UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

REVIDIRANJE BAZ PODATKOV

Ljubljana, avgust 2006 TOMAŽ VALJAVEC

IZJAVA:
Študent Tomaž Valjavec izjavljam, da sem avtor tega diplomskega dela,ki sem ga napisal pod mentorstvom dr. Aleša Groznika in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, 01.08.2006 Podpis: Tomaž Valjavec

KAZALO

Uvod

Razvoj tehnologije je povzročil spremembe v načinu poslovanja. Podjetja si izmenjujejo podatke v elektronski obliki, kar jim omogoča bistveno hitrejši prenos podatkov in hkrati zniževanje stroškov. Globalna konkurenca sili podjetja v optimizacijo stroškov, kar podjetja dosegajo s pravilno načrtovano implementacijo informacijskega sistema. Na trgu se pojavljajo sistemi, ki omogočajo povezanost organizacijskih enot pri izmenjavi informacij. Te se hranijo na enotnem mestu, v centralni bazi podatkov in tako predstavljajo pomemben del informacijskega sistema vsakega podjetja. Največji igralci na trgu, ki ponujajo celovite programske rešitve – sisteme ERP, so SAP, ORACLE, BAAN, Navision in drugi.

Informacijski sistem mora biti zasnovan tako, da omogoča pravilen tok izmenjave informacij in vgradnjo omejitev, ki preprečujejo zlorabe in prevare. Organizacija se mora zato ustrezno zaščititi z vzpostavitvijo notranjih kontrol, ki odkrivajo, preprečujejo ali popravljajo napake. V preteklosti so revizorji finančnih izkazov v okviru letne revizije finančnih izkazov podjetja v vseh večjih podjetjih opravili tudi revizijo delovanja notranjih kontrol, ki je, če je bil pregledovani poslovni proces podprt z informacijskim sistemom, vključevala tudi revizijsko preizkušanje podatkov informacijskega sistema. Ker pa se večji del poslovanja odvija s pretokom informacij znotraj informacijskega sistema, se je pojavila potreba po podrobnejšem pregledu kontrol, ki se nanašajo na sistem in ga izvajajo revizorji informacijskih sistemov.

Revizor informacijskih sistemov mora pregledati področja sistema z vidika zagotavljanja varnosti podatkov v fazi priprave, vnosa, obdelave in priprave izhodnih podatkov. Informacijski sistemi hranijo podatke v podatkovni bazi, zato mora biti ta ustrezno zavarovana. Ali izbrana baza izpolnjuje pričakovanja podjetja, ali podpira dolgoročne potrebe in usmeritve podjetja, ali omogoča podjetju hitro in učinkovito prilagajanje novim razmeram na tržišču, ali so zagotovljene potrebna varnost in zaščita podatkov, njihova dostopnost in integriteta, ali so razpoložljivi resursi izkoriščeni optimalno, ali je poskrbljeno za nadaljnje poslovanje podjetja, so le nekatera vprašanja, na katera si vodstvo prizadeva dobiti odgovor.

Revizija informacijskega sistema je ena od možnosti za pridobitev neodvisnega mnenja v sklopu odgovorov na nekatera zastavljena vprašanja. V večini primerov pokaže na ključne pomanjkljivosti in slabosti ter s primeri dobre prakse predlaga njihovo odpravo.

Namen in cilj diplomskega dela

Namen dela je predstavitev področja dela revizorja informacijskih sistemov s poudarkom na reviziji podatkovne baze, ki zajema pregled nastavitev baze ter priporočila za njeno optimalno in varno delovanje.

Ker se profesionalno ukvarjam z revizijo informacijskih sistemov v podjetju Deloitte & Touche, sem se odločil za obravnavo tovrstne tematike, z namenom pridobitve novih znanj s področja revizije baz podatkov. Moj doprinos k diplomskemu delu je predstavitev teoretičnih načel revidiranja, ki sem jih strukturiral v logično zaporedje faz, predpisanih s strani zakonodaje in standardov. Dodana vrednost naloge je predstavitev metodologije podjetja in pridobljeno praktično znanje z dosedanjih projektov revidiranja informacijskih sistemov, ki so mi bili v pomoč pri izbiri in obravnavi praktičnega primera.

Vse večja informacijska podpora poslovanju povzroča večje potrebe po reviziji informacijskih sistemov, zato se ta stroka v zadnjih letih sooča s trendom naraščanja števila poslov, kar je drugi razlog za izbor teme diplomskega dela Revizija baz podatkov.

Zasnova in struktura

Diplomsko delo je sestavljeno iz petih poglavij, ki so tematsko organizirana tako, da pristopijo iz splošnih opredelitev do natančnih podatkov in konkretnih primerov.

Delo v prvem poglavju opredeljuje pojem revidiranja in področje dela revizorja. Revizija informacijskih sistemov nastopa kot podpora reviziji računovodskih izkazov, ki je nujna za določen del organizacij, ali pa kot samostojen pregled informacijskega sistema, kar opisujem v drugem poglavju. Pregled je odvisen od zahtev stranke, ki želi preveriti pravilnosti delovanja sistema in zanesljivost kontrol, ki zagotavljajo varnost. Stranka se lahko odloči za splošen pregled sistema ali pa svoje zahteve opredeli zelo podrobno, usmerjeno le na dele informacijskega sistema. V to področje spadajo tudi revizijske naloge revizije baz podatkov, ki jih opredeljuje tretje poglavje diplomskega dela.

V tretjem poglavju so predstavljena področja, na katera mora biti revizor informacijskih sistemov, ki pregleduje bazo, še posebno pozoren. Varnost baze opredeljujejo področja logične in fizične zaščite podatkov, ki so podrobneje opredeljena v omenjenem poglavju.

Prva tri poglavja predstavljajo teoretične osnove, ki jih mora revizor obvladovati pri izvajanju svojega dela, četrto pa dva največja igralca, ki ponujata rešitve sistemov baz podatkov. Gre za primerjavo produktov podjetij Oracle (baza Oracle) ter IBM (baza DB2). Področja, predstavljena v nalogi, se nanašajo predvsem na varnost omenjenih produktov ter prednosti in slabosti, na katere mora biti kupec pozoren, ko se odloča za nakup.

Zadnje vsebinsko poglavje podrobno prikazuje področja in postopke revizijskega pregleda baze Oracle. Konkreten primer prikazuje nastavitve baze, ki so primarno vgrajene v sistem in imajo velik vpliv na celotno varnost baze v primeru nepravilne nastavitve vrednosti parametrov baze. Drugi del poglavja pa predstavlja pregled varnostnih nastavitev dejanskih uporabnikov baze.

1 Opredelitev revidiranja

Pojem revidiranje marsikdo zamenjuje ali enači s pojmom revizija. Slednjo lahko opredelimo kot neodvisno preiskovanje računovodskih izkazov ali z njimi povezanih računovodskih informacij pravne osebe ne glede na to, ali je usmerjena v ustvarjanje dobička ali ne, in ne glede na njeno velikost ali pravno obliko, če je cilj takšnega preiskovanja podati sodbo o njih (Mednarodni revizijski standardi, 1994, str. 19).

Revizija je rezultat dejavnosti revidiranja oziroma posamezni posel revidiranja za določenega naročnika z določenim namenom, medtem ko je revidiranje proces, opredeljen kot pretežno popravljalno, na izvedenskem mnenju zasnovano poznejše nadziranje poslovnih procesov in stanj (Turk et al., 1994, str. 3).

Revidiranje je ena izmed vrst nadziranja, zato bom najprej opredelil področja nadziranja. Nadziranje je presojanje pravilnosti in odpravljanje nepravilnosti. Je področje nalog, ki presojajo pravilnosti načrtovanja, pripravljanje izvajanja in izvajanja s stališča tistih, ki odločajo pa tudi odpravljajo pri tem ugotovljene nepravilnosti. Je tudi informacijsko področje nalog, ki zagotavlja pravilnosti podatkov in informacij (Turk, 2004, str. 778).

V okviru izvajalnega sestava je nadziranje sestavina vsake temeljne poslovne funkcije. Razlikovati je treba 3 zvrsti nadziranja: kontroliranje, inšpeciranje in revidiranje:

- »Kontroliranje je pretežno preprečevalno, na strokovnem ugotavljanju dejstev zasnovano vzporedno nadziranje; z njim se ukvarjajo v nadzirano poslovanje organizacijsko vključeni in po načelu stalnosti delujoči organi« (Slovenski računovodski standardi, 2001).
- »Inšpiciranje opravljajo organi, ki niso vključeni v organizacijo in ne delujejo po načelu stalnosti, ter zajema predvsem popravljalno, na strokovnem ugotavljanju dejstev zasnovano poznejše nadziranje poslovnih procesov in stanj« (Turk et al., 1994, str. 27).
- »Revidiranje je pretežno popravljalno, na izvedenskem mnenju zasnovano poznejše nadziranje. Z njim se ukvarjajo organi, ki niso organizacijsko vključeni v nadzirano poslovanje in v njem ne delujejo po načelu stalnosti« (Slovenski računovodski standardi, 2001).

1.1 Odgovornost revizorja

O svojih opažanjih in mnenjih morajo revizorji poročati lastnikom pa tudi drugim uporabnikom računovodskih izkazov; od slednjih so najpomembnejši udeleženci kapitalskih trgov oziroma javnost. Revizor je torej oseba, ki na podlagi svojega poglobljenega znanja pregleda (revidira) računovodske izkaze in izrazi mnenje (potrdilo zagotovilo), ali so (da so) računovodske informacije pravična in poštena slika (resničen in pošten prikaz) v skladu s splošno sprejetimi načeli računovodstva. Čeprav absolutnega

zagotovila pri revidiranju ni mogoče dati, zaradi vrste dejavnikov, kot so na primer potreba po presoji, uporaba preizkusov, omejitve, značilne za notranje kontroliranje, in to, da ima večina dokazov, ki so na voljo revizorju, bolj prepričevalno kot dokončno naravo, pa je revizorjevo mnenje izjemno pomembno tako za zunanje uporabnike računovodskih izkazov kot tudi za lastnika. Zaupajo namreč revizorjevi strokovnosti in neodvisnosti. Njegova odgovornost je izjemno velika; neupoštevanje revizorjevega mnenja, njegovo spreminjanje ali pa drugačno interpretiranje je nepremišljeno dejanje; pooblastilo za to pa ni dano nikomur (Odar, 1997, str. 355).

Pri pojmu revizije v večini primerov najprej pomislimo na pregled finančnega poslovanja in podajo mnenja revizorja, ki se največkrat navezuje na ustreznost izkazanih finančnih oziroma poslovnih izkazov podjetja. V senci revizije finančnega poslovanja se je pojavila revizija informacijskih sistemov. V začetku je finančnim revizorjem dajala le oceno, v kolikšni meri lahko zaupajo podatkom v informacijskih sistemih, kmalu pa si je utrla tudi svojo pot, povezano s spoznanji, da uspešna podjetja potrebujejo uspešne in učinkovite informacijske sisteme, da informacijska tehnologija zahteva posebna znanja in da se izjemno hitro spreminja (Javornik, 2003, str. 1).

2 Revizija informacijskih sistemov

Revizijo informacijskih sistemov lahko opredelimo kot proces, sestavljen iz načrtovanja, izvedbe pregleda, poročanja o ugotovitvah in spremljanja korekcijskih ukrepanj (Potočnik, Tajnik, 2003, str. 107).

Revizija informacijskih sistemov se je začela razvijati že leta 1970. Takrat so strokovnjaki v ZDA spoznali, da ni dovolj, da se pregleda vhodne podatke informacijskega sistema ter izhodne podatke in informacije informacijskega sistema, pač pa je treba pregledati tudi operacije obdelave in hrambe podatkov v informacijskem sistemu (Vrešnik Čemas, 2002, str. 8–9).

