tako zaznavalne kot preprečevalne. Preostale razlike se kažejo v tem, kdo je zadolžen za izvajanje oziroma nadziranje katere od obeh nivojskih skupin kontrol, pri čemer je izpostavljen položaj zaposlenega na hierarhični lestvici. Nadalje se visokonivojske za razliko od nizkonivojskih večinoma nanašajo na nek celoten proces in ne le del ter hkrati pokrivajo večje število transakcij, izvajajo pa se precej bolj poredko, najpogosteje tedensko ali celo mesečno, in ne dnevno kot večina nizkonivojskih.

Kar se tiče testiranja, izbiramo tiste kontrole, za katere domnevamo, da nam dajo zadostno zagotovilo glede trditev (assertions), ki jih potrebujemo pri finančnih izkazih. Trditve so v tem primeru predstavitve stanja, ki so podane s strani vodstva oziroma odgovornega za ravnateljevanje in so vključene v elemente finančnih izkazov. Potem ko pregledovalec zbere dovolj dokazov o vsaki od njih, razpolaga z zadostnimi dokazi za oblikovanje svojega mnenja glede učinkovitosti kontrol. Razdelimo jih lahko v pet skupin, ki so sledeče (Whittington, Pany, 2001, s. 136):

- obstoj (bilanca stanja)/pojav (izkaz poslovnega izida) [existance/occurance] - sredstvo ali obveznost obstaja na določen datum/transakcija ali dogodek se je dejansko zgodil;
- vrednotenje/merjenje [valuation/measurement] – sredstvo ali obveznost je zabeležena po pravi vrednosti/transakcija ali dogodek je zabeležen v pravem znesku;
- celovitost [completeness] – nezabeležena sredstva, obveznosti, transakcije, dogodki ali nerazkrite postavke ne obstajajo, velja tako za bilanco stanja kot za izkaz poslovnega izida;
- pravice in dolžnosti [rights and obligations] – velja le za postavke v bilanci stanja, sredstvo ali obveznost se res nanašata na pravi subjekt na določen datum;
- predstavitev in razkritje [presentation and disclosure] – postavka je razvrščena, opisana in razkrita v skladu s pravili.

Te trditve so sicer tudi del standardov revidiranja in se uporabljajo tako pri testiranju kontrol glede njihove učinkovitosti kot pri podrobnem preizkušanju podatkov. Njihov pomen se kaže v metodološkem pristopu, ki prispeva k sistematičnosti in celovitosti obravnavanja področja, zato je srečanje z njimi pri notranjih kontrolah neizbežno.

Vsaka vrsta kontrol ima prednosti in slabosti v določenih okoliščinah, zato je potrebno najti pravilno kombinacijo, ki kar najbolje ustreza potrebam dela. Pri izbiri si lahko pomagamo z napotilom, da moramo vedno stremeti k izdelavi učinkovitega sistema kontrol, ki mora upravičiti višino vlaganj vanj.

V organizacijah se vedno pogosteje uporabljajo kontrole temelječe na informacijski tehnologiji, ki se delijo na dve kategoriji: IT splošne kontrole in aplikacijske kontrole. Prve zagotavljajo, da informacijski sistem deluje pravilno in da so spremembe programske opreme ustrezno predlagane, potrjene in nazadnje tudi preverjene v testnem okolju. Nadalje mora biti dostop do te opreme nadzorovan, in sicer z dveh vidikov – eden se dotika politike

uporabniških imen in gesel, drugi pa fizične varnosti. Nekje vmes je varovanje pred vdori v omrežja, protivirusna zaščita in podobno. Po drugi strani se aplikacijske kontrole nanašajo na posamezne transakcije. Mednje lahko prištevamo potrjevanja in preverjanja ustreznosti podatkov določenim kriterijem, izračunavanja, vmesniki in podobno.
Kontrole, ki se zanašajo na računalniško pridobljene podatke, vendar še zahtevajo prisotnost človeka, se imenujejo IT odvisne ročne kontrole. Oboje, tako IT odvisne ročne kontrole kot aplikacijske, imajo isti cilj, to je zagotovitev zadostne verjetnosti, da so vse transakcije (Interno gradivo Ernst&Young):

- veljavne;
- odobrene;
- zabeležene;
- izpeljane v celoti;
- izvedene z zadostno mero natančnosti ter
- opravljene v ustreznem časovnem okviru.

Zagotovilo o učinkovitosti kontrole je odvisno predvsem od dveh dejavnikov, in sicer občutljivost kontrole in dokazilo, da je kontrola res v uporabi. Občutljivost se nanaša na lastnost kontrole, da je zmožna zaznati (in preprečiti, če je taka njena narava) napako, ki je materialno pomembna. Bolj kot je kontrola občutljiva, z večjo zanesljivostjo lahko domnevamo, da bomo odkrili vse nepravilnosti. Nadalje mora obstajati neko dokazilo o obstoju kontrole. Tu velja trditev, da kar ni dokumentirano, ni narejeno. Tako je v večini primerov potreben obstoj zapisa v formalni obliki, s katerim lahko preverimo izvedbo kontrole v določeni časovni točki ali obdobju in seveda tudi rezultat.
Preden se lahko zanesemo na aplikacijske ali ročne IT kontrole, moramo preveriti IT splošne kontrole, saj nam te zagotavljajo, da nihče nima prevelikega oziroma nenadzorovanega vpliva na informacijski sistem in bi lahko spreminjal potek transakcij. S tem ko zagotovimo njihovo učinkovitost in se posledično lahko zanesemo na aplikacijske ali IT odvisne ročne kontrole, si olajšamo nadzor nad transakcijami. Tu velja načelo, da če računalnik naredi nekaj pravilno, to lahko pri izpolnitvi določenih predpostavk ponovi poljubno mnogokrat. Tako lahko namesto podrobnega preizkušanja množice podatkov, preverimo le kontrolo na enem primeru in si s tem prihranimo dodaten trud.

2.2. IT splošne kontrole

Predpogoj, da se lahko zanašamo na aplikacijske notranje kontrole, je učinkovitost IT splošnih kontrol, ki zagotavljajo celovitost, natančnost in pravočasnost informacij, ki potujejo skozi informacijski sistem. Pomembno je vedeti, da se slednje nanašajo na posamezne aplikacije in se ne izvajajo na ravni transakcij. Najbolj pomembni sta kontroli dostopa in pa sprememb programske opreme, čeprav poznamo še ostale vrste, ki so povezane s področji arhiviranja, neprekinjenega poslovanja in podobno, vendar zaradi manjšega neposrednega vpliva na poslovanje ne bodo predstavljene samostojno, temveč bodo opisane skupaj kot kontrole IT poslovanja (IT operations).

2.2.1. Kontrole dostopa do programske opreme

V prvi vrsti je potrebno zagotoviti učinkovitost IT splošnih kontrol prek omejevanja dostopov. Z drugimi besedami to pomeni, da je dostopanje do podatkov in programov omejeno le na avtorizirane osebe, največkrat pa je potrebno dostop oziroma pravice definirati še bolj podrobno, in sicer na nivoju akcij – te so lahko poizvedovanje, izvajanje, brisanje, spreminjanje.

Preverjanje dostopov do programske opreme je običajno izvedeno v več fazah. Največkrat se začne s pregledovanjem splošnih nastavitev aplikacije in ugotavljanjem, če so le-te optimalne za učinkovito in varno delovanje. Sledi pregled ključnih elementov varnosti, ki se nanašajo na:

- dolžino gesel,
- sestavo gesla in njegova različnost od že uporabljenih,
- dobo po kateri je potrebno spremeniti geslo,
- zaklepanje po določenem številu napačno vnesenih gesel,
- kdo ima možnost spreminjanja gesla,
- dovoljen čas neaktivnosti preden se seja prekine,
- beleženje neuspešnih prijav v sistem in
- obvezno spremembo prvotno dodeljenega gesla.

Naslednja stvar, ki jo je potrebno preveriti, so sami uporabniki s pravicami dostopa do pomembnih informacij oziroma do orodij, s katerimi bi lahko vplivali nanje. Uporabnike je potrebno povezati z nalogami, ki jih opravljajo, in delovnimi mesti, na katerih so zaposleni, ter na ta način ugotoviti njihovo upravičenost do določenih pravic. Vsa ta preverjanja pa so brezpredmetna, če obenem ne preverimo tudi procedur dodeljevanja pravic in njihovega odvzemanja. Običajno imajo v podjetjih urejene predpise, kdo lahko zaprosi za dodelitev pravic, in kako ter v katerih primerih se le-te ukinjajo. Tu je potrebno omeniti slabost, in sicer to da informacija o odhodu zaposlenega iz podjetja ali prerazporeditev na drugo delovno mesto nemalokrat sploh ne pride do administratorjev aplikacij, čemur je krivdo mogoče pripisati slabi organizaciji. Pomembne izboljšave so lahko vpeljane z uvedbo enotne točke upravljanja z uporabniškimi računi, kar pa se zdi vodilnemu kadru v podjetju največkrat nepotrebno. Nadomestna kontrola oziroma kontrola, ki dopolnjuje pomanjkljivosti pri upravljanju z dostopi, je beleženje aktivnosti uporabnikov. To se lahko nanaša le na evidentiranje prijav v sistem ali pa tudi beleženje akcij, ki jih uporabniki izvajajo nad določenimi objekti. Vendar tudi to ni zadostno samo po sebi, temveč je potrebno sistematično spremljanje teh podatkov in ukrepanje ob srečanju z nepravilnostmi, saj le tako zagotovimo učinkovitost kontrole nad dostopi do programske opreme in s tem povezanimi elementi.

Pomembno področje pri dostopih je tudi fizično varovanje. Najpogosteje se v zvezi s tem zastavljajo vprašanja vstopa v določene prostore, med bolj pomembnimi je strežniška soba. Ta naj bi bila posebno varnostno opremljena, sredstva v njej pa naj bi lahko uporabljali le pooblaščeni zaposleni.

2.2.2. Kontrole sprememb programske opreme

Kot je že bilo omenjeno, se naslednja od pomembnejših vrst preveritev IT splošnih kontrol nanaša na pregled sprememb programske opreme. S tem se zagotovi, da so bile na aplikacijah, vmesnikih in infrastrukturnih elementih opravljene samo pravilno predlagane, testirane in potrjene spremembe, ki se lahko nanašajo na razvoj, vzdrževanje, popravke ali spremembe nastavitev. S testiranjem je potrebno izključiti tveganje oziroma ga zmanjšati na razumno mejo, da nepooblaščena oseba ni spreminjala programov, kar bi lahko vplivalo tudi na samo poslovanje podjetja. Najlažje je to zagotoviti prek razmejevanje dolžnosti. To pomeni, da je bil postopek same spremembe izpeljan po korakih, za katere so odgovorne različne, uradno določene osebe. Najprej je moral biti podan predlog, ki ga je pred nadaljnjo obravnavo preučila in potrdila njegovo primernost oseba, ki je odgovorna za takšne naloge. Po ustrezni analizi o izvedljivosti in smiselnosti realizacije je potrebna potrditev s strani druge ustrezne osebe, praviloma na višjem položaju. Od tu je potek postopka lahko zelo različen, vendar mora pripeljati do podobnih rezultatov, in sicer vpeljave nove funkcionalnosti ali popravka v informacijsko okolje organizacije. Še preden se opravi prenos v produkcijsko okolje je potrebno testiranje, ki mora biti praviloma opravljeno na ločenih sistemih, kar onemogoča morebitni negativni vpliv na informacijski sistem podjetja zaradi nepričakovanih napak; pozneje, po uvedbi je potrebno spremljanje samega delovanja. Vse faze morajo biti ustrezno dokumentirane, še posebno pozornost je potrebno nameniti prej omenjenim avtorizacijam na različnih stopnjah. V veliko pomoč so pri nadzoru nad spremembami računalniških programov orodja, kot je Visual Source Safe ali kakšen drug CVS (Concurrent Version System) sistem za nadzor nad spreminjanjem kode, seveda v primeru, da se programska oprema razvija interno.

2.2.3. Kontrole IT poslovanja

Med kontrole IT poslovanja se najpogosteje prišteva arhiviranje, ukrepe za neprekinjeno poslovanje in okrevanje po katastrofah, redkeje pa srečamo časovno razporejanje (Scheduling) ter upravljanje z napakami (Problem Management). Tako arhiviranje kot neprekinjeno poslovanje sta v nekaterih primerih tudi zakonsko predpisana, kar se nanaša na finančne ustanove oziroma bolj točno na banke. Arhiviranje je splošno znan koncept in ga ni potrebno posebej predstavljati. Omeniti velja le pomembnost odločitve o tem, kako pogosto se bodo izdelovali arhivi ter kje in koliko časa se bodo hranili. Potrebno je tudi ločevati pojma back-up in arhiv, saj je le slednji povezan s hranjenjem podatkov, ki niso nujno operativno potrebni skozi celotno obdobje. Neprekinjeno poslovanje se nanaša predvsem na ustrezen načrt, ki zagotavlja alternativne poti izvajanja poslovanja v primeru nepričakovanih dogodkov, ki bistveno vplivajo na infrastrukturo podjetja, druga stvar pri tem pa je načrt okrevanja. Ta predpisuje ukrepe, ki povrnejo poslovanje v prvotno stanje ali omogočajo poslovanje podobno tistemu pred samimi nepričakovanimi dogodki.

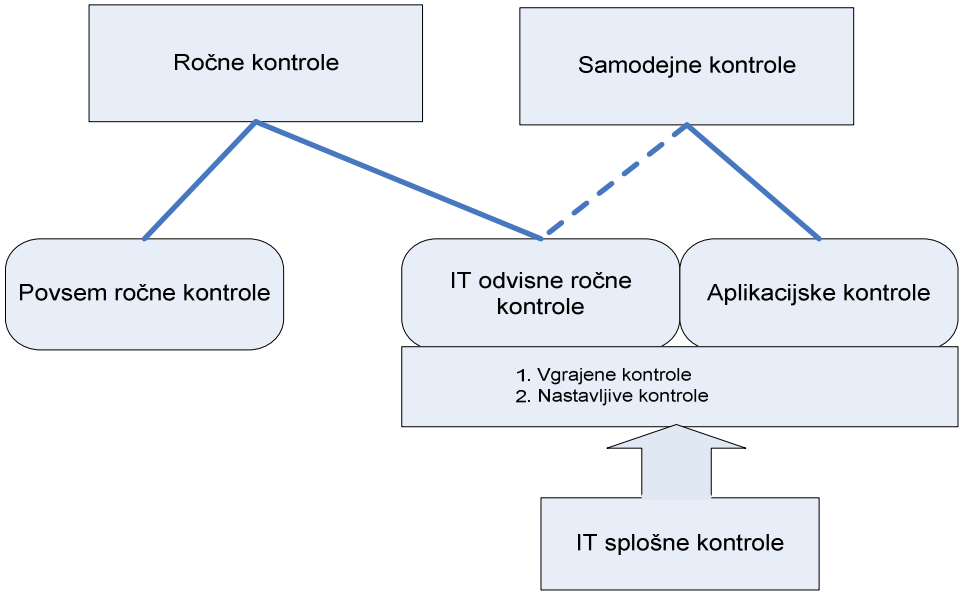
Časovno razporejanje je koncept, ki je povezan z načrtovanjem izvajanja programskih procedur. Nedeljiv del njega je tudi analiziranje odmikov od načrtov, ki bi se morebiti pojavili, in odprave vzrokov zanje. Nekakšno logično nadaljevanje je upravljanje z napakami,

ki pa zajema dosti širše področje, saj se ukvarja tako z odkrivanjem težav in nepravilnosti, njihovim dokumentiranjem, odzivom nanje ter njihovim preiskovanjem ter reševanjem.
Kontrole IT poslovanja se v primerjavi s kontrolami dostopa in sprememb programske opreme manj izpostavljajo, saj je njihovo nedelovanje manj kritično in ima običajno manjše neposredne posledice na poslovanje podjetja. Poleg tega je njihov pomen za delovanje aplikacijskih kontrol, ki so predstavljene v nadaljevanju, omejen.

2.3. Aplikacijske kontrole

Aplikacijske kontrole so avtomatski mehanizmi, ki se izvajajo na nivoju obdelave posamezne transakcije ter zagotavljajo ustrezen rezultat glede na parametre, ki so bili v tistem trenutku v veljavi. Njihov namen je nuditi ustrezno zagotovilo, da so vse transakcije veljavne, odobrene in zabeležene ter izvedene v celoti, z ustrezno natančnostjo in pravočasno. Umestitev aplikacijskih kontrol glede na ostale notranje kontrole je prikazana na sliki 1.

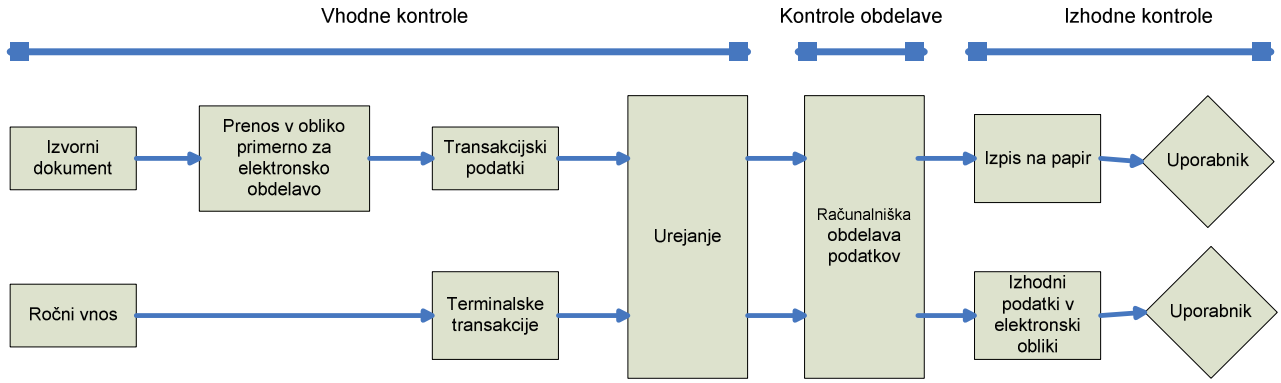
Slika 1: Shematski prikaz in umestitev notranjih kontrol



Vir: Interna dokumentacija Ernst&Young

Aplikacijske kontrole so ali že vgrajene ali pa so rezultat nastavitev. V prvem primeru so vključene v sami programski kodi in tako enovit del funkcionalnosti programske opreme, v drugem pa je kontrola rezultat nastavitev. To je pogost primer v celovitih programskih rešitvah (ERP sistemih). Dodatna razdelitev aplikacijskih kontrol, in sicer glede na fazo, v kateri se nahajajo podatki, je prikazana na sliki 2.

Slika 2: Razdelitev aplikacijskih kontrol glede na fazo, v kateri se nahajajo podatki



Vir: Wilkinson, Curello, 1997, s. 306

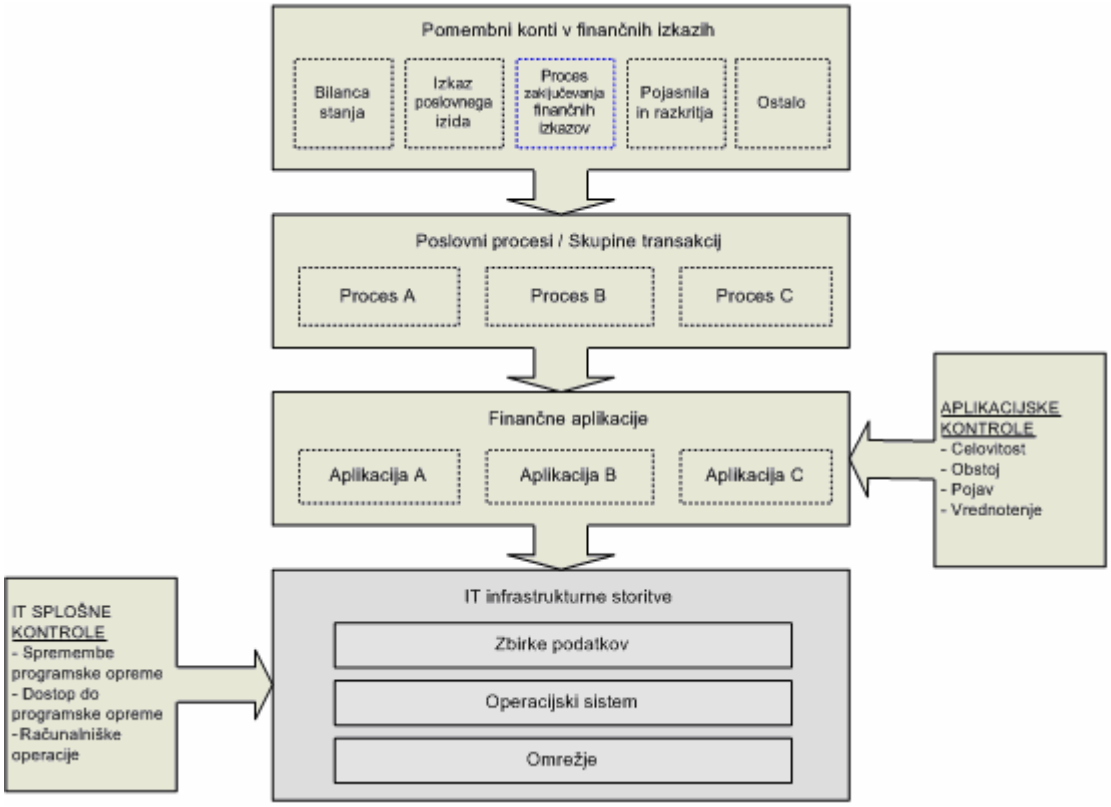
V praksi obstaja pet večjih skupin aplikacijskih kontrol, ki so predstavljene v nadaljevanju (Interna dokumentacija Ernst&Young):

- preverjanje vnosov (edit checks) – ta kontrola zmanjšuje tveganje, ki ga predstavljajo nepravilni vnosi, napačno procesiranje podatkov ali njihov nepravilni prikaz v smislu formata (na primer zneski morajo biti oblikovani kot številke);
- preverjanje veljavnosti (validations) – tudi ta kontrola zmanjšuje tveganje na podoben način kot prejšnja, in sicer pri vnosu, obdelavi in prikazu, le da se tu ne preverja format zapisa, temveč tolerančno območje, podvajanje in ujemanje (na primer, datum začetka projekta ne more biti starejši kot datum konca);
- izračuni (calculations) – kontrola, ki zagotavlja, da je rezultat računske operacije pravilen (kontrola je tu kar sam postopek izračuna);
- vmesniki (interfaces) – kontrola zmanjšuje tveganje nepravilnega vnosa, obdelave ali prikaza podatkov, ki so rezultat izmenjave z drugim sistemom (kot primer si je mogoče ogledati prenos podatkov iz saldakontov dobaviteljev v glavno knjigo, kjer popolnost prenosa preverimo s štetjem zapisov ali primerjavo vsote, lahko tudi s kontrolnim znakom) in
- avtorizacije (authorizations) – ta kontrola nam zagotavlja, da nepooblaščeni nimajo dostopa do pomembnih podatkov ali delov programske opreme, kjer bi lahko izvajali procedure, ki jim glede na delovno mesto in položaj niso dovoljene. Kontrola je lahko vzpostavljena s pomočjo razmejitev dolžnosti, preveritvami avtorizacij, omejitvami in hierarhijo (na primer, vloge so dodeljene v sistemu, ki dovoljujejo vnos novega dobavitelja samo določenim zaposlenim v nabavnem oddelku). Ta kontrola je zelo podobna skupini IT splošnih kontrol, ki se navezuje na kontrole dostopa do programske opreme. Pogosto se je mogoče zanašati na splošne kontrole, vendar je v nekaterih primerih potrebno preveriti dostop do neke točno določene table, modula ali drugega objekta, kateremu pri preverjanju splošnih kontrol ni bilo namenjeno zadosti pozornosti. Takrat je potrebno dodatno preveriti pravice dostopov, saj si le tako lahko zagotovimo, da z objektom upravljajo osebe, ki so pooblaščene za to.

Aplikacijske kontrole, na katere se bo podjetje oprlo pri nadzoru svojega poslovanja, se določijo (izmed vseh identificiranih) po tistem, ko so že opredeljeni pomembni procesi, kar pa

je neposredno odvisno od pomembnih kontov. Odnos med konti, procesi, aplikacijami in kontrolami, tako aplikacijskimi kot splošnimi, so prikazani na sliki 3.

Slika 3: Povezave med konti, procesi, aplikacijami in kontrolami



Vir: Verizon, 2006

Iz navedenega lahko sklepamo, da vse aplikacijske kontrole niso enako pomembne, temveč se lahko nekatere zanemarijo, in sicer iz dveh razlogov. Prvič, dve kontroli sta lahko povezani z istim tveganjem in v tem primeru je obravnavanje obeh povsem odveč. V drugem primeru pa se lahko kontrola nanaša na nek proces, ki ni bistven z vidika potrjevanja finančnih izkazov in tudi tukaj ni smiselno posvečati prevelike pozornosti takšni kontroli. To je seveda predstavljeno z vidika finančne revizije, povsem drugačen scenarij pa je mogoč pri gledanju z vidika podjetja. Nek proces je lahko podporni za drugega, nadvse pomembnega za poslovanje, in s tem pridobi na pomembnosti tudi kontrola vključenega v prvega. Bistveno pri tem je razumeti, da različni pristopi obravnavajo kontrole različno, zato je ključno v vsakem primeru upoštevati tudi vidike, ki niso očitni na prvi pogled, in tako maksimizirati koristi, ki jih kontrole prinašajo podjetju.

Izbira ustreznih aplikacijskih kontrol, na katerih se bo osnovalo kontrolno okolje, je pogojena tudi z zunanjimi faktorji gledano s stališča podjetja. Med njimi imajo najpomembnejšo vlogo zakonodaja, standardi in tehnologija, ki navsezadnje omogoča IT kontrole. Pri snovanju in uporabi slednjih moramo proučiti omejitve in možnosti vsakega posameznega prej omenjenega elementa, da pridemo do vzpostavitve kontrolnih mehanizmov, ki zadostujejo predpisom in potrebam ter hkrati ne onemogočajo optimalnega poslovanja.

3. Dejavniki, ki vplivajo na IT notranje kontrole

3.1. Zakonodaja

Nepravilnosti, ki se tičejo nepoštenega prikazovanja poslovnih rezultatov, so predvsem posledica pritiskov na vodstva podjetij, zlasti tistih, ki so kotirala na borzi, da ustvarjajo čim večje dobičke in tako vsaj kratkoročno povečujejo svojo vrednost. S tem privabljajo vlagatelje in ugodneje pridobivajo posojila in druge vire, s katerimi financirajo nadaljnje projekte. Na ta način so se mnoga podjetja ujela v začarani krog, ki jih je potiskal čedalje globlje v prirejanje finančnih izkazov. Na začetku so uporabljali le računovodske metode, ki jih zakonodaja ni predvidevala in zato sploh niso bili kaznivi, vendar to kmalu ni bilo dovolj. Za prikrivanje dejanskega stanja podjetja so začeli ponarejati dokumente, s čimer pa so stopili na pot računovodskih škandalov. Aferam so sledile razprave o ustreznosti dotedanjih zakonov in potrebnosti sprejetja novih. Glavne točke so bile poštenost vodstvenih in nadzornih organov pri upravljanju podjetij, notranje kontrole, usklajenost računovodskih in revizijskih standardov z zahtevami predpisov, računovodsko poročanje, neodvisnost revizorjev in analitikov.

Zakonodaja praviloma ne deli notranjih kontrol na ročne in na tiste, ki temeljijo na informacijski tehnologiji, temveč jih obravnava skupno. Obstajajo pa ločeni predpisi, ki se nanašajo na elektronsko poslovanje in posredno vplivajo na področje kontrol. Zato bo v nadaljevanju predstavljena splošna zakonodaja, pri čemer je potrebno upoštevati, da je njena implikacija na informacijsko tehnologijo pogojena še z ostalo zakonsko regulativo, ki pa zaradi obsežnosti in specifičnosti ni vključena v predstavitev.

3.1.1. Sarbanes-Oxleyev zakon

Že sam opis Sarbanes-Oxleyevega zakona pove, kaj je njegov namen. »Zakon za zaščito vlagateljev z uporabo izboljšane točnosti in zanesljivosti korporacijskih poslovnih poročil v skladu z zakoni o vrednostih papirjih in za druge namene« (To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes) sta pripravila senator Paul S. Sarbanes in kongresnik Michael G. Oxley. Vzroki zanj so bili našteti zgoraj, povod pa je bil škandal povezan z Enronovim primerom, slednje podjetje je bilo pred propadom leta 2001 sedma največja korporacija v ZDA. S tem dogodkom se je zaupanje delničarjev povsem porušilo in računovodsko-revizijsko sliko je bilo potrebno graditi znova. V skladu z zakonom je bil ustanovljen neodvisen zasebni nadzorni odbor za javno nadzorstvo računovodskih podjetij (PCAOB), ki ima nalogo, da vzpostavi računovodske in revizijske standarde ter nadzira in v določenih primerih tudi kaznuje računovodje in revizorje. Zakon poleg tega obravnava konflikt interesov, zahteva revizorjevo neodvisnost in osebno odgovornost vodstev podjetij za točnost finančnih poročil ter ščiti pred interesi investicijskih analitikov (The Business Forum Online: The Significance of the Sarbanes-Oxley Act, 2006).

Sarbanes-Oxleyev zakon (v nadaljevanju SOX) je razdeljen na enajst sekcij, vse so obvezne tako za velika kot majhna podjetja. Vsak del obravnava drugo temo, ki so naštete v spodnjem seznamu (Zakon Sarbanes-Oxley Act, 2006):

- Odbor za javno nadzorstvo delniških družb (Public Company Accounting Oversight Board, za odbor se uporablja kratica PCAOB),
- revizorjeva neodvisnost,
- korporacijska odgovornost,
- poudarjena finančna poročila,
- nasprotja interesov analitikov,
- sredstva in pooblastila SEC-a[2],
- študije in poročila,
- korporacijska in kriminalna odgovornost za prevare,
- povečanje kazni za kriminal belih ovratnikov,
- davek na dobiček korporacij,
- korporacijska prevara in odgovornost.

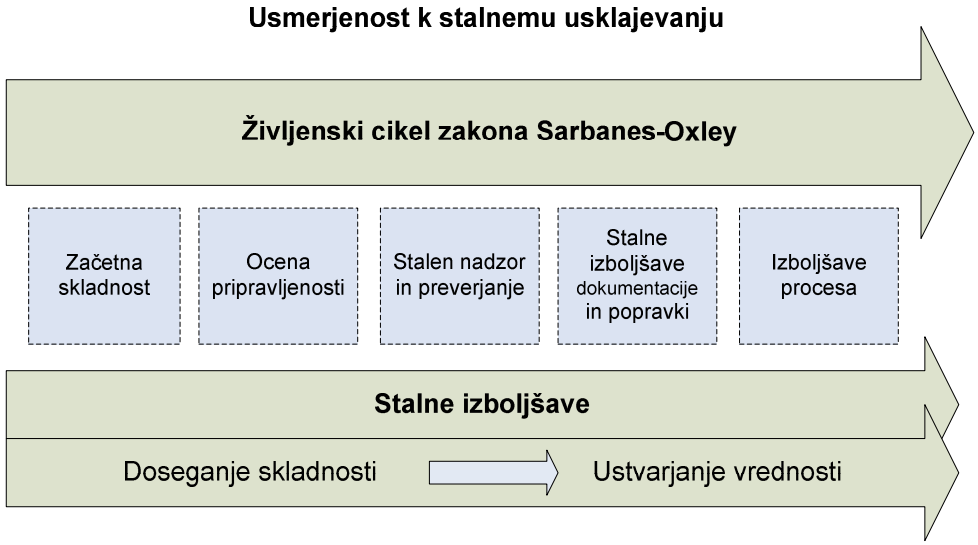
Ti deli se potem delijo še na nadaljnje sekcije, ki so označene glede na vrstni red. Tako je v tem primeru najbolj zanimiva četrta sekcija, ki se deli na sekcije od 401 do 409:

- razkritja v periodičnih poročilih (sekcija 401),
- poudarjeni ukrepi proti nasprotju interesov (sekcija 402),
- razkritja poslovodskih transakcij z vrednostnimi papirji (sekcija 403),
- poslovodska ocenitev notranjih kontrol (sekcija 404),
- izjeme (sekcija 405),
- etični kodeks poslovodstva podjetja (sekcija 406),
- razkritje finančnega strokovnjaka revizijskega odbora (sekcija 407),
- poudarjene zahteve pregledov razkritij v izdajateljevih periodičnih poročilih (sekcija 408) in
- pravočasna izdajateljeva razkritja (sekcija 409).

Z vidika tega magistrskega dela je najpomembnejša sekcija 404, ki se ukvarja z notranjimi kontrolami z vidika upravljanja podjetja, zato ji bo v nadaljevanju posvečeno več pozornosti.
Nekatere organizacije razumejo zahteve SOX-a le kot dodatni strošek, vendar lahko iz tega potegnejo koristi zase. Na ta način lahko bolje organizirajo poslovanje in izboljšajo nadzor nad procesi. Na sliki 4 je prikazan celotni cikel, ki ga zajema zakon.

[2] Security Exchange Commission (Komisija za vrednostne papirje in borze).

Slika 4: Grafični prikaz življenjskega cikla Zakona SOX



Vir: Prirejeno po KPMG, 2004, s. 30

Na podlagi SOX-a je PCAOB (Odbor za javno nadzorstvo delniških družb) pripravil Revizijski standard številka 2. Ta govori o reviziji notranjih kontrol pri izvedbi finančnega poročanja vključno z revizijo finančnih izkazov in sedaj v skladu z zakonom zahteva od vodstva, da oceni in poroča o učinkovitosti notranjih kontrol, ki se tičejo finančnega poročanja, od zunanjih revizorjev pa, da preverijo učinkovitost istih notranjih kontrol in poročajo o tem, poleg tega pa še ovrednotijo oceno vodstva. V okviru tega procesa mora vodstvo upoštevati več zahtev, in sicer (Interno gradivo EY):

- sprejeti odgovornost za učinkovitost notranjih kontrol finančnega poročanja v podjetju;
- pri ocenjevanju učinkovitosti notranjih kontrol se morajo posluževati konsistentne metodologije (ta ni predpisana, vendar se priporoča uporaba standarda COSO);
- sklepi morajo biti podprti z dokazili, največji pomen pri tem ima dokumentacija in
- konec vsakega poslovnega obdobja mora biti v pisni obliki pripravljena ocena učinkovitosti notranjih kontrol.

V primeru revizorjeve ocene, da je vodstvo naredilo to pomanjkljivo, je potrebno pisno opozorilo, pozitivno mnenje se ne sme izdati.

V okviru ocenjevanja kontrol s strani vodstva je izvedenih več korakov. Ti v začetni stopnji vključujejo odločitev o tem, katere kontrole bodo testirane, ocenjena mora biti možnost (kolikšna je verjetnost), da kontrole ne delujejo, kar se odraža v napakah materialne pomembnosti, ter v primeru, da je podjetje razdeljeno na več lokacij ali poslovnih enot, se mora sprejeti sklep, katere od njih bodo zajete v ta proces.

Revizorji smejo svoje mnenje oblikovati samo na podlagi neposrednih dokazov. To pomeni, da morajo pridobiti potrditev o učinkovitosti kontrole iz dejstev, ki so rezultat kontrole, ne smejo pa se zanašati na ocene vodstva. V okviru razpoložljivega časa in ostalih virov, ki jih imajo na razpolago, morajo sami preizkusiti delovanje kontrole v taki meri, da se lahko zanesejo nanje z zadostno mero verjetnosti. Poleg učinkovitosti same kontrole mora revizor

potrditi tudi zadostno dokumentiranost njene vzpostavitve in preizkušanja s strani vodstva. V primeru, da dokumentacija ne obstaja ali je nezadostna, se to označi kot notranja pomanjkljivost kontrole. Pri celotnem ocenjevanju kontrol se je potrebno zavedati še ene pomanjkljivosti – to je človeškega dejavnika. Zaradi tega se nikoli ne smemo popolnoma zanesti na kontrole, saj se lahko pojavi napaka zaradi neustrezne presoje ali pa kot posledica druge človeške napake.

Ocenjevanje notranjih kontrol v podjetju za potrebe finančnega poročanja mora biti, kot je že bilo omenjeno, izvedeno v takem obsegu, da zadosti potrebam potrditve ustreznosti vpeljave postopka in testiranje učinkovitosti same kontrole. Nadzor mora obsegati vsaj elemente predstavljene v tabeli 1.

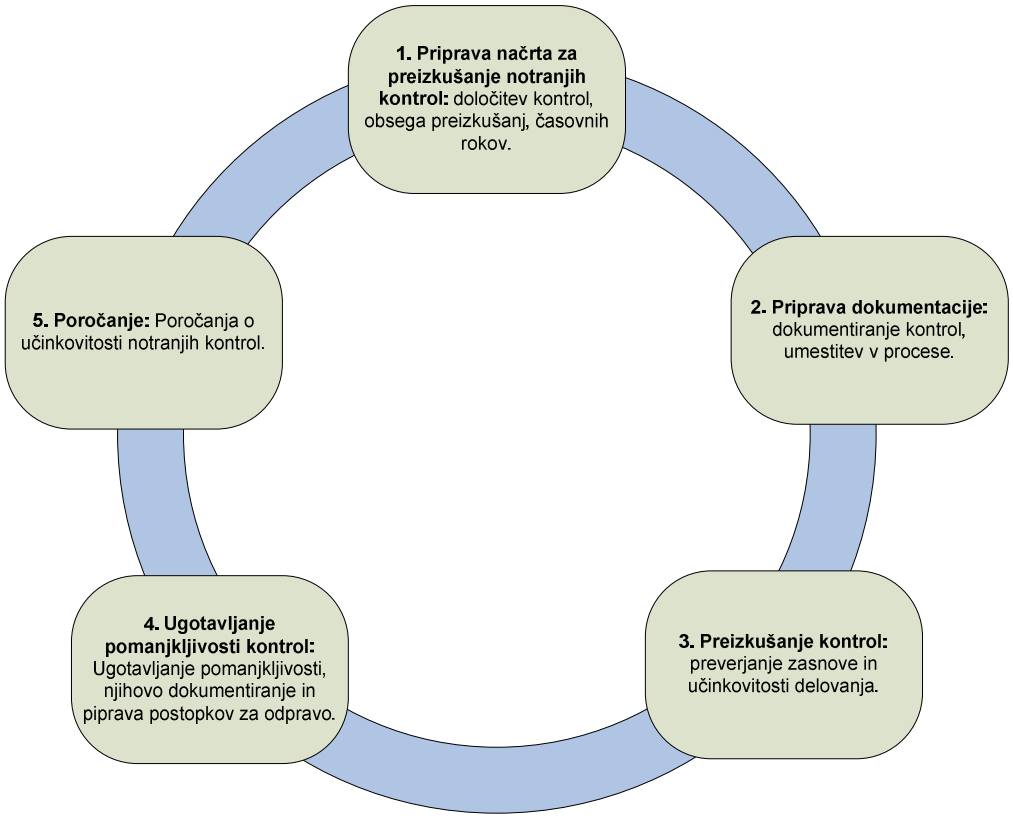
Tabela 1: Nadzor nad pomembnimi računovodskimi postavkami in razkritji za namene ocenjevanja učinkovitosti notranjih kontrol

Področje nadzora	**Opis**
Nadzor nad iniciativo, potrjevanjem (avtoriziranjem), evidentiranjem, izvajanjem in poročanjem o pomembnih računovodskih postavkah in razkritjih v povezavi z ustreznimi trditvami (assertions) v finančnih izkazih.	Pomembnost je odvisna od vrednosti, obsega in stopnje tveganja v povezavi s finančnim poročanjem v okviru izvedene transakcije.
Nadzor v povezavi z izborom in uporabo računovodskih načel, ki jih predpisuje GAAP (Generally Accepted Accounting Principles / Splošno sprejeta računovodska načela oziroma standardi revidiranja).	Vodstvo mora preučiti vpeljavo kontrol z namenom nadzora nad ustrezno uporabo računovodskih usmeritev in tolmačenj v pravem časovnem obdobju.
Nadzor, ki se nanaša na preprečevanje, identifikacijo in zaznavanje prevar.	Naloga vodstva je, da pripravi in izvaja programe ter kontrole, ki pravočasno zaznavajo in preprečujejo prevare. Poleg tega mora vodstvo skupaj s tistimi, ki neposredno skrbijo za nadzor nad finančnim poročanjem, dati posebno skrb za ustvarjanje in vzdrževanje ustrezne kulture v podjetju, ki temelji na poštenosti in visokih moralnih standardih.
Nadzor nad splošnimi IT kontrolami ali drugimi kontrolami, na katere se zanašajo ostale pomembne kontrole.	IT splošne kontrole so temelj za učinkovitost aplikacijskih kontrol, in sicer prek zagotavljanja nespremenjenega delovanja informacijskih sistemov.
Nadzor, ki se navezuje na proženje (initiating) in izvajanje nerutinskih in nesistematičnih transakcij.	Tu je poudarek pogosto na presoji in ocenah. Na ta način pri izbiri kontrole vnesemo pristranskost ocenjevalca, ki presodi kompleksnost opazovanega procesa.
Nadzor nad finančnim poročanjem konec poslovnega leta vključno s pripravo finančnih izkazov in razkritij.	Kontrole vključno s tistimi, ki se uporabljajo pri vnosu podatkov o transakcijah v poslovne knjige, pri različnih operacijah v glavni knjigi ter pri knjiženju popravkov v finančnih izkazih.

VIR: KPMG, 2004, s. 23

Ocenjevanje notranjih kontrol s strani vodstva in revizorjev (pri slednjih je dodatno potrebna še izdelava mnenja o oceni vodstva) je v nekaterih korakih podobna. Eden od načinov, kako se lahko procesa ocenjevanja loti vodstvo podjetja, da zajame zahteve zakona SOX, je predstavljen na sliki 5.

Slika 5: Proces ocenjevanja notranjih kontrol v skladu s SOX



Vir: Interno gradivo EY

Prva stopnja, to je načrtovanje, vključuje izbiro pristopa k dokumentaciji, identifikacijo kontrol, ki se bodo testirale, in obdobje, v katerem bo projekt izveden. Glede tega se ne določi samo končni datum, temveč tudi vmesne časovne točke, pri katerih morajo biti pomembni deli dokončani. V okviru planiranja se morajo definirati tudi morebitne politike in procedure, še posebno pozornost pa je potrebno nameniti izbiri ekipe. Ta je sestavljena iz sponzorja (dovolj vplivnega v podjetju), projektnega vodja ter osebja iz posameznih oddelkov podjetja, vsi od naštetih pa morajo imeti tudi zadostno razumevanje s področja notranjih kontrol in metodologije, ki se bo uporabljala. Če je njihovo znanje pomanjkljivo, je potrebno razmisliti o dodatnem izobraževanju, še preden se začne samo ocenjevanje notranjih kontrol.
Kot je že bilo rečeno, se v fazi planiranja določijo kontrole, ki se bodo testirale. PCAOB določa, da se morajo vključiti tiste kontrole, ki se nanašajo na pomembne računovodske postavke in razkritja v finančnih izkazih. V Standardu številka 2 je postavka prepoznana kot pomembna, če lahko vsebuje napako, ki ima sama ali skupaj z drugimi napakami, materialni pomen za finančne izkaze (PCAOB - Auditing Standard No. 2, 2006). Pri načrtovanju se

morajo sprejeti še odločitve, katere IT kontrole se bodo testirale, katere geografsko ali drugače razdeljene enote bodo vključene ter kako se bodo upoštevale storitve, ki jih opravljajo zunanji izvajalci. V zvezi s tem je mogoče od pogodbenih partnerjev zahtevati različne dokumente, seveda v smiselnem obsegu.

Naslednji korak je dokumentiranje kontrol, kar je zelo pomemben del procesa. Dokumentiranje dokazuje, da so kontrole bile identificirane, določene so bile dolžnosti zaposlenih v zvezi z njihovim izvajanjem ter da se spremlja njihovo delovanje. Dokumentiranje je odvisno od več dejavnikov, kot so velikost in organiziranost podjetja. Pri tem ni pomembno ali je dokument v grafični ali pisni obliki, vendar je priporočljivo, da se uporabljajo neki standardni vzorci. Kontrola mora biti ustrezno opisana (vključno z njeno vzpostavitvijo), enako velja za rezultat testiranja. Slednje mora biti predstavljeno v širši obliki, saj ni dovolj, da je samo zapisano ali je kontrola učinkovita ali ne. V primeru, da ni učinkovita, mora biti v dokumentacijo dodan predlog, kako jo izboljšati. Dokumentiranje je izredno pomembno, saj brez tega kontrola ne more biti prepoznana kot učinkovita, po drugi strani pa je tudi težavno. Po raziskavi revizijske hiše KPMG je prav ta korak najtežji od vseh (KPMG, 2004, 16).

Postopki, ki sledijo se nanašajo na preizkušanje učinkovitosti notranjih kontrol – tako z vidika vzpostavitve kot delovanja. Učinkovitost vzpostavitve kontrole se nanaša na vprašanje, če je bila kontrola zasnovana tako, da lahko prepreči ali zazna napako materialne pomembnosti pri neki trditvi (assertion) v zvezi s finančnim izkazom. Učinkovitost delovanja pa pomeni, da deluje v skladu z zasnovo. O učinkovitosti se lahko prepričamo na več načinov. Za preverjanje zasnove je dovolj tudi poizvedovanje, medtem ko se je za delovanje potrebno poslužiti opazovanja ali katere druge neposredne oblike testiranja.

Pri kontrolah, za katere smo ugotovili, da so neučinkovite, je potrebno natančno določiti pomanjkljivosti, njihovo pomembnost ter tudi kako to odpraviti. Pomanjkljivost pri notranji kontroli obstaja, ko njena vpeljava ali izvajanje ne omogoča zaposlenim, da zaznajo ali preprečijo nepravilnosti pri normalnem izvajanju poslovnih funkcij. Pomanjkljivost se lahko nanaša na samo zasnovo kontrole ali na njeno delovanje. Zasnova je nezadostna, če kontrola dejansko sploh ne obstaja ali pa je zasnovana napačno, tako da tudi takrat, ko se izvaja, ne zazna napake. Pomanjkljivost v delovanju se pojavi, ko kontrola na deluje tako, kot je bila zasnovana, ali pa oseba, ki jo izvaja nima potrebnih pooblastil oziroma znanj za njeno izvajanje. Pomanjkljivosti so lahko nepomembne, pomembne ali materialne. Samo pri nepomembni lahko ocenjevalec po predhodnem prepričanju, da tudi v povezavi z drugimi pomanjkljivostmi nima pomembnega vpliva na finančne izkaze, opredeli kontrolo kot učinkovito. Razlika med pomembno in materialno pomanjkljivostjo je samo v velikosti napake, ki se lahko pokaže kot posledica nedelovanja te kontrole v finančnih izkazih.

Zadnji korak v ocenjevanju kontrol, je poročanje. V letno poročilo mora biti v skladu z zahtevo SOX-a vključena ocena učinkovitosti notranjih kontrol. Poročilo vodstva organizacije mora vključevati (Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 2006):

- določilo o odgovornosti vodstva za zasnovo in izvedbo notranjih kontrol v podjetju, ki se nanašajo na finančno poročanje;

- predstavitev metodologije, ki je bila uporabljena pri ocenjevanju učinkovitosti notranjih kontrol;
- ocena učinkovitosti notranjih kontrol na koncu poslovnega leta, pri čemer mora biti za vsako kontrolo predstavljena njena ocena in
- izjavo, da je revizijska hiša podala mnenje na poročilo vodstva o notranjih kontrolah.

Potrebno je še poudariti, da oblika poročila ni formalno predpisana, ter da je kontrola na koncu poslovnega leta lahko prepoznana kot učinkovita, čeprav med letom ni bila. V tem primeru so morali biti sprejeti ukrepi, ki so izboljšali kontrolo do te mere, da so napake odkrite, sama kontrola pa mora biti dodatno preverjena.
Sarbanes-Oxleyev zakon zahteva tudi od revizorja, da oceni učinkovitost notranjih kontrol, obenem pa mora ovrednotiti oceno vodstva o tej temi. Sam potek procesa ocenjevanja je prikazan na sliki 6.

Slika 6: Koraki pri ocenjevanju notranjih kontrol v podjetju s strani revizorja

Vir: Avtor

Tudi na strani revizorja se vse začne z načrtovanjem, ki vključuje med drugim izdelavo strategije in odločitev o različnih faktorjih, ki vplivajo na izvedbo analize notranjih kontrol. Poleg tega je potrebno določiti materialnost, kar pomeni znesek, na podlagi katerega se določi pomembnost napak pri kontrolah. Logično je, da bodo preverjene tiste kontrole, ki so povezane s tveganji, katere imajo lahko pomemben vpliv na finančne izkaze. Določiti je potrebno tudi poslovne enote, ki bodo vključene v ocenjevanje. V zvezi s tem se odločitve sprejemajo na podlagi tega, kako finančno pomembne so te glede na celoto, in ali predstavljajo kakšno posebno tveganje. Za enote, ki so spoznane za finančno pomembne, mora revizor ovrednotiti dokumentacijo vodstva in preveriti kontrole za vse ustrezne trditve (assertions), ki se nanašajo na pomembne postavke in razkritja. Čeprav odstotek pokritosti poslovanja oziroma finančnega položaja ni natančno določen, naj bi izbrali tiste pomembne enote, ki bi pokrivale vsaj 65 odstotkov prvega ali drugega kriterija (PCAOB - Auditing Standard No. 2, 2006). Pri poslovnih enotah, ki so materialno pomembne, kadar jih združimo

glede na nek kriterij, je potrebno preveriti, če je vodstvo družbe vpeljalo in dokumentiralo kontrole na nivoju podjetja. To so tiste kontrole, ki nadzirajo poslovanje, kontrolno okolje in so povezane s postopki ocenjevanja tveganja. Če ne obstajajo ali niso učinkovite, potem se je treba spustiti na nivo notranjih kontrol v enoti in jih oceniti.
Naslednji korak se nanaša na vrednotenje ocenjevanja notranjih kontrol, ki je bilo opravljeno s strani vodstva. Revizor mora tako razumeti proces ocenjevanja, ki ga je pripravilo vodstvo podjetja, ter podati oceno, če so bile testirane prave kontrole – ali so se nanašale na ustrezne trditve (assertions), računovodske postavke in razkritja. S procesom mora biti seznanjen v taki meri, da lahko odloči tudi, če so bile vključene prave poslovne enote, ali so bili rezultati, ugotovljeni s strani vodstva podjetja, pravilno predstavljani in tudi ali so kontrole sploh učinkovite, in sicer tako z vidika delovanja kot dokumentiranja.
Revizor spozna notranje kontrole s poizvedovanjem pri osebju stranke, s preučevanjem dokumentacije, opazovanjem kontrole in spremljanjem transakcij skozi celotni cikel (walk-through). Za razliko od vodstva se revizor bolj osredotoči na kontrolni sistem kot skupek kontrol, ki se med seboj dopolnjujejo, in ne toliko na posamezne kontrole. V primeru, da neka kontrola že pokriva določeno tveganje, mu preostalih kontrol, ki se nanašajo na isto stvar, ni potrebno dodatno testirati. Nadalje mora revizor določiti pomembne procese in glavne skupine transakcij. Vodilna kriterija sta vpliv na finančne izkaze v kvantitativnem smislu in tveganje, ki se razume kot kvalitativni kriterij. Priprava finančnih poročil ob koncu obdobja je vedno pomemben proces, zato je podrobnejše seznanjanje z njim neizogibno. Za vsak razred pomembnih transakcij mora biti opravljen vsaj en »tokohod« (walk-through) skozi celoten potek, kar pomeni sledenje od samega začetka transakcije do knjiženja v glavno knjigo, tako v informacijskem sistemu kot z uporabo papirnih dokumentov.
Potem ko ima revizor zadostno razumevanje kontrolnega sistema, lahko preide na samo testiranje, na podlagi česar določi, če je kontrola zasnovana pravilno in ali deluje učinkovito. Do rezultatov lahko pride na podlagi različnih metod, od opazovanj, kar mnogokrat ni dovolj, do ponovitev operacij in podobno, pogosto pa velja, da so bolj preproste metode uporabnejše. Tudi za kontrole, ki so podprte z informacijsko tehnologijo velja, da jih je velikokrat moč preizkusiti na zelo preprost način.
Revizorjevo delo je vedno zaključeno z mnenjem, tako je tudi glede ocenjevanja notranjih kontrol. V določenih primerih lahko revizor izdelavo mnenja celo odkloni, na primer, ko ne more pridobiti podatkov. Obstaja tudi možnost, da revizor izda ločeni mnenji, eno za finančne izkaze in drugo za notranje kontrole. Za pomanjkljivosti Sarbanes-Oxleyev zakon zahteva, da revizor opozori vodstvo in revizijski odbor v podjetju še pred izdajo samega mnenja.
Kot je bilo razbrati iz zgornjega opisa Sarbanes-Oxleyevega zakona, so postopki glede zagotavljanja skladnosti dokaj natančni in strogi. Izven Združenih držav so predpisi bolj ohlapni, vendar je njihov namen dokaj podoben, kar bo razvidno iz njihove predstavitve v nadaljevanju.

3.1.2. Osma direktiva Evropske skupnosti

ZDA so, za razliko od Evropske skupnost, veliko bolj homogena tvorba, kar se odraža tudi na zakonodajnem področju. Vsaka evropska država ima še vedno veliko svojih pravil, ki

korenito posegajo v vsakodnevno življenje državljanov in poslovanje družb. Kljub težnjam, da bi se ustvaril enoten trg, skušajo predvsem večje države vsiliti svoje poglede in tako uveljaviti lastne interese.

V osnovi se ameriški in evropski zakoni ne razlikujejo dosti, vendar podrobnejši pogled razkriva drugačno sliko. V ZDA so stvari veliko bolj natančno določene, vsaj kar se tiče računovodskih predpisov, varovanja zasebnosti in varnostnih določil. Zakonodajalci v Evropi se trudijo doseči ravnovesje s pomočjo regulative, ki temelji na načelih, ki pa so manj stroga.

Osma direktiva se pogosto primerja z Zakonom Sarbanes-Oxley, vendar je med njima kar nekaj razlik. Prva in najpomembnejša je seveda ta, da direktiva še ni v polni veljavi, čeprav je bil predlog objavljen že 16. marca 2004, uvajati pa se je začela jeseni 2005. SOX je veliko bolj obsežen in tudi natančen kar se tiče notranjih kontrol. Še bolj pa zaostruje pravila na tem področju Standard številka 2, ki ga je izdal PCAOB, ustanovitev slednjega organa pa je neposredna posledica zakona (SOX-a). Osma direktiva je bolj skupek več direktiv in predpisov, nacionalnih vplivov in priporočil Odbora evropskih regulatorjev za vrednostne papirje (Committee of European Securities Regulators).

Že v letu 1999, še preden so se pojavili veliki finančni škandali, je Evropska komisija začela izvajati petletni načrt izboljšanja enotnega finančnega trga. Ta je imel tri glavne cilje (Internal Market and Financial Services, 2006):

- ustanovitev enotnega trga za celotne finančne storitve,
- odpreti in poskrbeti za varnost na kapitalskih trgih ter
- poostriti pravila v okviru smiselnega nadzora.

Na tem področju je Evropska komisija sodelovala z vladami držav članic, različnimi združenji in interesnimi skupinami ter razvila pravila, ki temeljijo na čezmejni tekmovalnosti, neoviranem dostopu do trgov, transparentnosti in integriteti trgov, njihovi finančni stabilnosti in učinkovitosti. Načrt za obdobje od leta 2005 do leta 2010 je že izdelan, v pripravi pa je tudi že naslednji za drugo petletno obdobje.

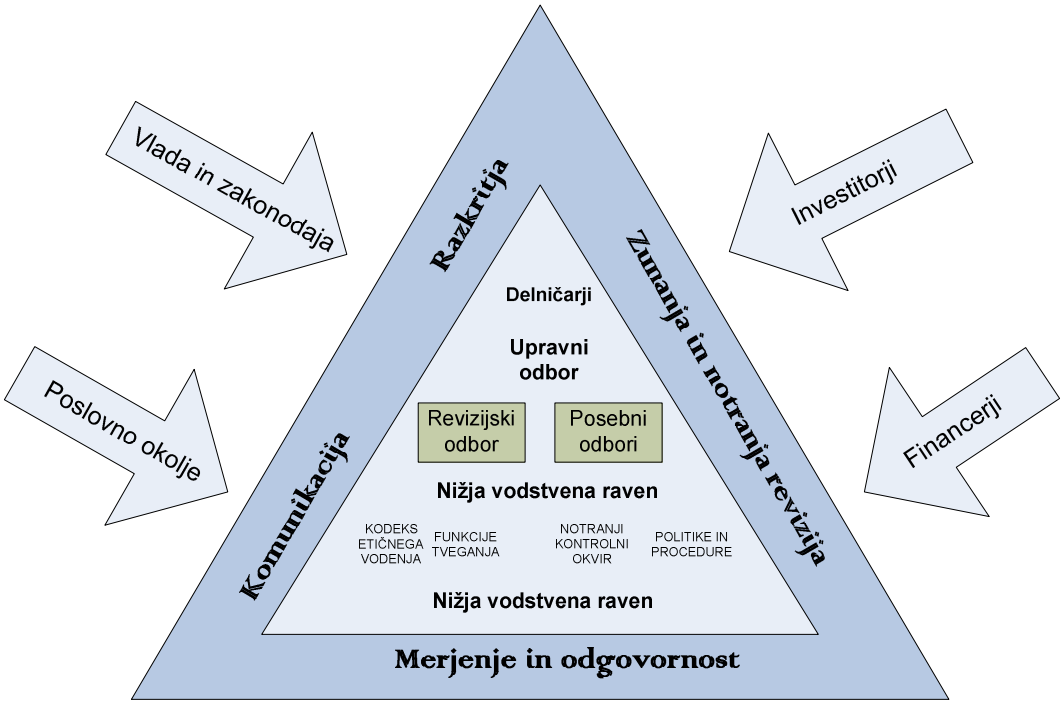
V Evropski skupnosti obstajajo vplivnejši predpisi od direktiv (slednje morajo posamezne države sprejeti v svojo zakonodajo), to so zakoni, ki veljajo za vse države članice, brez da bi jih te posebej potrjevale. Trije takšni, ki se nanašajo na finančni trg in posledično na računovodske ter revizijske prakse so:

- Evropski podjetniški statut (olajša podjetjem poslovanje v drugih državah, brez da bi jim zato bilo treba ustanavljati podružnice),
- predpis o čezmejnem plačevanju v evrih in
- mednarodni standardi računovodskega poročanja (zagotavljajo večjo transparentnost in preglednost finančnih izkazov; s 1.1.2005[3] morajo evropska podjetja, ki kotirajo na borzah, pripravljati izkaze tudi v skladu z mednarodnimi standardi za računovodsko poročanje).

[3] V skladu z mednarodnimi standardi računovodskega poročanja morajo poročati za poslovno leto, ki se začne s 1.1.2005 ali pozneje in za primerjalna obdobja.

Nekatere države si delijo skupno mnenje, da je sprejemanje skupne zakonodaje na nivoju Evropske skupnosti prepočasno, zato so same bolj aktivne na tem področju. V to jih silijo domači škandali ali pa mednarodni trendi. Takšna primera sta Francija in Velika Britanija.
Z vidika vodstva podjetja ima Osma direktiva predvsem dve pomembni točki, prva je odgovornost revizijskega odbora, druga pa odnosi z revizorji. Kar se tiče prve, je pomembno, da imajo vsa javna podjetja – to so tista, ki kotirajo na organiziranih trgih – revizijski odbor. Njegova glavna naloga bo skrb za upravljanje s tveganjem, za kar se bo potrebno bolj posvetiti funkciji interne revizije in sistemu notranjih kontrol. Druga točka, to je odnos z revizorji, se dotika izbora revizorjev. Za to bo sedaj odgovoren revizijski odbor, njegova naloga pa bo tudi skrb za revizorjevo neodvisnost. V to spada omejen, seveda v smiselnih mejah, odnos vodstva z revizorjem.
Iz zgoraj povedanega sledi, da bo z uveljavitvijo Osme direktive dokaj pomembno vlogo dobil revizijski odbor (njegova umestitev je razvidna s slike 7). Ta bo v dobršni meri spremenil sprejemanje odločitev glede računovodskega poročanja. V odboru bo morala biti najmanj ena oseba z dobrim finančnim in tudi računovodskim znanjem, ki bo zmožna izbrati primernega revizorja. Odbor bo tudi skrbel za komunikacijo revizorja in neizvršnih direktorjev podjetja brez vmešavanja najvišjega vodstva, kar bo prispevalo k neodvisnosti izvedbe same revizije. To pomeni, da bo vmešavanja sedaj manj in bodo tudi interesi vodstva izraženi v manjši meri. Vsekakor se je treba zavedati, da je to teorija, v praksi se potem marsikaj izkaže drugače, kot je bilo zamišljeno. Da vse ni tako črno, kažejo primeri, ko so podjetja že prehitela samo zakonodajo in so uvedla stvari, ki jih bo zahtevala šele v prihodnosti sprejeta zakonodaja.

Slika 7: Shema položaja revizijskega odbora v spremenjenih okoliščinah glede na Osmo direktivo



Vir: Turley, 2004

Kot je bilo že rečeno, bo imela Osma direktiva največji vpliv na revizijski odbor in njegovo spremljanje tveganja. Tako bo odbor moral spremljati notranje kontrole v podjetju in poročati o njihovi učinkovitosti. V primeru, da bo odkril pomanjkljivosti, bo od njega pričakovano, da predlaga ali izvede aktivnosti, ki bodo vodile v njihovo odpravo. Na plečih odbora bo tudi funkcija notranje revizije. Pri tem bo tesnejše sodelovanje z zunanjim revizorjem večjega pomena, kot je bilo do sedaj. Nenazadnje bo nov položaj določen z zakonodajo in bo razširjen na večje število organizacij, kot je zahtevano v tem trenutku. Zunanji revizor bo po drugi strani moral poročati revizijskemu odboru podjetja o vseh ugotovljenih stvareh, ki so pomembne za samo poslovanje ali pa izvajanje revizijske funkcije. Pri tem bo poudarek na materialnih pomembnostih v okviru notranjih kontrol, ki se tičejo računovodskega poročanja.
Naslednje področje, pri katerem bodo z Osmo direktivo nastopile največje spremembe, je razmerje med vodstvom podjetja in zunanjim revizorjem. To bo sedaj bolj uradno in manj intenzivno. Veliko revizijskega dela bo potekalo mimo glavnega vodstva, kar bo večjo pomembnost v tem opravilu dalo nižjim direktorjem. Za samo vodstvo pa se obeta še ena večja sprememba, in sicer bo njihova odgovornost za pravilnost in poštenost finančnih izkazov ter razkritij povečana.
Ena od predpostavk, ki jo vključuje regulativa, je tudi povečati transparentnost nadzora nad revizijskim poslom. To zajema pregled nad revizorji v vseh državah članicah, in sicer na osnovi, ki bo dovoljevala primerjavo. Naslednja predpostavka se dotika poenotenja etičnih načel in kvalitativnih standardov, ki jih bodo revizorji morali upoštevati. Vse to kaže na eno od pomembnejših sprememb, ki se obeta in je razvidna iz mnogih predpisov. To je prehod od samoregulative revizijskega poklica oziroma posla k zunanji, zakonodajalski regulativi. S tem namenom je bil v ZDA ustanovljen odbor PCAOB. V Evropi česa identičnega ni, vendar bi bilo koristno razmišljati v tej smeri, kar je tudi stališče nekaterih vidnejših revizijskih družb.
Sprejetje nekaterih stvari je precej odvisno od posameznih držav. Ena od takih je zamenjava revizijskega podjetja po sedmih letih (Sarbanes-Oxleyev zakon zahteva samo menjavo partnerja iz iste revizijske hiše). To je za nekatere sporno, saj naj bi trpela kvaliteta revizije. Največ napak se pojavi v prvih letih opravljanja pregleda, ko se podjetje šele spoznava. Tudi dela je več na začetku sodelovanja, saj revizor ne ve, čemu posvetiti več pozornosti in kako se lotiti posamezne naloge, da bo izpeljana kar čim bolj učinkovito.
Naslednja stvar, ki jo je moč očitati Osmi direktivi, so nejasnosti glede dovoljenja za opravljanje drugih storitev poleg same revizije. Nekateri škandali v preteklosti so bili ravno plod takšnega sodelovanja. Revizorji so bili obenem svetovalci podjetja, njihovi nasveti so vključevali nedovoljene prakse, ki jih potem v sami reviziji niso odkrili, ker tega niti niso hoteli. Direktiva naj bi bila naklonjena omejevanju dodatnih storitev. Temu nekateri nasprotujejo z argumentom, da bi tako uničili pozitivne učinke poznavanja podjetja. Vprašanje je, kdo lahko svetuje podjetju bolje kot revizijska hiša, ki ga dobro pozna, obenem pa razume trende in vplive iz okolice? Zaradi prej omenjenih dogodkov je potrebno razumeti tudi omejevalnost predpisa in iskati rešitev nekje na sredini.

3.1.3. Primerjava Sarbanes-Oxleyevega zakona in Osme direktive

Že hiter pregled da slutiti, da je Sarbanes-Oxleyev zakon obsežnejši in tako bolj podrobno obravnava ustrezne elemente ter določa, kaj je dovoljeno in na kakšen način. Hkrati so predpisane stroge kazni za kršitelje, in sicer do dvajset let zapora. Pristop k naložitvi odgovornosti samim direktorjem je veliko strožji in ima zato tudi večje posledice. Podjetja so se lotila usklajevanje poslovanja z njim bolj resno, zato je zagotavljanje skladnosti z njim tudi dražje.

Osma direktiva se v primerjavi z SOX-om zdi sprejeta prepozno, hkrati je blažja. Do popolnega sprejetja v nacionalne zakonodaje bo preteklo še kar nekaj časa, ocenjuje se, da bo povsem efektivna nekje do leta 2008 in še to ob predpostavki, da ne bo večjih zapletov. Nekatere države so že pripravile svoje zakone, ki so že sedaj naravnani k strožji obravnavi vodenja podjetij in bodo morale sprejeti le še drobne popravke, da bo usklajenost z direktivo zadovoljiva. Direktiva bo predpisovala le minimalne standarde, ki jih bodo morale države sprejeti, še vedno pa bo precej odvisno od nacionalnih zakonodajalcev. Tako bo na primer Francija, ki že ima predpise strožje od predvidenih v direktivi, ohranila svojo regulativo nedotaknjeno. Ostale države bodo nadgradile zahteve iz nje s posebnostmi, ki so aktualne za določeno področje.

Razlike med Osmo direktivo in SOX-om se dotikajo tudi revizijskih odborov. V ZDA so lahko člani le neizvršni direktorji, medtem ko zahteve v Evropi niso tako stroge. Tu mora biti neodvisen le en član, ki je kompetenten na področju financ in računovodstva. Razlike so podobne tudi na področju notranjih kontrol. Medtem ko SOX zahteva tako od vodstva kot od revizorjev, da ocenjujejo učinkovitost kontrol in poročajo o tem, so zahteve v skladu z direktivo milejše.

Tabela 2: Primerjava bistvenih elementov Osme direktive in Zakona Sarbanes-Oxley

Zadeva	Osma direktiva	Sarbanes-Oxleyev zakon
Revizijski odbor	Obvezen za kotirajoča podjetja. Biti mora neodvisen in imeti vsaj enega finančnega strokovnjaka. Nastavlja in razrešuje revizorja.	Zahtevani so tudi postopki za pritožbe, ki jih razkrijejo zaposleni in tudi ostali.
Notranje kontrole	Zahtevano je revizorjevo poročilo o ključnih temah, ki izvirajo iz revizijskega pregleda, še posebno pozornost je potrebno nameniti pomanjkljivostim (slabostim) pri notranjih kontrolah, ki so povezane s finančnim poročanjem.	Zahteve so zelo podrobne.
Javni nadzor nad revizorji	Države Evropske skupnosti določijo odbor, katerega naloga je nadzor nad revizorji, registracijo revizijskih družb in vzpostavitev preiskovalnega/disciplinskega sistema.	PCAOB nadzira revizije podjetij, ki so na borzi, predpisuje standarde za revidiranje, registracijo revizijskih družb, nadzor nad kvaliteto, etiko in neodvisnost teh družb.
Neodvisnost revizorja	Pojavlja se možnost popolne prepovedi nerevizijskih storitev.	Prepoveduje določene storitve in zahteva predhodno odobritev revizijskega odbora za ostale nerevizijske storitve.
Menjava revizijske družbe oziroma partnerja	Zahtevana je menjava tako revizijske hiše kot partnerja: revizijska hiša na sedem, partner pa na pet let.	Zahteva menjavo glavnega (lead) in ostalih (concurring) partnerjev na pet let, ne zahteva menjave revizijske hiše.
Odgovornost revizorja skupine podjetij	Revizorji skupine nosijo polno odgovornost za revizijo uskupinjenih izkazov – odgovornost je razširjena nad delo ostalih revizijskih hiš.	Brez dodatnih odgovornosti.

Vir: Turley, 2004, s. 20

Iz vsega povedanega sledi, da sta si Sarbanes-Oxleyev zakon in Osma direktiva po namenu zelo podobna, različne so le poti, kako skušata doseči svoj cilj. Težko je reči, da je Direktiva

manj dosledna, ker pušča večjo svobodo posameznim članicam, da oblikujejo končno zakonodajo nekoliko v skladu s svojimi potrebami. Dogodki v preteklosti so pokazali, da je potrebna naprednejša ureditev nadziranja poslovanja, vendar do tega ni samo ene poti, kar dokazujeta oba predpisa, ki sta poleg tehnološkega napredka najmočnejša dejavnika razvoja na področju IT notranjih kontrol.

3.2. Razvoj tehnologije

Na pomenu vedno bolj pridobivajo revizijske sledi, ki so namesto v papirni sedaj v elektronski obliki. S tem se spreminja tudi področje notranjih kontrol, kajti krepijo se potrebe po pregledih informacijskih sistemov in z njimi povezanimi kontrolnimi mehanizmi.
Pričakuje se, da bodo v okviru tega imele velik vpliv na IT notranje kontrole naslednje tri stvari:

- digitalizacija papirnih dokumentov,
- računalniška izmenjava podatkov in
- elektronski račun.

Vse skupaj je tesno povezano z ustrezno zakonodajo, ki že danes dopušča precej več aktivnosti na tem področju, kot pa jo dejansko je. V bližnji prihodnosti se pričakuje velik napredek, ki ga bo vzpodbudila še razvitejša infrastruktura, zaostrena konkurenca in v Evropski skupnosti večji poudarek notranjim kontrolam kot posledica sprejetja Osme direktive.

3.2.1. Digitalizacija papirnih dokumentov

Digitalizacija v tem primeru pomeni pretvorbo papirnatih dokumentov v elektronsko obliko. Tu se razprava ne omejuje na določene vrste dokumentov, temveč zajema vse na splošno. Posledično je na primer elektronski račun zaradi specifike in pomembnosti obravnavan v svojem delu.
Revizor, pa naj bo to notranji ali zunanji, se pri svojem delu opira predvsem na neposredne dokaze, vsaj kar se tiče področja kontrol. Trenutno je več dela namenjeno ročnim kontrolam, kar lahko ponazorimo s preprostim primerom. Revizor si izbere določen vzorec dokumentov in na njih pogleda, če neka stvar ustreza njegovim pričakovanjem, na primer, če je na vseh podpis odgovorne osebe. V primeru, da najde manjšo napako razširi vzorec na večje število primerkov, v primeru še ene najdene pomanjkljivosti na še dodatne in če pregled še vedno ne daje zadovoljivih rezultatov, potem je kontrola prepoznana kot neučinkovita. V primeru, da je potrebno samo preveriti prisotnost podpisa, to ne predstavlja večje težave. Stvari se zapletejo, ko mora na podoben način preveriti bolj kompleksne stvari. Listanje med stotinami papirnatih dokumentov je zamudno in pogosto ne da pričakovanih rezultatov. Situacija bo precej drugačna pri popolnoma brezpapirnem poslovanju. Veliko preprosteje je preveriti, če je dokument elektronsko podpisan. Tako je tudi možnost napake, da se nek dokument pozabi odobriti, veliko manjša. Na ta način je kontrola bolj zanesljiva, poveča se tudi sama učinkovitost izvajanja.
Glede na to, da Sarbanes-Oxleyev zakon in tudi predpisi v Evropski skupnosti, ki bodo temeljili na Osmi direktivi, zapovedujejo dokumentiranje notranjih kontrol, bo upravljanje z

dokumenti veliko lažje, ko bodo ti večinoma v elektronski obliki. Istovetnost bo z mehanizmi elektronskega podpisovanja še večje, olajšano pa bo njihovo prenašanje in pregledovanje. Na ta način bo prihranek časa občuten, bolj se bo moč posvetiti delu, ki prinaša stranki dodano vrednost, kot se poročila o ugotovitvah in priporočila.

Z brezpapirnim poslovanjem je povezan še en pojem – upravljanje življenjskega cikla informacije (Information Lifecycle Management, ILM). To je kombinacija procesov in tehnologije, ki določa tok podatkov v okolju (Computerworld – The new buzzwords: Information Lifecycle Management, Computerworld – The new buzzwords: Information Lifecycle Management, 2006) ter pomaga podjetjem doseči zahteve predpisov glede varovanja podatkov ter zahteve vedno bolj tekmovalnega okolja po učinkovitem upravljanju z informacijami. Upravljanje življenjskega cikla informacije je tesno povezan z arhiviranjem in hranjenjem podatkov na splošno ter zahtevami neprekinjenega poslovanja, saj obravnava podatke kot občutljivo blago, temu primerni pa so tudi ukrepi. Podatki se delijo na skupine glede na različne kriterije, med njimi lahko najdemo:

- tip podatkov,
- organiziranost podatkov,
- starost podatkov in
- vrednost podatkov.

Glede na razdelitev se potem oblikujejo različni pristopi do teh skupin podatkov. Za ponazoritev si lahko pogledamo razliko med podatki, katerih hrambo zahteva zakon, in računovodskimi podatki. Prvi so pomembni za daljše časovno obdobje, vendar se pregledujejo zelo poredko, drugi pa so aktualni kratek čas, vendar se v tistem obdobju zahtevajo velikokrat. Temu primerna mora biti njihova hramba. Področje notranjih kontrol je tesno povezano z upravljanjem s podatki, saj s tega vidika ni nepomembno kje so hranjeni in kakšna je politika dostopanja do njih. Revizijska stroka zahteva urejenost podatkov in prav to nudi upravljanje življenjskega cikla informacije.

3.2.2. Računalniška izmenjava podatkov

Poslovni partnerji si danes med seboj že pogosto izmenjujejo podatke v standardizirani elektronski obliki. Tako gre veliko naročil neposredno iz informacijskega sistema naročnika v informacijski sistem dobavitelja. Na ta način odpadejo različni postopki, ki so bili značilni za star način poslovanja, ko je bilo treba izpolniti naročilnico, jo avtorizirati, nato poslati dobavitelju, potem pa preverjati naročene količine z dobavljenimi. Sedaj poteka celoten proces od naročanja do knjiženja plačila v glavno knjigo, brez da bi bilo potrebno natisniti en sam dokument. Tudi usklajevanje na koncu je lažje, saj se najprej primerjajo le agregirani podatki in šele nato se analizirajo podrobnosti, kar izredno zmanjša možnosti, da bi bila katera od napak spregledana.

Pri računalniški izmenjavi podatkov je potrebno zagotoviti določen nivo varnosti, da je tovrstno poslovanje sprejemljivo za podjetje. Nabor kriterijev, katerim naj bi bilo zadoščeno, da ni dvomov o nepravilnostih, je naslednji (Škedelj, 1999, str. 38):

- overitev izvora (obstajati mora možnost preverjanja identitete udeležencev),
- zaupnost vsebine (tretje osebe ne smejo imeti pravic dostopa),

- neokrnjenost vsebine (podatki ne smejo biti spremenjeni),
- nezavračanje izvora (avtorstvo mora biti nedvoumno dokazljivo),
- dokazilo o dostavi (obstajati mora dokazilo o dostavi, brez da bi bilo kaj spremenjeno),
- dokazilo o predložitvi (obstajati mora dokaz, da je bilo sporočilo posredovano naprej),
- nezavračanje prejema sporočila (prejem mora biti dokazljiv) in
- nezavračanje predložitve sporočila (dokaz, da je prejemnik prejel sporočilo v izvorni obliki).

Izpolnjevanje kriterijev je odvisno od tega, kako je sporočilo pomembno za prejemnika ali pošiljatelja. Čim več od teh faktorjev je uresničeno, tem večja stopnja varnosti obstaja in bolj se lahko zanesemo na komunikacijo. Sama varnost pa je zagotovljena z implementacijo tehnologij, kot so šifriranje in podobno.

Primere notranjih kontrol, ki se navezujejo na računalniško izmenjavo podatkov, pogosto najdemo v procesih nabave ali prodaje. Po eni strani se navezuje na varovanje sredstev podjetja, po drugi pa na samo izvajanje poslovnih procesov, ki so vedno bolj odvisni od novih poslovnih modelov. Pri slednjih je ključnega pomena interakcija z drugimi udeleženci na dokaj neposrednem nivoju, ki pa mora biti ustrezno urejena in nadzirana, da ne predstavlja prevelikega tveganja za organizacijo.