Revidiranje informacijskih sistemov je interdisciplinarno opravilo, potrebno je poznavanje poslovanja revidiranja, informacijske tehnologije, organiziranosti servisov, tehnik revidiranja, standardov uporabe informacijske tehnologije in splošnih standardov informacijske tehnologije (Vrešnik Čemas, 2002, str. 8–9).

Revizija računalniško podprtih sistemov pridobiva v postopku kontroliranja poslovnih procesov vse večji pomen. Revizor mora poleg običajnih strokovnih znanj z vsebinskega področja revizije razpolagati z dodatnimi znanji s področja informacijske tehnologije in uporabe računalniških rešitev. Kontrole informacijskih sistemov se začnejo že pri proizvajalcih računalniške opreme (vgrajene kontrole), nadaljujejo pa pri uporabniku s kontrolo instalacije operacijske in preostale programske opreme. Podatki v bazah podatkov

naj bi bili zaščiteni in zavarovani tako pred uporabo nepooblaščenih oseb kot tudi glede napak in okvar v sistemu. Z aplikacijskimi kontrolami revizor preverja, ali se izhodni podatki ujemajo z vhodnimi, ter ugotavlja, kje je prišlo do morebitnih razhajanj. V fazi vhoda preverja predvsem popolnost in točnost vnosa podatkov, v fazi obdelave natančnost obdelovanja podatkov, v fazi izhoda pa točnost rezultatov obdelave (Perše, 200, str. 142–145).

Ne glede na to, za katero vrsto revidiranja gre in kateri organi revizijo izvajajo, je revidiranje v sodobnem času povezano z revidiranjem informacijskega sestava oziroma računalniškega obdelovanja podatkov. Revidiranje računalniške obdelave podatkov (Data Processing Auditing) je revidiranje učinkovitosti kontrol in njihovega izvajanja pri računalniški obdelavi podatkov; obsega razvijanje in izvajanje posamezne uporabnosti računalniške rešitve ter revidiranje računalniškega središča. Njegovi cilji so oceniti zanesljivost računalniške obdelave podatkov in predvideti možne nevarnosti v prihodnosti pa tudi presoditi izvajanje obstoječih kontrol ter potrebe po uvajanju novih in opuščanju obstoječih vrst kontrol; včasih ima isti pomen kot revidiranje informacijskega sestava (Turk, 2000, str. 645).

Cilji revidiranja IS so (Potočnik, 2001, str. 160):

- zagotoviti ekonomično razporejanje informacijskih virov, strojne opreme, periferne opreme, programske opreme in človeških virov v smislu doseganja poslovnih ciljev;
- pridobiti zadostna zagotovila, da je IT ustrezno varovana;
- pridobiti zagotovila, da so informacije na voljo pravočasno, da so točne in zanesljive;
- pridobiti razumna zagotovila, da so vse napake in nepravilnosti preprečene, odkrite, popravljene in se bo o njih poročalo;
- smotrna uporaba revizijskih virov.

2.1 Varnost informacijskega sistema

Varnost informacijskega sistema opredeljujejo tri komponente (Javornik, 2005, str. 51):

- zaupnost – zagotavljanje, da je informacija na razpolago le tistim, ki so pooblaščeni, da jo pridobijo – interne kontrole, ki podpirajo zaupnost:
    - ukrepi fizičnega varstva informacijske tehnologije,
    - klasifikacija podatkov in informacij glede na stopnjo zaupnosti in čas, za katerega določena stopnja zaupnosti velja,
    - ureditev logičnih pristopnih pravic v povezavi s potrebami dela,
    - individualna pooblastila,
    - beleženje pristopanja z ID – uporabnika in časovno znamko do podatkov in kontroliranje zapisov beleženja,
    - kodeksi poklicne etike ter
    - izvajanje vnaprej predvidenih sankcij za kršitve;

- celovitost/integriteta – varovanje točnosti in popolnosti informacij in postopkov procesiranja – interne kontrole, ki zagotavljajo celovitost:
    - zaščito podatkov in programov pred neavtoriziranimi spremembami, kot denimo vsi kontrolni postopki metodologij razvoja računalniških rešitev v življenjskem ciklu oz. metodologij za uvajanje sprememb,
    - kontrolirani postopki prenašanja programov iz razvojnih v testna oziroma produkcijska okolja, testiranja rešitev,
    - izdelani postopki procesiranja obdelav z vnaprej predvidenimi postopki obnovitev v primeru kakršnekoli prekinitve kot posledice skrite napake oziroma nedelovanja posamezne komponente informacijske tehnologije,
    - definiranje nezdružljivih dejavnosti in poročil o vnaprej definiranih izjemah, katerih prejemniki so posebno za to pooblaščene osebe,
    - dodelitev pristopnih pravic do podatkov in programov v skladu s potrebami dela s posebno skrbnostjo pri dodeljevanju visokih pooblastil ter
    - vgrajene aplikacijske kontrole logične pravilnosti podatkov;
- razpoložljivost – zagotavljanje informacij pooblaščenim uporabnikom v časih in na način, kot jih potrebujejo – interne kontrole, ki preprečujejo nerazpoložljivost:
    - zagotavljanje potrebnih kritičnih virov,
    - »help–desk« funkcija in
    - pogodbe za vzdrževanje, ki zagotavljajo odpravo okvar v predvidenih časih s strani lastnih delavcev ali izvajalcev.

2.2 Pristop k procesu revidiranja

Omejenost virov narekuje potrebo po identifikaciji in razumevanju tveganj, ki jim je opazovana organizacija izpostavljena. Vodje ali lastniki organizacije se morajo namreč biti sposobni odločiti, katerim tveganjem bodo posvetili vire organizacije, v kakšni obliki in obsegu. Kar je primerno za eno podjetje, je lahko popolnoma zgrešeno za drugo. Tako pridemo do potrebe izvedbe formalne analize tveganj, ki je praktično vedno specifična in odvisna od niza parametrov, ki opredeljujejo podjetje in okolje, v katerem to deluje. Formalna ocena tveganj je lahko del sodobnih poslovnih procesov, in ne samo enkraten dogodek za potrebe ugotovitve trenutnega stanja.

Analiza tveganj mora pripeljati do ocene posamičnega tveganja tako s strani vplivov tveganja na doseganje ciljev kot tudi s strani verjetnosti, da se tveganje uresniči. Splošno je smiselno posvetiti največ energije upravljanju tveganj, kjer je verjetnost, da se tveganje uresniči, visoko, hkrati pa je tudi vpliv tega tveganja zelo velik. Treba je poiskati najbolj izražena tveganja. Če analiza tveganj ni bila opravljena, bo revizor informacijskih sistemov v prvi fazi revizije skupaj z naročnikom določil revizijske cilje in pozneje pri izvedbi opredelil tveganja. Če so tako ugotovljena tveganja visoka, potem bo revizor na osnovi strokovne skrbnosti in izkušenj naročniku predlagal podrobnejši pregled (Potočnik, Tajnik, 2003, str. 106–109).

2.3 Tveganja in notranje kontrole

Vsako poslovanje je povezano s tveganji. Ta predstavljajo negotovost nastanka dogodka, ki lahko vpliva na doseganje zastavljenih ciljev. V skladu z naraščajočimi tveganji naraščata tudi obseg in raznolikost kontrol. Z vzpostavitvijo notranjih kontrol je tveganja mogoče zmanjševati ali celo preprečiti.

Pri poslovanju obstaja vedno določena stopnja tveganja (Inherent Risk), na katero ne moremo vplivati. To tveganje se zmanjšuje z vgrajevanjem kontrol. Obstoječe tveganje, zmanjšano z vgrajenimi kontrolami, predstavlja preostalo tveganje (Residual Risk) (Derek, 2002, str. 4).

Proces ravnanja s tveganji sestavljajo naslednji koraki (Derek, 2003, str. 2–4):

- Opredelitev sredstev organizacije ali groženj; opredelitev sredstev organizacije od pomembnejših do najmanj pomembnih glede na vrednost sredstev in vpliva na poslovanje. Glede na ranljivost sredstev se ovrednotijo grožnje, oceni verjetnost za nastanek in opredeli posledice morebitnih groženj.
- Opredelitev in ocena ustreznih notranjih kontrol, ki preprečujejo nastanek tveganj ali zmanjšujejo tveganja na sprejemljivo raven.

2.3.1 Kontrolno okolje

Temeljna naloga revizorja IS je prepoznati slabosti pri poslovanju in vodstvu pomagati pri zmanjševanju ali odstranjevanju izpostavljenosti tveganjem in nevarnostim. Z namenom zmanjševanja tveganj se v sistem vgrajujejo kontrole. Pri odločitvi o izbiri ustreznih kontrol je treba upoštevati, da prekomerne kontrole povečujejo stroške, ob tem, da bistveno ne vplivajo na zmanjšanje tveganj, nezadostne kontrole pa tveganja povečujejo. Zato mora vodstvo odločiti, kolikšno mero tveganja je pripravljeno sprejeti, in temu ustrezno implementirati kontrole (Sawyer, 2003, str. 591).

Notranje kontrole delujejo na vseh nivojih organizacije z namenom zmanjševanja izpostavljenosti poslovanja različnim tveganjem. Notranje kontrole so lahko (CISA Review Manual, 2003, str. 30):

- ročne ali avtomatizirane,
- preventivne ali detektivne ter
- formalne ali neformalne.

Učinkovitost obstoja in delovanja notranjih kontrol se ugotavlja z revidiranjem. Revizor oceni učinkovitost delovanja sistema notranjih kontrol in ovrednoti sistem notranjih kontrol. Revidiranje je učinkovito, če prepreči nastanek napak ali če so napake pravočasno odkrite. Pri revidiranju se preverja obstoj vseh notranjih kontrol z vidika tveganj in zaščite pred poslovnimi nevarnostmi, izvaja se presoja tveganja in predlagajo izboljšave (Brečko, 2001, str. 1–3).

2.3.2 Delitev kontrol

Kontrole se po času delovanja delijo na (CISA Review Manual, 2003, str. 33):

- Preprečevalne (Preventive Control): njihov namen je odkriti težavo, preden se pojavi. Preprečujejo nastanek nezaželenih dogodkov. Primeri kontrol so delitev nalog, ustrezno dokumentiranje postopkov, izdelava varnostnih kopij itd.
- Kontrole odkrivanja (Detective Control): kontrole, ki se uporabljajo za odkrivanje in poročanje nastanka nezaželenih dogodkov. Primeri kontrol odkrivanja so izvajanje notranjega revizijskega pregleda, dvakratno preverjanje izračunov, avtomatična sporočila o napaki itd.
- Popravljalne kontrole (Corective Control): kontrole, ki se uporabljajo po nastanku nezaželenih dogodkov. Uporabljajo se za zmanjševanje vpliva posledic in ugotavljanje vzroka težav. Primer popravljalnih kontrol je načrt neprekinjenega poslovanja.

2.3.3 Preizkušanje notranjih kontrol

Preizkušanje notranjih kontrol se izvaja s testiranjem obstoja notranjih kontrol. Med internimi kontrolami in količino potrebnega testiranja obstaja povezava. Če revizor ugotovi, da obstajajo ustrezne notranje kontrole, lahko temu primerno zmanjša število primerjalnih testov. Če pa testi ne pokažejo zadostnega števila notranjih kontrol, se lahko odloči za povečan obseg testiranja.