3.2.3. Elektronski račun

Vsak davčni zavezanec mora ob prometu blaga ali storitev izdati račun, je zapisano v Zakonu o davku na dodano vrednost (ZDDV). Davek, ki je obračunan na njem je eden pomembnejših proračunskih postavk večine držav sveta, enako velja tudi za Slovenijo. Pri nas je dovoljeno, da je račun izdan tudi v nematerializirani obliki, z drugimi besedami, lahko se uporablja elektronski račun. Zakon o elektronskem poslovanju in elektronskem podpisu ter Zakon o davku na dodano vrednost dajeta zakonsko osnovo za izdajanje elektronskih računov. Prvi enači elektronsko obliko s papirno, medtem ko drugi dovoljuje izdajo in hranjenje računov v nematerializirani obliki, če to dovoli davčni organ. Vsak račun, tudi elektronski, mora vsebovati naslednje podatke, da je veljaven (Zakon o davku na dodano vrednost, 2006):

- kraj in datum izdaje ter zaporedno številko;
- firmo oziroma ime in sedež oziroma stalno prebivališče ter davčno številko izdajatelja računa;
- firmo oziroma ime in sedež oziroma stalno prebivališče ter davčno številko prejemnika blaga oziroma storitve;
- datum odpošiljanja blaga oziroma opravljanja storitev;
- podatke o vrsti in količini prodanega blaga oziroma opravljenih storitev;
- cena blaga brez DDV, vrednost blaga oziroma storitve brez DDV, stopnjo oziroma stopnji DDV ter znesek DDV po različnih stopnjah in
- vrednost z vključenim DDV.

Gospodarska zbornica Slovenije je pripravila osnovno shemo elektronskega računa v XML formatu, s čimer ga je želela standardizirati in tako poenostaviti poslovanje poslovnim

subjektom na prostoru Republike Slovenije. Drugače je elektronski račun lahko načeloma v kateremkoli primernem formatu (doc, html, pdf in podobno), če se tako dogovorita stranki. Gospodarska zbornica Slovenije je v ta namen pripravila projekt e-Slog, katerega cilji so priprava in uveljavljanje standardov za e-poslovanje, uveljavljanje elektronskega podpisa za varovanje e-poslovanja ter priprava priporočil za rešitve e-poslovanja (Kratka predstavitev ciljev in rezultatov projekta e-Slog, 2006). Najbolj vidni rezultati so elektronska naročilnica, elektronska dobavnica in pa seveda elektronski račun. Račun, ki izhaja iz tega projekta, ustreza vsem zakonskim določilom, izdajatelj pa mora zadovoljiti še naslednje pogoje, da je e-račun po funkcionalnosti enakovreden tistemu v pisni obliki (Zakon o elektronskem poslovanju in elektronskem podpisu, 2006):

- dosegljivost podatkov v času predpisanega roka hranjenja računov,
- primernost podatkov v času predpisanega roka hranjenja računov,
- verodostojnost podatkov,
- jasno in razvidno identifikacijo pošiljatelja in prejemnika računa ter
- zanesljivost opreme in postopkov za preprečevanje nespremenljivosti podatkov.

Elektronski računi morajo biti elektronsko podpisani. Kot določa Zakon o elektronskem poslovanju in elektronskem podpisu mora biti uporabljeno kvalificirano digitalno potrdilo.
V okviru pregleda notranjih kontrol ima elektronski račun vrsto prednosti pred navadnim. Ravnanje z njim je lažje, predvsem pa je njegovo pregledovanje veliko hitrejše. Že samo pregled overovljenosti (podpis), kot to zahteva Slovenski računovodski standard 21, je bistveno manj naporen, seveda z uporabo ustreznih orodij. Še večje koristi se pokažejo pri preverjanju ostalih kontrol. Elektronski račun je bolj kot od človeškega faktorja odvisen od informacijskega sistema, ker je bistveno bolj zanesljiv, skorajda nezmotljiv, če je pravilno nastavljen. Če so z navadnim računom povezane ročne kontrole, so z e-računom povezane aplikacijske. Torej nam pod določenimi pogoji ni potrebno testirati vzorec precejšnega števila kontrol, temveč samo eno. Aplikacijske kontrole so običajno veliko bolj zanesljive kot ročne, kar nam prihrani delo pri ugotavljanju in odpravljanju pomanjkljivosti.
Zdi se, da vse govori v prid elektronskemu računu in da pred njegovo popolno prevlado stoji samo človeški odpor do novosti. Vendar ni vse tako, obstajajo vsaj še nekatere zakonske pomanjkljivosti in pa odpor nekaterih ljudi do novosti. Iz tega sledi, da dokler ne bodo rešene tovrstne težave, marsikdo ne bo prešel na e-poslovanje, pa čeprav ima veliko prednosti, med drugim tudi za revizijsko delo.

3.3. Standardi

Poenotenje poslovanja, s katerim si organizacije v končni fazi nadejajo prihranke, je eno glavnih vodil za uvajanje standardov. Njihova dodatna pozitivna lastnost se pokaže pri interakciji z zunanjimi partnerji, takšna primera sta zunanje izvajanje IT storitev (outsourcing), ko je prenos informacij ter znanj hitrejši, in revizija, pa tudi različne oblike svetovanja, kjer je spoznavanje standardiziranega okolja za udeležence veliko lažje in delo bolj sistematično. Standardi so najpogosteje formalno zapisane najboljše prakse, po katerih se lahko zgledujemo in se na tak način izognemo marsikateri napaki, ki bi bila sicer neizbežna. Po drugi strani ni potrebno dosledno slediti zapisanemu, temveč so mogoče prilagoditve, saj

so standardi največkrat de facto, kar pomeni priporočljivi, in ne de juro, obvezni (Oud, 2005, 27).

Danes obstaja več različnih standardov in predpisov, s pomočjo katerih se v podjetju lahko lotimo urejanja področja informacijske tehnologije. Pri odločanju med njimi naj bi upoštevali tudi naslednje kriterije (COBIT, 2004, s. 5):

- katerih področij se standard oziroma zbirka predpisov dotika;
- nivo podrobnosti;
- kaj naj bo merljivo;
- kaj naj bo avtomatizirano;
- kaj je najboljša praksa in
- ali je mogoče certificiranje.

V nadaljevanju bodo predstavljeni le nekateri standardi oziroma zbirke predpisov, in sicer ITIL, COSO, COBIT ter ISO/IEC 17799 oziroma ISO/IEC 27001. Njihov izbor temelji na pomenu, ki ga imajo za področje notranjih kontrol z vidika informacijske tehnologije po presoji avtorja, in sicer tako s teoretičnega kot praktičnega stališča.

3.3.1. ITIL

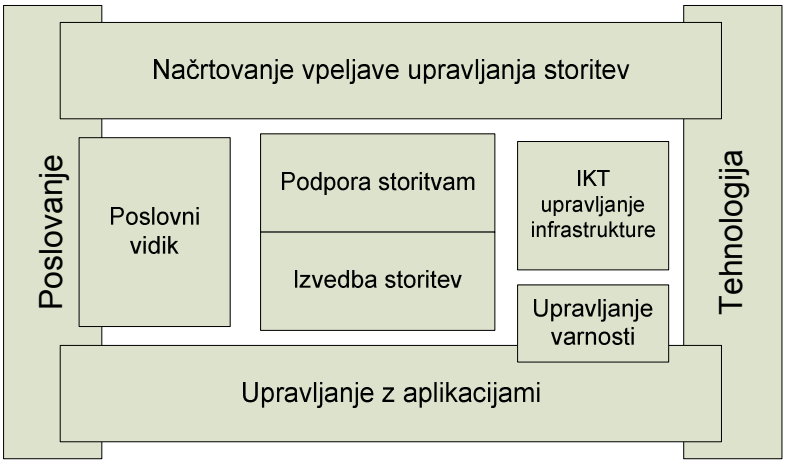
ITIL oziroma Information Technology Infrastructure Library je zbirka napotil izpeljana iz najboljših praks (best practises) za upravljanje storitev informacijske tehnologije. Razvila jih je Agencija za računalništvo in telekomunikacije (Central Computer and Telecommunications Agency, danes poznana kot Office of Government Commerce) kot odgovor na naraščajočo odvisnost podjetij od informacijske tehnologije. Kljub sponzorstvu s strani državne agencije, ITIL ni klasičen standard in zato certificiranje ni mogoče. Posledično sta se iz njega razvila standarda BS 15000 in najnovejši ISO 20000, ki presegata to pomanjkljivost, kajti za oba je mogoče pridobiti certifikat o presoji skladnosti.

Iz metodologije za uspešno in učinkovito rabo informacijske tehnologije v državnih organih Velike Britanije je bilo postopoma razvito prilagodljivo ogrodje, ki temelji na izkušnjah, in pomaga doseči zadovoljivo raven kvalitete storitev, izredno koristno pa je tudi pri preseganju težav povezanih z rastjo IT sistemov. O pomembnosti ITIL-a govori tudi podatek, da ga pri svojem poslovanju uporabljata v bolj ali manj prilagojeni obliki tudi Microsoft in HP. Standard sestoji iz več delov, ki so določeni predvsem s funkcijo, na katero se navezujejo, glede na različne vire se razlikujejo v podrobnostih, saj procesi niso povsem poenoteni. Pogosto je slabost procesov, ki so našteti v nadaljevanju, nezmožnost merljivosti, hkrati pa niso niti primerljivi glede opisov ali navodil za vpeljavo (ITSMF, 2004, s. 11):

- podpora storitvam (upravljanje z nepredvidenimi dogodki, upravljanje z nastavitvami, upravljanje s spremembami, upravljanje novih različic; z drugimi besedami: vsakodnevna opravila, ki so povezana z zagotavljanjem IT storitev),
- izvajanje storitev (upravljanje pogodb z zunanjimi partnerji, finančni vidik IT storitev, upravljanje s kapacitetami, zagotavljanje neprekinjenosti, zagotavljanje stalne dosegljivosti; tu je pomemben dolgi rok načrtovanja),

- načrtovanje vpeljave upravljanja storitev (načrtovanje, vpeljava in izboljšanje IT storitev; dotika se kulturnih in organizacijskih sprememb v podjetju ter vizije in strategije),
- upravljanje z varnostjo (potrebni ukrepi za zagotavljanje varnosti na področju informacijske tehnologije vključno s pripravo potencialnih ukrepov pri morebitnih nezgodah ter ocenjevanjem tveganj),
- upravljanje z informacijsko in telekomunikacijsko infrastrukturo (upravljanje z omrežji, strojno opremo v vseh fazah: od trenutka zaznave potrebe, testiranja, nameščanja, uporabe in izboljšav),
- poslovni vidik (nanaša se na poslovne odnose predvsem s strani zaposlenih v IT oddelku in njihov prispevek, zunanje izvajanje storitev (outsourcing), stalne izboljšave ter načine, kako z informacijami, komunikacijo in tehnologijo doseči prednost pred konkurenti) ter
- upravljanje s programsko opremo (razvoj programske opreme z uporabo življenjskega cikla, sistemi se razvijajo v skladu s potrebami uporabnikov).

Slika 8: ITIL okvir



Vir: ITSMF, 2004, s. 10

S slike 8 je razvidno, kako so posamezni procesi povezani s poslovanjem oziroma s tehnologijo. Tako je poslovni vidik veliko bolj povezan s poslovanjem kot na primer upravljanje s telekomunikacijsko in informacijsko infrastrukturo. Posebno, zelo pomembno področje pa predstavljata podpora storitvam ter izvajanje storitev.

Glavni razlogi, ki bi vplivali na izbiro ITIL-a kot metodologije za upravljanje informacijske tehnologije v podjetju, so pomoč pri določitvi storitvenih procesov, ki so v IT domeni, določitev in izboljšava kvalitete storitev, osredotočenost na uporabnika informacijske tehnologije ter vpeljava centralne podpore uporabnikom. Za razliko od COBIT-a se posveča predvsem izvajanju in podpori procesov, medtem ko načrtovanje, organiziranje, pridobitev, vpeljavo in nadzor procesov nekoliko zanemarja.

Iz ITIL dokumentov lahko uporabnik izve odgovore na vprašanji, kako se lotiti česa in kdo naj bo izvajalec, manj pa o vsebinski plati. Kot glavne naloge učinkovitega IT procesa navaja

izvajanje in vzdrževanje obstoječih sistemov, razvoj novih sistemov in stalno prilagajanje storitev namenjenih potrebam osnovnih poslovnih procesov. Poleg tega sta pomembni še dve stvari (COBIT, 2004, s. 18), in sicer celovito upravljanje storitev ter usmerjenost k uporabniku. Celovito upravljanje storitev je pomembno z vidika managerjev, ki morajo odločati o spremembah in razvoju procesov. Pri tem morajo upoštevati trenutno stanje in potrebe, ki se v poslovnem okolju konstantno pojavljajo, kar pomeni, da je potrebno ažurno uvajanje sprememb. S slednjimi pa je povezano testiranje in predvidevanje vplivov ter odzivanje nanje. Z usmerjenostjo k uporabniku je mišljeno zagotavljanje takšnega nivoja storitev, da so le-te stalno na voljo njihovim koristnikom, hkrati pa pomenijo koristno pridobitev za uporabnike. Pri tem so v pomoč svetovanje uporabnikom, zbiranje njihovih mnenj, še posebno pritožb, ter splošno spodbujanje uporabnikov k uporabi in medsebojni komunikaciji o zadevah, ki se nanašajo na, v tem primeru, uporabljeno informacijsko tehnologijo.

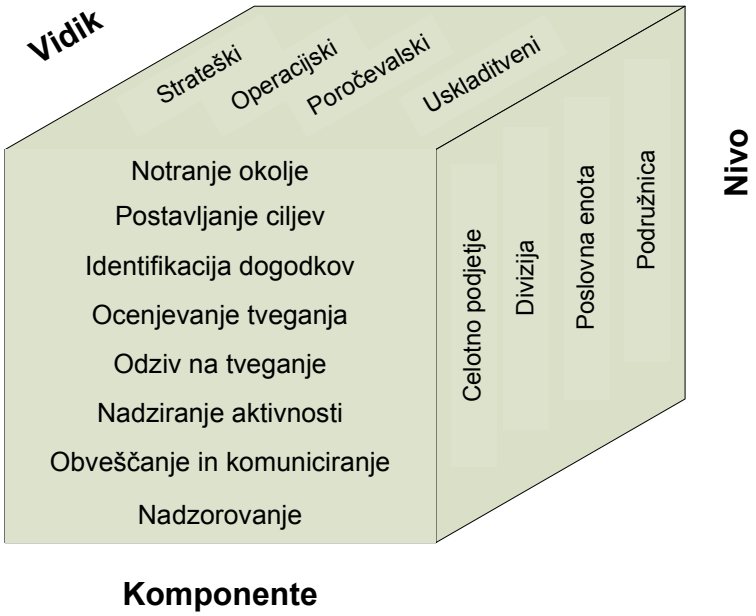
3.3.2. COSO

Za razliko od ostalih standardov je COSO le posredno povezan z informacijsko tehnologijo, saj obravnava notranje kontrole v širšem pomenu. Tu je predstavljen zaradi pomena, ki ga ima v povezavi z Zakonom Sarbanes-Oxley in regulativo v ZDA nasploh. Njegovo bistvo je ogrodje ali okvir, ki določa glavne komponente, uvaja enotno terminologijo in zagotavlja navodila za uspešno upravljanje s tveganji v podjetju (COSO – Enterprise Risk Management – Integrated Framework, 2006). Okvir sestavljajo tri dimenzije:

- vidik, s katerim preučujemo cilje poslovnega subjekta (strateški, operacijski, poročevalski in uskladitveni),
- nivoji delovanja poslovnega subjekta (raven celotnega podjetja, raven podružnice oziroma divizije in raven posameznih procesov poslovne enote) ter
- osem komponent nadzora (notranje okolje, postavljanje ciljev, identifikacija dogodkov, ocenjevanje tveganja, odziv na tveganje, nadziranje aktivnosti, obveščanje in komuniciranje ter nadzorovanje).

V skladu z zahtevami upravljanja tveganj je potrebno tveganje analizirati vsaj na dveh nivojih: celotnega poslovanja in posamezne poslovne enote, hkrati pa tudi preučiti prepletanja med samimi tveganji. Kot je bilo že zgoraj omenjeno, obstaja osem komponent, ki sestavljajo notranji nadzor oziroma kontrole. Način, kako se prepletajo in odzivajo ena na drugo, in tudi njihov vpliv na cilje organizacije je zajet v razumevanju sistema notranjih kontrol. Slednji je edinstven za vsako organizacijo, saj je splet tolikih faktorjev (velikost, panoga, kultura), da je podobnost z drugimi običajno izključena.

Slika 9: COSO okvir



Vir: Applying COSO's – ERM, 2006

Prva komponenta, ki je del COSO kocke (COSO, 2004, s. 3), se imenuje notranje okolje. Določena je s filozofijo, ki jo vodstvo podjetja uporablja pri soočanju s tveganji in zajema celotno okolje, v katerem ljudje delajo. Zaposleni v podjetju so najpomembnejši dejavnik vsakega poslovanja in prav od njih so odvisne etične vrednote, po katerih bo organizacija prepoznana s strani drugih. Postavljanje ciljev kot naslednja komponenta je udejanjena pri vsakem načrtovanju bodočega poslovanja z upoštevanjem tveganj. Takrat se vidi, koliko je vodstvo pripravljeno tvegati in na kakšen način, oziroma bolje rečeno, za kolikšno ceno namerava doseči cilje. Najpomembnejši stvari pri merjenju sta dovoljeni odmik od začrtanega cilja, ki še ne zahteva popravkov ali celo prekinitev prizadevanj, in po drugi strani dopuščanje nastanka tveganj brez odzivov organizacije na zahteve po dodatnih virih ali celo na spremembe načrtov. S tveganji je v tesni povezavi identifikacija dogodkov kot naslednja komponenta. Donosi so običajno v sorazmerni povezavi s tveganji, zato se podjetja in tudi posamezniki načrtno usmerjajo v projekte z višjimi stopnjami negotovosti, a boljšimi povrnitvami vložkov. Komponenta identifikacija dogodkov sloni na razlikovanju med tveganji in priložnostmi, prvo je dogodek, ki ima potencialen negativen končen vpliv na rezultat, pri priložnosti pa je ravno obratno. Slednje mora vodstvo podjetja upoštevati pri snovanju strategij, čeprav je razločevanje med obema vrstama dogodkov zelo težavno, še posebno velja to za načrtovanje na daljši rok, ko je marsikatera stvar še popolna neznanka. Tudi naslednja komponenta je nadgradnja razumevanja tveganja. Ocena tveganja, kot se imenuje, je predvidevanje stopnje, do katere lahko nezaželeni dogodki spremenijo postavljene cilje. Obstajata dva vidika, s katerih oblikujemo domneve: ena je verjetnost, da se dogodek sploh pojavi, druga pa je velikost vpliva, kar z drugimi besedami pomeni njegovo moč, s katerimi premika načrtovane cilje iz začrtanih smeri. V okviru te komponente se običajno

poleg ocenjevanja tveganj opravljajo tudi študije sprememb ciljev, z drugimi besedami, preverjanje različnih scenarijev, pri obeh procesih pa se upoštevajo tako kvalitativna kot količinska merila. Poleg tega ne smemo pozabiti upoštevati časa, saj je razlika pri načrtovanju na dolgi ali kratki rok običajno izredno velika. Logično nadaljevanje pri tveganjih je priprava ukrepov kot odziv na zaznavo nezaželenih dogodkov. Tako se bistvo v okviru komponente odziv na tveganje vrti okoli izbire in ocenjevanja različnih odzivov na tveganja. Dejavniki, od katerih je odvisna izbira, so predvsem sprejemljivost tveganja s strani podjetja, stroški v primerjavi s koristmi ter koliko lahko odziv zmanjša posledice ali verjetnost pojava nekega dogodka. Pri končni odločitvi je potrebno upoštevati tudi, kako se posamezni odzivi med seboj dopolnjujejo in kolikšen spekter prekrivajo, kajti priporočljivo je, da se ne določajo posamezni odzivi na specifična tveganja, temveč celoten sistem odgovora na nezaželene dogodke, ki bo nudil čim bolj uspešno in učinkovito obrambo zastavljenih ciljev ob različnih scenarijih. Najpogostejši odzivi so izogibanje tveganju, njegovo sprejemanje, zmanjšanje ali pa razdelitev tveganja. Šesta komponenta se nanaša na kontrolne aktivnosti. Pod svojim okriljem združuje postopke in politike, ki skrbijo za izvajanje opravil v zvezi s tveganji in tako pomagajo dosegati zastavljene cilje. Te politike in postopki določajo dejavnosti, ki jih je potrebno izvesti glede na določene okoliščine. Dejavnosti se izvajajo na vseh nivojih v podjetju in v okviru vseh funkcij ter tako zajemajo aplikacijske ter IT splošne kontrole. Pri naslednji komponenti, imenuje se obveščanje in komuniciranje, je potrebno razumeti, da so informacijski in telekomunikacijski sistemi potrebni za upravljanje procesov. Skupen sestav pa omogoča zaposlenim, da opravljajo svoje naloge, med katerimi pomembno mesto zasedajo kontrolne aktivnosti. Naloga vodstva je, da zazna in posreduje ustrezno informacijo v primerni obliki in ob pravem trenutku zaposlenim, ki jo potrebujejo pri svojem delu. Čeprav je v tem kontekstu poudarek na pretoku informacij od vodstva k ostalim, mora komunikacija potekati v vseh smereh in v različnih oblikah. Kot zadnja komponenta pa se navaja **nadzor**. Slednji je nepogrešljiv zaradi odkrivanja priložnosti za spremembe predvsem v smislu izboljšav. Vse pa se mora odvijati pravočasno, drugače je njegovo uvajanje brezpredmetno.

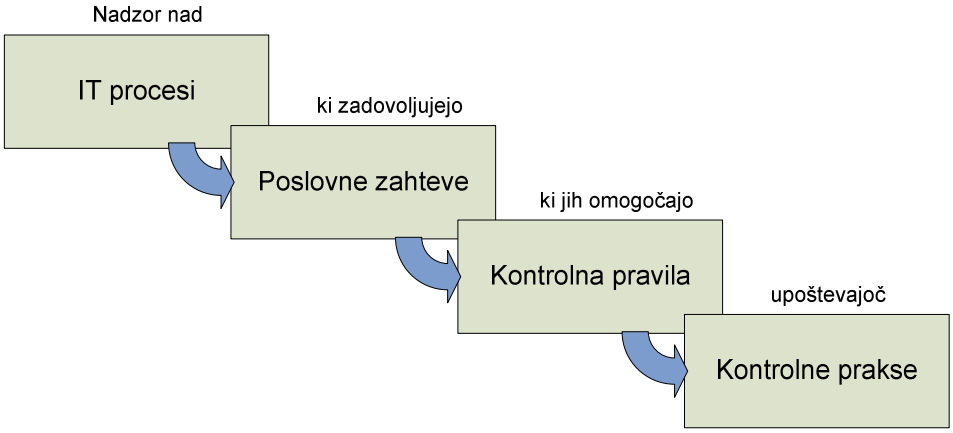
Zgoraj opisani okvir je bistvo metodologije COSO, ki je namenjena predvsem izboljšanju kvalitete finančnega poročanja in etike prek učinkovitih notranjih kontrol. Celotna zbirka se sicer deli na štiri dele: povzetek, okvir, poročanje zunanjim strankam in presojevalna orodja, ki se tičejo ocenjevanja sistema notranjih kontrol in predpostavljajo, da se lahko cilji organizacije delijo v tri skupine (COBIT, 2004, s. 47): poslovanje, finančno poročanje in skladnost z regulativo. Iz tega so izpeljani temelji, na katerih temelji učinkovitost sistema notranjih kontrol: razumevanje in zavedanje vodstva glede doseganja ciljev organizacije, zanesljivost finančnih informacij objavljenih s strani organizacije in skladnost z veljavnimi zakoni in predpisi.

3.3.3. COBIT

Strokovnjaki pogosto priporočajo COBIT kot celovit sistem za razumevanje IT nadzorstva, saj povezuje IT s poslovnimi potrebami na osnovi skrbništva nad določenimi procesi. Danes se veliko uporablja kot okvir za upravljanje z IT, in sicer zagotavlja metrična in zrelostna (maturity) orodja ravnateljstvu, s katerimi se opravlja nadzor. Razvit pa je bil z namenom, da

pomaga vzpostaviti kriterije varnosti ter uspešnega nadzora pri upravljanju na področju informacijske tehnologije. Nad njim bdi IT Governance Institute, ki ima največ zaslug za to, da je skupek standardov sprejet kot vzor za kontrolo nad informacijami ter informacijsko tehnologijo in z njo povezanimi tveganji nasploh. Njegova ideja je povzeta v shemi na sliki 10.

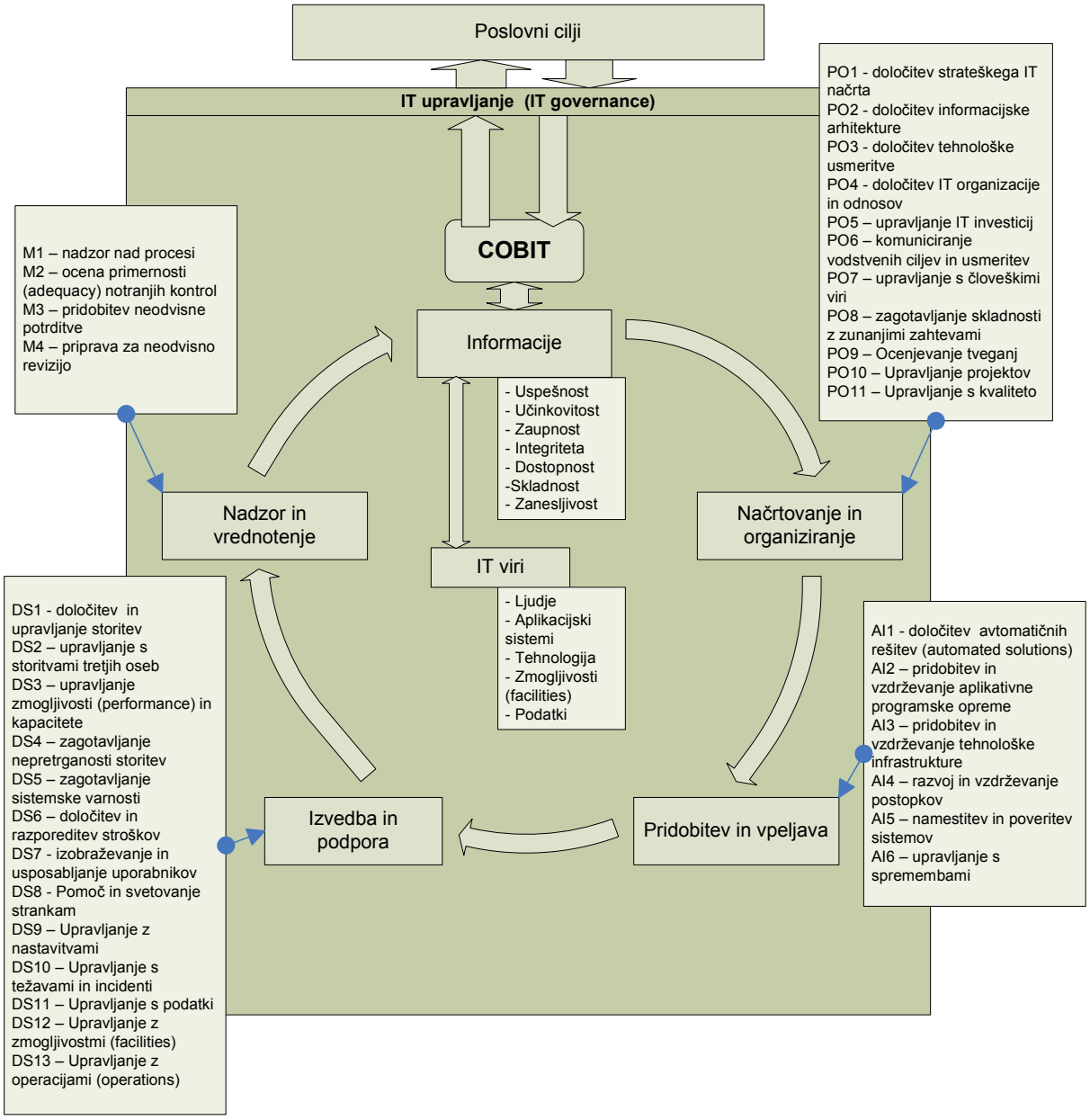
Slika 10: Koncept COBIT-a



Vir: Cobit (Framework), 1998, s. 21

COBIT je standard, ki v primerjavi z drugimi najbolj izpostavlja povezanost upravljanja organizacije z upravljanjem IT področja in je predmet neprestanih izboljšav. V povezavi s tem je potrebno omeniti PDCA cikel (Plan-Do-Check-Act Cycle), kajti celoten proces izboljšav temelji na njegovih štirih fazah (COBIT, 2004, s. 10): tako potreba po informacijah (upravljanje podjetja) kot njihova ponudba (upravljanje IT) morata temeljiti na merljivih in konstruktivnih kazalnikih (načrtovanje). Nadalje morajo biti informacije in informacijski sistemi predani v uporabo, da sploh lahko govorimo o IT vidiku poslovanja (izvedba). Rezultat je nato primerjan z načrtovanimi cilji v prvi fazi (pregled) in nadaljnji postopki so sprejeti glede morebitnih odmikov (ukrepanje), s čimer se zaključi en cikel.
Standard je bil zasnovan z namenom, da ravnateljstvu ponudi stično točko za različne potrebe, ki izhajajo iz poslovnih tveganj, zahtev po nadzoru in tehničnimi izboljšavami ter ponuja rešitve na temelju najboljših praks.
Njegovo bistvo je okvir, ki v trenutno aktualni verziji združuje štiriintrideset nadzornih ciljev za prav toliko IT procesov. Cilji so združeni v štiri skupine - planiranje in organiziranje, nabava in vpeljava, izvedba in podpora ter spremljanje oziroma nadzor. Nadzorni cilji, prek katerih skrbniki procesov zagotovijo zadosten pregled nad IT okoljem, se nadalje razdelijo na dvesto petnajst podrobnejših nadzornih ciljev.

Slika 11: COBIT okvir

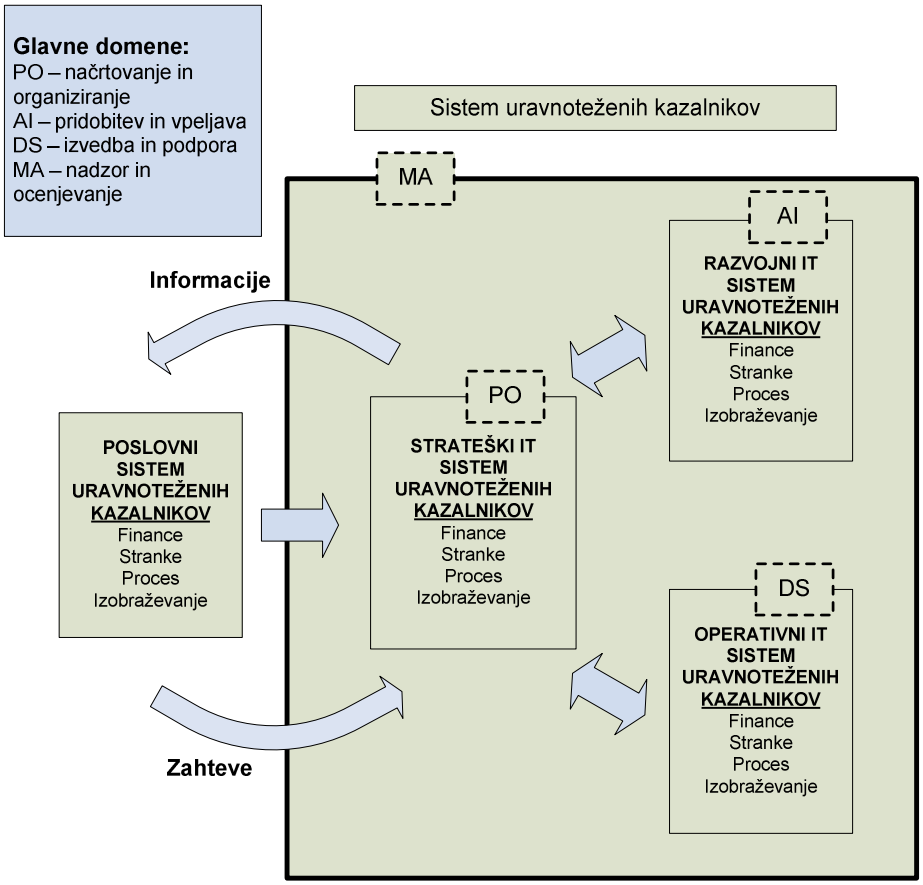


Vir: COBIT, 2000, s. 17

Kot je razvidno s slike 11, so procesi sestavljeni iz nadzornih ciljev, ki so združeni glede na lastnosti. Nadzorni cilj je koncept, ki zagotavlja (seveda le z določeno stopnjo verjetnosti), da se izognemo določenim tveganjem. Tveganje je možnost, da se dogodi nek nezaželen dogodek, kontrolna točka pa preprečuje njegovo udejanjanje (Kramer, 2003, s. 25). Upoštevajoč različna tveganja lahko izdelamo seznam, ki nam je v veliko pomoč pri sestavljanju revizijskega programa. Vanj moramo vključiti vse bistvene elemente za doseganje ciljev organizacije, ki so predmet revizije oziroma se nanašajo na ocenjevanje učinkovitosti kontrol. Tveganja, ki jih prepoznamo in vključimo v proces pregleda, moramo običajno zaradi preobsežnosti razdeliti po prioriteti, kajti večjo pozornost je potrebno posvetiti pomembnejšim.

Vsaka IT storitev mora biti v skladu s COBIT-om integrirana v obstoječe načrte, in sicer v okviru procesov, kot je tudi prikazano na sliki 11. Glede na to, da je nadzorna funkcija izredno pomembna, saj standard poudarja pomen PDCA[4] cikla, je to funkcijo priporočljivo prikazati in tudi v praksi udejaniti s pomočjo uravnoteženih kazalnikov, kar je razvidno s spodnje sheme na sliki 12.

Slika 12: Sistem uravnoteženih kazalnikov v povezavi s COBIT-om



Vir: COBIT, 2004, s. 13

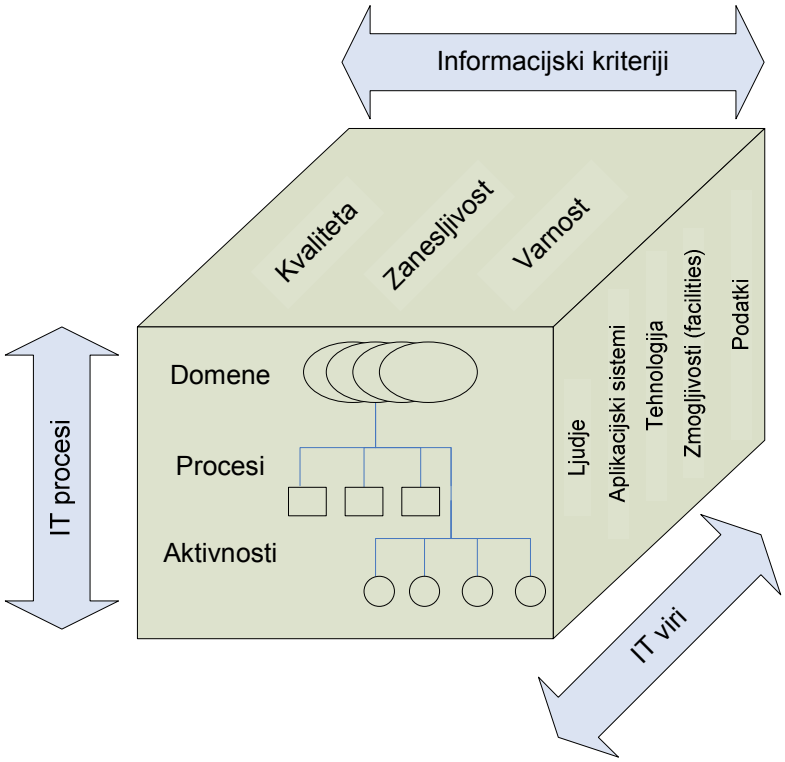
Pri samem razumevanju sheme nam bo v veliko pomoč upoštevanje dejstva, da so skupine procesov ali domene (v našem primeru štiri) sestavljene iz procesov, ki se delijo naprej v aktivnosti.

Smernice, ki jih ponuja COBIT so dveh vrst: managerske in revizijske. Prve povezujejo nadzor z upravljanjem IT področja. Pri pokrivanju organizacijskih in podobnih procesov, ugotavljanju doseganja zadanih ciljev in spremljanju ter optimiziranju posameznih IT procesov so te v veliko pomoč, saj so precej praktično usmerjene, hkrati pa dovolj generične, da so splošno uporabne. Po drugi strani pa revizijske smernice pomagajo pri izbiri aktivnosti, ki morajo biti izvedene, da lahko obvladujemo tveganje v okviru prej omenjenih štiriintridesetih nadzornih ciljev (COBIT, 2004, s. 11).

[4] PDCA cikel je sestavljen iz načrtovanja (plan), izvajanja (do), nadzora (check) in ukrepanja (act).

Najbolj celovito je COBIT predstavljen s tridimenzionalno kocko, ki ponazarja IT področje. Dimenzije sestavljajo informacijski kriteriji, IT viri in IT procesi. Kocka je prikazana na sliki 13.

Slika 13: COBIT kocka



Vir: COBIT (Control Objectives), 1998, s. 16

Vsak proces (v okviru štirih domen ali skupin procesov) je določen z naslednjimi determinantami (COBIT, 2004, s. 14): z visokonivojskimi nadzornimi cilji; podrobnimi nadzornimi cilji; viri informacijske tehnologije uporabljenimi v procesu; značilnostmi, odvisnih od zrelostne ravni; faktorji, od katerih je odvisen uspeh (critical success factors); ključnimi kazalniki delovanja (performance) in ključnimi dejavniki doseganja zastavljenih ciljev. Drugo dimenzijo predstavljajo informacijski kriteriji, ki služijo kot nekakšni filtri za informacije, ki so uporabljeni pri bistvenih (core) procesih v podjetju. Kriteriji so zahteve glede kakovosti (tu sta pomembni učinkovitost – informacija je plod produktivne in ekonomične rabe virov ter uspešnost – informacija je pomembna in relevantna za poslovni proces ter obenem pravočasna, pravilna, uporabljiva in konsistentna), varnosti (zaupnost – tiče se zaščite zaupnih podatkov pred razkritjem, integriteta – nanaša se na natančnost in celovitost informacij ter veljavnost in primernost s poslovnimi potrebami ter dostopnost – kar pomeni, da so informacije na voljo, ko so potrebne, hkrati pa so viri, ki služijo za pridobivanje informacij primerno varovani in obravnavani) in preverjenosti (fiduciary) (informacija je skladna z zakoni in drugimi predpisi ter zanesljiva). Tretja dimenzija se nanaša na IT vire, ki so dokaj široko definirani. Tako mednje uvrščamo podatke, aplikativne sisteme (skupek ročnih ali/in programskih postopkov), tehnologijo (strojna oprema, operacijski sistemi,

sistemi za upravljanje z zbirkami podatkov, omrežja in podobno), pripomočki za podporo informacijskih sistemov ter ljudi, vključno z njihovimi sposobnostmi planiranja, organiziranja, izvajanja, podpore in nadziranja.
Po COBIT-u je upravljanje IT področja in ustreznih procesov stalni in periodični proces ugotavljanja odstopanj od predvidenih vrednosti ter hkrati uvedba pravočasnih popravkov. Njegovi dobri strani sta poudarek na metričnosti in dokaj celovit pristop k IT kontrolam, vendar ima po drugi strani v primerjavi z ITIL-om nekatere pomanjkljivosti pri obravnavanju procesov. Oba pa sta šibkejša na področju varnosti, kjer prevladuje BS 7799 oziroma njegovi mednarodni različici, ISO 17799 in ISO 27001, ki vsak pokriva svoj del originalnega standarda.

3.3.4. ISO/IEC 17799 in ISO/IEC 27001

ISO/IEC 17799[5] je mednarodni standard, ki temelji na BS 7799-1 (angleški standard za informacijsko varnost – sestoji iz dveh delov: BS 7799-1 in BS 7799-2, prvi del se nanaša na informacijsko tehnologijo v smislu kodeksa upravljanja z informacijsko varnostjo, drugi del pa na sistem upravljanja varovanja informacij in daje poudarek implementaciji v praksi; v letu 2006 je izšel še BS 7799-3, ki se loteva področja upravljanja s tveganji, povezanimi z informacijsko varnostjo).
Pričakuje se skorajšnja nadomestitev standarda ISO 17799 s prenovljenim in preimenovanim v ISO 27002, ki bo tako postal član družine standardov ISO/IEC 27000, katerih vsebina je upravljanje z informacijsko varnostjo in bo sestavljena iz (About ISO 27000 Series, 2006):

- ISO 27000: izrazoslovje, temeljni principi in definicije za celotno družino standardov ISO/IEC 27000;
- ISO 27001: sistem upravljanja informacijske varnosti s priporočili za implementacijo;
- ISO 27002: kodeks upravljanja informacijske varnosti;
- ISO 27003: napotki za vzpostavitev sistema za upravljanje informacijske varnosti (implementation guide);
- ISO 27004: merila sistema za upravljanje informacijske varnosti;
- ISO 27005: upravljanje informacijskih tveganj in
- ISO 27006: predvidoma bo predstavljal smernice za ponovno vzpostavitev informacijskega sistema po katastrofi.

Standard, ki je trenutno v uporabi, ISO/IEC 17799, ponuja informacije, ki se tičejo informacijske varnosti znotraj organizacije. S tega vidika ga lahko razumemo kot osnovo za izdelavo varnostnih načel, ki pomagajo izboljšati varnost IT področja. Njegove odlike so predvsem (COBIT, 2004, s. 23) jasno definiranje sistema za upravljanje z informacijsko varnostjo, določitev kritičnih sredstev podjetja z uporabo ocenjevanja poslovnega tveganja, zvišanje nivoja zavedanja glede informacijske varnosti pri vodstvenem kadru, boljše definiranje obveznosti posameznikov in organizacijske strukture z vidika informacijske varnosti, boljše dokumentiranje IT zadev in jasnejši odnosi (večji poudarek je dan

[5] ISO in IEC sta akronima za International Organization for Standardization oziroma International Electrotechnical Commission, pogosto se pri poimenovanju standardov uporablja samo kratica ISO.

pogodbam). Za uspešno uvedbo tega standarda v organizacijo je potreben konsenz vodstva in tudi ostalega dela zaposlenih, ki sodeluje pri IT procesih, ter dosledno spoštovanje navodil (ukrepi se ne smejo podcenjevati).

Standard ISO 17799 temelji na dveh virih: zakonskih zahtevah in najboljših praksah. Pod prvo spadajo varovanje osebnih podatkov, notranje zaupne informacije in spoštovanje intelektualne lastnine, v drugo skupino pa politika varovanja informacij, določanje odgovornosti za informacijsko varnost ter skrb za zagotavljanje neprekinjenega poslovanja v izrednih razmerah (COBIT, 2004, s. 25). Standard je fizično razdeljen na deset razdelkov, ki skupaj vsebujejo šestintrideset ciljev in sto sedemindvajset kontrol in se nanašajo na začetno načrtovanje, vpeljavo in vzdrževanje informacijske varnosti. Pri vpeljavi je potrebno upoštevati, da ne zavira poslovanja (torej, da ni v nasprotju s poslovnimi cilji), kulturo organizacije, podporo in sodelovanje vodstva ter ostalih zaposlenih ter da je sistem prilagodljiv v takšni meri, da glede na povratne informacije dopušča spremembe. Informacijska varnost mora glede na standard pokrivati najmanj naslednja poglavja (ISO/IEC 17799:2005, 2006):

- varnostno politiko (vsebovati mora navodila, ki so potrjena s strani vodstva in znana zaposlenim),
- organizacijsko varnost (struktura organizacije mora podpirati uvedbo standarda, kar pomeni, da je potrebno spodbujati komunikacijo na to temo med managementom v formalni obliki, posebno pozornost je potrebno posvetiti koordinaciji; dolžnosti in pravice morajo biti zadosti natančno določene, vnaprej morajo biti predvidene oblike sodelovanja z zunanjimi partnerji; storitve zunanjih izvajalcev - njihovo izvajanje mora biti vnaprej urejeno s sprejetjem potrebnih ukrepov in tveganja, ki jih predstavljajo zunanji izvajalci določenih storitev, morajo biti pod nadzorom - urejeni odnosi z zunanjimi izvajalci),
- razvrstitev sredstev in nadzor nad njimi (tu je pomembna določitev odgovornosti za posamezno sredstvo),
- varnost, povezana z zaposlenimi (razporeditev odgovornosti med zaposlene, zaupnost dogovorov in pogodb, nadzor nad zaposlenimi, izobraževanja, ki bi povečevala nivo varnosti in zaupnosti ter poročanja o nepravilnostih s strani zaposlenih),
- fizična varnost (vsa sredstva bi morala biti fizično zavarovana pred uničenjem ali poškodovanjem, zagotovljeno bo moralo biti neprekinjeno napajanje z električno energijo, posebno skrb je potrebno posvetiti pozornost sredstvom, ki se nahajajo izven prostorov podjetja; ne smemo pozabiti tudi na splošne kontrole, kot so ne puščati pomembnih dokumentov na mizah in podobno),
- upravljanje komunikacije in poslovanja (poslovanje mora temeljiti na dokumentiranih postopkih, vse spremembe morajo biti zabeležene, ravnanje v izrednih situacijah mora biti predvideno in formalno zapisano, odgovornosti in pravice morajo biti ločene, kriteriji za odločanje glede uvajanja novih sistemov morajo biti definirani, poslovanje nasploh mora biti formalno opredeljeno s predpisanimi postopki, ki zagotavljajo zadosten nivo varnosti),

- kontrole dostopa (dostop do informacij mora temeljiti na premišljeni osnovi, ki je v skladu s potrebami posameznika glede na njegove zadolžitve, podobno velja za dostop do infrastrukture, politika dostopa mora biti formalno zapisana; predpogoj je, da so dolžnosti posameznika natančno določene),
- razvoj sistemov in njihovo vzdrževanje (varnostne zahteve morajo biti upoštevane že ob samem razvoju, spet so pomembne kontrole dostopov),
- neprekinjeno poslovanje (tudi v izrednih razmerah, kot so naravne nesreče, morajo obstajati alternativni postopki, ki zagotavljajo nadaljevanje s poslovanjem vsaj v bistvenih okvirih; to ne sme biti omejeno le na IT področje, pri tem je pomembno testiranje, kar pomeni, da se na alternativne postopke res lahko zanesemo) in
- skladnost (upoštevana mora biti veljavna zakonodaja, poleg tega morata biti usklajenost varnostne politike podjetja in upoštevani standard ISO 17799 periodično preverjana).

Zgoraj obravnavani standard ISO 17799 se nanaša predvsem na varnostne kontrole, ki jih uporabimo pri vzpostavljanju sistema informacijske varnosti. V skupini ISO že obstajajo različni standardi, ki pokrivajo poslovanje z različnih vidikov, na primer ISO 9001 kakovost, ISO 14000 pa okoljske zadeve. Čeprav nekateri standardi delno zajemajo tudi dobre prakse za upravljanje informacijskih storitev, informacijska varnost še ni pokrita v celoti. Zato je bil pred kratkim izdan standard ISO 27001, ki pokriva ta spekter informacijskih storitev in hkrati nadomešča drugi del standarda BS 7799. Naziv za novi standard je Zahteve za sisteme upravljanja informacijske varnosti (Information security management systems requirements specification) in je sestavljen iz naslednjih poglavij (OSL informator – ISO 27001- nova pomembna številka v informacijski varnosti, 2006):

- uvod,
- namen,
- normativi,
- pogoji in definicije,
- sistem upravljanja varovanja informacij (SUVI),
- odgovornost vodstva organizacije,
- nadzor vodstva organizacije nad SUVI-jem,
- izboljšave SUVI.

Posebno skrb so pri njegovem snovanju posvetili usklajenosti z ostalimi upravljavskimi standardi ISO in modelu PDCA oziroma Demingovemu krogu. Slednji ponazarja upravljanje skozi štiri korake (PMI Standards Comitee, 1996, s. 85): načrtovanje, ki zajema odkrivanje problemov poslovanja in načrtovanje rešitev; izvedbo, ki se posveča izvajanju načrtov izboljšanja varnosti poslovanja; preverjanja z namenom nadzorovanja, če aktivnosti potekajo v skladu z načrti in ukrepanja, ki se nanašajo na analiziranje dela ukrepanja v smislu načrtovanja novih, boljših varnostnih rešitev. Medtem ko se standard ISO 17799 ukvarja z varnostnimi kontrolami iz sistemov za upravljanje varovanja informacij na nivoju referenčne platforme, novi standard skrbi za praktično postavitev tega sistema z uporabo prej omenjenih

kontrol. To poteka prek (OSL informator – ISO 27001- nova pomembna številka v informacijski varnosti, 2006):

- definicije informacijske politike,
- definicije namena in cilja sistema upravljanja varovanja informacij,
- izvedbe ocene tveganja,
- upravljanja s tveganji,
- izbire kontrol, ki bodo uporabljene in implementirane,
- izjave o primernosti informacijske politike.

Standard ISO 27001 je v praksi zaživel oktobra 2005, prenovljena različica ISO 17799 pod imenom BS ISO/IEC 17799:2005 pa je izšla istega leta v mesecu juniju, medtem ko se pričakuje izid standarda pod številko 27002 v letu 2007. Sledila bo priprava in uvedba ostalih standardov iz družine 27000, s čimer bo področje informacijske varnosti pokrito dokaj celovito.

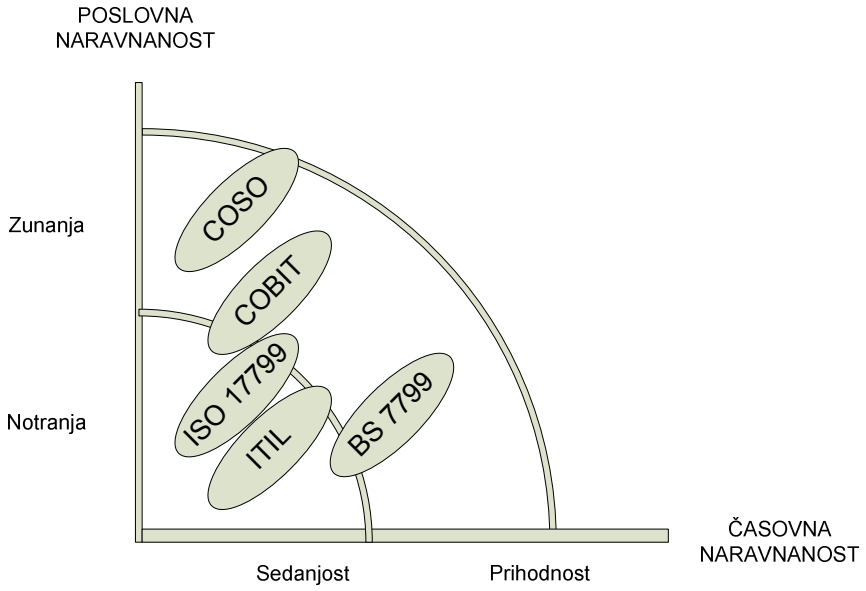
3.3.5. Primerjava standardov

COBIT, COSO, ISO 17799, ISO 27001 in ITIL se tako dopolnjujejo kot tudi tekmujejo med seboj. Tako COBIT pokriva širšo tematiko z IT področja kot ISO 17799 ali ISO 27001, vendar slednja bolj podrobno obravnavata informacijsko varnost. Če je za podjetje aktualna predvsem varnost, potem bo verjetno izbralo ISO standard. Za podjetja, ki se morajo podrejati Zakonu Sarbanes-Oxley, je prava izbira COSO, katerega lahko na področjih, kjer je šibkejši, kombiniramo s katerim od drugih standardov. COSO predpostavlja, da je notranja kontrola proces zasnovan s strani vodstva ali ostalih zaposlenih, in sicer z namenom, da zagotavlja določeno stopnjo gotovosti doseganja zastavljenih ciljev. Hkrati se ta standard osredotoča na uspešnost in učinkovitost poslovanja, zanesljivost finančnega poročanja in skladnost z zakonodajo in predpisi. Je najbolj obsežna obravnava notranjih kontrol, kar je razvidno tudi s fizičnega vidika, saj je njegova dokumentacija najbolj zajetna. COBIT-ov pristop je drugačen – kontrolo vidi kot informacijo oziroma vir informacije, ki je potrebna za podporo poslovanju in s tem povezanimi IT viri in procesi. COBIT-ov doseg je nekoliko razširjen, saj vključuje tudi kvalitativne in varnostne zahteve v sedmih kategorijah, ki vključujejo uspešnost, učinkovitost, zaupnost, integriteto, dosegljivost, skladnost in zanesljivost informacij. Te kategorije tvorijo osnovo nadzornih ciljev. Nadalje se pojavljajo precejšne razlike med uporabniki določenih standardov. Med koristnike COSO standarda se uvrščajo predvsem managerji, medtem ko je COBIT zelo uporaben tudi za revizorje in podobne uporabnike, ker poudarja IT kontrole z vidika varnosti. Če s COBIT-om primerjamo ITIL, slednji pokriva precej ožje področje, vendar dokaj podrobno. Tako sta izvedba in podpora obravnavani precej podrobno, po drugi strani pa so načrtovanje, organiziranje, nadziranje in ocenjevanje nekoliko zanemarjeni. Poudarek daje kvalitetni izvedbi IT storitev ter skrbi za uporabnika.

Uporaba standarda je v veliki meri geografsko pogojena. Tako se na primer COBIT v primerjavi z ITIL-om v ZDA uporablja pogosteje, medtem ko je slika v Veliki Britaniji ravno obratna. Tu ni potrebno posebej poudarjati, da v vsaki državi lokalne organizacije za standardizacijo preferirajo svoje predpise. Dobra stran velikega števila standardov, ki so na voljo, je, da lahko izberemo takšnega, ki je najbolj primeren za določeno situacijo. Izberemo

lahko le dele posameznih standardov in jih potem združimo. Primerjava med njimi in odločitev za pravega je težka, saj ne obstajajo nikakršni metastandardi, ki bi bili zaradi kompleksnosti področja že potrebni. Pomagamo si lahko z različnimi modeli, eden od njih je Petersenov, ki je prikazan na sliki 14.

Slika 14: Petersonov model primerjave standardov



Vir: Oud, 2005, s. 29

Pri primerjavi med standardi nam je lahko v pomoč tudi okvir za primerjavo standardov in zbirk dobrih praks, ki ga je razvila organizacija ISACA (Information Systems Audit and Control Association), ki prav tako bdi nad COBIT-om. Ne glede na vse povedano ni odveč še enkrat ponoviti, da se ni mogoče preprosto odločiti za enega od standardov, saj ima vsak svoje prednosti in slabosti, obenem pa niti posamezno niti skupaj ne zagotavljajo popolne varnosti ali uspešnega poslovanja. Prinesejo pa koristi, kot so sistematično obravnavanje tveganj, potrdilo akreditirane organizacije o sledenju najboljšim praksam oziroma standardu in večji ugled, kako pa bo podjetje to izkoristilo, je odvisno od njega samega.

4. Vzpostavitev IT notranjih kontrol v podjetju

Nadziranje je ena od osnovnih funkcij poslovodenja, poleg tega tudi različni predpisi zahtevajo nadzor nad poslovanjem v ustrezni meri. Posledično imajo podjetja vsaj osnovne notranje kontrole že oblikovane, vendar premalo pozornosti posvečajo njihovemu ocenjevanju in izpopolnjevanju. Primer postavljanja zahtev po izvajanju kontrol je mogoče najti v Slovenskem računovodskem standardu 21, ki govori o knjigovodskih listinah, predpisuje njihovo kontroliranje in sestavljanje za knjiženje na naslednji način (Slovenski računovodski standardi 2006, 2006):

Pri ročnem in polsamodejnem obravnavanju podatkov se kontrolirajo izvirne knjigovodske listine, in to pred knjiženjem. Pri računalniškem obravnavanju podatkov pa se kontrolira začetni vnos podatkov iz knjigovodskih listin v računalnik ali pri računalniškem izmenjavanju

podatkov prevzem podatkov od drugega podjetja; izpeljane knjigovodske listine se kontrolirajo po potrebi na podlagi posebnega računalniškega programa.
Knjigovodske listine se kontrolirajo, da se zadosti načelu resničnosti, torej da kažejo podatki v njih dejansko stanje in gibanje sredstev, obveznosti do njihovih virov, prihodkov in odhodkov. Knjigovodske listine so verodostojne, če se pri kontroliranju pokaže, da lahko strokovno usposobljene osebe, ki niso sodelovale v poslovnih dogodkih, na njihovi podlagi popolnoma jasno in brez kakršnihkoli dvomov spoznajo naravo in obseg poslovnih dogodkov.
Knjigovodske listine se pred knjiženjem kontrolirajo na enem ali več krajih (osredotočeno ali neosredotočeno), lahko tudi z računalnikom po računalniških programih, pripravljenih glede na vrste knjigovodskih listin.

Še bolj natančno je večina notranjih kontrol določena z internimi akti podjetja, ki jih sprejme organizacija in predpisujejo način ravnanja z računovodskimi listinami, organizacijo in zadolžitve računovodstva ter pravice in dolžnosti pooblaščenih oseb.
V tem poglavju bo beseda tekla o vzpostavitvi IT notranjih kontrol v podjetju z zahtevami sodobnega poslovanja. Na začetku je potrebno razjasniti še nekaj nejasnosti. Kot je bilo že predhodno ugotovljeno, notranje kontrole v podjetjih že obstajajo, saj je vodstvo podjetja odgovorno za vzpostavitev ustreznih informacijskih sistemov in z njimi povezanimi kontrolnimi mehanizmi (Howard, 1992, s. 26). Največkrat jih je le potrebno formalno definirati, jih dokumentirati in zaposlene tudi opozoriti na njihovo vlogo. Skratka, potrebno je začeti spremljati in ocenjevati kontrole na nek konsistenten način. Naslednji poudarek je namenjen razlikovanju med ročnimi in IT notranjimi (aplikacijskimi) kontrolami. Namen pri obeh vrstah je isti, glavna razlika med njima je v tem, da IT zahtevajo za upravljanje z njimi dodatna, predvsem informacijska znanja. Poleg tega je pri slednjih potrebno zagotoviti, da se v času ne spreminjajo nenadzorovano, kar zagotovimo s pregledom IT splošnih kontrol.
K zgoraj povedanemu je potrebno dodati, da bo v nadaljevanju velik vpliv na predstavitev področja notranjih kontrol imel Sarbanes-Oxleyev zakon, saj je to trenutno najbolj preskriptiven in celovit predpis na tem področju, še bolj pomembno pa je dejstvo, da je za marsikatero podjetje obvezen. Hkrati bodo upoštevane smernice, ki jih predlagajo največje svetovne revizijske hiše, ter v določenih primerih elementi metodologij COSO in COBIT.
Glavni koraki vzpostavitve in uskladitve IT notranjih kontrol v podjetju z zahtevami sodobnega računovodskega poročanja so naslednji:

- priprava projekta,
- določanje obsega (scoping) in načrtovanje,
- vključenost zunanjih partnerjev,
- dokumentiranja,
- preverjanje zasnove kontrol
- testiranje ter
- analiziranje pomanjkljivosti notranjih kontrol in poročanje.

Podrobneje bo zgoraj navedeno predstavljeno v nadaljevanju.

4.1. Priprava projekta

Preden začnemo s samim projektom je potrebno razmisliti, kaj sploh želimo doseči. Zastaviti si je treba jasne cilje in pri tem upoštevati vse omejitve, ki jih bo treba preseči. To načeloma velja za vsak projekt. Začetnemu navdušenju sledi ohladitev, ko ljudje ne sodelujejo tako, kot je bilo predvideno, hkrati se pojavijo dodatne, nepričakovane ovire. Še posebno v takih primerih, ko so vključeni različni oddelki, obstaja mnogo razlogov za nesodelovanje. Zato si je potrebno pridobiti sponzorje, ljudi, ki so zadosti vplivni, da si lahko izborijo privilegije in tudi ni odveč, če so karizmatični, da navdušijo ljudi za doseganje nekega cilja, brez da bi jih bilo treba k temu prisiliti na takšen ali drugačen način.

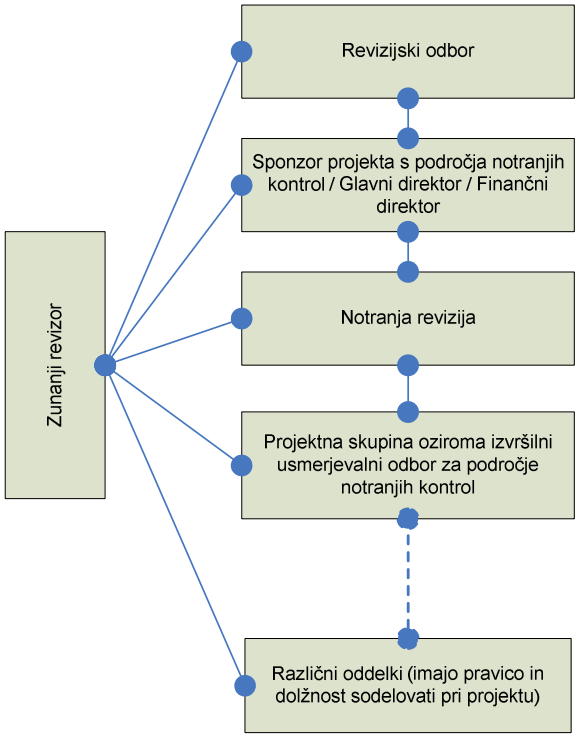
Tudi glede ostalih resursov je potrebno biti realističen. Velikokrat se ustavi ravno pri denarju. Slednji je poleg časa najbolj omejena dobrina v večini podjetij, zato zahteva posebno skrb. Kar se tiče porabe denarja, je dobrodošel podatek o tem, kako so se s tem spopadli v drugih podjetjih, vendar se je potrebno zavedati, da je to zelo občutljiva informacija in posledično težko dosegljiva. Pogosto nam ne preostane drugega, kot da smiselno ocenimo porabo časa in denarja, poleg tega si izborimo še določeno rezervo.

Vzpostavitev IT notranjih kontrol je običajno zahteven projekt, kjer gre lahko marsikaj narobe, zato je treba stalno spremljati napredek in dosežene rezultate primerjati z zastavljenimi cilji. Takoj ko je ugotovljeno bistveno odstopanje, je potrebno ukrepati, saj le tako lahko zagotovimo uspešnost projekta. Najbolje je, da opravljamo kontrolo doseženega vsak dan, vendar v omejenem obsegu, saj drugače za to porabimo preveč časa, ki nam ga že tako ali tako primanjkuje. Postaviti pa si je treba pomembne mejnike, ki so v bistvu nekakšni svetilniki. Ti nam omogočajo, da spremljamo smer, kamor se giblje projekt, in hkrati nadzorujemo časovno komponento.

Zelo pomembna je tudi komunikacija v podjetju. Ni dovolj, da zaposlene o projektu obveščajo njihovi neposredno nadrejeni. Dobrodošlo je, da so v to vključeni tudi višje vodje. Tako celotna stvar dobi pridih resnične pomembnosti in so posamezniki zavezani v večji meri k doseganju ciljev na tem področju. Obstajajo še drugi načini, kako razširiti zavedanje o tem v okviru podjetja. Večja podjetja imajo notranja glasila ali vsaj intranet, ki je lahko namenjen temu, in to lahko uporabijo za obveščanje zaposlenih. Najpomembnejši pa je seveda zgled. Če vodje niso naklonjeni nekemu cilju, potem tudi od zaposlenih ni moč pričakovati tega. Zato je potrebno od vodij zahtevati, da so ciljno osredotočeni in projektu posvečajo vso potrebno pozornost, saj le tako lahko prepričajo ostale, da jim sledijo. Seveda pa je marsikaj odvisno od same kulture v podjetju in temu je potrebno prilagoditi spodbujanje zaposlenih.

Ker vzpostavitev notranjih kontrol ni le postranska zadeva, ki bi bila hitro zaključena, je potrebno formalno osnovati skupine, ki bodo skrbele za to. V okviru teh je potrebno posebno pozornost nameniti zaposlenim, katerim se bo naložila skrb za IT kontrole, saj te zahtevajo poleg splošnih še dodatna znanja. Primer sheme organiziranosti ljudi, ki bodo v prvi vrsti skrbeli za doseganje učinkovitosti sistema notranjih kontrol je prikazan na sliki 15:

Slika 15: Organizacija in razmerja med zaposlenimi ter zunanjimi partnerji, ki skrbijo za vzpostavitev ročnih in IT notranjih kontrol



Vir: Prirejeno po PriceWaterhouseCoopers, 2004, s. 4

SOX in Osma direktiva zahtevata revizijski odbor kot uradno telo, ki se ukvarja s področjem notranjih kontrol v podjetju. Priporočljivo pa je, da se osnuje še predstavništvo vseh oddelkov (funkcijska, geografska in druge razdelitve oddelkov), ki skrbijo za kontrole na njihovem področju. V tej točki je potrebno misliti na pokrivanje kontrol informacijske tehnologije, zato je potrebno vključiti osebe, ki imajo tovrstno znanje, hkrati pa postaviti nekoga, ki bo odgovoren za IT kontrole. Seveda je to le priporočilo. Slika 15 in besedilo v nadaljevanju predstavljata eno od možnosti organiziranja, končna odločitev je odvisna od več dejavnikov, kot so na primer velikost podjetja, organiziranost, zakonodaje in podobno ter seveda od odločitev vodstva.

Oseba, ki je vodja projekta in običajno hkrati tudi revizijskega odbora, razdeli skrb za kontrole na določenem področju med vodje teh področij ali njihove predstavnike. Ti potem prevzamejo ključno skrb za kontrole v njihovem odseku. Pri tem ni pomembno, kdo je določen za končno dokumentiranje celotnega sistema ali testiranje, oseba mora poskrbeti, da v njenem odseku vse poteka, kot je bilo predvideno.

Čeprav mogoče na prvi pogled ni nejasnosti o dolžnostih, se v praksi velikokrat izkaže drugače. Zaposleni pogosto razumejo, da je celoten proces računovodskega poročanja izključno stvar računovodskega oddelka, vendar se prihodki večinoma ustvarjajo v prodaji in tam ima glavni računovodja manj vpliva kot pa vodja prodaje. Zato mora načeloma oddelčni vodja skrbeti za kontrole v svojem odseku, ne glede na to, če se ne nanašajo povsem na njegov proces. Prav zato je potreben nek višji organ, ki v okviru procesa vzpostavitve kontrol skrbi, da so le-te obravnavane celovito.

Tudi če je projekt še tako dobro vnaprej načrtovan, ne bo uspešen brez dobrega vodenja. Zato so v večini večjih podjetij na to nalogo razporejeni eden ali več managerjev, ki se ukvarjajo predvsem z razvojem in vzdrževanjem projektnih načrtov, sklicevanjem in vodenjem sestankov, uporabo orodij za spremljanje uspešnosti, poročanje ter podobno.
Ker pa se vsako podjetje razvija, je potrebno predvideti, da bodo nastopile določene spremembe v povezavi s kontrolami, ki so že bile obravnavane. Zato je potrebno poskrbeti še za dve stvari – ena je odkrivanje teh sprememb, druga pa posledično upoštevanje ponovnega ukvarjanja s kontrolami. Glede prve točke je potrebno zasnovati metodologijo in infrastrukturo tako, da novosti glede kontrol ne ostanejo neopažene. Neuspešnost, tako glede odkrivanja kot zmožnosti zagotovitve resursov za ponovno obravnavo, se odraža na končnem rezultatu. Skupni efekt je običajno podoben, kot da bi bile kontrole v procesu ocenjevanja prepoznane za neučinkovite.

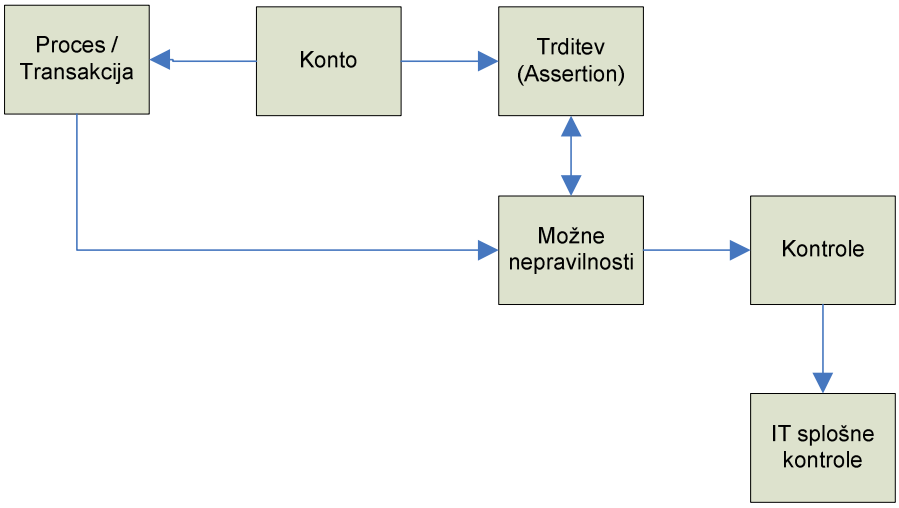
4.2. Določanje obsega in načrtovanje

Določanje obsega oziroma vsebine in načrtovanje izvedbe je eden bolj kritičnih procesov v procesu vzpostavitve sistema IT notranjih kontrol oziroma upravljanju notranjih kontrol nasploh. To je potrebno določiti za vsako pomembno postavko, razkritje in poslovni proces ter pri tem upoštevati vse enote podjetja, čeprav so te na različnih lokacijah. Najbolje je začeti pri določitvi pomembnih postavk, razkritij, poslovnih procesih/ciklih in podprocesih/podciklih. Opravilo se nadaljuje z izbiro primerne metodologije, v velikih primerih si podjetja izberejo za pomoč standard COSO. Dobrodošla je tudi vključitev zunanjega revizorja, saj se sprejemajo odločitve o pomembnih stvareh, ki vplivajo tudi na potek zunanje revizije s strani neodvisnega revizijskega podjetja. Odveč ni niti razmisliti o stvareh, ki lahko vplivajo na samo izvedbo postopkov v smislu potrebnega časa in ostalih virov (Howard, 1992, s. 73), in sicer:

- čas in sosledje izvajanja različnih faz;
- vključenost zaposlenih v izvajanje posameznih postopkov in
- opiranje na delo, ki je bilo oziroma bo izvedeno s strani notranje revizije.

Pri določanju pomembnih postavk/kontov in razkritij je potrebno upoštevati njihov pomen v finančnih izkazih ter kvalitativne in kvantitativne dejavnike. Na to se potem navezujejo poslovni procesi in podprocesi ter v nadaljevanju tudi trditve glede finančnih izkazov (assertions). Brez izdelave ocene tveganja za vsak poslovni proces in podproces preverjanja učinkovitosti notranjih kontrol ni popolno. V primeru, da je podjetje razdeljeno na več ločenih enot, je potrebno upoštevati tudi to. To vključuje ocenitev vpliva posamezne enote na pomembne konte in razkritja.
Posamezne kontrole je potreba povezati s trditvami (assertions), ki veljajo za določene konte in razkritja. Povezanost med kontrolami in finančnimi izkazi je prikazana na sliki 16.

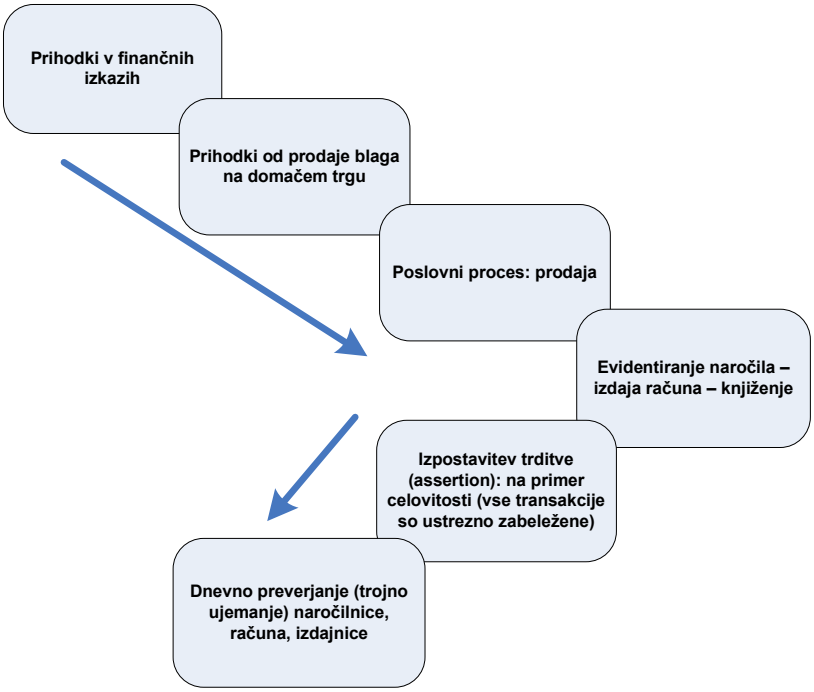
Slika 16: Povezanost kontrol z elementi finančnih izkazov



Vir: Interna dokumentacija EY

Za povezavo enega z drugim je potrebno začeti s finančnimi izkazi in pojasnili ter potem iti vedno globlje v podrobnosti. Končni cilj je določitev kontrolnih aktivnosti in postopkov, ki se nanašajo na ustrezne finančne trditve v povezavi s finančnimi izkazi. To v praksi zgleda tako, kot je prikazano na sliki 17 za proces prodaje.

Slika 17: Praktičen primer povezave kontrol in finančnih izkazov



Vir: Avtor

Mogoče ni odveč ponovno poudariti, kdaj je nek konto ali razkritje pomembno. Pogoj je, da obstaja verjetnost, da postavka vsebuje napako, ki sama ali v povezavi z drugimi materialno vpliva na finančne izkaze. Poleg kvantitativnih kriterijev obstajajo tudi kvalitativni kriteriji, saj je nek konto lahko veliko bolj pomemben od drugih, čeprav glede na denarno vrednost to

ni razvidno. Pomembni so lahko tudi konti, ki so kompleksni, kar pomeni na primer, da so povezani z velikim številom zapletenih transakcij in podobno.
Kljub govoru o prehodu s kvantitativnih na tako imenovane mehke, kvalitativne dejavnike, se v praksi prvi uporabljajo še v veliko večji meri. Posledično je treba določiti materialnost, ki je pojem za pomembnost in običajno temelji na določeni postavki iz izkaza poslovnega izida. Na primer, pri njenem izračunu upoštevamo dobiček pred davki, tako vzamemo pet odstotkov od zneska in dobljeni rezultat primerjamo s posameznimi postavkami. Tako določimo, če so le-te pomembne ali ne.
Pri določanju pomembnosti nekega konta je potrebno upoštevati tudi težko merljive – kvalitativne – dejavnike, med katerimi so (AICPA - Proposed Statement on Auditing Standards - Audit Risk and Materiality in Conducting An Audit, 2006):

- sestava konta,
- občutljivost na napake ali prevare,
- obsežnost transakcij, njihova kompleksnost, raznolikost transakcij,
- vrsta konta,
- računovodska in poročevalska »težavnost« konta,
- izpostavljenost izgubam določenega konta (na primer iz različnih pogodb),
- verjetnost nastanka nepredvidenih obveznosti, ki izhajajo iz narave konta,
- obstoj transakcij povezanih oseb in
- spremembe v zvezi s kontom glede na preteklo obdobje.

Vse te elemente je potrebno upoštevati, da dosežemo ustrezno zajetost kontov in lahko nadaljujemo na naslednjih ravneh brez bojazni, da smo že v osnovi začeli iz napačnih predpostavk.
Za ponazoritev si poglejmo izračun kriterija materialnosti za podjetje X, srednje veliko trgovsko-storitveno družbo. Materialnost bo določena na treh nivojih:

- načrtovana materialnost (velja za celotne finančne izkaze),
- tolerančna napaka (velja za posamezen konto ali skupino kontov) ter
- materialnost celote revizijskih razlik (velja za posamezne transakcije).

Materialnosti za ta zgled so določene z revizijskega vidika. Posledično bo v primeru, da revizijske napake presegajo načrtovano materialnost, izdano negativno mnenje družbi glede finančnih izkazov, kar pomeni, da ti ne predstavljajo poštene in pravilne slike finančne situacije, rezultatov in denarnih tokov. Tudi v primeru preseganja tolerančne napake izdano mnenje praviloma ne bo pozitivno. Po drugi strani zneski, ki ne bodo presegali materialnosti celote revizijskih razlik, na samo mnenje ne bodo imeli vpliva, vse to pa posredno vpliva na izvedbo testiranja notranjih kontrol.
Pri analizi finančnih podatkov podjetja ugotovimo, da podjetje v zadnjih letih dosega stabilno rast dobička iz poslovanja, temu trendu pa sledi tudi celoten dobiček pred obdavčitvijo. Večjih sprememb ni ne glede sredstev niti kapitala, tudi ostale računovodske kategorije ne izkazujejo večjih premikov v primerjavi s prejšnjimi obdobji. Na podlagi tega se lahko odločimo za izračun na podlagi dobička pred obdavčitvijo. Pri tem je potrebno poudariti, da mednarodni standardi revidiranja, ki veljajo tudi v Sloveniji, ne določajo natančno samega

izračuna, temveč v veliki meri prepuščajo opravilo presoji izvajalca. Glede na to, da je podjetje ustvarilo 145.000 EUR dobička pred obdavčitvijo, se načrtovana materialnost določi na 10.150 EUR, kar je enako sedmim odstotkom dobička pred davki. Sedem odstotkov je izbranih na podlagi metodologije revizijske hiše, ki priporoča izbiro v območju med petimi in desetimi odstotki za podjetja, ki izpolnjujejo določene kriterije, skratka za podjetja z dobrimi poslovnimi rezultati. Izračun bi lahko napravili tudi na podlagi prihodkov, sredstvi, bruto marže, kapitala, poslovnega rezultata pred obrestmi, davki in amortizacijo. Na izbiro točno sedmih odstotkov so vplivala sledeča dejstva:

- ugotovljene revizijske razlike v preteklih letih so bile zanemarljive, nepopravljenih ni bilo;
- podjetje deluje v stabilnem poslovnem okolju in panogi;
- narava posla družbe ni tvegana;
- notranje kontrole so predhodno ocenjene kot učinkovite;
- podjetje ne kotira na borzi, ima samo enega lastnika, kar pomeni, da se računovodski izkazi pripravljajo za omejeno število uporabnikov;
- zasebno, ne posebej regulirano podjetje;
- revizijska družba opravlja revizijo že vrsto let ter
- podjetje nima dolga, s katerim se javno trguje.