- S testom skladnosti (Compliance Test) se preverja, če so implementirane kontrole v skladu z zakonodajo, politikami in predpisanimi postopki in če delujejo, kot so opredeljene. Ta test se izvaja najprej.
- Primerjalni test (Substantive Test) je strožji in predstavlja poglobljena testiranja. Izvaja se v odvisnosti rezultatov testa skladnosti. Z njim se testira dejansko izvajanje progama (Karnet, Tajnik, 2003, str. 15).

2.4 Revizijski pregled

Postopek revizijskega pregleda je sestavljen iz različnih faz. Na koncu vsake faze revizor utvari določen produkt, ki mu služi za razumevanje nadaljnjega postopka revidiranja.

2.4.1 Revizijski pregled na osnovi ocene tveganj

Revizijska metodologija je nabor dokumentiranih revizijskih procedur, namenjenih za dosego načrtovanih revizijskih ciljev. Revizor informacijskih sistemov sledi fazam revizijskega pristopa z namenom, da pridobi razumevanje o predmetu revizije, da lahko oceni kontrolno strukturo, preizkusi in ovrednoti kontrole. V primeru izdelane ocene tveganj naročnik na osnovi ocene tveganj izbere ustrezne revizijske cilje. Revizija se tako začne z zbiranjem informacij, proučitvijo sistema internih kontrol, kot so kontrolno okolje in kontrolni postopki, ter oceno tveganja. Nadaljuje se preizkušanje oziroma poglobljeno preizkušanje kontrol, v kolikor je to potrebno, in konča z ugotovitvami in priporočili ter izdelavo revizijskega poročila (Potočnik, Tajnik, 2003, str. 108–109).

2.4.2 Splošni pristop k izvedbi revizije

Če naročnik ni opravil analize tveganj, revizor informacijskih sistemov za posamezne revizijske cilje določi obseg revizije, izvede predrevizijsko načrtovanje, določi revizijske postopke in postopke za pridobitev podatkov ter šele po končanem pregledu oceni velikost in materialnost tveganja in jo v revizijskem poročilu ustrezno dokumentira (Potočnik, Tajnik, 2003, str. 108).

2.4.3 Revizijsko poročilo

Revizija kot takšna ima namen odkriti pomanjkljivosti in jih predstaviti naročniku skupaj s predlogi za izboljšanje z namenom odprave nepravilnosti, neskladnosti in pomanjkljivosti, ki lahko vplivajo na uspešnost, učinkovitost in varnost informacijskega sistema. Vse te ugotovitve je treba v ustrezni obliki predstaviti poslovodstvu, da lahko na podlagi njih razume možna tveganja, ki jih prinašajo pomanjkljivosti, in ustrezno ukrepa. Zaradi tega je kakovost poročanja enako pomembna kot kakovost opravljene revizije.

Osnovno načelo pri pisanju poročila je biti čim bolj jedrnat, hkrati pa natančen in jasen: poročilo mora biti pisano z zornega kota njegovega prejemnika, osredotočeno na tiste elemente, ki so zanj najprepoznavnejši. Revizijska ocena, namenjena najvišjim upraviteljem, ne sme vsebovati preveč strokovnega izrazja (Podgoršek, 2004, str. 239).

2.4.4 Revizorjevo mnenje

Revizorjevo delo je pri ocenjevanju kakovosti informacijskega sistema sestavljeno iz pregleda določene komponente ali dejavnosti glede izpolnjevanja enega ali več revizijskih kriterijev. Rezultat preiskave naj bi bilo mnenje, namenjeno določenim uporabnikom revizijskega poročila. Mnenje pooblaščenega revizorja mora obsegati oceno o stopnji resničnosti in poštenosti računovodskih izkazov in je lahko pritrdilno, s pridržkom ali odklonilno:

- S pritrdilnim mnenjem se oceni, da računovodski izkazi resnično in pošteno prikazujejo finančno stanje in poslovni izid – to pomeni, da so bili s predmetom revidiranja povezani revizijski kriteriji ustrezno ocenjeni in da je revizor pridobil zadostna zagotovila, da lahko informacijski sistem oceni kot kakovosten (Zakon o revidiranju, 2001).
- Z mnenjem s pridržkom se izrazi pridržek glede resničnosti in poštenosti prikazovanja posameznih kategorij v računovodskih izkazih (Zakon o revidiranju, 2001).
- Z odklonilnim mnenjem se oceni, da računovodski izkazi niso resnični in pošteni (Zakon o revidiranju, 2001). V tem primeru revizorju z revizijskimi postopki ni uspelo zbrati zadostnih revizijskih dokazov za potrditev, da predmet revidiranja ustreza vsem proučevanim revizijskim kriterijem. Podajanje negativnega mnenja uporabnikom poročila, ki niso hkrati tudi naročniki revizije, ima lahko daljnosežne posledice, ker se z njim zelo spodkoplje zaupanje v revidirani informacijski sistem (Skitek, 2001, str. 305).

Revizijsko poročilo mora biti nepristransko, jasno, zgoščeno in pravočasno. Vsebovati mora (Lešnik, Korbar, 2001, str. 10):

- uvod,
- cilje in področje revidiranja,
- revizijske izsledke,
- priporočila, predloge za izboljšavo ali potrdilo o zadovoljivem delovanju.

2.4.5 Revizijska sled

Revizijska sled je skupek vseh informacij, ki so potrebne, da se predstavi zgodovinski zapis o vseh pomembnejših dogodkih oziroma dejavnostih, povezanih s shranjenimi podatki in informacijami ter sistemi za zbiranje, obdelovanje in arhiviranje podatkov. Revizijska sled mora omogočati predstavitev časovnega zaporedja vseh dogodkov, povezanih s posameznim poslovnim dogodkom in shranjenimi informacijami. Informacije, ki jih revizijska sled vključuje, morajo biti zadostne, da dokazujejo celovitost shranjene informacije, njihov nastanek in hramba pa morata zagotavljati njihovo neoporečnost in uporabnost v vsem času hranjenja informacij (Javornik, 2005, str. 3).

Pri računalniški obravnavi računovodskih podatkov so sledi o delovanju nekaterih notranjih kontrol na razpolago le kratek čas in še to pogosto v elektronski obliki. Revizor je tako v situaciji, da vseh dokazov ne more pridobiti v papirni obliki; za nekatere dokaze, ki pa morda obstajajo v tej obliki, pa pogosto nima zagotovila, da so enaki tudi v elektronski obliki. Vprašanje ustreznosti dokazila je še pomembnejše v pogojih računalniške obravnave podatkov. Informacija o osebni identifikaciji izvajalca in času transakcije v računalniškem zapisu še ni zadostno dokazilo, da je nekdo transakcijo izvedel, če ni mogoče zanesljivo dokazati, da pristopna pravica ni bila zlorabljena (Javornik, 2005, str. 3).

Postopki za pridobitev revizijskih dokazov se v okolju računalniške obravnave podatkov ne razlikujejo bistveno od klasičnih, obstajajo pa nekateri novi (Javornik, 2005, str. 75):

- poizvedbe,
- opazovanja,
- kontrolni pregled,
- potrditve stanj,
- ponovitev izvedbe in
- nadziranje.

2.5 Orodja revizorja informacijskih sistemov

Zakonodaja predpisuje neodvisno zunanjo revizijo podjetij, ki ustrezajo določenim pogojem (velikost, kotiranje na borzi, dejavnost v zvezi s financami). Iz specifičnih poslovnih razlogov, posebno povečanja zaupanja investitorjev in poslovnih partnerjev, se za revizijo lahko odločijo tudi druga podjetja. V principu je revizija namenjena temu, da

neodvisni revizor pregleda ustrezne dokumente, ki kažejo poslovanje podjetja, ter poda mnenje o tem, ali so pripravljeni v skladu s predpisanimi standardi in ali odražajo resnično in pošteno sliko stanja v podjetju. Orodja, ki jih mora revizor informacijskih sistemov upoštevati, so:

a) Zakonodaja: mednarodna in slovenska
    - Zakon o varstvu osebnih podatkov (ZVOP)
    - Zakon o elektronskem podpisu in elektronskem poslovanju (ZEPEP)
    - Uradni list:
        - Banke
            - Sklep o revidiranju poslovanja bank in hranilnic
            - Uradni list Republike Slovenije 6/95, 31. 01. 1995 – izdal Svet Banke Slovenije
        - Borznoposredniške družbe
            - Sklep o najmanjšem obsegu ter vsebini revizijskega pregleda in revizorjevega poročila borznoposredniške družbe
            - UL RS 6/00, 27. 01. 2000 – izdala Agencija za trg vrednostnih papirjev
        - Zavarovalnice
            - Sklep o podrobnejši obliki in najmanjšem obsegu ter vsebini revizijskega pregleda in revizorjevega poročila zavarovalnice
            - UL RS 6/01
b) Revizijski standardi
    - Mednarodni: ISACA, IIA, NIVRA, ISO 17799 itn.
    - Slovenski: Slovenski inštitut za revizijo (SIR)
c) Revizijske smernice
    - Slovenske: Slovenski inštitut za revizijo (SIR)
    - Mednarodne: COBIT, CONCT (ISACA/F), Basel Committee (http://www.bis.org/publ/)
d) Revizijski programi
    - AIS (Audit Information System o SAP)
    - OICM (Oracle Internal Controls Manager)
e) CAAT(Computer Assisted Audit Techniques)
    - Računalniško podprto revidiranje
    - ACL, IDEA
f) Stalni nadzor (Continuous Monitoring)
g) Dnevniki varnosti (LOG – datoteke)
h) Dokumentacija

(Moškon, 2006, str. 11-12)

2.6 Revizija informacijskih sistemov v Sloveniji

Zakon o revidiranju (Uradni list RS, št. 11/01), ki ureja predvsem revidiranje računovodskih izkazov, omenja revidiranje informacijskih sistemov kot strokovno

področje, ki je povezano z revidiranjem, in ga v tem kontekstu tudi ureja. Zakon tako pooblašča Slovenski inštitut za revizijo, da sprejema standarde s področja revidiranja informacijskih sistemov, določa strokovna znanja in izkušnje, potrebne za pridobitev naziva »preizkušenega revizorja informacijskih sistemov«, organizira izobraževanje in podeljuje naziv »preizkušenega revizorja informacijskih sistemov«. V predpisani izobraževalni program spada tudi opravljanje izpita za pridobitev mednarodnega naziva CISA (Certified Information Systems Auditor), ki ga organizira ISACA (Information Systems Audit and Control Association, www.isaca.org) iz ZDA. Navedene podlage so razlog, da so revizorji informacijskih sistemov v Sloveniji profesionalno združeni v sekcijo revizorjev informacijskih sistemov v okviru Slovenskega inštituta za revizijo. Omeniti velja tudi, da zakon pooblašča inštitut za izdajo dovoljenja za opravljanje dejavnosti revizijskim družbam in izvaja nadzor nad revizijskimi družbami (Javornik, 2003, str. 3).

2.7 Spoznavanje računalniških kontrol

Spoznavanje splošnih računalniških kontrol informacijskega sistema je del revizijskega postopka revizije računovodskih izkazov. Poznavanje informacijskega sistema je eden od pomembnejših pogojev za razumevanje poslovanja podjetja. Točnost računovodskih izkazov je v veliki meri odvisna od zanesljivosti informacijskega sistema in verodostojnosti kontrol znotraj poslovnih aplikacij.

Obseg spoznavanja zajema razumevanje desetih področij splošnih računalniških kontrol:

1. Strategija in načrtovanje podatkovnih virov
2. Delovanje informacijskih sistemov
3. Odnosi z zunanjimi izvajalci – dobavitelji
4. Logično in fizično varovanje podatkov
5. Načrtovanje neprekinjenosti poslovanja
6. Uvedba in vzdrževanje aplikacij
7. **Uvedba in vzpostavitev baze podatkov**
8. Mrežna podpora
9. Podpora sistemske programske opreme
10. Podpora strojne opreme

(Povzeto po metodologiji Deloitte & Touche Methodology)

Pri izbiri kontrol za obvladovanje tveganj na področju informatike in za preizkušanje delovanja splošnih aplikativnih kontrol so na razpolago različni kontrolni okvirji, navodila in standardi. V nadaljevanju sta predstavljena dva najpomembnejša:

- BS 7799 – Kodeks varovanja informacij (posodobljen na ISO/IEC 17799:2000) je kodeks dobre prakse in osnova za varnostne standarde na področju upravljanja varovanja informacij v organizaciji. V desetih poglavjih definira kontrole na desetih področjih varovanja informacij. Priročnik je namenjen vodstvu in zaposlenim, ki so v organizaciji odgovorni za pobudo, uvajanje in vzdrževanje varstva informacij.

- COBIT (Control Objectives for Information and Related Technology, v nadaljevanju COBIT) je priročnik, ki definira 34 kontrolnih ciljev na najvišjem nivoju in 318 kontrol, ki so predstavljene na štirih področjih. COBIT predstavlja model oziroma metodologijo za upravljanje IT (COBIT Framework, 2000, str. 13).

Kot navaja sistemski okvir metodologije COBIT, trenutno obstajata dve skupini kontrolnih modelov, in sicer poslovni kontrolni modeli (kot npr. COSO) ter specializirani poslovni modeli za IT. COBIT poskuša premostiti vrzel med obema skupinama. Oblikovan je tako, da ponuja celosten pristop in nudi delovanje na višjem nivoju kot preostali standardi za upravljanje IS (COBIT Framework, 2000, str. 13).

2.8 COBIT

Cobit (Control Objectives for Information and Related Technology) Framework (ogrodje) je orodje lastnikov poslovnih procesov za določanje odgovornosti. Metodologija temelji na predpostavki, da procesi informacijske tehnologije koristijo vire informacijske tehnologije tako, da zagotovijo informacije, ki jih podjetja potrebujejo za dosego svojih ciljev.

Da zadovoljijo poslovne cilje, morajo informacije izpolnjevati določena merila, ki so:

- **Učinkovitost** (Eficiency): Informacije so posredovane z optimalno izrabo virov.
- **Zaupnost** (Confidentiality): Zaščita občutljivih in zaupnih informacij pred nepooblaščenim razkritjem.
- **Celovitost** (Integrity): Neoporečnost, točnost in popolnost informacij glede na poslovno vrednost in pričakovanja.
- **Razpoložljivost** (Availability): Informacije morajo biti v sedanjosti in prihodnosti na razpolago takrat, ko jih poslovni procesi in pooblaščeni uporabniki potrebujejo. Potrebni viri in pripadajoče zmogljivosti morajo biti ustrezno varovani.
- **Skladnost** (Compliance). Skladnost informacij z zakoni, predpisi in pogodbenimi sporazumi, ki se nanašajo na poslovne procese v podjetju.
- **Verodostojnost in zanesljivost informacij** (Reliability). Informacije predstavljajo ustrezno podlago vodstvu pri vodenju podjetja, pri sprejemanju odločitev in poročanju (Inštitut za revizijo, 2006).

Procesi so združeni v štiri področja:
1. Planiranje in organizacija
2. Pridobitev in uvedba
3. Postavitev in podpora
4. Opazovanje in nadzor

Vsakemu izmed 34 procesov odgovarja kontrolni cilj na najvišjem nivoju. Lastniki poslovnih procesov zagotavljajo, da je uveden primeren kontrolni sistem za okolje informacijske tehnologije, v kolikor so doseženi kontrolni cilji na najvišjem nivoju. Pri doseganju teh ciljev upoštevamo poslovne zahteve za učinkovitost, uspešnost, zaupnost,

celovitost, razpoložljivost, skladnost in zanesljivost. Glavni cilj projekta COBIT je zagotoviti jasno politiko in dobro prakso za vpeljavo kontrol informacijske tehnologije v vseh vejah industrije (Potočnik, Tajnik 2003, str. 110–111).

Sredstva, s katerimi informacijska tehnologija dostavlja podatke, potrebne za poslovne procese, so:

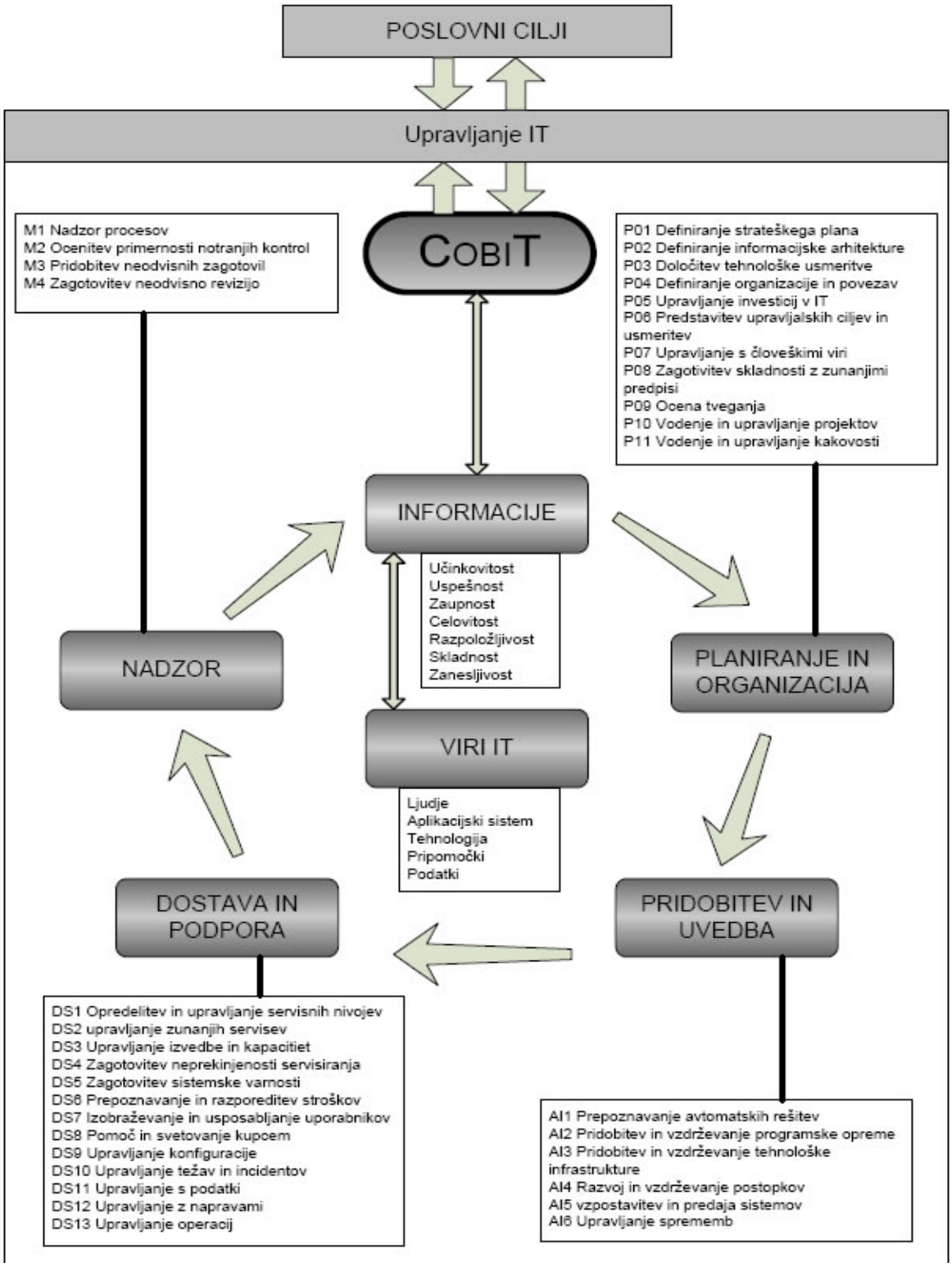
- podatki – računalniške rešitve (aplikacije – avtomatizirani postopki poslovnih funkcij),
- tehnologija (strojna in sistemska programska oprema, sistemi za opravljanje baz podatkov, računalniške mreže ...),
- pomožne računalniške naprave ter ljudje, njihovo znanje in izkušnje (IT Governance Institute – Cobit Mapping, 2000 str. 5).

Implementacija metodologije COBIT je običajno predmet pri naslednjih poslovnih primerih:

- potreba po upravljanju IT (IT Governance),
- storitve informacijske tehnologije je treba uskladiti s poslovnimi cilji in politiko,
- informacijske procese je treba standardizirati,
- potreba po celovitem ogrodju procesov informacijske tehnologije,
- potreba po poenotenju procesov,
- potreba po ogrodju za kakovosten sistem upravljanja,
- potreba po definiranju strukturiranega pristopa k reviziji,
- v primerih združitve in prevzemov,
- potreba po stroškovnem nadzoru,
- v primerih predajanja dela informacijske tehnologije zunanjim izvajalcem (Outsourcing) in
- v primeru združljivosti s potrebami zunanjih sistemov (IT Governance Institute – Cobit Mapping, 2006 str. 6).

V povezavi z neskladnostmi se pojavljajo različna tveganja, kot so neusklajenost storitev IT in posledično tudi slaba podpora doseganju poslovnih ciljev. Zelo hitro se lahko zgodi, da podjetje zamudi poslovno priložnost (kratki časi odprtosti poslovnih oken). Znanje oziroma »know – how« je domena posameznikov, ne pa organizacije, kar je v današnjem času velike konkurence na področju povpraševanja po strokovnjakih, posebno tistih izkušenih, veliko tveganje za podjetja (IT Governance Institute – Cobit Mapping, 2006 str. 8).

Slika 1: Struktura metodologije COBIT



Vir: Pohorec, 2006, str. 15

3 Revizija baz podatkov

Z zahtevkom za revidiranje podatkovne baze se najpogosteje srečujemo v širšem sklopu revidiranja IS in IT. Lahko se dogodi, da je revidiranje omejeno bolj ali manj na specifično okolje. V tem primeru je v nekaterih segmentih treba pregledati širše področje IS/IT, saj se obe področji običajno prepletata in povezujeta. Pomembno je tudi, kako je uporaba aplikacij in baze vpeta v organizacijsko strukturo in procese, ki v organizaciji potekajo, in kako se izpolnjujejo pričakovanja vodstva ter dosegajo cilji podjetja (Javornik, 2003, str. 5).

3.1 Sistem baz podatkov

Sistem baz podatkov sestavljata dva bistvena dela:

- baze podatkov in
- sistem za krmiljenje baz podatkov (Database Management System).

Sistem deluje v povezavi z drugimi deli računalniške opreme in računalniških rešitev v celotnem računalniškem sestavu (MSR, 1997, standard 1003).

3.1.1 Opredelitev baze podatkov

Baza podatkov je zbirka medsebojno povezanih podatkov, shranjenih v računalnikovem pomnilniku brez nepotrebnega podvajanja na način, ki omogoča njihovo uporabo različnim uporabnikom z različnimi potrebami glede uporabe. Podatki so shranjeni tako, da so neodvisni od programov, ki jih uporabljajo (Grad, 1985, str. 1).

Za definiranje baze podatkov in izvajanje operacij s podatki (branje, pisanje, spreminjanje, brisanje, iskanje) in za nadzor učinkovitosti izvajanja operacij skrbijo sistemi za upravljanje baz podatkov (Database Management System). Večina jih vsebuje jezik, ki je namenjen tudi končnim uporabnikom in jim omogoča, da sami izvajajo določene operacije.