Nadalje se določita še tolerančna napaka in materialnost celote revizijskih razlik. Prva kot 50 odstotkov, druga pa 10 odstotkov načrtovane materialnosti, kar znaša 5.075 EUR oziroma 1.015 EUR. Slednja bi bila lahko po metodologiji višja, vendar je bila z namenom podrobnejšega pregleda sprejeta odločitev za nižjo vrednost.

Naslednji korak je določitev pomembnih procesov in podprocesov ter njihova povezava s pomembnimi konti in razkritji. Z razumevanjem in dokumentiranjem poslovnih procesov vodstvo dokaže, da je sposobno določiti kontrolne aktivnosti, ki se nanašajo na cilje v zvezi z obdelavo informacij kot tudi morebitne pomanjkljivosti pri kontrolah. Povezovanje pa je nujno, da preverimo, če so vsi pomembni konti podprti s poslovnimi procesi in da so bili od slednjih vsi vključeni v obravnavo. Če to ni bilo uresničeno, potem se na kontrole ne moremo zanašati, saj smo nekatere izpustili iz procesa ocenjevanja. Največja težava je, ker se podjetja razlikujejo med seboj in moramo dati poudarke različnim procesom. Tu lahko samo pomislimo na trgovsko podjetje na eni strani in finančno institucijo na drugi.

Če doslej povedano povežemo s podjetjem X, moramo izvesti aktivnosti v dveh stopnjah. Najprej določimo pomembne procese in nato konte. Procese določimo na podlagi poznavanja podjetja in razumevanja poslovanja, in sicer se v tem primeru delijo na: zaključevanje finančnih izkazov, izplačila, vplačila, prodajo in terjatve, oblikovanje popravkov za dvomljive terjatve in stroške slabega dolga, zaloge in stroške prodanega blaga, oblikovanje popravkov za zaloge, fizično preveritev zalog, nabavo blaga in obveznosti, nabavo storitev in obveznosti, obračun davka ter plače. Naslednji korak je določitev pomembnih kontov – tu določimo vse tiste, ki po vrednosti presegajo za podjetje določeno tolerančno napako, ki je v tem primeru 5.075 EUR, za konte bilance stanja se upoštevajo stanja na koncu obdobja, za konte izkaza poslovnega izida pa promet v obdobju. Med njimi izločimo tiste, ki glede sestave ne spadajo v to skupino – najpogostejša vzroka za to sta nekompleksnost in majhno število enostavnih

transakcij. Po drugi strani pa vključimo konte, ki sicer ne dosegajo zahtevane vrednosti, vendar so zaradi narave transakcij ali iz drugih razlogov bolj tvegani in zato zahtevajo podrobnejši pregled. Nadalje konte, ki ne spadajo med pomembne, razdelimo še na nepomembne (not significant) in nematerialne (insignificant). Slednji so po vrednostih dokaj irelevantni, revizijski postopki izvedeni v zvezi z njimi pa so minimalni.
Končni rezultat razvrščanja kontov na pomembne, nepomembne in nematerialne je za podjetje X razviden iz tabele 3 (pojasnila vsebujejo le najpomembnejše dejavnike za odločitev glede razvrstitve).

Tabela 3: Razvrstitev kontov podjetja X na pomembne, nepomembne in nematerialne

Seznam pomembnih kontov	**Pojasnilo**
Odložene terjatve za davek	Visok znesek, prvič oblikovan po novih standardih
Zaloge	Visok znesek, večje tveganje
Kratkoročne finančne naložbe	Visok znesek, večje tveganje
Kratkoročne poslovne terjatve	Visok znesek, večje tveganje
Denarna sredstva	Veliko transakcij, na splošno je tveganje večje
Rezervacije in dolgoročne PČR[6]	Visok znesek, pri oblikovanju je pomembna subjektivna presoja vodstva
Kratkoročne finančne obveznosti	Visok znesek, večje tveganje
Kratkoročne poslovne obveznosti	Visok znesek, večje tveganje
Kratkoročne pasivne časovne razmejitve	Visok znesek, veliko število transakcij
Čisti prihodki iz prodaje	Visok znesek, večje tveganje
Stroški blaga, materiala in storitev	Visok znesek, veliko število transakcij
Stroški dela	Visok znesek, večje tveganje
Drugi poslovni odhodki	Visok znesek, večje tveganje
Davek iz dobička	Privzet pomemben konto

Seznam nepomembnih kontov	**Pojasnilo**
Neopredmetena sredstva in dolgoročne AČR[7]	Ni večjih sprememb, nezapletene transakcije
Opredmetena osnovna sredstva	Ni večjih sprememb, nezapletene transakcije
Dolgoročne finančne naložbe	Nezapletene transakcije
Kratkoročne aktivne časovne razmejitve	Majhno število transakcij, nezapletene transakcije
Kapital	Majhno število transakcij, nezapletene transakcije
Dolgoročne finančne obveznosti	Majhno število transakcij, nezapletene transakcije
Odpisi vrednosti	Vključeno v pregled dolgoročnih sredstev
Finančni prihodki	Pregledano pri dolgoročnih naložbah, s katerimi so povezani
Finančni odhodki	Pregledano pri dolgoročnih finančnih obveznostih, s katerimi so povezani

Seznam nematerialnih kontov	**Pojasnilo**
Naložbene nepremičnine	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke
Dolgoročne poslovne terjatve	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke
Sredstva za prodajo	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke
Dolgoročne poslovne obveznosti	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke
Odložene obveznosti za davek	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke
Obveznosti, vključene v skupine za odtujitev	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke
Drugi prihodki	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke
Drugi odhodki	Majhna vrednost, nizko tveganje glede na transakcije oziroma dogodke

Vir: Avtor

Nadalje moramo za vsak pomemben konto in razkritje najti ustrezne trditve, ki se nanašajo na finančne izkaze. Trditve so lastnosti, ki jih lahko pripišemo posamezni postavki in tako

[6] Pasivne časovne razmejitve.
[7] Aktivne časovne razmejitve.

pokrijemo neko tveganje. V osnovi obstaja pet takšnih trditev, ki so bolj podrobno opisane v poglavju 2.1:

- obstoj oziroma pojav,
- celovitost,
- ovrednotenje oziroma merjenje,
- pravice in dolžnosti ter
- predstavitev in razkritje.

Iz zgornjega seznama je razvidno, da sta v nekaterih primerih na voljo dve zelo podobni trditvi – katero bomo uporabili je odvisno ali gre za presek ali tok, torej ali postavka izhaja iz bilance stanja ali izkaza poslovnega izida.
Odgovorni se morajo odločiti za ustrezne povezave med trditvami in konti še pred testiranjem kontrol, oziroma še preden se odvijajo kakršnekoli aktivnosti glede tega, saj je od trditev odvisno, kaj sploh bomo testirali. Če preverjamo obstoj, je testni postopek povsem drugačen od tistega pri zagotavljanju pravic in dolžnosti glede nekega konta. Za nekatere izbrane pomembne konte pri podjetju X so ustrezne trditve prikazane v tabeli 4.

Tabela 4: Trditve (assertions) za izbrane pomembne konte podjetja X

KONTO	TRDITVE (ASSERTIONS)			
Denarna sredstva	Obstoj	Pravice in dolžnosti		
Zaloge	Celovitost	Obstoj	Merjenje	Pravice in dolžnosti
Stroški dela	Celovitost	Pojav	Merjenje	
Rezervacije in dolgoročne PČR	Celovitost	Vrednotenje	Obstoj	Pravice in dolžnosti
Čisti prihodki iz prodaje	Celovitost	Pojav	Merjenje	
Kratkoročne poslovne obveznosti	Celovitost	Obstoj	Vrednotenje	Pravice in dolžnosti

Vir: Avtor

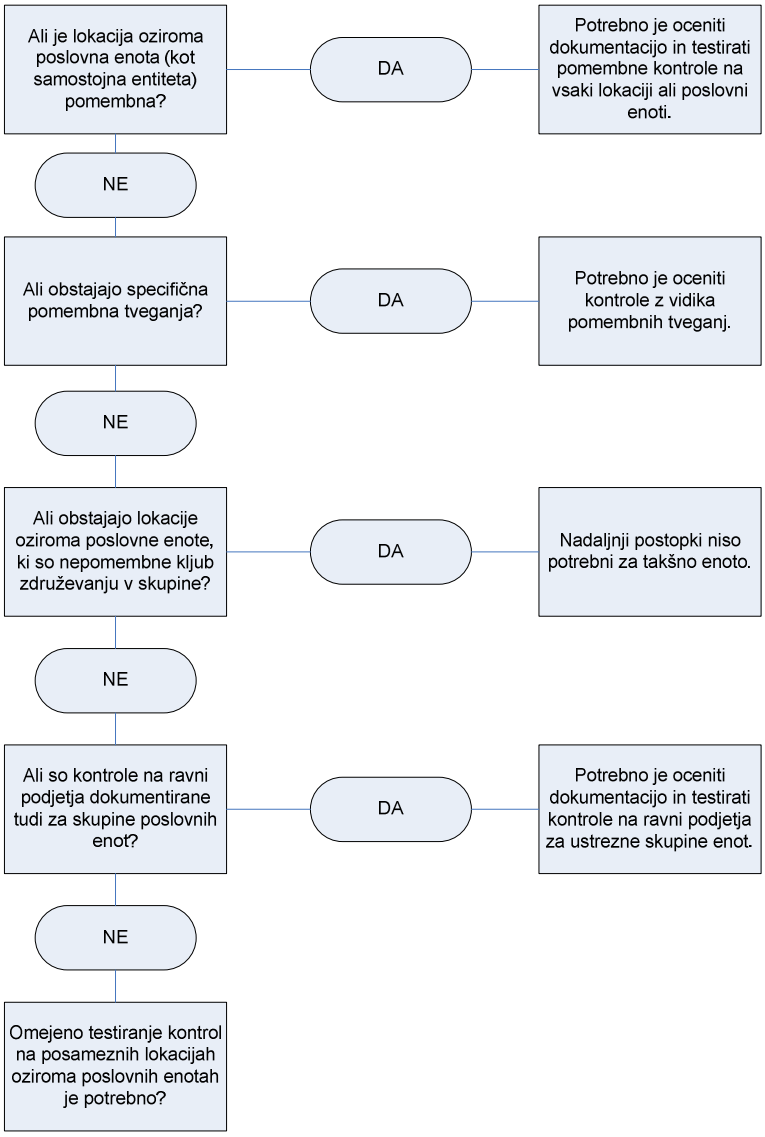
Sledi ugotavljanje tveganj znotraj poslovnih procesov in podprocesov, ki imajo lahko materialni vpliv na finančne izkaze. To je pomembno, da lahko predvidimo naravo, potreben čas in obseg testiranja notranjih kontrol. Tako lahko tiste kontrole, ki se nanašajo na manj tvegane procese, pomaknemo v sredino poslovnega leto, saj ni tako nujno, da jih testiramo blizu datuma zaključka poslovnega leta, prav tako pa je lahko testiranje manj podrobno. To ne pomeni, da smo lahko pri tem površni, ampak lahko pripravimo manj podroben program. Ta mora seveda še vedno vsebovati vse pomembne točke, ki pokrivajo celotno kontrolo. Program mora biti pripravljen tako, da zajame vse komponente in potem, če zaznamo, da se mogoče na nekem delu skriva napaka, tam testiramo podrobneje in obsežneje.
Ocenjevanje tveganja zahteva veliko subjektivne presoje, zato ni vseeno, kdo to delo opravlja. Biti mora kompetentna oseba, ki ne samo, da pozna področje, ampak tudi razume povezane procese in okolje ter na ta način predvidi tveganja, ki so mogoče manj veščim osebam skrita. To je zlasti pomembno za področje informacijske tehnologije, ki se stalno spreminja in

obsega veliko med seboj različnih tehnologij. Dostikrat je težko najti osebo, ki bi razumela poslovni proces in bila obenem poznavalec informacijske tehnologije. Zato je v bolj kompleksnih okoljih priporočljivo sodelovanje dveh ali več oseb, katerih znanje se dopolnjuje.

4.3. Podjetje z več enotami

Če se poslovanje podjetja odvija na več lokacijah, je potrebno sprejeti odločitve, katere od lokacij bodo vključene v proces ocenjevanja notranjih kontrol. Pri tem je potrebno ločiti, katere so pomembne individualno in katere v povezavi z drugimi enotami. Za ameriška podjetja pride v poštev standard, ki ga je izdal PCAOB in je vanj vključeno drevo odločanja, ki je prikazano na sliki 18. Glede na to, da je metodologija velikih revizijskih in svetovalnih družb v veliki meri vezana na ameriško zakonodajo, ima predpis vpliv tudi v drugih državah.

Slika 18: Drevo odločanja, ki pomaga pri odločitvi, katere enote naj bodo vključene v proces ocenjevanja notranjih kontrol in v kolikšni meri



Vir: PriceWaterhouseCoopers, 2004, s. 22

Splošni kriteriji, ki so pomembni pri tem so (vir: PriceWaterhouseCoopers, 2004, s. 22):

- splošna finančna pomembnost in pomembnost poslovanja določene enote,
- tveganje za materialno nepravilnost, ki jo predstavlja enota in
- mera, do katere so poslovni procesi in pripadajoče kontrole povezane s centralno enoto, ali si delijo skupne storitve.

Še dodatne težave glede odločanja o vključenosti v testiranje velja za enote, ki niso v popolni lasti matičnega podjetja. V takšnih primerih mora biti to skupaj z razlogi razkrito v poročilu.
Pri odločanju o obsega testiranja sistema notranjih kontrol naj bi veljalo, da bi bila pokritost poslovanja podjetja zadostna za pridobitev ustrezne stopnje zagotovila. To vključuje poleg matične enote tudi ločene pomembne enote. Seveda je ponovno vse odvisno od mnogih dejavnikov. Tako naj ne bi upoštevali dobička v primeru, da transferne cene predstavljajo pomemben dejavnik, po drugi strani pa so primeren kriterij sredstva, če gre za proizvodno podjetje, ki ima veliko vrednost v zalogah, terjatvah in dolgoročnih sredstvih. Kontrole je potrebno oceniti v posameznih enotah, ki so pomembne glede na izbrani kriterij, četudi bi z vključitvijo samo centrale dosegalo zadostno pokritost. Enako velja za večje število takšnih enot – čeprav bi lahko z nekaj največjimi presegli kriterij in dosegli pokritost, to ni dovolj, temveč moramo upoštevati vse pomembne enote.
Povsem drug primer je, ko ima podjetje večje število manjših enot. Z njihovo vključitvijo v proces vzpostavitve IT notranjih kontrol, se doseže le majhna pokritost. Ob predpostavki, da so procesi v vseh enotah podobni, je dopustno, da izberemo nek vzorec in na njem testiramo učinkovitost kontrol. Seveda mora biti ta vzorec reprezentativen za celotno populacijo, zato je pomembno, kako ga izberemo.
V nekaterih primerih je neka enota pomembna z vidika tveganja, četudi to ni očitno glede na finančne kazalce. To velja predvsem za tiste, ki opravljajo neko specifično nalogo za celotno skupino podjetij. V takih primerih se morajo testirati kontrole, ki se nanašajo na tveganja izhajajoča iz teh posebnih opravil. Glede na vrsto poslovanja, ki ga opravlja posamezna enota, moramo vsako od njih povezati z ustreznim procesom na nivoju celotne skupine. To je potrebno zato, ker so nekatere zadolžene le za en proces oziroma za omejeno število procesov, vsi drugi se izvajajo nekje drugje. Primer je distribucijski center, ki edini skrbi za manipulacijo z nekim določenim materialom ali blagom, slednji pa je pomemben za proizvodnjo na nivoju celotne skupine podjetij.

4.4. Ocenjevanje IT notranjih kontrol

Sarbanes-Oxleyev zakon in tudi splošna praksa zahtevata analizo notranjih kontrol z vidika posameznih komponent. V skladu z metodologijo COSO kot referenco na tem področju se glavne komponente, ki so (COSO – Enterprise Risk Management – Integrated Framework, 2006) kontrolno okolje, presoja možnosti prevar, učinkovitost revizijskega odbora, ocenjevanje tveganja, nadzorne aktivnosti, informiranje in komuniciranje ter spremljanje, delijo še naprej v posamezne podkomponente in v skladu z njimi je potrebno izvesti ocenjevanje.
Kontrolno okolje je temelj za vse ostale komponente in se navezuje predvsem na kulturo organizacije, vrednote in predpise, skratka na oblikovanje strategij doseganja ciljev. Najbolje

je to razvidno iz hierarhične strukture podjetja in odnosov med zaposlenimi. Pri tem so najbolj pomembna razmerja med ljudmi na različnih nivojih. Kar se tiče prevar, mora biti vsaka kontrola, če obstaja le najmanjša možnost tovrstne nepravilnosti, preverjena tudi s tega vidika, ki se najpogosteje nanaša na dolžnosti in pravice zaposlenih. Učinkovitost revizijskega odbora ocenjuje uprava. Dejavniki, ki vplivajo na sposobnost doseganja naloženih ciljev, so neodvisnost, jasnost nalog in kakovost razumevanja s strani članov odbora, nivo sodelovanja z zunanjim revizorjem in drugimi udeleženci v procesu ter njihovo kompetentnostjo na področju, kjer delujejo. Ocenjevanje tveganja je pomembno z vidika učinkovitega izvajanja kontrol, saj je potrebno razumeti nevarnosti, ki grozijo poslovanju podjetja, da je upravljanje z njimi uspešno. V skladu s tem je priporočljivo, da podjetje izvaja ocenjevanje tveganja na neki smiselni periodični osnovi, da posveti dovolj pozornosti izbiri oseb, ki bodo to izvajale in o tveganjih komunicira tudi s preostalimi zaposlenimi, seveda v okviru zmožnosti. Nadzorne aktivnosti skrbijo, da so sklepi vodstva tudi udejanjeni. Potrebno je, da se izvajajo v vseh funkcijah in na vseh nivojih, da smo prepričani o celovitem izvajanju procesa testiranja kontrol in spremljajočih zadev. Te aktivnosti vključujejo predvsem (Howard, 1992, s. 28):

- organiziranje (organization): podjetje mora imeti pregled nad organizacijo, razporejanjem pravic in dolžnosti ter poročanjem, delegiranje pravic in dolžnosti mora biti natančno določeno;
- razmejitev dolžnosti (segregation of duties): posameznikom so dodeljene pravice le za izvajanje dela postopka, posledica tega je nadzor;
- fizično varovanje (physical safeguarding): to obsega predvsem nadzor nad sredstvi in papirno dokumentacijo;
- odobritve in potrjevanje (authorization and approval): vse transakcije morajo biti potrjene;
- preračuni in beleženje (arithmetical and accounting): v to skupino se uvršča preverjanje točnosti izračunov, primerjave postavk in pravilnosti beleženja:
- osebje (personnel): zaposleni morajo biti kompetentni za izvedbo zadolžitev;
- nadzor (supervision): spremljanje s strani za to zadolžene osebe in
- vodstvo (management): nadzorne aktivnosti, ki jih izvaja vodstvo, primer je primerjava načrtovanih z doseženimi rezultati.

Nekatere praktične izvedbe nadzornih aktivnosti, kot jih predlaga COSO, so naslednje (Applying COSO's – ERM, 2006):

- visokonivojski pregledi (primerjava doseženega z načrtovanim, napovedmi, glede na preteklo obdobje in konkurenco),
- funkcijski nadzor ali nadzor nad aktivnostmi (managerji pregledujejo poročila o poteku izvajanja aktivnosti, s čimer stalno spremljajo poslovanje oddelka ali skupine, ki jim je bila dodeljena),
- obdelava informacij (nadzor nad točnostjo, celovitostjo in avtoriziranostjo transakcij),
- fizična kontrola nad sredstvi (fizična zaščita in dovolj pogosto usklajevanje dejanskega stanja z evidenco),
- kazalniki izvajanja (analiziranje odstopanj) in

- ločevanje pravic in dolžnosti (z delitvijo opravil v več korakov in razdelitvijo dolžnosti za njihovo opravljanje dosežemo tudi določen nadzor, ki ga izvajajo zaposleni sami).

Da lahko osebje učinkovito opravlja svoje zadolžitve in da so računovodska poročila pripravljena tako, kot je zahtevano, je potrebno, da so na voljo informacije v pravilni obliki in ob pravem času. S tem se ukvarja komponenta informiranje in komuniciranje, ki je povezana z identificiranjem, zajemom in izmenjavo informacij. Ta komponenta je še toliko bolj pomembna, ker opravlja tudi funkcijo povezave med ostalimi. Konec koncev je današnja doba označena kot informacijska, zato ni nenavadno, da je toliko pozornosti namenjeno ravno temu področju. Pri analiziranju te komponente je potrebno upoštevati podatke, ki so pridobljeni interno ter tudi iz zunanjih virov. To je zahtevano za pripravo računovodskih poročil in razkritij, kjer se z notranjimi podatki prepletajo zunanji, in sicer predvsem panožni, splošni ekonomski in regulatorni. Pri vsem tem je pozornost potrebno nameniti tudi varovanju podatkov, kar ne obsega samo omejevanje dostopa do njih, temveč tudi njihovo arhiviranje.

Spremljanje kakovosti izvajanja IT notranjih kontrol je stalen proces, za katerega je odgovorno vodstvo. Nekateri primeri tega so:

- notranje revizije,
- pregledi vodstva,
- aktivnosti revizijskega odbora in
- samoocenjevalni pregledi.

Obstajajo še druge podkomponente, in sicer sta pomembni predvsem stalno in periodično spremljanje aktivnosti ter poročanje o pomanjkljivostih. Razlika med stalnim in periodičnim spremljanjem je poleg pogostosti izvajanja tudi v tem, da drugega izvaja višje vodstvo ter da je obseg pri posameznih izvajanjih lahko različen, saj je odvisen od ocene tveganja. Pri poročanju o pomanjkljivostih je potrebno paziti, da je poročilo namenjeno osebam, ki bodo sposobne in pripravljene izvajati akcije z namenom odprave teh pomanjkljivosti.

IT notranje kontrole pridejo v veliki meri v poštev v procesu priprave poročila ob koncu poslovnega leta. To se nanaša predvsem na prenose in obdelavo in pri tem je možna visoka stopnja avtomatizacije kontrol, poudarek je predvsem na različnih usklajevanjih. Za razliko od nekaterih ostalih kontrol je sodelovanje zunanjega revizorja tu manj pomembno, saj je glavna odgovornost naložena vodstvu.

Pri finančnem poročilu so enako pomembna kot številke tudi razkritja, saj je marsikaj odvisno od usmeritev, ki jih upošteva podjetje. Pri tem se kontrole nanašajo predvsem na delitev odgovornosti, kar pomeni potrjevanje in izvajanje opravil, ter določanje virov informacij in podatkov. V slednje spadajo tudi manipulacije s podatki, kot so različni izračuni, pretvorbe in podobno. Po drugi strani pa so IT notranje kontrole dokaj omejene pri postavkah, ki so v veliki meri plod ocen in presoj. Tu je še vedno najpomembnejši človeški dejavnik, vendar je informacijska tehnologija lahko v izdatno pomoč.

Pri analizi posameznih komponent je potrebno upoštevati še dve stvari. V prvi vrsti so to IT splošne kontrole, druga pa so kontrole na ravni podjetja. Prve so namenjene zagotavljanju pravilnosti delovanja informacijskega sistema, kar je pogoj za učinkovito delovanje aplikacijskih kontrol. Z njimi je tesno povezana komponenta, ki se navezuje na informiranje

in komuniciranje, poleg tega je integriteta računovodskih izkazov v veliki meri odvisna od zaključenosti, točnosti in pravočasnosti informacij in tako posledično od IT splošnih kontrol. Način, kako so te kontrole vključene v proces ocenjevanja učinkovitosti kontrol, je odvisen od organizacije in uporabe informacijske tehnologije nasploh. V prvi vrsti morajo pokrivati aplikacijske kontrole in jim zagotavljati temelj za učinkovito delovanje. Zato morajo odgovorne osebe razumeti, kako se finančni podatki pridobivajo in spreminjajo v informacije ter nadalje povezati finančne izkaze in poslovne procese ter podprocese z računalniškimi sistemi. V testiranje mora biti vključena tudi vsa relevantna infrastruktura. Bolj natančno, vključeni morajo biti naslednji elementi:

- IT kontrolno okolje,
- razvoj aplikacij,
- spremembe programske opreme,
- dostop do aplikacij in
- izvajanje programov.

V želji po popolnem zajemu kontrol vodstvo oziroma odgovorni zaposleni velikokrat pretiravajo, saj ne upoštevajo le tistih kontrol, ki so povezane s pomembnimi konti in razkritji, temveč naložijo sebi, predvsem pa sodelavcem, dosti odvečnega dela. Kot je že bilo omenjeno, so druga skupina kontrole na ravni podjetja. Tudi glede njih je potreben premislek, v kolikšni meri bodo vključene v program ocenjevanja kontrol. Te kontrole zagotavljajo, da deluje nadzor nad celotnim podjetjem. Preveriti jih je potrebno še preden se odgovorni začno ukvarjati s kontrolami na nižjih nivojih. Nadvse so pomembne za podjetja, ki imajo več ločenih enot, vendar jih ne smemo zanemariti v nobenem primeru.

4.5. Vključenost zunanjih partnerjev

Vodstvo podjetja je seveda odgovorno tudi za delo zunanjih pogodbenih partnerjev. Za finančno poročanje o tem mora ravno tako vzpostaviti sistem notranjih kontrol, mnoge od njih se navezujejo v največji meri ravno na partnerjevo poslovanje. Pri IT notranjih kontrolah je stvar še toliko bolj zapletena. Lahko obstaja potreba po »vpogledu« v informacijski sistem drugega podjetja, v primeru, da si podjetja delita vire informacijske tehnologije, pa je potrebno še toliko več naporov vložiti v zagotovitev učinkovitost IT splošnih kontrol. Če je partnersko podjetje glede informacijskega sistema ločeno, potem je v veliko pomoč lahko poročilo SAS 70, tip II, ki natančno opisuje notranje kontrole ravno za potrebe koristnikov zunaj podjetja in je podrobneje opisano v poglavju 4.6.3 SAS 70 in SysTrust. Na žalost so takšna poročila izven ZDA precej redka, zato se je potrebno posluževati alternativnih postopkov, kot sta testiranje notranjih kontrol s strani podjetja naročnika storitev ali dogovor s partnerjevim revizorjem, da opravi testiranje kontrol.

Primer koriščenja tujega informacijskega sistema obstaja tudi v podjetju X, saj uporablja za naročanje blaga aplikacijo dobavitelja iz tujine, kamor se vnašajo vsa naročila. V sami aplikaciji se nastavijo oziroma so že vneseni vsi parametri, ki vplivajo na poslovno transakcijo, vključno s ceno, popusti in ostalimi pogoji oziroma elementi, potrebnimi za izvedbo posla. Urejanje pravice dostopov je izključno v domeni tujega partnerja. Glede na to, da se podatki iz aplikacije dobavitelja prenašajo avtomatsko v informacijski sistem podjetja

X, bi bilo zaželeno, da se opravi revizijski pregled same aplikacije. Vendar to ni mogoče, saj podjetje X nima niti najmanjšega vpliva na upravljanje z aplikacijo, poleg tega dobavitelj ne bi pristal na pregled, saj je pogajalska moč domače družbe zaradi različne velikosti obeh podjetij (seveda v prid tujemu dobavitelju) zanemarljiva. To je eden od primerov, kjer bi z neodvisnim poročilom o IT notranjih kontrolah, lahko pridobili zagotovilo o pravilnosti podatkov pridobljenih iz računalniškega programa ter opustili nekatera ročna, zamudnejša preverjanja. Namesto tega se morajo uporabiti IT odvisne notranje kontrole, ki jih je vzpostavilo podjetje X, saj se zaveda nujnosti kontroliranja pravilnosti naročil. Slednje so vezane na tedensko izpisovanje podatkov o naročenem blagu iz sistema, usklajevanju s pogodbo in ceniki ter poročanje vodji oddelka nabave, ki tako nadzoruje delo svojih podrejenih. To se preveri tudi s strani zunanjega revizorja, in sicer se izbere reprezentativen vzorec naročil ter preveri s podporno dokumentacijo in podatki v sistemu podjetja X.
V proces testiranja notranjih kontrol ni potrebno vključiti izvajalcev vseh storitev. Tako se lahko izključijo podjetja, ki opravljajo storitve v okviru nepomembnih procesov, enako velja za enkratne, ozko namenske storitve, ki se sicer nanašajo na pomembne procese. Pri oceni IT notranjih kontrol poslovnih partnerjev je potrebno upoštevati še nekaj dejavnikov – tako se ocena lahko bistveno spremeni ob naslednjih pogojih: fluktuaciji pomembnih zaposlenih, spremembah v poslovanju in ugotovljenih napakah pri njihovem poslovanju.

4.6. Dokumentiranje

Za področje notranjih kontrol je splošno znano reklo, da kar ni dokumentirano, ni narejeno. Iz tega lahko sklepamo na pomembnost naslednje faze, to je dokumentiranje, ki mora biti izvedeno v takšnem obsegu, da je učinkovitost vzpostavitve kontrol nedvomno potrjena in preverljiva. To ima dva vidika – prvi je, da je potrjena samo ustreznost kreiranja kontrol na tej stopnji, drugi vidik pa mora omogočati osebi, ki je povprečno izobražena o teh zadevah, izvedbo testiranja kontrol s pomočjo te dokumentacije. Odločitev za preobsežno dokumentacijo nadalje vpliva na preveč podrobno testiranje in posledično neracionalno izrabo virov. Po drugi strani premalo natančno dokumentiranje onemogoča spoznavanje z notranjimi kontrolami in tudi negativno vpliva na samo testiranje. Dokumentiranje kontrolnih aktivnosti mora vsebovati odgovore vsaj na naslednja vprašanja:

- katero tveganje se obvladuje s to kontrolo,
- na kakšen način obvladujemo tveganje,
- zakaj se nadzorna aktivnost izvaja,
- kdo oziroma kaj (na primer kateri del računalniškega sistema) izvaja nadzorno aktivnost,
- kdaj oziroma kolikokrat se aktivnost izvaja in
- kakšna orodja so uporabljena pri izvajanju aktivnosti.

Dokumentiranje naj bi potekalo po nekem smiselnem vrstnem redu z namenom zagotovitve konsistentnost. Vrsti red naj bi bil že predviden pri načrtovanju in naj bi bil dovolj splošen, da je uporaben pri različnih kontrolah, hkrati pa dovolj podroben, da zadovoljivo pokriva vse potrebe. Tako naj bi prvi korak obsegal določanje obsega dokumentacije. Osnovni napotki so bili podani že zgoraj, še bolj podrobni pa v poglavju 4.2 Določanje obsega in načrtovanje. Za

obnovitev naj še enkrat navedem, da naj bi bile testirane in tako tudi dokumentirane IT notranje kontrole, ki se nanašajo na bistvene konte, razkritja in procese.
V okviru dokumentiranja se morajo poleg samih kontrol vsaj v osnovi opisati celotni procesi in transakcije. Tako je veliko lažje razumeti kontrole in v primeru nepravilnosti najti in odpraviti le-te. Pri tem si lahko pomagamo z različnimi tehnikami, še posebno koristni so razni shematski prikazi, ki jih dopolnjujejo opisi. Potrebno je upoštevati, da mora biti dokumentacija razumljiva in ne preveč zapletena, saj je v tem primeru potrebnega preveč časa za razumevanje poteka procesov. Pomembno pa je, da je nedvoumna in s tem možnost napak zmanjšana. Hkrati je potrebno povedati, da lahko podjetje že uporabi obstoječo dokumentacijo, če ta obstaja. Tako je ni potrebno sestavljati znova, temveč jo le prilagodi in dopolni. Največkrat je tako uporabljena dokumentacija, ki je bila pripravljena za postopke pridobivanja standardov ISO.
Precejšnjo pozornost je potrebno nameniti opisu samih IT notranjih kontrol. To pomeni, da je potrebno navesti podrobnosti glede njihove sestave v povezavi z računovodskim poročanjem. Vsaka kontrola se more povezati s trditvami (assertions), ki se nanašajo na pomembne konte.
V nadaljevanju je podan opis za proces nabave blaga v podjetju X. Najprej je v tabeli 5 predstavljen opis procesa z navedenimi aplikacijami, ki podpirajo določen del procesa, ter ugotovljenimi kontrolami v vsakem podprocesu, nato so v tabeli 6 predstavljene povezave med nekaterimi potencialnimi nepravilnostmi, izbranimi kontrolami in trditvami. Naštete kontrole tu niso podrobneje opisane, ker bo to narejeno za izbrane primere v poglavju 4.8 Testiranje notranjih kontrol.

Tabela 5: Opis procesa nabave blaga z relevantnimi kontrolami

OPIS	APLIKACIJA	KONTROLA
Glede na pripravljene letne načrte podjetja in trenutno povpraševanje na trgu v podjetju X določijo okvirno nabavno količino za naslednje tri mesece. Dobava traja približno dva tedna, zato je dolžnost nabavnega referenta, da naroči ustrezno količino blaga na mesečni ravni. Pri tem je potrebno pridobiti soglasje vodje nabavne službe, ki potrdi pripravljene podatke glede nakupov, ki so podlaga za vnos naročil v sistem dobavitelja.		Predhodna potrditev nabave s strani vodje oddelka.
Naročilo se kreira v aplikaciji dobavitelja (iz Evropske skupnosti). Vsak nabavni referent ima svoje uporabniško ime, s katerim se prijavi v program. V sistemu so že vnesene cene, dogovorjeni popusti, pogoji dobave in plačila – vse to je dogovorjeno s pogodbo in se preveri ob naročilu. Vsak artikel se zaradi njegove visoke vrednosti naroča samostojno, kar pomeni, da za eno blago obstaja ena naročilnica.	Aplikacija dobavitelja	Preveritev cene, popustov, pogojev dobave in plačila s pogodbo, cenikom in drugo dokumentacijo. Avtomatično številčenje naročila.
S strani dobavitelja oziroma njegove aplikacije vsak artikel dobi unikatno identifikacijsko številko, ki blago spremlja skozi vse nadaljnje procese do prodaje kupcu.		Vsak artikel dobi unikatno identifikacijsko številko, ki enolično označuje blago.

S paketno obdelavo se opravi prenos podatkov iz aplikacije dobavitelja v aplikacijo podjetja X. Vmesnik je nastavljen tako, da če prenos ni uspešen, samodejno pošlje sporočilo skrbniku aplikacije.	Aplikacija dobavitelja, aplikacija podjetja X, vmesnik	Ob neuspešnem prenosu podatkov iz aplikacije dobavitelja v aplikacijo podjetja X se pošlje opozorilo skrbniku aplikacije.
Nekaj dni pred prejemom blaga podjetje X dobi tudi račun od dobavitelja, in sicer v papirni obliki. Podatke na računu preveri referent s podatki v aplikaciji dobavitelja (naročilo) in ga vnese v aplikacijo podjetja X. Hkrati se račun avtomatsko poknjiži – beleži se kot blago na poti in obveznosti do dobavitelja. Celotna nabavna vrednost se izračuna glede na predhodno nastavljene parametre – nakupni vrednosti se doda pol odstotka pribitka za odvisne stroške.	Aplikacija dobavitelja, aplikacija podjetja X	Uskladitev podatkov na računu z naročilom.
Blago se dobavi v skladišče pogodbenega partnerja podjetja X. Tam skladiščnik pregleda blago in podpiše prevzemne dokumente. Najpomembnejši z vidika podjetja X glede prevzema je CMR, ki mora biti obvezno potrjen tudi s strani prevoznika. CMR se po faksu pošlje v podjetje X.		Skladiščnik pred prevzemom preveri blago in podatke na prevzemnem dokumentu, preden ga potrdi.
Prevzem se vnese v aplikacijo podjetja X, uporabijo se podatki od predhodno vnesenega računa. Ob tem se sestavi prevzemnica (v elektronski obliki), ki se primerja s potrjenim prevoznim dokumentom (CMR), prejetim iz pogodbenega skladišča.	Aplikacija podjetja X	Avtomatska uporaba podatkov z računa za kreiranje prevzemnice. Primerjava prevzemnice in prevoznega dokumenta.
S kreiranjem prevzemnice in potrditve prevzema se blago prenese s konta blago na poti na konto prodajno skladišče. Hkrati se poveča analitična evidenca in opravi avtomatičen prenos v glavno knjigo.	Aplikacija podjetja X, glavna knjiga	Avtomatičen prenos iz analitične evidence v glavno knjigo.
Tedensko se izpiše poročilo iz aplikacije dobavitelja, ki vsebuje podatke o naročilih in dobavah. Podatki se primerjajo s tistimi v aplikaciji podjetja X, poleg tega se naredi primerjava s prejšnjimi obdobji in načrti.	Aplikacija dobavitelja, aplikacija podjetja X	Tedenska uskladitev podatkov v aplikaciji dobavitelja in aplikaciji podjetja X ter primerjava s prejšnjimi obdobji in načrti.

Vir: Avtor

Na podlagi poznavanja procesa se določijo možne nepravilnosti, zanje se poiščejo kontrole in določijo trditve (assertions). Izbrani primeri možnih nepravilnosti, kontrol in trditev so prikazani v tabeli 6.

Tabela 6: Povezave med nekaterimi nepravilnostmi, ki se lahko pojavijo, izbranimi kontrolami, ki te nepravilnosti pokrivajo, in trditvami (assertions)

Možna nepravilnost	Izbrana kontrola	Trditev
Cena naročenega blaga je napačna.	Preveritev cene, popustov, pogojev dobave in plačila s pogodbo, cenikom in drugo dokumentacijo.	Zaloge in z njimi povezani stroški prodanega blaga – merjenje oziroma ovrednotenje. Obveznosti do dobavitelja in povezani konti v izkazu poslovnega izida – merjenje oziroma vrednotenje.
V skladišče je prevzeto napačno blago.	Skladiščnik pred prevzemom preveri blago in podatke na prevzemnem dokumentu, preden ga podpiše	Zaloge in z njimi povezani stroški prodanega blaga – obstoj oziroma pojav. Zaloge in z njimi povezani stroški prodanega blaga – celovitost.
Nabava je knjižena v napačno obdobje.	Avtomatičen prenos iz analitične evidence v glavno knjigo.	Zaloge in z njimi povezani stroški prodanega blaga – celovitost. Obveznosti do dobavitelja in povezani konti v izkazu poslovnega izida – celovitost.