Primer takšnega jezika je strukturiran poizvedovalni jezik (Structured Query Language – SQL), ki je standardiziran in zelo podoben naravnemu jeziku.

Baza podatkov ima naslednje značilnosti (Damij, Grad, Jaklič, 1995, str. 40):

- je urejena zbirka med seboj povezanih podatkov, ki je shranjena na disku ali v kakšnem drugem pomnilniškem mediju;
- uporablja jo množica paketnih in interaktivnih uporabnikov, ki opravljajo s podatki operacije, kot so doseganje, shranjevanje, brisanje in dodajanje;
- je integrirana, kar pomeni, da vsebuje podatke za veliko uporabnikov, pri čemer posameznega uporabnika zanima le del celote.

3.1.2 Upravljanje z bazami podatkov

V sodobnih organizacijah so baze podatkov postale pomemben vir podjetja, zato morajo podjetja z njimi smiselno upravljati, kar pomeni (Damij, 1993, str. 13):

- zagotavljanje razpoložljivosti podatkov, saj je zelo pomembno, da imajo uporabniki učinkovit dostop do vseh podatkov, ki jih potrebujejo, takrat, ko jih potrebujejo, tudi sočasno, pomemben pa je tudi kratek odzivni čas pri uporabi baze podatkov;
- nadzor nad bazo podatkov mora zagotavljati obnavljanje baze, nadzor nad sočasnim dostopom do podatkov in preverjanje vhodnih podatkov, saj je, če so vhodni podatki netočni, ves trud v zvezi z bazo podatkov zaman;
- zagotavljanje celovitosti podatkov:
    - s preverjanjem vhodnih podatkov, saj pri vnosu vedno obstaja možnost napak;
    - z zagotavljanjem mehanizmov za obnovitev podatkov v primeru njihovega uničenja;
    - z zagotavljanjem sočasnega dostopa do podatkov, tudi če ravno takrat poteka ažuriranje baze podatkov;
- uporabo podatkov v skladu z njihovim namenom:
    - pomembno je, da uporabnik razume pomen podatkov, saj jih bo le tako lahko pravilno uporabil;
    - obstajati mora sistem nadzora dostopa do posameznih mest podatkov, da se zagotovi njihova tajnost (pravica do branja, dodajanja, spreminjanja in brisanja podatkov.

3.1.3 Splošni pristopi k varovanju podatkov

Varnost podatkov postaja vse pomembnejše področje, ki se nanaša tudi na baze podatkov. To lahko zagotovimo s splošnimi pristopi k varovanju podatkov. Delimo jih na:

- Politiko varovanja – skupek zakonov, pravil in praktičnih napotkov, kako naj neka organizacija upravlja, ščiti in porazdeljuje občutljive informacije. Sestavljajo jo zahteve po tehničnih varnostnih ukrepih in po fizičnem, uporabniškem in proceduralnem varovanju.
- Varovalne ukrepe, ki jih naprej delimo na (Brumen, 1998, str. 31–32):
    - fizične ukrepe, kot je npr. shranjevanje medijev s podatki na način, ki onemogoča dostop nepooblaščenim osebam;
    - tehnične ukrepe, kot je npr. večnivojsko preverjanje avtorizacije dostopa do podatkov;
    - proceduralne ukrepe, kot je npr. prepisovanje podatkov;
    - uporabniške ukrepe, kot je npr. preverjanje uporabnikove zgodovine.

Le pravilna kombinacija vseh teh ukrepov bo privedla do učinkovitega sistema za varovanje podatkov (Brumen, 1998, str. 31–32).

3.2 Notranje kontroliranje v okolju z bazami podatkov

V okolju z bazami podatkov mora notranje kontroliranje običajno zagotoviti učinkovite kontrole v zvezi z uporabo baze podatkov, programi za krmiljenje baz podatkov in uporabniškimi rešitvami.

Zaradi souporabe podatkov, njihove neodvisnosti in drugih značilnosti sestavov z bazami podatkov utegnejo biti splošne kontrole računalniškega informacijskega sestava za take sestave pomembnejše kot kontrole v uporabniških rešitvah. Splošne kontrole nad bazo podatkov, programi za krmiljenje baz podatkov in dejavnosti službe, ki je v podjetju odgovorna za skrbništvo baz podatkov, zelo vplivajo na uporabniške rešitve. Splošne kontrole računalniškega informacijskega sistema, ki so zlasti pomembne v okolju z bazami podatkov, se lahko razvijejo v te skupine (MSR, 1997, standard 1003):

- standardni načini razvijanja in vzdrževanja programov z uporabniškimi rešitvami,
- lastništvo nad podatki,
- dostop do baze podatkov in
- ločevanje dolžnosti.

3.2.1 Standardni načini razvijanja in vzdrževanja programov

Ker si podatke deli več uporabnikov, je nadzor mogoče okrepiti tako, da se za razvijanje vsakega novega programa z uporabniškimi rešitvami in dopolnjevanje teh programov uporablja standardne metode – gre za spoštovanje predpisanega postopka, razdeljenega na stopnje, ki ga morajo upoštevati vsi, vpleteni v razvoj. Gre tudi za analiziranje vpliva novih in obstoječih poslov na bazo podatkov, kadar so potrebne dopolnitve. Analiza pokaže posledice sprememb na varnost in neoporečnost baze podatkov. Uporaba standardnih metod za razvijanje in vzdrževanje programov z uporabniškimi rešitvami lahko poveča točnost, neoporečnost in popolnost baze podatkov (MSR, 1997, standard 1003).

3.2.2 Lastništvo nad podatki

V računalniškem okolju z bazami podatkov, kjer lahko več uporabnikov uporablja programe za vnašanje podatkov, mora skrbnik baze podatkov jasno in natančno določiti, kdo je odgovoren za točnost in neoporečnost vsakega posameznega podatka. Za določanje pravil dostopa in varstva podatkov mora biti odgovoren le en lastnik podatkov. Če lahko o točnosti in neoporečnosti odloča več posameznikov, je možnost zlorabe podatkov večja (MSR, 1997, standard 1003).

3.2.3 Dostop do baze podatkov

Uporabnikom baze podatkov se dostop lahko omeji z uporabo gesel. Take omejitve se nanašajo na posameznike, terminalske naprave in programe. Učinkovitost gesel in s tem varnost informacijskega sistema je treba določiti z ustreznimi postopki, ki definirajo frekvenco spreminjanja, kompleksnost in minimalno število dovoljenih znakov. V politiki gesel morajo biti opredeljene minimalne zahteve prej omenjenih varnostnih zahtev, definiranih za različne nivoje odgovornosti v organizaciji. Skrbništvo baze podatkov mora

biti dovoljeno izključno skrbnikom baze, ki naj bi za dostop uporabljali višjenivojska gesla – večja kompleksnost in večja dolžina gesla.

Neustrezna politika gesel pomeni veliko tveganje nedovoljenega dostopa do sredstev in/ali podatkov v informacijskem sistemu. Taki dostopi lahko ostanejo neodkriti in imajo za posledico nepooblaščeno spreminjanje ali razkritje podatkov (Metodologija Deloitte & Touche).

3.2.4 Ločevanje dolžnosti

Opravljanje različnih dejavnosti v zvezi z oblikovanjem, izvajanjem in delovanjem baze podatkov si deli tehnično, skrbniško, oblikovalsko in uporabniško osebje. Med njihovimi dolžnostmi so tudi oblikovanje sestava in baze podatkov, skrbništvo in uporaba baze v praksi. Ustrezno ločevanje naštetih dolžnosti zagotavlja popolnost, neoporečnost in točnost baze podatkov (MSR, 1997, standard 1003).

3.3 Vpliv baz podatkov na revizijske postopke

Za sestave z bazami podatkov je značilna večja zanesljivost podatkov kot za sestave brez baz podatkov. K večji zanesljivosti podatkov prispevajo poleg ustreznega kontroliranja naslednji dejavniki (MSR, 1997, standard 1003):

- večja doslednost podatkov, ker se evidentirajo in ažurirajo le enkrat,
- večja neoporečnost podatkov zaradi uspešne uporabe možnosti, ki jih vsebujejo programi za krmiljenje baz podatkov, kot so ponovna vzpostavitev podatkov, ponovni zagon programa, splošni podprogrami za urejanje in ugotavljanje pravilnosti podatkov ter varnostne in kontrolne dejavnosti,
- druge kontrole programov za krmiljenje baz podatkov, ki lahko olajšajo kontrolne in revizijske postopke.

Ko revizor ocenjuje tveganje, lahko pri ugotavljanju, koliko se lahko opre na notranje kontrole, upošteva, kako se zgoraj navedene kontrole uporabljajo v tej ureditvi. Če se odloči opreti na omenjene kontrole, mora opraviti ustrezne preizkuse kontrol, kjer lahko uporabi programe za krmiljenje baz podatkov za (MSR, 1997, standard 1003, str. 11):

- pripravo preizkusnih podatkov,
- zagotavljanje sledi revidiranja,
- preverjanje neoporečnosti podatkov,
- zagotavljanje dostopa do baze podatkov ali kopij ustreznih delov baz podatkov, ki omogoča uporabo računalniških rešitev za pomoč pri revidiranju, in
- pridobivanje podatkov, potrebnih za revizijo.

Če revizor uporablja možnosti v programu za krmiljenje baz podatkov, mu ni treba pridobiti ustreznih zagotovil o njegovem pravilnem delovanju (MSR, 1997, standard 1003, str. 11).

4 Primerjava varnosti sistema za upravljanje baz podatkov – Oracle in IBM

Različni pristopi dveh največjih igralcev na trgu (Oracle in IBM) pri zagotavljanju vgrajene varnosti v sistemu za upravljanje baz podatkov zahtevajo dobro poznavanje prednosti in slabosti, ki jih prinaša implementacija sistema v poslovanje organizacije. Pred nakupom je zato treba pretehtati vsaj naslednja področja:

- vgrajena funkcionalnost za zagotavljanje varnosti,
- kompatibilnost z operacijskim sistemom,
- stroške, povezane z zagotavljanjem varnosti v sistemu (potreba po programskih rešitvah, ki omogočajo varnost na primernem nivoju),
- vzdrževanje sistema – členi pogodb, ki se nanašajo na zagotavljanje rednega vzdrževanja sistema,
- nadzor – vgrajena funkcionalnost nadzora sistema,
- osebje – potreba po dodatnem izobraževanju ali zaposlitvi novih kadrov za upravljanje s sistemom ter
- nadgradnje – pogodbene obveze dobavitelja o zagotavljanju nadgradenj sistema – stroški varnostnih nadgradenj.

4.1 Pristop k varnosti

Bistvena razlika med obema sistemoma za upravljanje baz podatkov je pristop k zagotavljanju varnosti podatkovne baze. Produkti Oraclea imajo vgrajene varnostne funkcionalnosti, ki ob pravilni konfiguraciji parametrov zagotavljajo visoko stopnjo varnosti brez potrebe dodatnih rešitev, medtem ko baza DB2 sama po sebi, brez dodatnih produktov IBM, ne predstavlja nikakršne varnosti. Strategija Oraclea je v vsak produkt vgraditi kar najvišjo stopnjo varnostnih funkcionalnosti, kar sistemu omogoča popolno neodvisnost od drugih sistemov ter programskih rešitev. S tem si zelo poveča kompatibilnost z različnimi operacijskimi sistemi, kar pa ne velja za podatkovno bazo DB2. IBM omogoča primerno stopnjo varnosti podatkovne baze le z uporabo operacijskega sistema IBM ter dodatnih programskih rešitev, kot je Tivoli SecureWay. Podatkovna baza DB2 nima vgrajene funkcionalnosti, ki bi zagotavljala varnost, temveč ji to na vseh nivojih (avtentikacija uporabnika, varnost mrežnih povezav na bazo …) zagotavlja operacijski sistem (npr: AS400, OS390, UNIX, LINUX). Z nakupom DB2 stopnja varnosti ni povsem znana, saj je popolnoma odvisna od različnih verzij operacijskih sistemov ter verzij dodatnih produktov, ki skupaj gradijo varnost podatkovne baze (An Oracle White Paper, 2002, str. 4).

Omenjena razlika pri zagotavljanju varnosti obeh podatkovnih baz močno vpliva na odločitve o nakupu sistema in njegovo implementacijo. Pomanjkljivosti IBM so tako naslednje (An Oracle White Paper, 2002 str. 5):

- težavnost dodajanja ravni višjega nivoja varnosti,

- višji stroški – potreba po dodatnih IBM – produktih, ki omogočijo varnost podatkovne baze,
- višji stroški dolgoročnega vzdrževanja in nadgrajevanja – potreba po nadgrajevanju vseh sistemov, ki skupaj tvorijo varnost (DB2, OS in Tivoli),
- visoka stopnja kompleksnosti nastavitev različnih IBM – produktov, ki morajo skupaj zagotavljati primeren nivo varnosti.

Razlika med DB2 in Oracle je tudi v tem, da IBM varnost podatkovne baze obravnava ločeno od aplikacijskega nivoja, medtem ko Oracle združuje varnost podatkovnega nivoja z aplikacijskim. Razlog za to najdemo v razvoju produktov. Razvoj baze DB2 je ločen od razvoja njene varnosti (dva različna poslovna oddelka), medtem ko je razvoj pri Oracleu voden pod enotnim okriljem (An Oracle White Paper, 2002 str. 5).

4.1.1 Zagotovitev primerne varnosti

Zaradi velikega števila ponudnikov sistemov baz podatkov se pri odločitvi za nakup pojavijo težave. Različni načini zagotavljanja varnosti, funkcionalnosti baze in kompatibilnost z obstoječim operacijskim sistemov organizacije so večinoma ključni faktorji pri procesu nakupnega odločanja, kjer je pri ocenjevanju varnosti pomemben faktor ocena neodvisnih strokovnjakov. Oracle je prvi neodvisni pregled opravil že leta 1994 in do leta 2002 (letnica nastanka članka) uspešno prestal že 14 ocenjevanj. Ocenjevanje ne pokriva le področja pregleda programske kode, temveč razširi njegovo obzorje na pregled standardov programiranja in celotnega razvoja, vključno s preverjanjem podporne dokumentacije. Omenjena zagotovila pregleda zunanjih neodvisnih organizacij kupcu olajšujejo odločitve nakupa, še posebno pri ocenjevanju varnostnega sistema. V nasprotju z Oracleom pa IBM še ni prestal nobenega ocenjevanja varnosti sistema (An Oracle White Paper, 2002, str. 8).

4.2 Podrobnejši pregled varnostnih zmogljivosti

Večja, kot je stopnja varnostnih zmogljivosti/funkcionalnosti, ki so primarno vgrajene v sistem, večjo varnost omogoča sistem. Hkrati pa zahteva premišljene aktivacije in nastavitve vrednosti parametrov. Nekaj najpomembnejših je predstavljenih v naslednjih točkah naloge.

4.2.1 Avtentikacija (prepoznavanje) uporabnika

Primerjava funkcionalnosti Oraclea in IBM pri zagotavljanju visoke stopnje varnosti pri avtentikaciji uporabnika se razlikuje le v tem, da IBM dopušča možnost avtentikacije na nivoju baze ali operacijskega sistema, medtem ko avtentikacija uporabnika pri Oracleu poteka na nivoju baze, operacijskega sistema, certifikatov, shranjenih v bazi, ali drugih zunanjih podjetij, ki ponujajo storitve avtentikacije na nivoju mrežne povezave – Kerberos in CyberSafe. Visoka stopnja varnosti ne vključuje le prepoznavanja uporabnika z vpisom uporabniškega imena in gesla, temveč tudi zmožnost avtentikacije z uporabo biometričnih

naprav, magnetnih kartic ter mrežnih storitev (npr: RADIUS[1]) (An Oracle White Paper, 2002, str. 11).

4.2.2 Avtorizacija in kontrole dostopa

Tako DB2 kot Oracle vsebujeta funkcionalnost, ki omogoča uporabniku omejen dostop do podatkov, glede na dodeljene uporabniške pravice. Pravice omejuje na pravice branja, spreminjanja, brisanja in pregledovanja podatkov. Obe bazi imata zmožnost kreiranja različnih poročil, ki ravno tako vsebujejo le informacije, do katerih ima uporabnik pravico dostopa. Problem se pojavi pri omejevanju informacij v kompleksnejših poročilih, kjer se omejitve, določene v SQL – stavku, nanašajo na več povezanih tabel med različnimi oddelki ali aplikacijami. Drugi problem je omejitev varnosti direktno na poročilu, ki se ga lahko omeji glede na pravice prijavljenega uporabnika, medtem ko se tistim, ki imajo naloge ustvarjanja poročil po potrebi in s tem pravico izvajanja direktnih SQL – ukazov na bazo, pravic ne more povsem omejiti (An Oracle White Paper, 2002, str. 14).

Prav zaradi zgoraj omenjenih problemov je Oracle razvil VPD (Virtual Private Database[2]), RLS (Row Level Security) in FGAC (Fine Grained Access Control[3]). Vse to so kratice in nazivi za eno samo novo funkcionalnost, ki jo je prinesla podatkovna baza Oracle 8i. Gre za povsem nov koncept zagotavljanja nadzora dostopa do podatkov. Doslej se je za podatke na sistemskem nivoju lahko omejil le dostop do podatkov na ravni posamezne tabele, odslej pa je dostop lahko nadziran na ravni posamezne vrstice oziroma njene vsebine (Publikacija SRC.SI Info, 2002).

IBM v svojem produktu DB2 ne omogoča podobne varnostne funkcionalnosti, niti ni vgrajena v paket produktov, ki skupaj tvorijo varnost podatkovne baze (Tivoli, AS/400).

4.2.3 Uporaba šifriranja

Razvoj interneta prinaša nove izzive na področju zagotavljanja varnega prenosa informacij z uporabo javnega internetnega omrežja, zato je uporaba šifriranja zaupnih informacij postala nujen del zagotavljanja varnosti informacij. Na nivoju podatkovnih baz se šifriranje uporablja pri shranjevanju informacij v bazo. Te se najprej šifrira z ustreznim algoritmom in šele nato shrani v bazo.

IBM je funkcionalnost šifriranja v DB2 vgradil prvič leta 2001. Aplikacija omogoča šifriranje podatkov pred zapisom (vložek – Input) in dešifriranje pred prikazom rezultata (produkt – Output) z uporabo algoritma RC2, ki uporablja 128–bitno šifriranje. DB2 šifrira vse podatke v določenem stolpcu tabele z uporabo šifrirnega gesla, kar predstavlja zelo

[1] RADIUS – Internetni standard za prepoznavanje oddaljene prijave uporabnika – Remote Authentication Dial in User Services.

[2] V okviru sistema so podatki posameznika povsem zaščiteni, zato se te podatkovne baze tudi imenujejo Virtual Private Database

[3] FGAC (Fine Grained Access Control) je opcija podatkovne baze Oracle, ki je vključena v ceno Oracle 9i Enterprise Edition in omogoča izvajanje varnostne politike nad podatki na nivoju zapisa (vrstice) v tabeli.

preprosto rešitev, ki pa ima tudi nekaj pomanjkljivosti (An Oracle White Paper, 2002 str. 16):

- metoda še ni bila preverjena s strani zunanjega neodvisnega ocenjevalca,
- minimalna dolžina gesla ni določena – odgovornost organizacije, da določi pravila gesel – sistem ne omejuje dolžine in kompleksnosti gesel,
- šibka politika gesel – možnost napada besed iz slovarja (Dictionary Attack).

Oracle je funkcionalnost šifriranja, ki je zagotavljala zaščito občutljivih informacij, v svoj produkt prvič implementiral leta 1999, v nadaljnjih letih pa jo je izboljševal in prišel do uporabe trojnega algoritma DES[4] (Triple DES Algorithm). Trenutno Oracle uporablja algoritem DES s šifriranjem dveh ali treh ključev (Triple DES Algorithm) (An Oracle White Paper, 2002, str. 17).

4.2.3.1 Šifriranje omrežja

Ker se danes večina informacij prenaša prek omrežja, je treba zagotoviti ustrezno zaščito med prenosom zaupnih informacij. DB2 nima vgrajene nikakršne funkcionalnosti, ki bi omogočala šifriranje podatkov pred prenosom v omrežje. IBM je funkcionalnost šifriranja vgradil v operacijski sistem (npr: OS/390) z uporabo navideznega lokalnega omrežja (VPN – Virtual Private Network), ki uporablja javno telekomunikacijsko omrežje, kjer šifriranje podatkov zagotavlja z uporabo »tunel« protokola (Tunneling Protocol) (vir: www.netunlimited.com/glossary.html). Druga možnost uporabe šifriranja podatkov pred prenosom pa je uporaba paketa Tivoli, ki podatke šifrira s protokoloma SSL (Secure Socket Layer) in DES (Data Encryption Standard) (An Oracle White Paper, 2002, str. 17).

Oracle ponuja funkcionalnost »Napredna varnost v Oracleu« (Oracle Advanced Security), s katero zagotavlja šifriranje podatkov pri vseh prenosih. Oracle ima na voljo več vrst šifriranja (An Oracle White Paper, 2002 str. 17):

- RC4 v 256–, 128–, 56– ali 40–bitni verziji,
- DES v 56– in 40–bitni verziji ali
- trojni standard DES (3DES) z uporabo 112– in 168–bitnih ključev ločeno, kar zagotavlja največjo stopnjo zaščite.

Tako Oracle kot IBM ponujata uporabo šifriranja, ki zagotavlja ustrezno zaščito podatkov med prenosom; razlika je le v načinu, saj Oracle ponuja funkcionalnost šifriranja v paketu, IBM pa jo zagotavlja na nivoju operacijskega sistema ali dodatnih aplikacij (An Oracle White Paper, 2002, str. 18).

4.2.4 Revidiranje sistema

Funkcionalnost, ki omogoča tvorjenje revizijskih sledi, predstavlja pomemben varnostni mehanizem, saj beleži dogodke, ki jih organizacija in revizor potrebujeta pri ugotavljanju pravilnosti ali zlorab sistema.

[4]Data Encryption Standard – Standard šifriranja.

Obseg beleženja dogodkov v DB2 je odvisen od nastavitve vrednosti parametrov, kjer skrbnik baze določi, katere dogodke naj baza beleži. Nekateri najosnovnejši parametri, ki omogočajo najnižjo stopnjo zagotavljanja revizijskih sledi, so že vključeni v bazi in se jih lahko izključi le s popolno deaktivacijo funkcije revidiranja. DB2 ima možnost ločevanja beleženja dogodkov s strani skrbnikov baze, ki imajo ponavadi najvišje pravice dostopa, zato mora biti nadzor nad njim še posebno podroben, dostop do datoteke, kamor se beležijo dogodki, pa ustrezno zaščiten, tako da jih skrbniki ne morejo spreminjati ali izbrisati. DB2 zagotavlja široko paleto funkcionalnosti revidiranja, ki omogoča beleženje izbranih dejavnosti uporabnikov ter uspešne in neuspešne prijave v bazo in njene objekte. Skrbnik lahko izbira med možnostjo sinhronega ali asinhronega beleženja revizijskih sledi. Prvo predstavlja beleženje dogodka, ko se ta shrani na disk, kar pomeni, da so vsi dogodki ustrezno zabeleženi, drugo pa dogodke shranjuje v navidezni datoteki, ki jo zapiše ob določenih intervalih, kar bolje vpliva na učinkovitost baze, saj je manj obremenjena, a hkrati predstavlja večjo možnost potencialne izgube podatkov (An Oracle White Paper, 2002, str. 19).