Vir: Avtor

Način in oblika dokumentiranja je v veliki meri prepuščena avtorjem, vendar se morajo kljub temu običajno držati določnih pravil. Katera so to, je odvisno predvsem od namen preverjanja IT notranjih kontrol in komu se bo poročalo, njihove značilnosti pa so predstavljene v nadaljevanju.

4.6.1. Zahteve dokumentiranja in poročanja

Dokumentiranje je neločljivo povezano s področjem notranjih kontrol v podjetju, saj je ena od pomembnih faz v opredeljevanju učinkovitosti kontrolnih mehanizmov in je v veliki meri odvisno od zahtev izbranega standarda. Navezuje se na utemeljitev obsega področja, analizo celotnega sistema notranjih kontrol, opis in oceno priprave ter izvedbe testiranj in analizo rezultatov dobljenih pri testiranju, skratka na celoten proces obravnavanja notranjih kontrol.
V osnovi so razlike med revizijskimi kontrolami in tistimi, ki jih uporablja vodstvo, zelo majhne, pri slednjih je samo še poudarjen vpliv drugih aktivnosti, kot so načrtovanje, organiziranje, kadrovanje in vodenje (Chamber et al, 1987, s. 46). To velja tudi za področje dokumentiranja in poročanja, zato je v nadaljevanju opisan predvsem revizijski vidik kontrol, ki pa je kot je že bilo rečeno, v osnovi enak vodstvenim.

Priporočila glede dokumentiranja revizijskih postopkov podaja Mednarodni standard revidiranja 230 in ga lahko v večini primerov vzamemo kot vodilo pri dokumentiranju postopkov glede notranjih kontrol. Standard določa pripravo in hranjenje dokumentacije v obliki in obsegu, ki vsebuje zadostne dokaze za podporo revizijskemu mnenju in potrjuje, da so bili postopki opravljeni v skladu z ustreznimi predpisi in standardi. Posledično mora biti dokumentacija zadosti podrobna, da je iz nje možno razbrati[8] (IFAC, 2006, s. 356):

- naravo, časovno komponento in obseg revizijskih postopkov;
- rezultate izvedenih postopkov in pridobljene revizijske dokaze ter
- pomembne zadeve, ki so bile ugotovljene med revizijo, in zaključke ter sklepe.

Poleg tega mora biti vsak dokument opremljen s podatki, kdo je izvajal določeno nalogo ter kdaj, katera metodologija je bila uporabljena, kaj je bil namen dela, osnovnimi podatki o podjetju, ustrezno morajo biti označene tudi vse dopolnitve in popravki. Z namenom večje učinkovitosti dela pa je priporočljiva uporaba standardnih obrazcev, ki se lahko prilagajajo po potrebi. Obenem je pomembno tudi ustrezno obravnavanje dokumentov po tistem, ko so že kreirani, saj je potrebno zagotoviti njihovo zaupnost in nedosegljivost nepooblaščenim osebam, hkrati pa jih hraniti za celotno obdobje, ki je zahtevano s strani zakonodajalca oziroma snovalca drugih predpisov ali pa je to potrebno zaradi narave dela.

Kot je mogoče že delno sklepati iz doslej navedenega, vsebina in oblika dokumentov glede notranjih kontrol nista natančno predpisani, vendar morajo biti obvezno jasno razvidni osnovni podatki o izvedenih aktivnostih, odgovornostih, času poteka aktivnosti ter rezultati. Pri tem je potrebna pozornost, da pri dokumentiranju ni zajet samo proces ali aktivnost, temveč da je natančno definirana tudi sama kontrola. To najbolje ponazori primer, in sicer preveritev prodanih količin (trojno ujemanje: naročilnica-račun-dobavnica[9]), pri čemer si pomagamo s predstavitvijo podatkov v tabelarični obliki. Kreiranje tabele kot pomoč pri usklajevanju podatkov je aktivnost v procesu, medtem ko se sama kontrola nanaša na raziskovanje ujemanja oziroma odstopanja s strani določene osebe oziroma sistema. V to spada označitev, katera oseba je izvajala preverjanje, kdaj je to počela in za katero obdobje ter kaj je ugotovila oziroma drugi ustrezni podatki. Zajete naj bi bile tudi vse podkomponente posamezne kontrole ter podporno dokumentacija, kot so na primer osnovni podatki o podjetju, podatki o naročilnici, računu, dobavnici in podobno.

V prvem koraku je potrebno opisati kontrolo. Najbolj pregledno je to narediti tabelarično, kjer umestimo kontrolo v ustrezen del procesa, jo povežemo s pravimi trditvami (assertions) in določimo še ostale parametre. Primer takšnega opisa je razviden iz tabele 7.

[8] Kot reprezentativna oseba je določen izkušen revizor brez predhodnega poznavanja tega določenega projekta.

[9] Čeprav je trojno ujemanje zelo uporabna kontrola in preprosta za preveritev, ima svoje pomanjkljivosti – denimo količina na naročilnici je lahko različna od tiste na računu oziroma dobavnici, ker dobavitelj ni imel na zalogi dovolj enot blaga.

Tabela 7: Kontrolna matrika

Proces	Možna napaka	Kontrola	Opis in pogostost kontrolne aktivnosti	Vrsta kontrole	Trditev (assertion)	Vrsta kontrole	Postopek, ki sledi
Prodaja (vključuje terjatve)	Fiktivna ali podvojena naročila so vnesena v sistem (drug primer: Vse izdaje blaga niso zaračunane)	Preveritev trojnega ujemanja	Preden se račun odobri (podpiše) se preverijo podatki (količine) na naročilnici, računu in dobavnici, dnevno	IT odvisna ročna kontrola (temelji na dokumentih, ki jih kreira sistem; pregled opravi oseba)	Celovitost, pojav, obstoj, vrednotenje, merjenje	Zaznavalna kontrola	Izbira vzorca 25 primerov kompletov vseh dokumentov in preveritev ujemanja količin ter cene in ustrezne odobritve računa (podpis)

Vir: Avtor

Pomembno je, da obstajajo natančni opisi procesov, saj je tako lažje določiti točke, kjer bi lahko šlo kaj narobe in zanje poiskati kontrole za obvladovanje tveganj. Ti opisi so lahko v obliki diagramov, navodil, vprašalnikov ali katerikoli drugi, pomembno je le, da jih lahko uspešno uporabimo pri obravnavanju kontrol.

Pri dokumentiranju kontrol je pogosto priporočljivo najprej pokriti zasnovo (design) kontrol. Tako si zagotovimo, da ne obstajajo resnejše pomanjkljivosti na nobenem od nivojev kontrolnega okolja, ocenjevanja tveganj, kontrolnih aktivnosti, informiranja in komuniciranja ter nadzora. Za vsakega od teh področij je potrebno pripraviti dokumentacijo, ki je dovolj podrobna, da podpira določanje in ocenjevanje samih kontrol. V primeru, da je dokumentiranje pomanjkljivo, ne moremo zagotovi, da sistem notranjih kontrol zagotavlja okolje, v katerem lahko vzpostavimo mehanizme, ki bi preprečevali materialne napake. Ta faza dokumentiranja je odvisna od odločitve, katere kontrole bomo zajeli v testiranje, saj temu prilagodimo obravnavo zasnove kontrol. Oblika dokumentov je prepuščena njenim ustvarjalcem, potrebno je le paziti, da je v vsebini zajeto vse potrebno, in sicer podatke, ki osebi s povprečnim znanjem omogočajo oceno zadostnosti kontrole ter pripravo načrta testiranja.

Aplikacijske kontrole se ne razlikujejo bistveno od ročnih, večje razlike so pri IT splošnih kontrolah. Kar se tiče slednjih, morajo biti zajete komponente, ki so prikazane v tabeli 8.

Tabela 8: Komponente, ki morajo biti zajete pri dokumentiranju IT splošnih kontrol

KOMPONENTA	VSEBINA	TRDITVE (ASSERTIONS), KI MORAJO BITI POKRITE
IT kontrolno okolje	Vse pomembne aplikacije in infrastruktura.	Vse.
Spremembe programske opreme	Vse spremembe programske opreme (povezane s pomembnimi procesi), tako zaključene kot šele v pripravi.	Vse.
Dostopi do programske opreme	Logični dostopi do programske opreme (povezane s pomembnimi procesi) in relevantne infrastrukture.	Vse, vendar je poudarek na celovitosti (completeness) in obstoju (existance).
Računalniške operacije	Opravila povezana z izvajanjem nalog in njihovo spremljanje v IT okolju.	Vse, vendar je poudarek na celovitosti.

Vir: Prirejeno po PriceWaterhouseCoopers, 2004, str. 51

Tudi v primeru IT splošnih kontrol niti oblika niti natančna vsebina dokumentacije nista predpisani. Zahtevano je, da vsebuje dovolj podrobnosti, na podlagi katerih je mogoče sklepati o uspešni zasnovi in nadalje učinkovitosti izvajanja kontrol.
V okviru same dokumentacije pa ne smejo izostati opisi postopkov testiranja kontrol in končna ocena. V primeru, da je bila ugotovljena pomanjkljivost ali neučinkovitost posamezne kontrole, je potrebno vključiti dokumentacijo nadaljnjih postopkov. Način dokumentiranja je tudi v tem primeru v precejšni meri prepuščen presoji izvajalca aktivnosti.

4.6.2. Standardi poročanja

Standardi so dolgo časa urejali predvsem področje skrbništva in hranjenja dokumentacije, medtem ko so bila navodila glede vsebine in namena papirjev zelo nejasna. Tudi na tem področju prednjačijo ZDA, ki v marsikaterem pogledu pomenijo vodilo za druge države. Uredba revizijskih standardov SAS 41 (Statement on Auditing Standards[10]) iz leta 1982, ki je

[10] AICPA je izdala deset zahtev, ki jih morajo revizorji upoštevati pri svojem delu, v okviru desetih Splošno sprejetih revizijskih standardov (Generally Accepted Auditing Standards). Ti se delijo v tri smiselne sklope: splošni standardi, standardi dejanskega revidiranja ter standardi poročanja. Kot dopolnilo in pomoč pri razlagi v obliki bolj jasnega opredeljevanja revizijskih postopkov in predpisovanja oblike ter vsebine poročil so bile

nasledil SAS 38, ureja osnovno dokumentiranje opravljenega revizijskega dela in zagotavlja dokaz, da je (Levy, 2005, s. 30):

- bilo delo pravilno načrtovano in nadzorovano,
- da so bile notranje kontrole pravilno preučene in ocenjene ter
- da pridobljeni dokazi zadostujejo za izdajo mnenja.

Pomanjkljivost uredbe SAS 41 v zvezi z notranjimi kontrolami je v tem, da so bile pomanjkljivost slednjih lahko obravnavane tudi samo ustno. Tekmovalnost med revizijskimi hišami je vodila k čim večji učinkovitosti dela, ki se je odražala tudi v pomanjkljivi dokumentaciji, česar ni izboljšala niti uredba SAS 96, ki je bila izdana leta 2001. Posledica Zakona Sarbanes-Oxley je bila ustanovitev odbora PCAOB, ki je na področje dokumentiranja posegel s svojim Standardom številka 3. Slednji je vplival tudi na AICPA-jev odbor za revizijske standarde (Auditing Standards Board), ki ga je uporabil kot osnovo za pripravo naslednika uredbe SAS 96, ki bo praviloma prišel v poštev pri revizijah opravljenih za poslovno leto 2006 (ki se končajo na 15. decembra 2006 ali pozneje) (Levy, 2005, s. 30). Na splošno bo standard zahteval jasne dokaze, da je bila revizija opravljena v skladu z veljavnimi predpisi ter nedvoumne zaključke glede posameznih trditev (assertions) in finančnih izkazov na splošno. V osnovi je potrebno vključiti podatke o naravi, času in obsegu postopkov, opravljenem delu, namenu opravljenega dela, virih informacij in podatkov, ki so bili uporabljeni in sklepe, ki so osnovani na izvedenih postopkih, vse pa mora biti predstavljeno z natančnostjo, ki omogoča izkušeni osebi razumevanje opravljenega dela. Standard številka 3 in uredba SAS 96 se ukvarjata z revizijsko dokumentacijo na splošno in sta tu obravnavana, ker se v veliki meri nanašata na notranje kontrole, saj določata naravo in obseg potrebnih dokumentov, hranjenje in avtorizacijo. Na drugi strani obstaja uredba SAS 70, ki olajša storitvenim organizacijam[11] razkritje kontrolnih aktivnosti in s tem povezanimi procesi v enotni obliki, torej se v večji meri nanaša na področje notranjih kontrol. Zaradi aktualnosti s tega vidika, bo uredba predstavljena v nadaljevanju.

4.6.3. SAS 70 in SysTrust

V svetu sta znana predvsem dva koncepta preizkušanj notranjih kontrol, katerih pomembna dela sta končni poročili, eden je že omenjeni SAS 70, drugi pa je SysTrust. Namen slednjega je testiranje informacijskega sistema, če ustreza kriterijem na štirih področjih (Whittington, Pany, 2001, s. 762):

- dosegljivosti (availability) – preverja se, če je sistem dosegljiv za uporabo v predvidenih časovnih okvirih;
- varnosti (security) – preverja se zaščitenost informacijskega sistema z vidika fizične in logične varnosti;
- konsistentnosti (integrity) – preverja se, če so izvedeni procesi popolni, točni, pravočasni in odobreni;

---

izdane še Uredbe revizijskih standardov (Statements on Auditing Standards). Slednji služijo kot eno glavnih vodil pri revizijskem delu (Weirich, Reinstein, 1992, s. 57).

[11] S pojmom storitvena organizacija je tu mišljena družba, ki opravlja zunanje izvajanje storitev (outsourcing) za svoje stranke.

- vzdrževanosti (maintainability) – preverja se, če je sistem možno vzdrževati tako, da ni ogrožen kateri od zgoraj naštetih kriterijev.

Poročilo za SysTrust testiranje se lahko izdaja za eno samo področje ali kakršnokoli kombinacijo večih. Z njim pooblaščeni revizor potrdi učinkovitost kontrol na relevantnem področju oziroma v nasprotnem primeru, podobno kot za finančno revizijo, izda mnenje s pridržkom ali negativno mnenje. Osnovatelja SysTrust koncepta sta Ameriški inštitut preizkušenih računovodij (American Institute of Certified Public Accountants – AICPA) in Kanadski inštitut pooblaščenih računovodij (Canadian Institute of Chartered Accountants – CICA), ki sta tudi pripravila seznam kriterijev, ki morajo biti preverjeni in dobljeni rezultati navedeni v poročilu, ki je namenjeno vodstvu podjetja, strankam in poslovnim partnerjem.
SAS 70 se uporablja za ugotavljanje, predvsem pa dokumentiranje učinkovitosti kontrol pri organizacijah, ki ponujajo storitve drugim podjetjem. Značilen primer so ponudniki outsourcing storitev, zanje revizorji preučijo kontrolno okolje in izdajo mnenje o zasnovi kontrol, izvajanju oziroma uporabi in sami učinkovitosti. Poročilo je dveh vrst, tip ena in tip dva, razlika med njima je v tem, da samo drugi tip vsebuje poročilo o testiranju učinkovitosti. Razlike med obema vrstama so predstavljene v tabeli 9.

Tabela 9: Primerjava med SAS 70 poročiloma tipa ena in tipa dve

VSEBINA POROČILA	**POROČILO VRSTE ENA**	**POROČILO VRSTE DVE**
1. Neodvisno revizijsko poročilo, ki se tiče servisne organizacije (mnenje revizorja).	Vključeno	Vključeno
2. Opis kontrol servisne organizacije.	Vključeno	Vključeno
3. Informacije podane s strani neodvisnega revizorja, ki vključujejo opis testiranj učinkovitosti delovanja kontrol in njihove rezultate.	Opcijsko	Vključeno
4. Ostale informacije podane s strani servisne organizacije (na primer slovar izrazov).	Opcijsko	Opcijsko

Vir: SAS 70, 2005

Tudi SAS 70 je bil razvit s strani Ameriškega inštituta preizkušenih računovodij kot vodilo in pomoč storitvenim organizacijam pri razkrivanju svojega kontrolnega okolja strankam (uporabnikom storitev) in njihovim revizorjem v enotni obliki. To ni nekakšen seznam stvari, ki morajo biti pregledane, temveč zbirka napotkov za preverjanje, zagotavljanje zadostnega

nivoja kvalitete ter poročanja in se največkrat uporablja pri ponudnikih programske opreme dostopne prek spleta, centrih za obdelavo zahtevkov, računskih centrih in podobno.
Glede na dejstvo, da sta bila oba standarda, tako SAS 70 kot SysTrust razvita v veliki meri s strani AICPA, je zanimivo pogledati razlike med njima in preučiti okoliščine, v katerih je uporaben eden od njiju. Njune bistvene značilnosti so primerjalno prikazane v tabeli 10.

Tabela 10: Primerjava koncepta SAS 70 in SysTrust

	SAS 70	**SysTrust**
Namen	Rezultat je poročilo o kontrolah storitvenega podjetja v povezavi s finančnimi izkazi in relevantnimi trditvami (assertions).	Rezultat je poročilo o zanesljivosti sistema z upoštevanjem standardnih načel in kriterijev za vsa preverjanja.
Ali obstajajo že vnaprej pripravljeni kontrolni cilji oziroma kriteriji?	Ne.	Da.
Cilj	Razkrivanje informacij (information sharing) in jamstva (assurance); predstavljene so natančne informacije o zasnovi sistema in kontrol; mnenje o opisu sistema in kontrol ter rezultati revizijskih postopkov.	Jamstvo (assurance) za sistem. Podrobnosti o postopkih, ki se tičejo kontrol, niso vključeni.
Tipi sistemov, ki so predmet preverjanj	Sistemi, ki obdelujejo transakcije ali podatke za stranke.	Katerikoli sistem.
Dostopnost poročila	Običajno dostopen servisni organizaciji (naročniku), uporabniku storitev servisne organizacije in potencialnim bodočim strankam.	Ni omejitev.

Vir: SysTrust Assurance, 2006

Zgoraj opisana primera sta le dva od mnogih formaliziranih oblik dokumentiranja, vendar sta med pogosteje uporabljenimi. Največja notranja pomanjkljivost dokumentiranja je, da se ne izvaja že med posameznimi fazami, ampak se velikokrat prelaga na zaključek samega

ocenjevanja kontrol. Takrat pa bistveno vplivajo na njegovo slabšo kvaliteto časovni pritiski, poleg tega se nekatere stvari v nekaj dnevih ali tednih že pozabijo. Tako ostaja dokumentiranje eno od področij, kjer je mogoče doseči največje izboljšave, ki so zaradi pomembnosti samega področja tudi potrebne.
Cilj vsega tega je priprava na določitev učinkovitosti kontrole, vendar se v tem koraku določi samo sestava kontrole in se še ne testira, kajti pred tem je potrebno preveriti še ustreznost njene zasnove.

4.7. Preverjanje zasnove notranjih kontrol

Dokumentiranju sledi ocenjevanje vzpostavitve kontrol, v kar je vključeno preverjanje, ali so zasnovane ustrezno, da bodo preprečile ali zaznale nepravilnosti. Potrebno se je zavedati, da to še ni preizkušanje delovanja kontrol, kar bo opisano pozneje kot samo testiranje. Pri pregledu zasnove IT notranjih kontrol je pomembno, da (PriceWaterhouseCoopers, 2004, s. 52):

- so kontrole usklajene s tveganji;
- kontrole pokrivajo trditve (assertions) v ustrezni meri;
- bo kontrola zaznala nepravilnost pravočasno;
- imajo zaposleni, ki sodelujejo pri izvajanju kontrol, zadostna znanja in izkušnje;
- so pristojnosti zaposlenih zadostno ločeno, da je možnost prevar majhna;
- se kontrole stalno spremljajo ter anomalije obravnavajo ažurno,
- so informacije, na katerih temelji delovanje kontrol, zanesljive in
- da kontrole pokrivajo celotno časovno obdobje poslovanja.

Glede na zgornje kriterije imajo IT notranje kontrole vrsto prednosti pred ostalimi, saj so avtomatizirane, z njimi se ukvarjajo višje izobraženi in največkrat bolj izkušeni zaposleni, so praviloma kontrole na podrobnejši ravni, izvajajo se na celotni populaciji in ne le na vzorcu ter se izvajajo stalno, ne na nek periodičen časovni rok.
Da smo pravilno razumeli namen kontrole in njeno izvajanje v določenem obdobju, opravimo še tokohod oziroma walk-through skozi proces. V primeru procesa nabave blaga v podjetje X v ta namen od skrbnikov posameznih delov procesa pridobimo dokumente, ki potrjujejo obstoj in delovanje posameznih notranjih kontrol. Najbolj smiselno je, da zasledujemo določeno transakcijo skozi celoten sistem, kar je predstavljeno na primeru naročila proizvodnega stroja z dne 6.3.2006, kar je prikazano v tabeli 11.

Tabela 11: Primer tokohoda skozi proces nabave blaga (v povezavi s kontrolami) za podjetje X

TOK TRANSAKCIJE / KONTROLA	**REZULTATI TOKOHODA**	**UGOTOVLJENE POMANJKLJIVOSTI GLEDE DOKUMENTIRANJA ALI ZASNOVE**
Predhodna potrditev nabave s strani vodje oddelka	Potrdilo o odobritvi nabave artikla: od prodajnega referenta smo pridobili podpisano potrdilo s strani vodje nabave; potrdilo je z dne 6.3.2006 za 1 artikel (stroj za proizvodnjo); oznaka potrdila: P 2006/0024.	Ne
Vnos podatkov naročila in določitev parametrov	Preveritev pogojev naročila z dogovorjenimi: iz aplikacije dobavitelja smo s pomočjo nabavnega referenta pridobili izpis naročila številka 2006-540-000401 z dne 6.3.2006, pridobili smo pogodbo, ki ureja odnose med podjetjem X in dobaviteljem ter se nanaša na omenjeno naročilo in vsebuje določila o načinu plačila in dobavi; pridobili smo tudi aneks številka 3 k pogodbi, s katerim so določene cene in popusti. Uskladili smo podatke o ceni, pogojih plačila in dobave.	Ne
Avtomatično številčenje naročila.	Zaporedno številčenje naročil: s pomočjo nabavnega referenta smo ponovili postopek naročanja, pri tem smo bili pozorni na dejstvo, da aplikacija sama določi oznako naročila, ki je sestavljena iz tekoče letnice, oznake področja in vrste naročila ter šestmestne zaporedne številke, ki se inkrementalno povečuje za 1. Nabavni referent nima vpliva na spreminjanje oznake naročila.	Ne
Izbira artikla v procesu naročanja	Unikatna identifikacija artikla: pri ponovitvi naročila je bilo preverjeno, da se identifikacijska oznaka artikla določi v aplikaciji avtomatsko glede na vrsto izbranega blaga. Nabavni referent oznake ne more spremeniti, niti ne more nadaljevati z naročilom brez te številke. V izbranem naročilu številka 2006-540-000401 je artikel imel oznako WTTREPI7652.	Ne

Prenos podatkov iz aplikacije dobavitelja v aplikacijo podjetja X	Zagotovitev uspešnosti prenosa podatkov: s pomočjo sistemskega administratorja smo pridobili log datoteko z zapisi o uspešnosti prenosa podatkov; podatki z naročilom 2006-540-000401 so bili preneseni uspešno; od nabavnega referenta smo pridobili datumsko najbližjo opozorilo glede neuspešnega prenosa, in sicer z dne 4.6.2006.	Ne
Uskladitev podatkov na računu z naročilom	Uskladitev prejetega računa in naročila: primerjali in zagotovili smo istovetnost podatkov na prejetem računu od dobavitelja z oznako FAE06-111-87-4633 za artikel WTTREPI7652 in naročilnici 2006-540-000401 izpisani iz aplikacije dobavitelja.	Ne
Prevzem blaga v skladišču	Preveritev in potrditev ustreznosti blaga in njegove količine: Pridobili smo CMR, ki se nanaša na dostavo artikla WTTREPI7652 v skladišče; preverili smo, da je ustrezno potrjena s strani dostavljavca in prevzemnika/skladišča.	Ne
Kreiranje prevzemnice	Avtomatična uporaba podatkov z računa za prevzemnico: pridobili smo prevzemnico PRB-2006-3-R115, ki je bila kreirana na podlagi prevzema blaga z oznako WTTREPI7652 ter preverili, da se podatki ujemajo z računom FAE06-111-87-4633. Bili smo prisotni pri kreiranju nove prevzemnice, kjer smo se prepričali, da se le-ta ustvari lahko samo na podlagi prej vnesenega računa ter ugotovili, da referent v nabavi ne more spreminjati podatkov.	Ne
Primerjava prevzemnice in prevoznega dokumenta.	Uskladitev prevzemnice in prevoznega dokumenta: primerjali smo prevzemnico PRB-2006-3-R115 in CMR za artikel WTTREPI7652 in ugotovili, da se podatki ujemajo.	Ne
Prenos iz analitične evidence v glavno knjigo	Uskladitev analitične evidence in glavne knjige: preverili smo zapise za mesec marec v analitični evidenci in glavni knjigi ter si zagotovili, da so bili prenosi popolni, še dodatno smo preverili prenos za artikel WTTREPI7652. Za marec smo pridobili log datoteke, v katere se zapisujejo opravljeni prenosi. Ugotovili smo, da v omenjenem obdobju neuspešnih prenosov ni bilo.	Ne

Tedenska uskladitev podatkov v aplikaciji dobavitelja in aplikaciji podjetja X ter primerjava s prejšnjimi obdobji in načrti.	Uskladitev podatkov v aplikaciji dobavitelja in podjetja X ter primerjava s prejšnjimi obdobji in z načrti: pridobili smo dokumentacijo za celotno poslovno leto, ki dokazuje uskladitev med podatki v aplikaciji dobavitelja in aplikaciji podjetja X ter opravljeno analizo primerjave prometa s prejšnjimi obdobji in načrtovanim prometom. Rezultati analize so posredovani vodstvu, opravljeno delo dokazuje podpis referenta v računovodstvu na dokumentaciji. Podrobneje smo preverili opravljene naloge za poročilo z dne 13.3.2006, ki se nanaša na predhodni teden.	Ne

Vir: Avtor

Poseben primer so IT splošne kontrole. Vsak njihov del (IT kontrolno okolje, spremembe programske opreme, dostop do programske opreme in podatkov ter računalniške aplikacije) mora biti povezan z vsemi trditvami (assertions), toda vse niso enako pomembne, na primer pri kontrolah dostopov sta bistvena celovitost in obstoj. Kot zaključek faze dokumentiranja oziroma že uvod v naslednjo fazo, testiranje, se mora vodstvo oziroma odgovorni v podjetju odločiti, katere IT notranje kontrole se bodo testirale z vidika učinkovitosti izvajanja. Izbor je potrebno vsaj začeti že v tej točki, saj ga moramo opisati skupaj z navedbo razlogov oziroma dejavnikov, ki so vplivale na našo odločitev. Pri tem upoštevamo rezultate, ki smo jih pridobili pri preverjanju sestavov kontrol, precej veliko vlogo pa igra strokovna presoja. Kot je bilo že večkrat povedano, morajo kontrole pokrivati vse ustrezne trditve (assertions) za pomembne konte in razkritja, pri čemer ne smemo pozabiti na organiziranost podjetja (poslovanje razdeljeno v več enot in podobno) ter tveganja, ki ogrožajo podjetje.

4.8. Testiranje notranjih kontrol

Testiranje IT notranjih kontrol se mora sklicevati na vse komponente predstavljene v poglavju 4.2 Določanje obsega in načrtovanje za vse pomembne konte in razkritja na lokacijah podjetja, ki so pomembne individualno, ter tudi za tiste enote, kjer obstaja možnost povečanega tveganja zaradi posebnih razlogov. Celoten proces testiranje se običajno izvede v štirih korakih:

- določitev kontrol za testiranje v povezavi s fazo dokumentiranja,
- določitev oseb odgovornih za izvedbo testiranja,
- priprava programa testiranja in samo testiranje ter
- ovrednotenje rezultatov.

Obstaja tudi možnost ciklične iteracije teh korakov ali katera od njihovih kombinacij. To je odvisno od presoje vodje testiranja in odraža trenutne razmere. Pri načrtovanju testiranja je potrebno določiti kaj se bo testiralo, na kakšen način in kdaj. Načrt je potrebno pripraviti z mislijo na zadovoljivo raven zagotovila, ki jo bodo nudile kontrole, glede zaznave ali

preprečevanja nepravilnosti. Zadovoljiva raven ne pomeni absolutne gotovosti, saj te ni mogoče doseči oziroma je zanjo potrebno preveč sredstev glede na doseženi rezultat, temveč visoko verjetnost obvladovanja tveganja. Na kakšen način bo kontrola preizkušena je odvisno od notranjega revizijskega odbora oziroma drugega organa ali zaposlenih, ki so določeni, da vodijo aktivnosti v zvezi z zagotavljanjem in preverjanjem učinkovitosti kontrol. Revizorji najpogosteje testirajo kontrole z izbiro smiselnega vzorca določenega z metodologijo in potem s preizkušanjem na njih pridejo do sklepov o učinkovitosti. Samo podjetje ima pri tem več svobode in pride do rezultatov prek drugih postopkov ali celo kombinacije teh, saj ima praviloma na voljo več časa in ostalih virov. Prav tako ima pogosteje dostop do drugih informacij, na podlagi katerih lahko sklepa o učinkovitosti kontrol in tako zmanjša vzorec (če se odloči za ta način testiranja), ki je potreben za pridobitev neke stopnje zagotovila. Drug primer je uporaba kombinacije kontrol. Tudi na ta način si lahko zaposleni olajšajo delo in predvidijo uporabo več kontrol hkrati za obvladovanje istega tveganja. S takim kombiniranjem lahko pridejo do enakih rezultatov na lažji in hitrejši način. Seveda mora biti vse ustrezno dokumentirano in pojasnjeno, da ne prihaja do dvomov o nepopolni izvedbi testiranja kontrol.

Kot primer si poglejmo testiranje aplikacijske kontrole, in sicer prenos podatkov iz nabavno-prodajne aplikacije v glavno knjigo podjetja X, ki ji je dodano še razreševanje napak kot IT odvisna kontrola. Prenos se opravi na podlagi kreiranja prevzemnice oziroma izdajnice, hkrati se potrdi tudi dejanski prevzem ali izdaja blaga. Načrtovanje testiranja je predstavljeno v tabeli 12.

Tabela 12: Načrtovanje testiranja kontrole prenosa podatkov

Podjetje:	Podjetje X
Kontrola:	Avtomatski prenos podatkov iz nabavno-prodajne aplikacije v glavno knjigo (vmesnik)
Narava (tip) kontrole, frekvenca kontrole, obseg testiranja	Aplikacijska (razreševanje napak je IT odvisna ročna kontrola), dnevna, na enem primeru (ugotavljanje in razreševanje napak: na reprezentativnem vzorcu 10-ih odstotkov)
Opis kontrole:	Kreiranje prevzemnice v nabavno-prodajni aplikaciji pomeni potrditev prevzema, kreiranje izdajnice pa potrditev izdaje blaga. Hkrati s kreiranjem dokumenta se sproži tudi prenos v glavno knjigo. Prenos podatkov je popolnoma avtomatski, torej je kontrola aplikacijska, in sicer na podlagi predhodnih nastavitev.
Potrebno testiranje:	Potrebno je zagotoviti: - da se ob kreiranju prevzemnice/izdajnice (potrditev prevzema/izdaje) sproži prenos podatkov – testiranje na enem primeru prejema blaga in enem primeru izdaje blaga; - da se prenesejo vsi podatki in to pravilno – testiranje agregatnih podatkov, - da se podatki prenesejo v pravo obdobje in na prave konte – testiranje nastavitev; - da se morebitne napake ugotovijo pravočasno in sledi ustrezen odziv – pregled log datotek in testiranje na vzorcu 10-ih odstotkov napak.
Izvajalec testiranja:	Revizor informacijskih sistemov

Vir: Avtor

Kot je že bilo omenjeno, je prenos podatkov aplikacijska kontrola in spada v skupino vmesnikov. Njeno testiranje je sestavljeno iz več delov, in sicer preveritev sprožitve prenosa ter preveritev pravilnosti in uspešnosti prenosa. Glede na to, da je kontrola aplikacijska, se vse testira na enem primeru, razen razreševanje napak, ki je IT odvisna kontrola, saj vključuje človeški dejavnik, in se zato testira na vzorcu 10-ih odstotkov vse populacije. Tu se pojavlja dilema, če ne bi bilo primerneje obravnavati ugotavljanje in razreševanje napak kot samostojno kontrolo, kar po specifikaciji tudi je. Zaradi soodvisnosti je tu testirana v okviru samega prenosa. Poleg tega ne smemo pozabiti, da mora biti za testiranje aplikacijskih kontrol izpolnjen še en pogoj, in sicer učinkovitost IT splošnih kontrol. Samo testiranje je podrobneje opisano v tabeli 13.

Tabela 13: Dokumentiranje postopkov testiranja aplikacijske kontrole prenosa podatkov iz nabavno-prodajne aplikacije podjetja X v glavno knjigo in razreševanje morebitnih napak

Podjetje:	Podjetje X
Zadeva:	Testiranje kontrole prenosa podatkov iz nabavno-prodajne aplikacije v glavno knjigo
Datum bilance stanja (obdobje preverjanja):	31.12.2006
Datum testiranja:	11.1.2007
Testiranje izvedel:	X.X., revizor informacijskih sistemov
Pregledal:	Y.Y., vodja projekta
Izvedeni postopki:	Od skrbnika nabavno-prodajne aplikacije smo pridobili tehnično dokumentacijo, v kateri je navedeno, da kreiranje prevzemnice v nabavno-prodajni aplikaciji pomeni potrditev prevzema, kreiranje izdajnice pa potrditev izdaje blaga, hkrati se sproži tudi prenos podatkov v glavno knjigo. Pridobili smo zagotovilo, da sprememb glede tega ni bilo – učinkovite IT splošne kontrole (pripoznano na podlagi testiranja). Od podjetja X smo pridobili naključno izbrano prevzemnico 2006-540-000566 z dne 4.5.2006 in naključno izbrano izdajnico 2006-110-001901 z dne 16.11.2006. Za oba primera smo preverili podatke v nabavno-prodajni aplikaciji in glavni knjigi ter jih uskladili. Prav tako smo pridobil elektronski izpis podatkov tako glede nabave kot prodaje iz nabavno-prodajne aplikacije in glavne knjige za mesec maj in november ter jih uskladili. Preverjali smo število zapisov in skupno vrednost prenosov. Dodatno smo pridobili agregiran izpis iz obeh aplikacij za celotno leto 2006 in jih uskladili vrednostno. Sistemski administrator nam je pripravil izpis nastavitev sistema, pri čemer smo posebno pozornost posvetili kontnim pravilom. Od računovodstva, ki skrbi za njihovo vzdrževanje, smo pridobili veljavne nastavitve in jih uskladili med seboj, poleg tega smo preverili smiselnost oziroma ustreznost nastavitev vključno s kontnimi pravili. Nadalje smo pridobili log datoteko z zapisi (ne)uspešnosti prenosov za celotno leto 2006. Ugotovili smo, da sta bila v vsem obdobju skupaj dva neuspešna prenosa, zaradi majhne populacije smo preverili oba, zanju smo pridobili dokumentacijo in pojasnila glede nadaljnjega ukrepanja.
Ugotovitve:	Pri uskladitvi zapisov glede izbrane nabave oziroma prodaje blaga nepravilnosti ni bilo ugotovljenih. Zapisi so identični. Prav tako ni bilo ugotovljenih razlik med podatki v obeh aplikacijah za izbrana meseca, niti za celotno leto. Pri nastavitvah, vključno s kontnimi pravili, nepravilnosti niso bile ugotovljene. Oba neuspešna prenosa sta bila posledici tehničnih težav na strežniku in sta bila uspešno izvedena ob prvi ponovitvi, kar je razvidno iz pridobljene dokumentacije.
Zaključek:	Nepravilnosti oziroma napake niso bile ugotovljene. Kontrola je učinkovita.

Vir: Avtor

V tabeli 13 je opis testiranja rahlo prirejen, saj se praviloma dodaja podporna dokumentacija vključno z delnimi izpisi elektronskih podatkov. Čim natančnejše dokumentiranje je priporočljivo tudi v primeru, da ni potrebno z vidika standardov, saj je tako ponovitev v naslednjem letu lažja.

Neko splošno vodilo pri presojanju zadostnosti kontrolnega okolja je primerjava dejanskih in pričakovanih kontrol. Postopek lahko strnemo v štiri korake (Kinsella et al, 1995, s. 56):

- ugotavljanje na podrobnem nivoju, katera so pomembna tveganja;
- predvidevanje, katere kontrole bi praviloma zmanjševale ta tveganja;
- preverjanje, če kontrole, ki so dejansko v uporabi, služijo temu namenu in
- preverjanje, če so v uporabi nadomestne kontrole.

Ugotovitve iz zgornjih postopkov se potem uporabijo v pripravi testiranja.

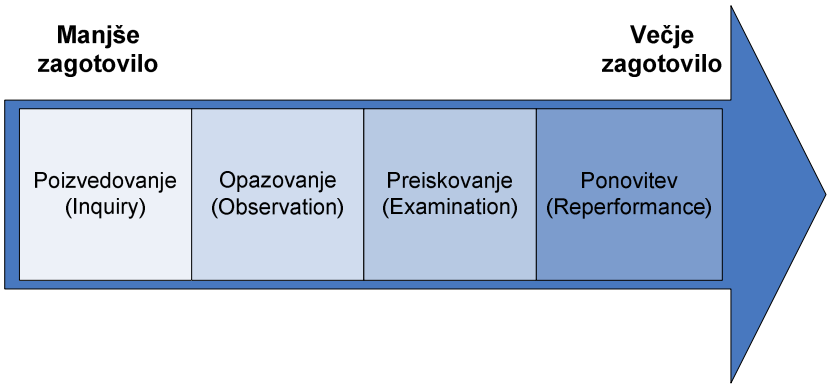
Oseba, ki je zasnovala in vzpostavila neko kontrolo lahko ocenjuje tudi njeno učinkovitost, vendar se v tem primeru pojavijo nekatere omejitve. Vsaj z vidika zunanjega revizorja, ki se ne more zanašati na kontrole v takšni meri, kot bi se sicer lahko, če bi bile vloge bolje razmejene. Zato je običajno primerneje, da kontrole testirajo zaposleni v oddelku notranje revizije ali posebej izbrane osebe in ne njihovi kreatorji.