Oracle ponuja možnosti revidiranja glede na objekt, dogodke, pravice ali uporabnika, kjer se beleži uspešne ali neuspešne prijave v bazo. Oracle hrani zapise na nivoju baze, do njih pa je mogoče dostopiti z uporabo »ad–hoc« poizvedb ali ob pomoči ustreznih orodij. Funkcionalnost revidiranja je na voljo skupaj s podatkovnim strežnikom in ponuja širok izbor nastavitev beleženja dogodkov. Največji slabosti Oraclea sta prav dostop do revizijskih sledi in priprava poročil, ki jih zaradi kompleksnosti pripravljajo usposobljeni programerji. Slabosti Oraclea pri zagotavljanju revizijskih sledi so podrobneje predstavljene v petem poglavju z naslovom Slabosti funkcionalnosti zagotavljanja revizijskih sledi (An Oracle White Paper, 2002, str. 20).

Stopnja natančnosti beleženja dogodkov je odvisna od posamezne organizacije, ki mora upoštevati, da beleženje negativno vpliva na učinkovitost baze, saj povečuje njeno obremenjenost (An Oracle White Paper, 2002, str. 20).

5 Revidiranje podatkovne baze Oracle – praktični primer

Oracle je eno od najhitreje rastočih podjetij na področju informacijske tehnologije in je danes še vedno prvo na svojem področju. Iz podjetja, ki je bilo nekoč znano le po podatkovnih zbirkah, je nastalo podjetje, ki se pojavlja povsod, kjer programska oprema rešuje težave pri vzpostavljanju informacijskih sistemov. Tehnologijo Oracle najdemo v skoraj vsaki panogi po svetu, saj Oracle z več kot 200.000 uporabniki deluje v več kot stopetinštiridesetih državah.

Oracle je vodilni svetovni dobavitelj programske opreme za informacijsko poslovanje in drugo največje neodvisno podjetje za programsko opremo na svetu. Podjetje nudi podatkovne zbirke, orodja in aplikacijske proizvode skupaj s storitvami svetovanja, šolanja in tehnične podpore (Oracle, 2006).

Nove verzije baze se distribuirajo v obliki CD–paketa (možno jih je tudi prenesti s spletnih strani), nameščajo pa se z grafičnim orodjem Universal Oracle Installer. Poleg baze in orodij za skrbništvo se v procesu namestitve namešča tudi tako imenovane pakete (Packages) za podporo dela z raznimi vrstami podatkov, ki se bodo hranili in obdelovali v bazi. Za uporabo nekaterih od teh paketov je treba pridobiti posebno licenco (Javornik, 2003, str. 5).

V nadaljevanju diplomskega dela bom predstavil različna področja varnosti podatkovne baze, ki naj bi jih revizor pregledal in ocenil njihovo učinkovitost glede na želeno kontrolno okolje podjetja. Informacije se bodo nanašale na Oracleovo bazo verzije 9i.

5.1 Poizvedovanje splošnih informacij podatkovne baze

Varnost podatkovne baze Oracle je določena z vrsto parametrov, nastavljenih na gostujočem operacijskem sistemu in v bazi. Revizor mora imeti a dostop do teh informacij pravice uporabe ukaznega okna, kjer z ukazi zahteva želene podatke, za katere mora imeti dodeljene ustrezne pravice (Mookhey, 2003, str. 2):

- kot »sys« uporabnik (sistemski uporabnik) s privilegiji SYSDBA – najvišji nivo pravic dostopa ali
- z uporabo nižjenivojskih pravic dostopa, kjer mora imeti pravico SELECT v vseh sistemskih tabelah in poročilih na SYS in SYSTEM Tablespace.

V nadaljevanju diplomskega dela bom upošteval, da je oseba, ki opravlja revizijo prek ukaznega okna, povezana s sistemom z enim od zgoraj omenjenih uporabniških računov, kar ji omogoča dostop do vseh datotek/podatkov, potrebnih za izvedbo revizije. Z enim od omenjenih uporabniških računov se revizor poveže na SQL*Plus–aplikacijo, kjer lahko začne z izvajanjem ukazov. SQL*Plus je orodje, ki omogoča direkten dostop, konfiguracijo baze in njeno skrbništvo ter izvajanje »ad–hoc[5]« poizvedb (Mookhey, 2003, str. 2).

Pri povezovanju v bazo je potreben vnos uporabniškega imena, gesla in identifikacijske številke baze – SID (System Identifier). Če revizor ne pozna SID–številke, jo lahko najde v datoteki init.ora, ki je na nivoju operacijskega sistema. Omenjena datoteka vsebuje ključne nastavitve podatkovnega strežnika, ki jih potrebuje operacijski sistem pri vsakem zagonu podatkovnega strežnika. Datoteka vsebuje vrsto parametrov, ki jih bom analiziral v poglavju Konfiguracijske nastavitve podatkovne baze (Mookhey, 2003, str. 3).

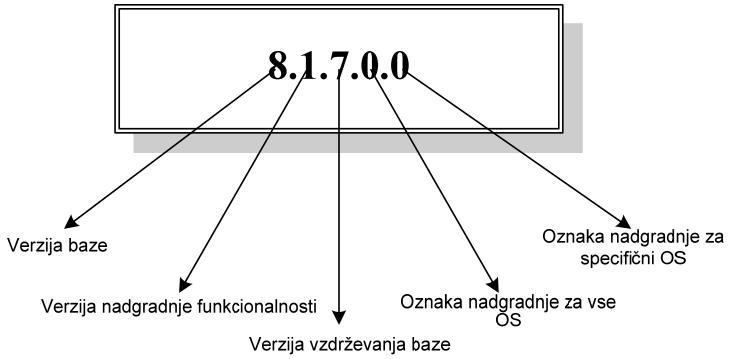
[5] Ad-hoc – poizvedovanje po potrebi.

Na podatkovnem strežniku je lahko več podatkovnih baz, zato lahko revizor v tem primeru naleti na večje število datotek, ki se med seboj razlikujejo po SID–številki (init<SID>.ora). V takšnem primeru lahko svetuje, da skrbnik baze pripravi le eno init.ora datoteko z globalnimi nastavitvami parametrov, ki jih uporablja podatkovni strežnik, in znotraj datoteke še IFILE–oznake, ki bi narekovale pot do konfiguracijskih datotek posamezne baze na tem strežniku. S tem je možnost napake pri vzdrževanju manjša, saj je v primeru sprememb konfiguracije podatkovnega strežnika skrbništvo potrebno le na enem mestu (Mookhey, 2003, str. 3).

Revizor mora na začetku svojega pregleda pridobiti informacijo o verziji podatkovne baze in komponent baze, ki jo revidira. Te informacije revizorju povedo stopnjo vgrajenih varnostnih funkcij, ki so prvotno vgrajene v bazo, in nadgradnje posameznih komponent. Revizor nato primerja nameščene verzije z verzijami in varnostnimi paketi, ki jih priporoča proizvajalec. Informacije o varnostnih paketih lahko poišče na spletni strani http://otn.oracle.com/deploy/security/alerts.htm.

Serijsko številko in nameščene komponente revizor pridobi s SQL–ukazom:
*SQL> Select * From Product_Component_Version.*

Slika 2: Rezultat poizvedbe: serijska številka v sledečem formatu



Vir: Lastni vir
Pomen oznak (Mookhey, 2003, str. 2):

- Verzija baze – številka predstavlja glavno izdajo verzije baze.
- Verzija nadgradnje funkcionalnosti – predstavlja novosti v glavni izdaji.
- Verzija vzdrževanja – predstavlja verzijo (nadgradnjo) z vidika vzdrževanja.
- Verzija nadgradnje – identificira nadgradnje programa z namenom popravljanja napak za vse operacijske sisteme, največkrat gre za varnostne izboljšave.
- Verzija nadgradnje – identificira nadgradnje programa z namenom popravljanja napak za specifičen operacijski sistem.

V nadaljevanju bom predstavil področja revidiranja Oracleove baze z vidika varnosti:

- varnostne nastavitve pri namestitvi podatkovne baze na operacijski sistem:
    - Unix in

    - Windows;
- konfiguracijski parametri v bazi;
- uporabniki in profili uporabnikov;
- vloge in pravice uporabnikov;
- varnost mrežne povezave baze;
- zagotavljanje neprekinjenosti poslovanja.

5.2 Varnostne nastavitve pri namestitvi podatkovne baze Oracle

Oracle je v minulih letih oglaševal svoj produkt kot »nezlomljiv«, kar pa se je hitro izkazalo kot neresnično, saj so bile odkrite mnoge varnostne pomanjkljivosti baze, ki jih je Oracle reševal z novimi verzijami ali nadgradnjami že obstoječih. Oracle je verzijo 9i opremil s tako imenovano varnostjo najmanjše enote, ki zagotavlja možnost revidiranja tabele na osnovi uporabnika ali posameznega polja (Finnigan, 2003, str. 2).

Varnost se nanaša predvsem na ustreznost varnostnih politik in njihove implementacije pri dostopu uporabnikov do Oraclea in podatkov, shranjenih v podatkovni bazi. Temeljno pravilo je, da lahko uporabnik dostopa le do teh podatkov in na način, ki ustreza njegovim nalogam (Javornik, 2003).

5.2.1 Namestitev Oracleove baze na operacijski sistem Unix

Namestitev Oraclea na operacijski sistem Unix kreira uporabniško ime »Oracle« in skupino »Oinstall« ter hkrati naredi skupino DBA (skrbnik baze podatkov), ki vsebuje vlogi OSDBA (skrbnik operacijskega sistem) in OSOPER. Ker se omenjene nastavitve kreirajo ob vsaki namestitvi enako, predstavljajo varnostno pomanjkljivost, če se jih ne spremeni v unikate. Nastavitve so tako splošno znane, kar povečuje verjetnost ugotovitve in s tem možnost nepooblaščenega vdora v sistem.

Priporočeno je, da podjetje ne uporablja generičnega uporabniškega računa DBA, temveč da vsak skrbnik baze uporabi unikatno ime, ki ga enolično identificira. Uporaba generičnih imen ni priporočljiva, ker ne omogoča jasne identifikacije uporabnika baze, kar pomeni, da spremembam v bazi ali podatkih ni mogoče določiti storilca (Deloitte & Touche Metodologija).

V operacijskem sistemu Unix so te informacije v datoteki /etc/group/, kjer mora revizor preveriti »umask« vrednost uporabnikov, kar mu da informacije o osebi, ki ima pravice kreiranja novih datotek in uporabnikov. Oracle priporoča, da podjetje enolično določi lastnika baze podatkov, ki mu je dodeljena »umask« vrednost 022 (Simson, Spafford, 2003, str. 119).

Pri namestitvi Oraclea je nujna stroga omejitev pravic dostopa v namestitvene datoteke, ki so v mapi ORACLE_HOME. Dostop do mape mora biti še posebno omejen, kar pomeni, da (Mookhey, 2003, str. 2):

- mora imeti uporabniški račun skrbnika vse pravice nad datotekami znotraj te mape;
- morajo imeti uporabniki skupine »Oinstall« pravice branja, pisanja in izvajanja v mapi OraInventory, v preostalih mapah pa ne smejo imeti pravic pisanja;
- vsi preostali uporabniki ne smejo imeti pravic pisanja v teh datotekah.