Program testiranja je sestavljen iz več elementov, in sicer naslednjih (Interna dokumentacija EY):

- seznam kontrol, ki so predvidene za testiranje, na nivoju trditev računovodskih izkazov (assertions),
- tehnike uporabljene pri testiranjih,
- obseg testiranja z navedenim številom obravnavanih enot in pojasnjenimi razlogi za takšno odločitev,
- čas izvajanja testa, časovno obdobje, ki bo pokrito s testiranjem in morebitno dodatno testiranje po potrebi,
- osebe, ki bodo izvajale testiranje, priporočljivo je, da so navedene še vse ostale bistvene okoliščine,
- opis postopkov uporabljenih pri testiranju,
- dokumentacija, ki mora biti sestavljena ob testiranju ter
- opredelitev postopkov obravnavanja izjem.

Seznam kontrol mora biti v tej točki že pripravljen, saj so bili postopki izvedeni tekom prejšnjih aktivnosti, paziti moramo le, da jih predstavimo na pravem nivoju. Bolj nova je izbira tehnike testiranja kontrol. Na voljo imamo štiri vrste, vsaka od njih nam da različno stopnjo zagotovila, kar je razvidno s slike 19.

Slika 19: Vsaka od štirih različnih tehnik testiranja IT notranjih kontrol nam da različno stopnjo zagotovila o obvladovanju tveganj



Vir: Interno gradivo EY

Poizvedovanje nam daje najnižjo stopnjo zagotovila in kot taka ni zadostna tehnika, da bi lahko na podlagi njenih rezultatov trdili o učinkovitosti kontrole. Opazovanje je že boljše, vendar moramo rezultate uporabljati previdno. Za razliko od tistih pri preiskovanju jih moramo analizirati z večjo mero skeptičnosti in mogoče tudi kombinirati s katero od drugih tehnik, ki so v tem primeru izvedene v omejenem obsegu.
Težavo v nekaterih primerih predstavlja tudi priznavanje kopij elektronskih dokumentov. Da se lahko zanesemo na podatke v elektronski obliki morajo biti izpolnjeni naslednji pogoji (Zveza ekonomistov Slovenije, Zveza računovodij, finančnikov in revizorjev Slovenije, 2000, s. 303):

- obvezna je klasifikacija dokumentov v njihovem življenjskem ciklu z vidika nastanka, hranjenja, pravice in načina dostopa pri pregledovanju, postopke preverjanja, dopolnjevanja in uničenja;
- zahtevana je vzpostavitev sledljivosti vseh aktivnosti z upoštevanjem zakonskih predpisov in standardov;
- potrebno je upoštevati zahteve po dokumentiranih postopkih za uporabnike sistemov upravljanja;
- kontrolno okolje mora vključevati mehanizme, ki zagotavljajo revizijske sledi, pravila obdelave dokumentov, tehnik kompresiranja in postopkov izbrisa ter
- zapisi, ki pomenijo revizijsko sled, morajo nastajati avtomatsko in biti dosegljivi za pregledovanja.

Pri samem testiranju se aplikacijske kontrole ločijo od ročnih predvsem po obsegu testiranja. Za večino od njih je dovolj, da testiramo eno samo, le v izjemnih primerih, ko so lahko parametri skozi čas precej različni, moramo upoštevati tudi ta dejavnik in ustrezno prilagoditi postopke. Običajno je potrebno testirati le ustrezne IT splošne kontrole in preveriti sistem, da deluje enako v vseh okoliščinah. Če ta dva pogoja nista izpolnjena se morajo opraviti bolj rigorozni postopki. Tako je potrebno pregledati programsko kodo ali preizkusiti vse logične načine uporabe. Pri visoko standardiziranih programskih paketih je dovolj, da preverimo vse nastavitve in se prepričamo, da jih ne more spreminjati vsakdo, ki ima znanje in tehnične zmožnosti, temveč obstajajo predpisi, kako to poteka, in se tudi dejansko upoštevajo. Pri

ročnih kontrolah, ki se zanašajo na računalniško pridobljene podatke, je potrebno oba dela preveriti ločeno. Takšen primer kontrole je, ko nek zaposleni izpiše iz informacijskega sistema dva seznama (oba sta rezultat programskih operacij) ter jih ročno primerja. Ročne kontrole se morajo testirati na večjem vzorcu, natančno število je rezultat več dejavnikov, tudi presoje preizkuševalca. Tudi pri aplikacijskih kontrolah se lahko odločimo za večje število testiranj, pomembnejši dejavniki pri odločitvi so: ali je kontrola sestavljena iz več podsistemov, ali lahko vplivajo na kontrolo zunanji dejavniki, kdo sodeluje pri izvajanju kontrole ter koliko trditev, ki se nanašajo na računovodske izkaze (assertions), kontrola pokriva. Če posplošim, glavna kriterija sta pomembnost kontrole in doseganje stopnje zagotovila o obvladanju tveganja.

Na primeru podjetja X si lahko nazorno ogledamo primerjavo med značilnostmi, predvsem pa razliko med testiranjem IT odvisnih notranjih kontrol in aplikacijskih kontrol. To je možno, ker so v podjetju uvedli elektronsko odobravanje prejetih faktur za nabavo storitev, medtem ko se računi za nabavljeno blago potrjujejo še na klasičen način. Slednje je dobro poznano in ga ni potrebno posebej predstavljati. Naj ponovim le osnovne korake v procesu, ki zajemajo prejem fakture, vpis v knjigo prejetih faktur, ročno preverjanje fakture in uskladitev z naročilnico, dobavnico in drugimi dokumenti, če je potrebno, pridobitev avtorizacije s strani pooblaščene osebe in nato knjiženje v saldakonte in glavno knjigo. Pri računih, ki se potrjujejo elektronsko je tok podoben, drugačen je način obravnavanja. Takoj ob prejemu računa se le-ta poskenira ter vnese v posebno aplikacijo, ki nadomešča vhodno fakturno knjigo. Nato se opravi vsebinska likvidacija, kar pomeni, da se pošlje k vodji določenega stroškovnega mesta, ki ga mora odobriti po prehodnem pregledu. Nadalje se račun pošlje v odobritev k vodji oddelka, v primeru, da je znesek na njem višji od 8000 EUR je zahtevana odobritev finančnega direktorja podjetja, nad zneskom 20.000 EUR pa tudi glavnega direktorja. Če se na katerikoli stopnji ugotovijo pomanjkljivosti ali napake, je račun možno vrniti prejšnjemu uporabniku. Po izvedbi vseh potrditev, se račun samodejno pošlje v računovodstvo, kjer se še enkrat pregleda, preverijo se vsi komentarji, ki so jih dopisali potrjevalci, ter pravila knjiženja, nato se status računa spremeni v zaprt, kar sproži tudi knjiženje. Elektronsko potrjevanje računov je omogočeno z uporabo treh glavnih aplikacij – programa za skeniranje, dokumentnega sistema in programa za podporo procesov. V slednjem so določeni vsi tokovi, ki usmerjajo potek procesa, ter hierarhična struktura, na kateri temelji potrjevanje računov. Tu je potrebno poudariti, da v primeru ročnega upravljanja računov in ročnega potrjevanja obstaja mnogo več možnosti za napake, hkrati pa je vzpostavitev notranjih kontrol predvsem pa nadzor nad njimi veliko težji. Z uvedbo elektronskega potrjevanja računov se je v podjetju optimiziral podproces v okviru nabave storitev, vpeljale so se dodatne kontrole, kot je na primer opozarjanje na zamude v potrjevanju, obenem se je olajšalo izvajanje preverjanj notranjih kontrol, kar skupaj pomeni bistvene izboljšave in prihranke.

Idealno bi bilo, da bi vse kontrole testirali konec poslovnega leta, kar bi nam ob predpostavki, da so enako delovale tudi prej, nudilo zagotovilo o učinkovitosti skozi celotno obdobje. Vendar je to nemogoče, saj nam omejitve virov ne omogočajo hkratnega testiranja, še posebno pa ne na koncu obdobja, ko je potrebno narediti še veliko drugih stvari. Naslednja

stvar, ki govori v prid testiranju še pred koncem poslovnega leta, so morebitne pomanjkljivosti kontrol, ki jih je potrebno odpraviti in tako izničiti njihov vpliv na pripravo letnega poročila, kar tudi terja svoj čas.
Pri izbiri časovnega termina testiranja je potrebno poiskati nekakšen kompromis, saj zgodaj preverjene kontrole ponujajo manjše zagotovilo o učinkovitem delovanju, kar zahteva še dodatne postopke proti koncu leta. To ne velja v tolikšni meri za aplikacijske kontrole in zato njihovo testiranje lahko izvedemo že v predreviziji. Seveda se moramo v glavni reviziji prepričati, da pri njih ni prihajalo do sprememb.
Velik del sprememb lahko nadzorujemo s preverjanjem IT splošnih kontrol. Slednje so usmerjene v spremljanje razvoja programske opreme, spremembe programske opreme, dostopanja do programov in podatkov ter izvajanje računalniških operacij. Pri razvoju programske opreme se je potrebno prepričati, da so spremembe predhodno potrjene s strani odgovorne osebe, preverjene, odobrene za sprejem v uporabo, pravilno nameščene in seveda, da je vse dokumentirano. Odobritev priprave spremembe in potem potrditve ustreznosti spremembe, ko je ta že izvedene, vendar še ne implementirana, mora priti z dveh strani, in sicer od odgovornega za poslovno in za tehnično področje. Testiranje mora biti opravljeno v testnem okolju, saj sicer lahko pride do nepredvidenega vpliva na podatke, postopek se lahko opravlja pri izvajalcu sprememb, če je ta zunanji, ali v samem podjetju, lahko tudi kot kombinacija obeh. Zunanji izvajalec za potrebe preverjanj ne sme pridobiti pravih podatkov, temveč le podobne, razen če to ni res nujno. V tem primeru se mora varstvo tajnosti podatkov urediti pogodbeno. Tu je še en vidik ravnanja s podatki, kajti pri vsaki spremembi se mora zagotoviti, da pri migraciji podatkov ne pride do njihovega spreminjanja. Ne smemo pa pozabiti na dokumentacijo, ki se deli na tehnično in uporabniško. Prva opisuje same spremembe in omogoča naročniku razumeti, kaj je sploh dobil, druga pa skrbi za to, da zaposleni lahko uporabljajo novosti v takšni meri, kot je bilo predvideno. S slednjim je povezano tudi izobraževanje uporabnikov. Podobno kot za razvoj programske opreme velja tudi za njihove spremembe. Razlika je v tem, da spremembe ne prinašajo bistveno novih funkcionalnosti, temveč le optimizirajo proces. Vendar so kljub temu potrebni postopki, ki zagotavljajo avtorizacijo sprememb, njihovo testiranje, dokumentiranje, izobraževanje in ustrezno ravnanje s podatki.
Če doslej povedano povežemo s podjetjem X, ugotovimo, da imajo formalno določene in ustrezno izvajane postopke spreminjanja programske opreme, ki so del varnostne politike in temeljijo v veliki meri na standardih ISO 17799 in Cobit. Podrobnosti za nabavno-prodajno aplikacijo so razvidne iz tabele 14, identificirane kontrole pa so tudi predmet testiranja z namenom ugotovitve učinkovitosti IT splošnih kontrol.

Tabela 14: Postopki in kontrole glede sprememb programske opreme

KORAKI SPREMINJANJA PROGRAMSKE OPREME IN KONTROLE V POSTOPKIH	IZVAJALEC KONTROLE
Zahtevo za spremembo pošljejo uporabniki vodji informatike.	Vodja informatike
Vodja informatike pregleda zahtevo in odloči o nadaljnjem poteku – lahko jo zavrne, če ni upravičena, drugače pa potrdi. V slednjem primeru obstajata dva različna scenarija: če je zares pomembna, sam vodi nadaljnje postopke, v nasprotnem primeru jo preda drugemu zaposlenemu (podrejenemu) v IT oddelku.	Vodja informatike
V primeru pomembnega vpliva spremembe na izvajanje nekega poslovnega procesa, je potrebno pridobiti soglasje skrbnika tega procesa. Soglasje pomeni tudi, da bo skrbnik sam spremljal potek spreminjanja programske opreme, da ne bo prihajalo do motenj in napak v procesu, poleg tega bo po potrebi izvajal svetovalno funkcijo.	Vodja področja
Vodja informatike oziroma njegov podrejeni v IT oddelku opiše zahtevo po spremembi v formalni obliki na predpisanem obrazcu in jo pošlje razvijalcu sistema. Vodja informatike mora biti obvezno seznanjen s tem postopkom.	Vodja informatike oziroma njegov podrejeni iz oddelka informatike
V podjetju razvijalcu informacijskega sistema podjetja X se zahteva zabeleži v njihov sistem v helpdesku, do katerega imajo dostop tudi zaposleni v podjetju X na podlagi individualnih gesel. Razvijalci preučijo zahtevo in nazaj sporočijo svoj odgovor, ki vsebuje potrebni čas, ceno in morebitne druge pomembne podatke.	Razvijalec programske opreme
Vodja informatike dokončno odloči o spremembi. Če ocena vrednosti spremembe programske opreme presega znesek 2000 EUR, je potrebno dobiti tudi soglasje finančnega direktorja v pisni obliki. Tudi naročilo za izvedbo spremembe je potrebno poslati razvijalcu v pisni obliki ali pa z elektronsko podpisano e-pošto.	Vodja informatike, finančni direktor
Po končanem razvoju, v katerega so po potrebi vključeni tudi zaposleni iz podjetja X, in testiranju pri razvijalcu se nova verzija ali dodatek namesti v testno okolje podjetja X , in sicer s strani razvijalca ali pa zaposlenih v IT oddelku podjetja X. Spremembo najprej testirajo delavci iz IT oddelka, nato pa še izbrani zaposleni podjetja X. Potek in obseg testiranja določi vodja informatike v sodelovanju z vodjem oddelka oziroma skrbnikom procesa, na katerega se sprememba nanaša. Testiranje in ugotovitve se dokumentirajo, na koncu se sestavi zapisnik, ki ga mora podpisati vodja testiranja, najpogosteje je to eden od ključnih zaposlenih na ustreznem področju ali pa sistemski administrator, če je to primerneje. Potrjen zapisnik je podlaga za prenos v produkcijsko okolje.	Vodja testiranja, ki ga predlaga vodja informatike
Prenos v produkcijsko okolje po predpisanem protokolu opravijo zaposleni v IT oddelku podjetja X, po potrebi tudi s pomočjo zunanjih svetovalcev.	Zaposleni v IT oddelku
Izvede se izobraževanje zaposlenih, prevzame se tehnična in uporabniška dokumentacija. Na začetku je novost še v delni testni uporabi, saj se rezultati dodatno preverjajo, večja pozornost se posveča napakam v sistemu, v kar sodi tudi počasnejše delovanje računalnikov in podobno. To traja najmanj tri dni do največ dveh tednov, potem se podpiše prevzemni zapisnik, kar je podlaga za plačilo računa.	Zaposleni v podjetju X, vodja informatike (podpis prevzemnega zapisnika)

Vir: Avtor

Določitev formalnih postopkov glede razvoja in popravkov aplikacij omogoča podjetju nadzor nad programskimi spremembami, tako da je v vsakem trenutku znamo, kakšne funkcionalnosti jim programska oprema nudi ter kako jih izkoristiti, obenem pa se lahko s precejšno verjetnostjo zanesejo, da ni bilo nepooblaščenih sprememb, ki bi omogočale zlorabe ali pa vplivale na napačno izvajanje operacij. V tabeli 13 so opisani postopki glede sprememb obstoječe programske opreme in razvoj manjših dodatnih funkcionalnosti. Korenite spremembe in razvoj povsem novih modulov se vodi kot projekt in je za ta namen osnovana posebna projektna skupina.

Na drugi strani je vedno pomembnejše varovanja dostopa do programov in podatkov. V podjetju mora biti sprejeta politika glede tega, ki celostno obravnava področje in je obvezna za vse zaposlene in tudi ostale, ki jih to zadeva. V njej morajo biti predpisani postopki za dodeljevanje uporabniških imen in gesel, njihovo onemogočenja in brisanje, upravljanje z gesli ter ostale stvari, ki se nanašajo na dostope, in sicer tako logične kot fizične. Za vsako področje morajo biti predpisani časovni roki, ki opredeljuje kdaj morajo biti postopki izvedeni in na koliko časa naj se izvajajo pregledi.

Dejanski primer postopkov si lahko ponovno ogledamo v povezavi s podjetjem X. Slednje premore formalne predpise v okviru varnostne politike, ki določajo izvajanje aktivnosti upravljanja z dostopi. Osnovni postopki za nabavno-prodajno aplikacijo so zbrani v tabeli 15.

Tabela 15: Postopki in kontrole dostopanja do nabavno-prodajne aplikacije v podjetju X

POSTOPKI UPRAVLJANJA Z DOSTOPI DO PROGRAMSKE OPREME IN Z NJIMI POVEZANE KONTROLE	IZVAJALEC KONTROLE
Vodja oddelka, v katerem se zaposli nov delavec ali se opravi premestitev delavca, izpolni in podpiše obrazec za dodelitev ustreznih pravic dostopa do programske opreme, ki jih zaposleni glede na delovno mesto in pripadajoče zadolžitve potrebuje.	Vodja oddelka
Obrazec se pošlje v IT oddelek, kjer ga najprej pregleda in potrdi vodja ter nato izroči sistemskemu administratorju. Slednji je zadolžen za upravljanje s pravicami dostopanja v sami aplikaciji.	Vodja informatike
V aplikaciji se določijo pravice dostopa na treh nivojih – najprej dostop do določenega modula (da/ne) in nato še na nivoju aplikacijskih oken. Sledi dodeljevanje nivoja pravic – branje, spreminjanje. Pravice je mogoče določiti z razvrščanjem uporabnikov v ustrezne skupine ali z individualno nastavitvijo.	Sistemski administrator
Začetno geslo nastavi sistemski administrator, ki ga sporoči uporabniku, vendar se mora spremeniti ob prvi prijavi v sistem. Geslo mora biti dolgo najmanj šest znakov, vsebovati mora najmanj eno številko in eno veliko črko ter ne sme biti podobno zadnjim šestim geslom. Vsakih 60 dni je zahtevana njegova sprememba.	Nastavitve aplikacije
Brisanje uporabniških imen poteka na podlagi razdolžnice, ki jo izda kadrovska služba in jo mora podpisati vodja informatike, s čimer jamči, da je bila vrnjena vsa IT oprema in je bilo uporabniško ime ukinjeno. Brisanje oziroma onemogočanje uporabniških imen vodja informatike delegira sistemskemu administratorju, ki izvedbo ustrezno označi na dogovorjenem obrazcu, ga podpiše in hrani skupaj z zahtevki za dodelitev dostopov do aplikacij.	Vodja informatike, sistemski administrator
Vodja informatike je zadolžen, da opravi četrtletne preglede upravičenosti zaposlenih do uporabniških pravic. Od kadrovske službe mora v ta namen pridobiti seznam zaposlenih s specifikacijami njihovih delovnih mest in zadolžitev. V primeru, da opazi neskladja z dodeljenimi pravicami glede programske opreme, na to opozori sistemskega administratorja, ki mora popraviti napake oziroma izvesti druge ustrezne naloge. Vsa ta opravila je potrebno dokumentirati.	Vodja informatike
Tedensko se pregledujejo log datoteke, in sicer s strani sistemskega administratorja, ki išče morebitne nepravilnosti oziroma indikatorje zlorab pravic. Mednje spadajo aktivnosti ob neobičajnih urah, nepojasnjeno povečanje aktivnosti nekega uporabnika na določenem področju – statistika dostopov in podobno.	Sistemski administrator

Vir: Avtor

V tabeli 15 niso omenjeni postopki glede upravljanja dostopov do operacijskega sistema, zbirk podatkov ter fizičnega dostopanja, če omenimo samo najbolj osnovne, ki prav tako bistveno vplivajo na varnost informacijskega sistema. V zvezi z njimi velja omeniti vsaj to, da so postopki v osnovi dokaj podobni tistim, ki veljajo za v tabeli 12 omenjeno aplikacijo, razen za fizične dostope, ki so dokaj specifični.

Na koncu ovrednotimo rezultate testiranj z namenom, da se prepričamo o izpolnjevanju zahtev, ki jih postavljajo trditve finančnih izkazov (assertions). Pri tem je potrebno imeti v mislih tveganje, ki ga določena trditev naslavlja in kontrola obvladuje. V procesu ovrednotenja rezultatov odločamo ali kontrola deluje ali ne. Obstajati sme le zanemarljiva možnost, da kontrola mogoče ne opravi zahtevanega dela, drugače je neučinkovita. Vsaka pomanjkljivost pri kontrolah mora biti raziskana in vzroki zanjo določeni ter tudi odpravljeni. Če to ni mogoče oziroma obstajajo kakršnekoli ovire, je potrebno začeti razmišljati o alternativnih kontrolah. Odpravljanja pomanjkljivosti se je potrebno lotiti sistematično, zato moramo pripraviti sistem, ki določa prioriteto in način odpravljanja pomanjkljivosti in to vključno s celotnim postopkom dokumentirati.

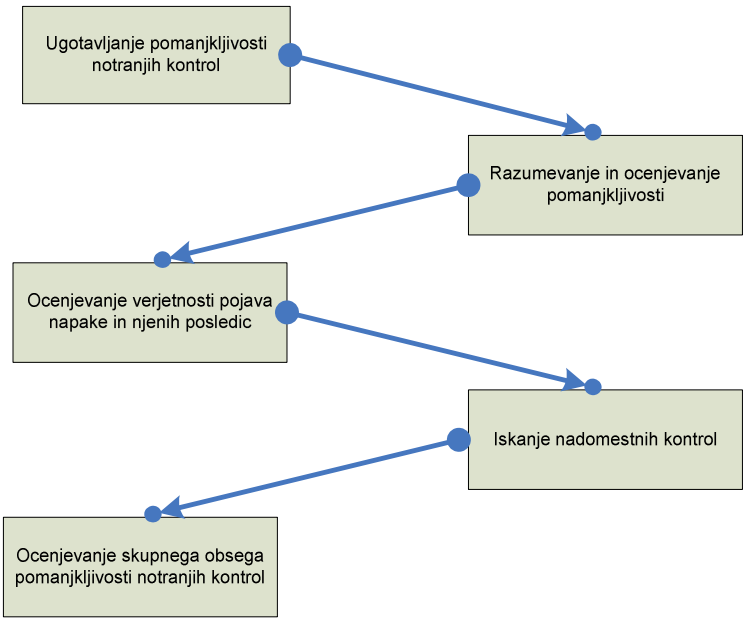
4.9. Analiziranje pomanjkljivosti notranjih kontrol in poročanje

Poslovodstvo podjetja mora biti seznanjeno s pomanjkljivostmi, vendar jih morajo osebe, ki so opravile testiranje IT notranjih kontrol, pred tem analizirati in ovrednotiti. Pomanjkljivosti lahko razdelimo v tri skupine (PCAOB - Auditing Standard No. 2, 2006):

- notranje pomanjkljivosti kontrol (kontrola kljub predvidenemu delovanju ne zazna pravočasno nepravilnosti, napaka se skriva v njenem ustroju),
- pomembne pomanjkljivosti (pomanjkljivost kontrole, ki se odraža v nepravilni pripravi računovodskih poročil, verjetnost, da nepravilnost ne bo odkrita ni zanemarljiva, vendar ne bo imela materialnega vpliva),
- materialne pomanjkljivosti (obstaja nezanemarljiva verjetnost, da kontrola ne bo sposobna odkriti oziroma preprečiti nepravilnosti, ki bo imela materialen vpliv na računovodske izkaze).

Priporočljivo je, da se pripravi postopek ravnanja ob odkritju pomanjkljivosti pri IT notranjih kontrolah in se tako zagotovi konsistentna obravnava. Vključeni morajo biti koraki, ki so prikazani na sliki 20.

Slika 20: Koraki, ki morajo biti izvedeni v okviru obravnavanja pomanjkljivosti IT notranjih kontrol



Vir: Avtor

Poročanje je v veliki meri odvisno od ugotovitev pri analiziranju pomanjkljivosti notranjih kontrol, saj vodstvo zanimajo slabosti, ki jih je potrebno odpraviti. Pri tem pa ne smemo pozabiti vključiti v zadostni meri ostale faze, ki sestavljajo proces vzpostavitve notranjih kontrol, saj le tako na celovit način predstavimo področje in vplive zainteresiranim stranem.
Tudi v primeru podjetja X je bila odkrita pomanjkljivost, in sicer v povezavi z IT splošnimi kontrolami dostopa – torej urejanja pravic dostopanja do programske opreme in pravic izvajanja opravil v določenih modulih. Glede na ažurni seznam delavcev, ki je bil pridobljen v kadrovskem oddelku, je bilo ugotovljeno, da v programu za podporo prodaji eden od delavcev, ki je prekinil delovno razmerje tri mesece pred pregledom, ni bil odstranjen iz seznama uporabnikov. Njegov račun je bil sicer onemogočen, vendar ne odstranjen. Glede na varnostno politiko bi moralo biti izbrisano v roku enega meseca. Poleg tega je bilo razvidno, da je administrator prejel obvestilo o prenehanju delovnega razmerja, saj je bilo to ustrezno označeno v dokumentaciji. Pojasnilo je bilo pridobljeno pri skrbniku aplikacije, ki je razložil, da iz razloga notranje omejitve aplikacije, in sicer zaradi ohranitve zgodovinskih podatkov, ki so potrebni za trenutno izvajanje aktivnosti, popolna odprava tega določenega uporabnika trenutno še ni mogoča. Zaradi ostalih sprejetih ukrepov tveganje zlorabe tega uporabniškega računa in posledično nepooblaščenega dostopa sicer ni bilo veliko, poleg tega se je že prej med spoznavanjem s procesi ugotovilo, da obstaja nadomestna kontrola, ki je bila tudi predmet tokohoda (walk-through) in kjer se je preverila njena zasnova in obstoj v preverjalnem obdobju. Nadomestna kontrola se je nanašala na beleženje aktivnosti uporabnikov v log datoteke, kar se je periodično preverjalo s strani skrbnika aplikacije. Ta je preverjal med drugim, da niso bile z uporabniškim imenom nekdanjega delavca zabeleženi poskusi prijave v sistem. Opravljanje pregleda log datotek je bilo tudi ustrezno

dokumentirano, kar je botrovalo ob ustreznem testiranju s strani revizorjev k pripoznavi IT splošnih notranjih kontrol za učinkovite.
Analiziranje pomanjkljivosti notranjih kontrol in poročanje se v veliki meri navezujeta na predhodne faze in pomenita zaključek cikla vzpostavitve notranjih kontrol. Hkrati predstavljata tudi začetek nekega novega procesa, slednje velja predvsem za poročanje, saj se s tem odpira splošna razprava o učinkovitosti in potrebnih izboljšavah notranjih kontrol v podjetju.

5. Pomen IT notranjih kontrol za poslovanje

V organizacijah se vse bolj zavedajo, da je celovit in dobro premišljen sistem za nadzor nad poslovanjem veliko bolj učinkovit, in dolgoročno gledano tudi cenejši, kot pa nekakšni ad-hoc razviti mehanizmi, ki ponujajo parcialne pristope. Slednji se prekrivajo, ne pa tudi dopolnjujejo, kar se odraža v nedoslednosti in ostalih težavah. Te se ne nanašajo le na slabo izvedbo nadzora in preprečevanja napak, temveč je vsaj tako pomembna tudi težava z dokumentiranjem ugotovitev. Na nasprotni strani dober notranji kontrolni sistem ne le da olajša izvedbo revizije finančnih izkazov ter pripravo poročil, temveč doda svoj prispevek na področju strategije podjetja. Na ta način lahko organizacija doseže cilj z manjšo porabo različnih virov in bistveno hitreje, kar je v današnjem času bistvenega pomena. Bolj natančno povedano, nadzorni mehanizmi prispevajo velik delež k zanesljivim in pravočasnim informacijam ter posledično učinkovitejšem odločanju. Poleg tega pa je v zvezi s tem potrebno omeniti tudi vpliv na notranjo komunikacijo, analizo poslovnih dogodkov in uspešno izvedbo transakcij. Vse to naj bi omogočal notranji kontrolni sistem, ki ustrezno združuje napotila, politike, prakse, postopke in mehanizme z naslednjimi cilji (Cangemi, Singleton: Managing the Audit Function, s. 3.1):

- zavarovati sredstva,
- zagotoviti natančnost in zanesljivost zajetih podatkov in pridobljenih informacij,
- prispevati k učinkovitosti poslovanja,
- zagotavljati usklajenost s predpisi podjetja,
- zagotavljati usklajenost z zakonodajo in
- zmanjšati pomen, če že ne preprečiti negativnih vplivov poneverb, prevar in ostalih nelegalnih dejanj.

Predvsem v večjih podjetjih, kjer nadzor nad procesi ni enostaven, lahko marsikaj pridobimo z vzpostavitvijo ustreznega sistema notranjih kontrol. Ostale koristi, ki imajo vpliv na poslovanje ter na nadzorstveno funkcijo, so med drugim še splošno zmanjšanje tveganja, kar se odraža v optimalnejšem poslovanju in manjšem obsegu potrebnih revizijskih postopkov. Na splošno lahko vse te koristi razdelimo v tri skupine: zanesljivost, natančnost poročanja, večja uspešnost, donosnost, še posebno pa učinkovitost organizacije in sledenje regulativi. Kontrole so uporabljene, da zmanjšajo negativne finančne posledice zaradi človeške napake, okvare sistema ali prevare. Poleg tega nudijo zagotovilo vodstvu, da so poročila stvarna slika dogajanja.

5.1. Koristi uspešnega obvladovanja IT notranjih kontrol

Na splošno je namen notranjih kontrol izpolnitev ciljev organizacije z upoštevanjem naslednjih vidikov (Romney, Steinbart, Cushing, 1997, s. 432):

- učinkovitosti in uspešnosti poslovanja,
- zanesljivosti finančnih izkazov ter
- skladnosti z zakonodajo in predpisi.

Velik del tega je povezano z revizijami, ki se opravljajo z namenom potrditi poštenost in pravilnost računovodskih izkazov in razkritij ter tako prispevati k učinkoviti alokaciji virov v družbi (Whittington, Pany, 2001, s. 6). Slednjo trditev lahko razčlenimo na potrjevanje pravilnosti izkazov, na zagotovilo, da se podjetje pri poslovanju ni posluževalo prevar in drugih nepravilnosti, da je vodstvo delovalo po pričakovanjih, da je podjetje delovalo družbeno odgovorno in da ni znamenj nenadne prekinitve delovanja. Del revizije se lahko opravi s preverjanjem notranjih kontrol, kar lahko bistveno olajša delo. Poleg tega so kontrole povezane s pravnim področjem in vplivajo na način izvajanja poslovnih funkcij. Z dopolnitvijo doslej povedanega lahko predpostavimo, da so bistvene prednosti, ki jih dosežemo z ustrezno uporabo notranjih kontrol, naslednje:

- zanesljivejše informacije,
- manjši obseg podrobnega preizkušanja podatkov pri reviziji,
- manjše tveganje kršenja zakonodaje,
- boljši nadzor nad poslovanjem ,
- izboljšanje poslovnih procesov,
- boljše varovanje sredstev podjetja,
- nižje splošno tveganja in
- večje zaupanje v podjetje.

5.1.1. Koristi pri poročanju

V okviru poročanja se združuje večina koristi IT notranjih kontrol. Mednarodni računovodski standard 1 določa, da morajo finančni izkazi pošteno prikazovati finančni položaj, poslovanje in denarni tok organizacije. To vključuje resnično sliko transakcij in dogodkov v skladu z določili in kriteriji posameznih standardov za prepoznavanja različnih poslovnih kategorij (MRS 1, 2006). Podobno zahtevajo tudi slovenski standardi, ki se vse bolj zgledujejo po mednarodnih. Da smo zares prepričani o pravilnosti izkazovanja posameznih kategorij, je potrebno vzpostaviti sistem notranjih kontrol na nivoju transakcij. Tako si zagotovimo obveščanje o odstopanjih od predvidenih oziroma želenih vrednosti.

Ena od skupin nepravilnosti, ki so ali pa bi lahko bile zaznane z učinkovitimi notranjimi kontrolami, se nanašajo na pripoznavanje prihodkov. Med njimi velja omeniti:

- zaračunavanje transakcij, ki se v resnici ne izvedejo;
- prikriti dogovori;
- pogojne prodaje, ko se pravice in dolžnosti ne prenesejo na drugo stranko;
- nepravilno obravnavane konsignacije;
- neavtorizirane izdaje blaga ali izvedbe storitev in

- pripoznavanje prihodkov v napačnem obdobju.

Vse te nepravilnosti je mogoče v večini primerov preprečiti ali odkriti s kontrolami, katerih koristi bistveno presegajo njihove stroške in na ta način izboljšati finančno poročanje. Tu si lahko izdatno pomagamo z IT notranjimi kontrolami, ki celovito obravnavajo poslovne transakcije, mednje lahko vključimo avtorizacije in beleženje prihodkov na podlagi povezanih dokumentov.

Koristi so predvsem posredne in težko izmerljive, med drugim lahko sem prištevamo tudi višje cene delnic na borzah. To lahko razložimo z dejstvom, da vlagatelji povezujejo kvalitetna in zanesljiva finančna poročila z nižjim informacijskim tveganjem, kar vpliva na višjo učinkovitost finančnih trgov in nadalje višjo ceno vrednostnih papirjev. Na naslednji stopnji pa to pomeni lažje in cenejše financiranje podjetij prek borznih kotacij, ki denar potrebujejo za nadaljnja vlaganja.

Če torej povzamem ugotovitve, nam IT notranje kontrole zagotavljajo zanesljive in poštene informacije ob pravem času. To je vedno bolj pomembno, saj so tolerance glede odstopanj vse manjše tako s strani zakonodajalcev kot investitorjev in širše javnosti. V skladu z višanjem zahtev glede poročanja, je vzpostavitev vedno bolj naprednih kontrol vse bolj ekonomsko upravičena. To je v prid kontrolam, ki temeljijo na informacijski tehnologiji, saj je njihova vpeljava pogosto dokaj zahtevna in tudi draga, ki pa se povrne na daljši rok.

5.1.2. Koristi pri reviziji

Učinkovite IT notranje kontrole lahko revizorjem prihranijo veliko dela, saj omogočajo zmanjšanje obsega podrobnega preizkušanja podatkov. Slednje je največkrat rutinsko opravilo, ki zahteva kar nekaj ponovitev in posledično tudi precej časa. Temu se je mogoče izogniti, če najdemo kontrolo, ki zagotavlja, da je bil nek postopek izpeljan pravilno in zagotavlja rezultat enak pričakovanemu. Če se revizor lahko zanese nanjo, mu ni potrebno izbirati vzorca in na njem opraviti preizkuse. Takšen primer je lahko preračun zneskov iz tujih valut. Danes je že zelo redko, da najdemo podjetje, kjer to delajo ročno. Še ne tako dolgo časa nazaj pa so zaposleni preračunavali zneske na računih, ki so jih izstavili poslovni partnerji v tujini, v domačo valuto na podlagi tečajev iz časopisov. Preveritev se je morala opraviti na zadosti velikem vzorcu dokumentov, v primeru, da je bila ugotovljena napaka, se je moral vzorec razširiti. Napaka je bila lahko le minimalna in osamljen primer, vendar je bilo kljub temu potrebno opraviti dodatno delo. Delo je precej olajšano, če se preveri le ustrezna aplikacijska kontrola.

Obstajajo pa tudi primeri, ko je odločitev za uporabo IT notranjih kontrol skoraj nujna. Za razliko od ročnih običajno IT kontrole zagotavljajo višjo stopnjo gotovosti in jih danes že v veliki meri zato tudi nadomeščajo. Razlog je tudi v tem, da informacijski sistemi vse bolj celovito pokrivajo poslovanje in je zato tudi smiselno, da se v večji meri uporabljajo kontrole vezane na informacijsko tehnologijo. V določenih primerih pa morajo IT notranje kontrole nadomestiti podrobno preizkušanje podatkov, saj to zahteva obseg knjiženih transakcij. To je nujno pri večjih podjetjih, ki zagotavljajo storitve velikemu številu strank. Na ta način izstavijo večje število približno enakovrednih računov in tudi pri majhnem tveganju, ko izberemo minimalni vzorec, je potrebno preveriti veliko število dokumentov. Taka izvedba

revizije je praktično nemogoča, saj so viri preveč omejeni, da bi jih lahko uporabljali na tako potraten način. V tem primeru si neupoštevanje IT notranjih kontrol ne moremo več predstavljati, konkreten primer so elektrodistribucijska podjetja in ponudniki telekomunikacijskih storitev.

5.1.3. Usklajenost z zakoni in predpisi

Skladnost z zakoni in predpisi, ki jo zagotavljajo IT notranje kontrole, lahko opazujemo z dveh vidikov. Prvi je zakonski okvir, ki neposredno zahteva vzpostavitev takšnih kontrol - primer je Sarbanes-Oxleyev zakon. To lahko razumemo kot pomoč, ki nam ga nudijo kontrole v prilagajanju poslovanja zakonodaji in ostalim predpisom. Za primer si poglejmo slovenski Zakon o varstvu osebnih podatkov (ZVOP) in sicer določili iz 3. in 4. člena (Zakon o varstvu osebnih podatkov, 2006) splošnih določb (I. del).

3. Člen
Osebni podatki se lahko obdelujejo le, če je obdelava osebnih podatkov določena z zakonom ali, če ima upravljavec zbirke osebnih podatkov pisno privolitev posameznika.
4. člen
Obdelava osebnih podatkov, ki se nanašajo na rasno in drugo poreklo, politična, verska in druga prepričanja, pripadnost sindikatu, spolno vedenje, kazenske obsodbe in zdravstveni podatki, mora biti posebej označena in zavarovana.

Njuno bistvo je, da prvi določa nujnost pisne privolitve posameznika o obdelavi njegovih osebnih podatkov, drugi pa posebno ravnanje z občutljivimi osebnimi podatki. Ker je takšnih podatkov običajno veliko, so IT notranje kontrole (aplikacijske) zelo primerne za uporabo v tem primeru. Z njimi si lahko pomagamo, da ne kršimo zakona ZVOP, in sicer z vzpostavitvijo mehanizmov, ki onemogočajo njihovo zlorabo. Na ta način se lahko izognemo morebitnim težavam, ki spremljajo nepravilno ravnanje s podatki, med katere spadajo sankcije s strani zakonodajalca oziroma organov, ki imajo nalogo odkrivati in kaznovati nepravilnosti s tega področja, ter tudi morebitnim tožbam, ki se lahko končajo z resnimi finančnimi posledicami.
Danes je zakonodaja zelo obsežen in zapleten inštrument, s katerim se regulira delovanje posameznikov in organizacij. Njihovo razumevanje je marsikdaj naporno tudi za strokovnjake, zato je potrebno razbremeniti zaposlene, kar je moč doseči s sistemom notranjih kontrol, ki je prilagojen zakonodaji in predpisi ter skrbi za izvajanje poslovnih procesov v skladu z njimi.
Kar se tiče vrednostne primerjave stroškov in koristi lahko samo preletimo kazni, ki so zagrožene za kršenje določenih zakonov. Izbrani (delni) podatki so zbrani v tabeli 16.

Tabela 16: Zagrožene kazni za kršenje izbranih zakonov

Zakon	Kazen (izbrani podatki)
Zakon o varstvu osebnih podatkov (ZVOP-1)	Od 1.000.000 SIT do 3.000.000 SIT
Zakon o prevzemih (ZPre-1)	Od 1.000.000 SIT do 10.000.000 SIT
Zakon o spremembah in dopolnitvah Zakona o zaposlovanju in zavarovanju za primer brezposelnosti (ZZZPB-F)	Od 300.000 SIT do 15.000.000 SIT
Zakon o gospodarskih družbah (ZGD-1)	Od 20.000 EUR do 62.000 EUR
Zakon o davčnem postopku (ZDavP-1)	Od 400.000 SIT do 6.000.000 SIT
Zakona o spremembah in dopolnitvah Zakona o trgu vrednostnih papirjev (ZTVP-1B)	Od 3.000.000 SIT do 10.000.000 SIT

Vir: Uradni list RS, 2006

Poleg denarnih kazni, ki so za kršitelje zakonov v nekaterih primerih res visoke, je potrebno upoštevati tudi morebitne druge negativne posledice neskladnosti s predpisi, kot je na primer izguba ugleda in posledično manj poslov. Čeprav so kazni, ki jih predpisuje Sarbanes-Oxleyev zakon, veliko večje, so tudi slovenske zagrožene v takšni višini, da upravičujejo vlaganja v sistem notranjih kontrol.

5.1.4. Boljši nadzor nad poslovanjem

Vodstvo lahko uporabi informacije, ki jih nudijo IT notranje kontrole, kot pomoč pri odločanju. Učinkovite kontrole nudijo aktualne informacije, ki so še kako dobrodošle pri upravljanju podjetja. Seveda je potrebno, da se kontrole že vnaprej predvidijo za to funkcijo in po potrebi tudi prilagodijo. Na ta način se poveča verjetnost, da bodo doseženi cilji podjetja, saj so kontrole osnovane v skladu z njim in nudijo informacijo, ali poslovanje poteka po načrtih. Kontrole so vzpostavljene na različnih nivojih in spremljajo transakcije z več vidikov, zato lahko nudijo podroben vpogled v trenutno poslovanje.

Med notranje kontrole se v širšem pomenu uvrščajo tudi ključni kazalniki poslovanja, ki kažejo napredek v smislu približevanja zastavljenim ciljem. Te kontrole so sicer višjenivojske in so manj natančne, zato se v osnovnem pomenu kontrol uporabljajo manj. Težava je v tem, da so manj občutljive in zato obstaja manjša verjetnost, da bodo zaznale nepravilnosti. Kljub temu so koristne pri pridobivanju informacij o poslovanju in nudijo vodstvu v marsikaterem primeru podlago za pomembno odločitev glede nadaljnjih korakov v poslovnem svetu.

Analiza stroškov in koristi notranjih kontrol v povezavi z nadzorom nad poslovanjem in posledično vplivom na odločitve poslovodstva je v veliki meri stvar subjektivne presoje in zato navedbe različnih raziskav niso primerne v tem kontekstu. Tako je denimo težko določiti, koliko je na uspeh podjetja vplivala informacija kot rezultat kontrolnih mehanizmov, in koliko vpliva so imeli drugi dejavniki, nenazadnje tudi splošno stanje v gospodarstvu. Velja pa, da imajo nezanesljive in prepozne informacije velik vpliv na neuspešnost podjetja, kar potrjujejo v svojih razpravah mikroekonomski strokovnjaki (Ooghe, De Prijcker, 2006, s. 6). Raziskave so bile opravljene na propadlih podjetjih, ki so prepozno spoznala pomen notranjih kontrol v povezavi z zagotavljanjem informacij kot podlago strateškim odločitvam, kar je lahko resno opozorilo organizacijam, ki zanemarjajo to področje.

5.1.5. Izboljšanje poslovnih procesov

Poslovni procesi so odraz poslovnega modela in strategije, ki sta izbrana s strani podjetja, zato je njihovo optimalno izvajanje še toliko bolj pomembno. Optimalnost je z najmanj napora mogoče meriti prek odzivnih časov na spremembe v okolju in kakovosti poslovanja.

V povezavi z notranjimi kontrolami pri izboljšanju poslovnih procesov ne gre za njihovo popolno prenovo, temveč večinoma samo za prilagajanje načina dela. Pri vzpostavljanju notranjih kontrol in njihovem spremljanju odkrivamo, kje v poslovnih procesih so šibke točke, ter jih odpravimo. Do pred kratkim je bila zelo aktualna informatizacija poslovanja, ki največkrat tudi pomeni prehod z ročnih na IT notranje kontrole, a hkrati ne konec možnosti za izboljševanje poslovnih procesov. Pri analizi kontrolnega sistema se pokažejo točke, kjer je mogoče postoriti še marsikaj. Pri kontrolah, kjer se pojavljajo težave z zagotavljanjem njihove učinkovitosti s kateregakoli vidika, je potrebno premisliti, če ni to indic za slabosti v samem procesu in s tem potreba po ukrepanju.

Izboljšanje poslovnih procesov prek IT notranjih kontrol je usmerjeno predvsem v racionalnejšo izrabo virov. Ti so omejeni, IT notranje kontrole pa lahko preprečujejo njihovo usmerjanje v porabo, ki ni povezana z zagotavljanjem koristi v okviru poslovanja podjetja. Na takšen način je poskrbljeno za jasno skrbništvo nad njimi in v povezavi s tem preverjanje njihove razpoložljivosti in izrabe.

5.1.6. Varovanje sredstev podjetja

Pri varovanju sredstev je pomembno dodeljevanje odgovornosti, saj tako dosežemo, da so sredstva povezana z osebami, ki zanje tudi odgovarjajo. Še bolj pomembno pa je, da je nadzor nad sredstvi konstanten in v takšni obliki, da omogoča odkrivanje zlonamernih manipulacij na eni strani in morebitnih negativnih vplivov okolja na sredstva na drugi strani. V zvezi s tem je potrebno omeniti IT splošne kontrole, v katere spada omejevanje dostopa do informacijske tehnologije ter podatkov, ki predstavljajo vse pomembnejši element vsakega podjetja.

Zelo informativna je raziskava, ki jo je izvedla revizijska hiša KPMG leta 2000 in nato ponovila leta 2005, in se nanaša na analizo prevar in nepravilnosti v zvezi s kupci, dobavitelji, delničarji in širšo skupnostjo. Pri tem je bilo ugotovljeno, da je v podjetjih z izdelanim etičnim sistemom in dorečenim konceptom skladnosti s predpisi, bistveno manj nepravilnosti, zaposleni so veliko bolj motivirani glede zaznavanja in opozarjanja nanje, poleg tega imajo zaposleni veliko večje zaupanje v vodstvo (KPMG, 2006, s. 4). Opazne so tudi razlike med letoma 2000 in 2005. Tako se je delež zaposlenih, ki je verjel, da se notranja pravila ne upoštevajo v praksi, zmanjšal s 73 na 52 odstotkov, na splošno pa rezultati kažejo večje zaupanje v delovanje notranjih kontrol in poštenost vodstva.

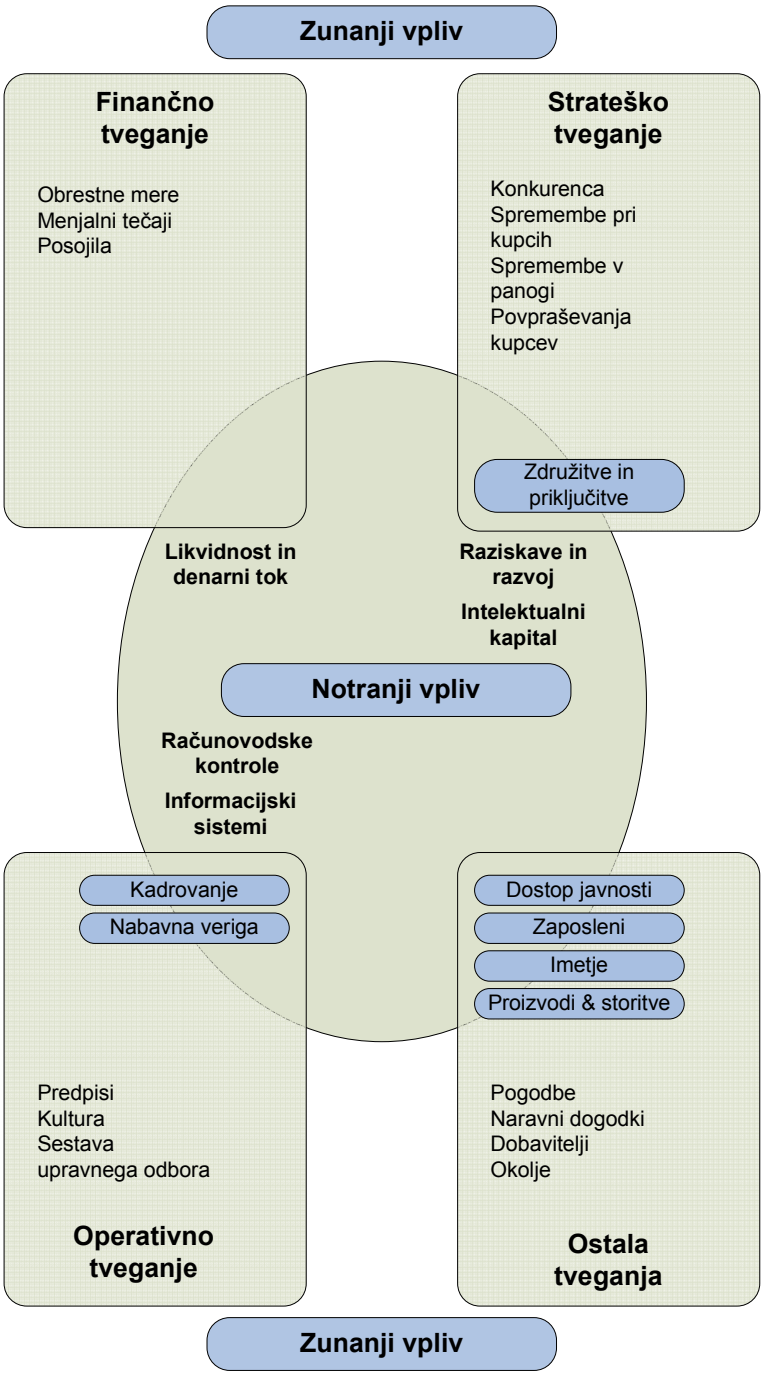
V slovenskem prostoru je zavedanje o notranjih kontrolah ponekod še vedno na zelo nizki ravni oziroma, kar je še bolj zaskrbljujoče, neprilagojeno na sodobno poslovanje. V dobi, ko povsod prevladuje informacijska tehnologija, nekateri še vedno izvajajo kontrole bolj primerne papirnemu poslovanju. Slednje sicer ne velja v tolikšni meri za banke, ki nadpovprečno veliko sredstev namenjajo temu področju, vendar se kljub temu dogajajo primeri, kot je SKB banka, kjer si je uslužbenka v treh letih prisvojila 89 milijonov SIT. Vsota je precejšna, zato velja razmisliti o ureditvi notranjih kontrol vključno z IT tehnologijo.

Slednja je bila v zadnjem času predmet precejšnih vlaganj, zato velja proučiti, če IT notranje kontrole niso mogoče zapostavljene.
Tudi v slovenskih podjetjih se občasno odkrivajo tako imenovane »teeming and lading« goljufije, ko si zaposleni prisvajajo denar delodajalca. To izvedejo tako, da denar, ki naj bi ga prejel določen dobavitelj, nakažejo na svoj račun, pozneje pa obveznosti poravnajo z denarjem, ki je namenjen drugemu dobavitelji, in to ponavljajo dokler se jih ne odkrije. V večini primerov se to početje lahko prepreči na dokaj preprost način, in sicer ustrezno razmejitvijo dolžnosti, kar je najpogosteje posledica ustrezno urejenih IT splošnih kontrol. Slednje je dokaz, da imajo relativno majhni vložki v sistem notranjih kontrol lahko relativno velike pozitivne posledice.

5.1.7. Nižje tveganje

Kot je razvidno s slike 21, za podjetje predstavljajo grožnjo štiri glavne skupine tveganj – finančna, strateška, operativna in ostala tveganja; vsa so sestavljena iz notranje in zunanje komponente.

Slika 21: Tveganja, katerim je izpostavljeno podjetje



Vir: The Institute of Risk Management. 2002, s. 3

Nekatera od teh tveganj obvladujemo težje kot druga, vendar si lahko z notranjimi kontrolami pripravimo sistem, ki nas pravočasno opozarja na nepredvidene dogodke in se tako izognemo v redkih primerih tudi usodnim posledicam.
Nižje tveganje lahko razumemo kot končno stopnjo, ki nam jo zagotavljajo učinkovite IT notranje kontrole, saj se koristi kažejo v prvi vrsti v razbremenjenih zaposlenih, ki se lahko posvečajo opravilom z višjim donosom, skratka delo lahko porazdelimo bolj učinkovito. Tudi preostale vire lahko usmerimo v učinkovitejše koriščenje, saj ni potrebno, da jih hranimo v tolikšni meri za morebitne nepredvidene dogodke oziroma za ukvarjanje s tveganji, ki

vključuje napore v zvezi z nadzorom nad njimi, njihovo preprečevanje, prenos tveganj in financiranjem posledic (zavarovanje in podobno) in na splošno blaženje morebitnih negativnih vplivov. Vse to vpliva na samo strategijo, ki jo je izbralo podjetje za doseganje zastavljenih ciljev, vključno s finančno komponento. Seveda pa moramo upoštevati ceno kontrol, ki so povezane s posameznimi tveganji, da ne presežejo pričakovanih posledic potencialne uresničitve tveganj.

5.1.8. Večje zaupanje v podjetje

Pomen zaupanja se je v zadnjem času poudarjal predvsem v ZDA, in sicer zaradi računovodskih škandalov v podjetjih, ki so visoko kotirala na organiziranih kapitalskih trgih, kar se tiče priljubljenosti pri vlagateljih. Kljub temu je tema enako pomembna tudi v drugih državah, na primer v Nemčiji, kjer se podjetja financirajo predvsem s finančnimi posojili in ne preko borze vrednostnih papirjev. Podjetje ima z ustreznim sistemom notranjih kontrol precejšne koristi. Ti se kažejo v cenejšem pridobivanju finančnih virov in lažjem sklepanju poslov, pri čemer niso izjeme javni razpisi.

Seveda pa ni dovolj samo, da vzpostavi učinkovit sistem IT notranjih kontrol – o tem mora ustrezno obvestiti vlagatelje, pa naj bodo to posamezniki ali institucije, ter ostale deležnike, ki pri svoji odločitvi, komu bodo zaupali denar ali sklenili z njim posel, vse bolj upoštevajo ta vidik poslovanja. V ZDA, kjer so stvari urejene institucionalno, je primerjava med podjetji s tega vidika lažja, vendar ureditve, ki to omogočajo, stopajo vse bolj v ospredje tudi v drugih delih sveta. Propad Enrona je povzročil zmanjšanje borzne kapitalizacije za okoli 70 milijard USD (Rezaee, 2002, s. 2), in sicer na škodo investitorjev, zaposlenih, predvsem pa je bilo to boleče za upokojence, ki so vanj vlagali po pokojninskem načrtu. Če prištejemo še WorldCom, Qwest, Tyco in Global Crossing, se izguba povzpne prek 460 milijard USD. Tolikšna vsota pa je zadostni razlog, da se posveti več pozornosti in sredstev notranjim kontrolam, kar dokazuje tudi raziskava, ki jo je izvedla organizacija Financial Executives International (FEI). V okviru slednje so ugotovili na vzorcu 217-ih podjetij, da naj bi v povprečju podjetje z več kot 5 milijardami USD letnih prihodkov prilagoditev Sekciji 404 Sarbanes-Oxleyevega zakona stala 4,36 milijona USD, kar ni nezanemarljivo, vendar naj bi se vsota vsako leto bistveno zmanjšala, velik delež pa prispevajo k takšni številki tudi svetovalci, ki pogosto nerealno predstavljajo potrebne ukrepe. Višji stroški vzpostavitve notranjih kontrol bistveno bolj prizadenejo manjša podjetja, pri katerih je potreben temeljitejši razmislek o načinu izboljšanja kontrolnega okolja. Tu je še poseben poudarek potreben pri odločitvi med ročnimi in IT kontrolami, saj slednje na dolgi rok prinašajo še dodatne prihranke.

Trenutno obstaja več kritikov prilagoditve na strožjo zakonodajo, kot pa njenih zagovornikov. Pri tem prvi opozarjajo na oceno SEC-a, ki je predpostavil, da naj bi stroški prilagoditve znašali 91.000 USD na podjetje, kar pa se je pomnožilo na končno številko tudi več milijonov USD. Kljub takšnemu porastu se morajo podjetja zavedati, da učinkovit sistem notranjih kontrol ni le stvar zakonodajalca in zaščite investitorjev ter ostalih vključenih oseb, temveč prispeva tudi k uspehu podjetja. Če podjetja kljub vsemu ne prepoznajo prednosti naprednih notranjih kontrol ali pa je to zaradi določenih razlogov zanje nepomembno, imajo večinoma možnost umika z ameriških borz, kar so nekatera tuja podjetja že storila. Če torej neposredno

primerjamo stroške in koristi, ki jih prinašajo učinkovite notranje kontrole, v ameriškem primeru skladne s Sarbanes-Oxleyevem zakonom, je mogoče na prvi pogled res očitna prevlada potrebnih sredstev. Ob tem je potrebno pomisliti, da nam koristi pritekajo v daljšem časovnem roku ter na dejstvo, da je stroške lažje ovrednotiti kot pa koristi, ki so pogosto izpuščene iz študij, kar pa tehtnico nagne v drugo stran.
Splošno stopnjo zaupanja je skoraj nemogoče zanesljivo izmeriti. Najbolj objektivne in dosegljive kazalnike nudi Indeks zaupanja investitorjev (StateStreet, 2006), ki se izračunava glede na delež bolj tveganih naložb v celotnem portfelju in se meri na pomembnejših svetovnih borzah (ZDA, Evropa ter Azija-Pacifik), ter primerjava gibanja borznih indeksov. Indeks zaupanja investitorjev kaže, da je bilo lokalno dno doseženo konec leta 2002, kar nekako sovpada z največjimi računovodskimi škandali. V letu 2003 se je stanje bistveno izboljšalo, nato pa je zaupanje spet padlo, kar pa lahko pripišemo drugim vzrokom, predvsem divji rasti cene nafte. Pri analizi gibanja vrednosti borznih indeksov, kot posrednih kazalnikov zaupanja investitorjev, si lahko pomagamo z MSCI US Equity, ki je zaradi svoje sestave med najbolj reprezentativnimi predstavniki ameriškega trga kapitala. Indeks je dosegel dno v začetku leta 2003, k čemur so vsekakor prispevali različni dejavniki, vključno z računovodskimi škandali. Če primerjamo podatke iz obeh virov, lahko ugotovimo, da podpirajo tezo o pozitivnem vplivu učinkovitih notranjih kontrol na večje zaupanje investitorjev. Iz povedanega lahko ponovno sklepamo na upravičenost vlaganja v kontrolne mehanizme.

6. Sklep

Nesporno je dejstvo, da notranje kontrole vedno bolj pridobivajo na pomenu, pa naj bo to zaradi poslovne nuje ali pa zahtev regulatorjev. V zadnjem času so k hitremu razvoju pripomogli računovodski škandali, ki so vzpodbudili k prenovi ureditve področja notranjih kontrol in zaostritvi predpisov, ter tehnološki napredek okolja, v katerem poslujejo podjetja. Za slednja pa ni dovolj, da samo spremljajo stanje in se prilagajajo zakonskim zahtevam, temveč morajo aktivno načrtovati in izvajati nadzorne funkcije, če hočejo izkoristiti vse pridobitve, ki jih notranje kontrole ponujajo. To danes pomeni predvsem angažiranost v zvezi z informacijskim sistemom, saj je slednji ključni dejavnik pri poslovanju vsakega sodobnega podjetja.
V zvezi z notranjimi kontrolami se pogosto omenja zakonodaja in ostali predpisi, pri čemer v ospredje stopata Sarbanes-Oxleyev zakon v ZDA in Osma direktiva v Evropski skupnosti. Prvi ima kar nekaj let prednosti, pa tudi različni interesi raznih skupin so imeli pri njegovem snovanju manjši vpliv, tako da je natančnejši, predvsem pa že v polni uporabi. Glede na to, da je bil sprejet leta 2002, je že preteklo zadosti časa, da so se izoblikovala ustrezno argumentirana mnenja o njegovi uporabnosti. Veliko strokovnjakov meni, da uporaba ni ekonomsko upravičena ter da bi prilagoditev, predvsem pa omilitev zahtev zakona imela pozitiven vpliv, kar pa pogosto dokazujejo z nepopolnimi in pristranskimi analizami. Dejstvo je, da samo izvajanje zakona, ker je pač to zahtevano s strani oblasti, ne prinaša veliko koristi, še posebno je to očitno v primerjavi s stroški, ki ga spremljajo. Potrebno se je zavedati, da večino zlorab zakrivi poslovodstvo ali drugi ključni zaposleni, ki imajo znanje, kako zaobiti

notranje kontrole. Posledično je potrebno kontrole smiselno zasnovati v skladu s specifikami posameznega podjetja, uvesti zadostno ločevanje dolžnosti in odgovornosti ter vključiti neodvisne osebe kot so člani revizijskega odbora in revizorji, da je delovanje kontrol učinkovito in obseg koristi nad stroški očiten.

Danes je zelo težko najti podjetje, ki za podporo svojih pomembnih poslovnih procesov ne uporablja informacijske tehnologije. Sčasoma se bo digitalizirala tudi večina dokumentacije, kar bo pomenilo, da se bo korenito zmanjšal delež povsem ročnih kontrol. Že v tem trenutku je v povprečnem slovenskem podjetju zavezanem reviziji njihov delež manjši od polovice in še opazno pada vsako leto. Tako bo vedno večja odgovornost za uspešno in učinkovito poslovanje padla na IT notranje kontrole, čemur so bo potrebno prilagoditi oziroma bolje povedano, se je že bilo potrebno prilagoditi. Kdor šele sedaj razmišlja o notranjih kontrolah temelječih na informacijski tehnologiji, je že zamudil nekaj let, ki jih bo težko nadoknaditi. Nobeno presenečenje ni, da so takšna, neprilagojena, podjetja praviloma manj uspešna in z večjim številom zlorab, od katerih se jih dosti odkrije z velikim časovnim zamikom in še to večinoma po naključju, hkrati pa so najglasnejša pri kritiziranju novih predpisov, ki zahtevajo ureditev stanja na tem področju. Zato je brez odlašanja potrebno zasnovati in uvesti IT notranje kontrole, ki bodo zagotavljale ustrezen nadzor nad poslovanjem, uspešno poročanje ter skladnost z zakonodajo in predpisi.

Kot je bilo ugotovljeno v tem delu, so skupne koristi notranjih kontrol ob pravilni zasnovi in uporabi večje od potrebnih stroškov za njihovo uvedbo in vzdrževanje. V prid temu govorijo prihranki pri zagotavljanju točnih in pravočasnih informacij, lažjem pregledu poslovanja, bolj optimalnem izvajanju poslovnih procesov, uspešnejšem varovanju sredstev, poleg tega so prednosti opazne tudi na drugih poslovnih področjih, skratka njihova uporaba prispeva k učinkovitejšemu upravljanju s tveganji, ki se odraža v lažjem doseganju zastavljenih ciljev. Hkrati so IT kontrole v večini primerov boljše od ročnih, kar napeljuje k sklepu, da so IT notranje kontrole v današnjem času nepogrešljiv dejavnik uspešnega poslovanja. Čeprav so ročne in IT notranje kontrole običajno substituti, je z vidika večje zanesljivosti na eni ter nižjih stroškov na dolgi rok na drugi strani priporočljivo nadomestiti ročne v čim večji meri s takšnimi, ki temeljijo na informacijski tehnologiji. Tako se lahko izognemo marsikateri napaki, ki izvira iz človeškega dejavnika, obenem pa je tudi tveganje zaradi prevar manjše. K temu lahko dodamo še prednost hitrejšega izvajanja, lažjega nadzora in komplementarnost s sodobnimi načini izvajanja poslovnih funkcij, kar še dodatno prevesi tehtnico pri izbiri na stran IT notranjih kontrol.

V prihodnje se na podlagi dosedanjega razvoja predvideva velik porast pomena IT notranjih kontrol. Trenutno imajo vodilne celovite rešitve že dodane posebne module, ki so namenjeni temu področju, takšen primer je AIS pri SAP-u, kmalu pa se pričakuje razširitev uporabe posebnih programov, ki bodo beležili in tudi analizirali vse transakcije. S tem se bo odprlo novo poglavje za IT notranje kontrole, saj bodo postale neločljiv element vsakega poslovnega okolja.

7. Literatura

1. Arens, Alvin A.: Auditing : An Integrated approach. Upper Saddle River (New Jersey): Prentice Hall, cop. 2000. 828 str.
2. Brand, Koen; Boonen, Harry: IT Governance: A Pocket Guide Based on COBIT. Zaltbommel: Van Haren Publishing, 2005. 151 str.
3. Cangemi, Michael P., Singleton Tommie: Managing the Audit Function: A Corporate Audit Department Procedures Guide. New York: Wiley, 2003. 384 str.
4. Carmichael, Douglas R.: Auditing Concepts and Methods: A Guide to Current Theory and Practice. New York : McGraw-Hill, 1996. 656 str. New York : McGraw-Hill, 1996. 672 str.
5. Carpenter, Scott: The IT Director's Practical Guide to Sarbanes-Oxley Compliance. Portsmouth: Ecora, 2004. 17 str.
6. Chambers et al.: Internal Auditing. London: Pitman, 1987. 481 str.
7. Champlain, Jack J.: Auditing Information Systems, 2nd Edition. New Jersey: Willey Publishing, Inc., 2003. 451 str.
8. Chorafas, Dimitris N.: Implementing and auditing the internal control system. Basingstoke, New York : Palgrave, 2001. 365 str.
9. COBIT: Governance, Control and Audit for Information and Related Technology. Rolling Meadows (Ill.): Information Systems Audit and Control Foundation, 1998. 354 str.
10. COBIT: COBIT Mapping – Overview of International IT Guidance. Rolling Meadows (Ill.): Information Systems Audit and Control Foundation, 2004. 56 str.
11. COBIT: Control Objectives 3rd Edition. Rolling Meadows (Ill.): Information Systems Audit and Control Foundation, 2000. 148 str.
12. COSO: Enterprise Risk Management – Integrated Framework. New York: Committee of Sponsoring Organizations of the Treadway Commission, 2004. 7 str.
13. Fight, Andrew: Measurement & Internal Audit. New York: John Wiley & Sons, 2001. 106 str.
14. Global accounting & control : A Managerial emphasis. New York, Chichester: J. Wiley, Cop., 2001. 224 str.
15. Guldentops, Erik, Lainhart, John H., Hardy, Gary: Information Security Governance – Guidance for boards of Directors and Executive Management. Rolling Meadows: IT Governance Institute, 2002. 28 str.
16. Guy, Dan M.: Auditing. Fort Worth : The Dryden Press, 1996. 889 str.
17. Heschl, Jimmy: Cobit mapping. Rolling Meadows: IT Governance Institute, 2004. 56 str.
18. Howard, Leslie R.: Auditing. London: Pitman, 1992. 340 str.
19. IFAC (International Federation of Accountants): Handbook of International, Auditing, Assurance, and Ethics Pronouncements. Nwe York: IFAC, 2006. 1095 str.

20. ITGI: IT Control Objectives for Sarbanes-Oxley. Rolling Meadows: IT Governance Institute, 2004. 86 str.
21. ITSMF: An Introductory Overview of ITIL. London: ITSMF, 2004. 39 str.
22. Karol, T.J.: A guide to cross-border privacy impact. NewYork: Delloite&Touche, 2004. 28 str.
23. Kinsella, Ray Et Al: Internal Controls in Banking. New York : John Wiley & Sons, 1995. 140 str.
24. Kiger, J. E.: Auditing. 2nd edition. New York: Houghton Mifflin, 1997. 918 str.
25. Koletnik, Franc: Raziskovanje in dosežki v reviziji. Maribor : Ekonomsko-poslovna fakulteta, 1996. 132 str.
26. KPMG: Integrity Survey 2005-2006. New York: KPMG, 2006. 32 str.
27. KPMG: Sarbanes-Oxley Section 404 – An Overview of the PCAOB's Requirements. Toronto: KPMG, 2004. 48 str.
28. Kramer, J. B.: The CISA prep guide. Indianapolis: Willey Publishing, Inc., 2003. 591 str.
29. Levy, B. Howard: Audit Documentation: It’s a Whole New World. New York: The CPA Journal, June 2005. Str. 30.
30. Meigs, Robert F.: Accounting: The Basis for business decisions. New York : McGraw-Hill, 1996. 1096 str.
31. Musaji, Yusufali F.: Auditing and Security: AS/400, NT, Unix, Networks and Disaster Recovery Plans. New York: Willey Publishing, Inc., 2001. 553 str.
32. Ooghe, Hubert; De Prijcker, Sofie: Failure processes and causes of company bankruptcy: a typology. Gent: Universiteit Gent, 2006. 49 str.
33. Oud, Ernst Jan: The Value to IT of Using International Standards. New York: Informations Systems Control Journal, Volume 3, leto 2005. Str. 27-31.
34. PriceWaterhouseCoopers: Sarbanes-Oxley Act 404 – Practical Guidance for Management. Delaware: PwC, 2004. 146 str.
35. Rezaee, Zabihollah: Causes, consequences, and deterence of financial statement fraud. Memphis: Academic Press, 2002. 22 str.
36. Romney, Marshall B., Steibart, P. J., Cushing, B. E.: Accounting information systems. Upper Saddle River (N.Y.) : Prentice Hall, 2000. 796 str.
37. Samec, Nataša: Sarbanes-Oxley Act - nova pravila Corporate Governance v ZDA. Ljubljana: Pravna praksa, št. 36/37, leto 2003. Str. 14-17.
38. Škedelj, Miran: Uporaba sodobnih telekomunikacijskih storitev v poslovanju Veledrogerije. Magistrsko delo. Ljubljana: Ekonomska fakulteta, 1999. 97 str.
39. The Institute of Risk Management: A Risk Management Standard. London: AIRMIC, 2002. 20 str.
40. Turley, James S.: Get ready for the EU's 8th Directive. Directorship. Atlanta, June, 2004. 21 str.
41. Turk, Ivan: Standardi notranjega revidiranja. Ljubljana : Zveza računovodij, finančnikov in revizorjev Slovenije, 2003.

42. Walton, Peter: International Accounting. London : International Thomson Business Press, 1998. 458 str.
43. Wilkinson, Joseph W., Cerullo, Michael J.: Accounting Information Systems : Essential Concepts and Applications. New York : John Wiley & Sons, 1997. 984 str.
44. Weirich, Thomas R, Reinstein, Alan.: Accounting & Auditing Research: A Practical Guide. Cincinnati (Ohio) : South-Western Publ., 1992. 182 str.
45. Whittington, Ray, Pany, Kurt: Principles of auditing and other assurance services. Boston : Irwin/McGraw-Hill, cop. 2001. 816 str.
46. Zveza ekonomistov Slovenije, Zveza računovodij, finančnikov in revizorjev Slovenije: Simpozij o sodobnih metodah v računovodstvu, financah in reviziji. Ljubljana: Zveza ekonomistov Slovenije: Zveza računovodij, finančnikov in revizorjev Slovenije, 2000. 475 str.

8. Viri

1. About ISO 27000 Series. [http://www.iso27001security.com/html/iso27000.html], 9.8.2006.
2. AICPA - Proposed Statement on Auditing Standards - Audit Risk and Materiality in Conducting An Audit. [http://www.aicpa.org/download/auditstd/2005_06_Risk_Assessment/05-ED_SAS_Audit_Risk_Conduct_Audit.pdf], 10.3.2006.
3. AICPA: Summary of Sarbanes-Oxley Act of 2002. [http://www.aicpa.org/info/sarbanes_oxley_summary.htm], 8.4.2005.
4. AICPA: SysTrust Q&A. [http://www.aicpa.org/assurance/systrust/press/faq.htm], 21.1.2006.
5. Applying COSO's – ERM, [http://www.coso.org/publications/erm/coso_erm.ppt], 8.8.2006
6. Computerworld – The new buzzwords: Information Lifecycle Management. [http://www.computerworld.com/hardwaretopics/storage/story/0,10801,79885,00.html], 9.7.2006.
7. COSO – Enterprise Risk Management – Integrated Framework. [http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf], 10.6.2006.
8. COSO – Internal Control Issues in Derivatives Usage. [http://www.coso.org/publications/executive_summary_derivatives_usage.htm], 11.3.2006.
9. COSO Definition of Control. [http://www.coso.org/key.htm], 22.8.2006.
10. EY Glossary: Auditing terms, 2005.
11. Energija, časopis skupine HSE. Ljubljana: HSE, december 2004. 24 str.
12. Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. [http://www.sec.gov/rules/final/33-8238.htm], 10.8.2006.

13. Hewlett-Packard Development Company: HP ITSM and HP OpenView: an approach to attaining Sarbanes-Oxley compliance. Palo Alto, 2004. 8 str.
14. Interno gradivo Ernst&Young.
15. Investor Confidence Index Summary. [http://www.statestreet.com/industry_insights/investor_confidence_index/summary.pdf], 22.12.2006.
16. Internal Market and Financial Services. [http://ec.europa.eu/internal_market/finances/actionplan/index_en.htm#actionplan], 1.7.2006.
17. ISO/IEC 17799:2005, [http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=], 26.12.2006.
18. ISACA: IS Standards, Guidelines and Procedures for Auditing and Control Professionals. ISACA, 2004, 190 str.
19. Kratka predstavitev ciljev in rezultatov projekta e-Slog. [http://www.gzs.si/ASPDatoteka.asp?ID=10206], 9.7.2006.
20. Logan, Debra: Get Ready For European 'Sarbanes-Oxley' Audit Rules. Stamford: Gartner Group, 2004.
21. MRS 1. [http://www.iasb.org/uploaded_files/documents/8_63_ias01-sum.pdf], 11.11.2006.
22. OSL informator – ISO 27001- nova pomembna številka v informacijski varnosti, [http://www.gambit.si/izm/2005/izm140705/izm140705_clanki.htm, 9.8.2006], 9.8.2006.
23. PCAOB - Auditing Standard No. 2. [http://www.pcaob.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.2.aspx], 11.6.2006.
24. SAP: SAP Auditing Manual R/3. Walldorf: SAP, 2004. 168 str.
25. SAS 70, [http://www.sas70.com/about.htm], 8.4.2005.
26. Slovenski računovodski standardi 2006. [http://www.si-revizija.si/racunovodje/SRS_2006.php], 11.3.2006.
27. SysTrust Assurance, [http://www.sas70.com/systrust.html], 22.1.2006.
28. Tarrani, Mike: Understand IT's role with the Sarbanes-Oxley Act. [http://www.amazon.com/exec/obidos/tg/guides/guide-display/-/2JIB11X44X36K/ref=cm_aya_av.sylt_sylt/103-8542523-4795845], 5. april 2005.
29. The Business Forum Online: The Significance of the Sarbanes-Oxley Act. [http://www.businessforum.com/SEC01.html], 18.2.2006.
30. TheStreet.com: Cracking the Books II: Reliving Equity Funding, [http://www.thestreet.com/stocks/brokerages/791614.html], 8.4.2005
31. Turk, Ivan: Pojmovnik računovodstva, financ in revizije. Ljubljana : Zveza računovodij, finančnikov in revizorjev Slovenije, 2002. 1082 str.
32. Uradni list RS, [http://www.uradni-list.si], 29.12.2006.

33. Verzion: IT controls, [http://www22.verizon.com/it/products-services/Case%20studies/Stream%204/Bearing%20Point.ppt], 9.7.2006.
34. Wyman, Peter: How do Europe's 8th Directive and Sarbanes-Oxley Compare? [http://www.gtnews.com/article/5847.cfm?cfid=4859373&cftoken=68386067&pass1=1%25.%5CO%3A%24%3CL14%26%2B'MBDWE3K4Z%3C%20%0A], 8.4.2005.
35. Zakon o davku na dodano vrednost. [http://zakonodaja.gov.si/rpsi/r05/predpis_ZAKO1345.html], 9.7.2006.
36. Zakon o elektronskem poslovanju in elektronskem podpisu.[http://www2.gov.si/zak/Zak_vel.nsf/4c1d8c547755fffac1256616002dd5e1/c12563a400338836c12568fd00505349?OpenDocument], 19.12.2006.
37. Zakon o varstvu osebnih podatkov. [http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.html], 9.7.2006.
38. Zakon Sarbanes-Oxley Act. [financialservices.house.gov/media/pdf/hr3763ah.pdf], 18.2.2006

9. Slovarček slovenskih prevodov tujih izrazov

American Institute of Certified Public Accountants (AICPA) – Ameriški inštitut preizkušenih računovodij
Application controls – Aplikacijske kontrole
Audit committee – Revizijski odbor
Automated controls – Samodejne kontrole
Business Continuity Plan – Načrt neprekinjenega delovanja
Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Odbor izbranih organizacij za področje poslovne etike, finančnega poročanja in notranjih kontrol
Computer operations – Računalniške operacije
Canadian Institute of Chartered Accountants (CICA) – Kanadski inštitut pooblaščenih računovodij
Concurent Version System – Sistem za upravljanje z verzijami
Configurable controls – Nastavljive kontrole
Consolidated financial statements – Uskupinjeni finančni izkazi
Control design – Zasnova kontrol
Control objective – Nadzorni cilj
Control Objectives for Information and related Technology (COBIT) – Nadzorni cilji za informacijsko in sorodne tehnologije
Disaster Recovery Plan – Načrt okrevanja po nepredvidenih dogodkih
Disclosure committee – Odbor za razkritja
Executive steering commitee – Izvršni usmerjevalni odbor
Financial Statements – Finančni izkazi
Financial Statements Assertions – Trditve
IT dependant manual controls – IT odvisne ročne kontrole
IT general controls – IT splošne kontrole
IT operations controls – Kontrole IT poslovanja
Key performance indicators – Pomembni kazalniki poslovanja
Operational risk – Operativno tveganje
Port – Vrata
Problem management – Upravljanje z napakami
Public Company Accounting Oversight Board (PCAOB) – Odbor za javno nadzorstvo delniških družb
Sarbanes-Oxley Act (SOX) – Sarbanes Oxleyev zakon
Scheduling – Časovno razporejanje
Statements on Auditing Standards (SAS) – Uredbe revizijskih standardov
Triple match – Trojno ujemanje
What could go wrong – Možne nepravilnosti