Zgoraj omenjeno predstavlja minimalne varnostne nastavitve v mapi ORACLE_HOME, ki morajo biti izpolnjene, revizor pa lahko predlaga implementacijo strožjih varnostnih kontrol (Mookhey, 2003, str. 2):

- uporabniški račun »Oracle«, ki je bil ustvarjen pri namestitvi baze, ne sme imeti pravic dostopa po končani namestitvi – uporabniški račun naj bi bil zaklenjen;
- pri namestitvi naj se ustvari skupina »Oradba«, ki se povezuje na OSDBA, pod katero naj se ustvari vse uporabniške račune skrbnikov;
- pravica pisanja naj bo v skupini »Oradba« odvzeta v datotekah $ORACLE_HOME/rdbms/log in $ORACLE_HOME/rdbms/audit, kar preprečuje možnost spreminjanja datotek, ki zagotavljajo revizijsko sled;
- odvzem vseh pravic nad datotekami:
    - Listner.ora $ORACLE_HOME/network/admin – nastavitve mrežnih povezav in dostopov,
    - $ORACLE_HOME/dbs/orapw<SID> – datoteka, kjer so gesla za oddaljeno skrbništvo (Remote Administration),
    - Snmp*.ora datoteka $ORACLE_HOME/network/admin_directory – nastavitve mrežnih povezav in dostopov.

5.2.2 Namestitev Oracleove baze na operacijski sistem Windows

Oracle mora biti nameščen pod uporabniškim računom, ki pripada skupini skrbnikov in za katerega je priporočljivo spremeniti vgrajeno ime »Oracle«. Enako kot pri namestitvi na sistem Unix, morajo biti tudi tukaj uporabniški računi vseh skrbnikov enolično določeni, tako da je identifikacija uporabnika – skrbnika mogoča. Vsi računi skrbnikov morajo biti v skupini ORA_DBA.

Lastnik vseh datotek, ki so v mapi ORACLE_HOME, mora biti le ena oseba, ki jo organizacija določi za lastnika podatkov. Dostop do omenjene mape mora biti strogo omejen. To revizor preveri z desnim klikom na mapo ORACLE_HOME, kjer izbere opcijo »lastnosti – varnost – dovoljenja – napredno«. Skupina ORA_DBA mora imeti vsa dovoljenja, medtem ko uporabniški račun »kdorkoli« (Everyone) ne sme imeti nikakršnih pravic.

Oracle priporoča, da na strežniku Windows, kjer stoji Oracle, ni nameščenih drugih aplikacij in da je dostop do administracije strežnika omejen le na skrbnike baze (Mookhey, 2003, str. 3).

5.3 Nastavitve konfiguracijskih parametrov v bazi

Konfiguracijski parametri za Oracleove baze so shranjeni v datoteki <SID>.ora, ki jev mapi $ORACLE_HOME/admin/<SID>/pfile. Zaradi velikega števila parametrov, ki so na voljo v tej datoteki, je z vidika revizije smiselno preučevanje le dela parametrov, do katerih najlažje dostopimo z izvedbo naslednje SQL–procedure:

select name, value, description from v$parameter where NAME in ('O7_DICTIONARY_ACCESSIBILITY', 'audit_trail', 'db_name', 'dblink_encrypt_login', 'instance_name', 'log_archive_start', 'os_authent_prefix', 'os_roles', ' 'processes ', 'remote_login_passwordfile', 'remote_os_authent', 'remote_os_roles', 'resource_limit', 'sessions ', 'sql92_security', 'utl_file_dir')
(Mookhey, 2003, str. 6).

V spodnji tabeli so podrobneje predstavljeni parametri in njihov vpliv na varnost baze.

Tabela 1: Obrazložitev predlaganih vrednosti parametrov.

IME	OPIS	OBRAZLOŽITVE PREDLAGANIH VREDNOSTI SPREMENLJIVKE
O7_DICTIONARY_ACCESSIBILITY	Verzija 7, podpora dostopu do slovarja	Uporabniki s privilegijem dostopa ANY (vsi) imajo omogočen dostop do objektov (tabel, poročil, sprožilnikov) v SYS–shemi. Ker gre za zelo kritične objekte z občutljivimi informacijami, je bolje onemogočiti dostop do teh informacij, kljub privilegiju ANY, tako da vrednost spremenljivke nastavimo na FALSE. Pod nobenim pogojem ni priporočljivo, da ima vrednost TRUE.
Audit_trail	Omogoča revizijo sistema	Da omogočimo shranjevanje revizijskih sledi, moramo parametru AUDIT_TRAIL nastaviti spremenljivko na DB. To bo sprožilo avtomatsko proizvajanje revizijskih sledi, ki se bodo shranile v bazo.
db_name	Ime baze	Gre le za informacijo, ki pove ime baze podatkov.
dblink_encrypt_login	Vsiljevanje kriptiranih gesel za oddaljeno prijavo v bazo	Če je ta parameter nastavljen na TRUE in povezava na bazo ne uspe, je Oracle ne poskuša ponoviti. Če pa je nastavljen na FALSE, pa v primeru neuspele povezave Oracle poskuša spet vzpostaviti povezavo, tokrat s pošiljanjem nešifriranega gesla.
Log_archive_start	Zagon procesa arhiviranja na SGA	Omogoča avtomatsko shranjevanje skupin (Filled Groups) pri vsakem zagonu baze. Za zagon arhiviranja »log« podatkov je treba parameter nastaviti na TRUE.
os_authen_prefix	Uporaba identifikacije na operacijskem sistemu (OS)	Če je dostop do baze omogočen z avtentikacijo uporabnika na nivoju operacijskega sistema, je to razvidno iz uporabniškega imena. Privzeta vrednost parametra je OPS$, kar pomeni, da je ime, npr. uporabnik z uporabniškim imenom joze_novak, v bazi shranjeno kot OPS$joze_novak.

os_roles	Prikaže vloge – pravice na OS	Če želimo, da baza uporabi vloge (role) – pravice, dodeljene ob prijavi v operacijski sistem, mora biti parameter postavljen na TRUE. Ko se poskuša uporabnik prijaviti v bazo, ta uporabi domeno uporabnika na OS za določitev pravic dostopa v bazo.
processes	Uporabniški procesi	Parameter, ki določi maksimalno število procesov na posameznem operacijskem sistemu, hkrati povezanih v isto bazo. Vrednost parametra mora vsebovati 5 procesov, ki tečejo v ozadju (Background Process), in enega za posameznega uporabnika. Če je v bazi hkrati 50 uporabnikov, mora biti to število 55.
remote_login_passwordfile	Uporaba datoteke za gesla	Ta parameter pove Oracleu, ali naj preveri avtentikacijo uporabnika iz datoteke »Orapwd« ali iz tabele »SYS.USERS$«. To se največkrat uporablja za oddaljen dostop. Priporočena vrednost spremenljivke je NONE, ki ne dovoljuje tega dostopa. Drugi vrednosti sta še EXLUSIV (dostop dovoljen eni instanci) in SHARED (dostop dovoljen mnogim instancam).
Remote_os_authent	Uporaba avtentikacije na OS za oddaljene prijave	Zelo priporočljivo je, da je ta parameter nastavljen na FALSE. Z nastavitvijo TRUE je oddaljenemu uporabniku, ki je avtoriziran na svojem OS, omogočeno, da se brez vpisovanja gesla prijavi v bazo.
Remote_os_roles	Uporaba pravic avtentikacije OS za oddaljen pristop	Parameter mora biti nastavljen na FALSE, kar pomeni, da onemogoča oddaljen dostop neavtoriziranim uporabnikom, ki bi za dostop do baze uporabili avtentikacijo na svojem OS.
Sessions	Seje uporabnika in OS	Parameter pove maksimalno število sej, ki so hkrati lahko povezane v bazo.
Sql92_security	Dovoljen SELECT za spreminjanje in brisanje	Standard SQL92 (SQL3) dovoljuje dodelitev privilegijev SELECT uporabniku, ko se ti uporabljajo za brisanje ali spreminjanje podatkov v bazi. Uporaba je dovoljena le v stavkih SET ali WHERE, da se sklicuje na spreminjanje ali brisanje le določene vrstice.
utf_file_package	Dovoljenja na paketih UTL_FILE	Paketi UTL_FILE dovoljujejo Oracleovim uporabnikom pravici branja in pisanja na gostujočem OS. Dostop do paketa UTL_FILE mora biti strogo prepovedan.
utf_file_dir	Mape, do katerih paket UTL_FILE lahko dostopa	UTL_FILE dovoljuje Oracleu pravici branja in pisanja datotek na gostujočem operacijskem sistemu. Parameter ne sme biti nastavljen na vrednost *, kar pomeni, da ima paket UTL_FILE pravici branja in pisanja v vseh mapah. Na napakah, kjer se izvaja proceduralni jezik PL/SQL, mora biti onemogočena pravica pisanja (WRITE).

Theriault, Heney, 1998, str. 279

Primer datoteke init.ora z nastavitvami vrednosti konfiguracijskih parametrov je v Prilogi 2.

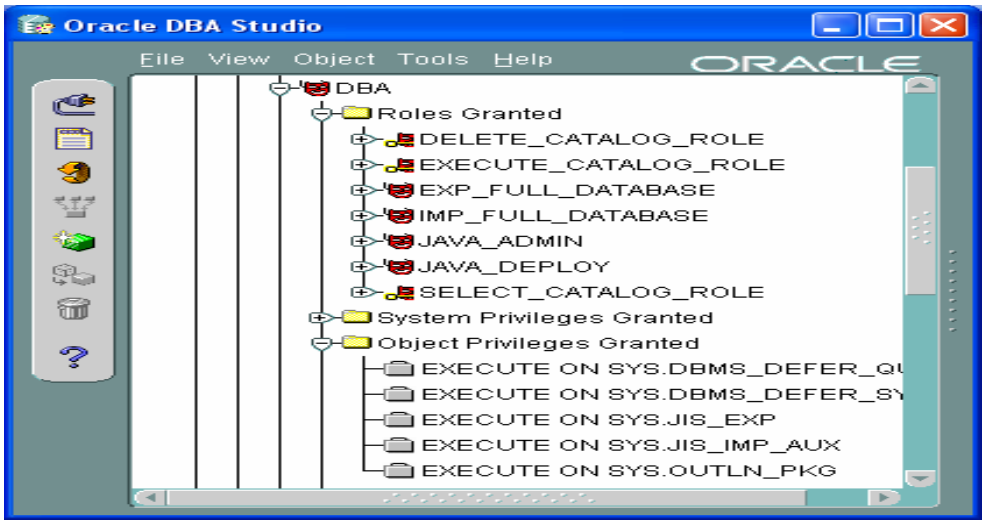
5.4 Uporabniki in njihovi profili

Za pridobitev informacij o uporabnikih in njihovih profilih mora imeti revizor dostop do poročil v SYS–shemi (Mookhey, 2003, str. 3):

1. DBA <ime_poročila>: poročilo, namenjeno skrbnikom baze podatkov – vse informacije;
2. ALL <ime_poročila>: poročilo priskrbi vse informacije razen najobčutljivejših;
3. USER <ime_poročila>: informacije o trenutno prijavljenem uporabniku.

Za pridobitev vseh potrebnih informacij si revizor lahko pomaga z orodjem Oracle DBA studio, ki mu omogoča poglede v dodeljene privilegije uporabnikov.

Slika 3: Grafični vmesnik omenjenega orodja



Vir: Javornik, 2003a

Prva naloga revizorja pri preverjanju uporabniških računov je preveriti, ali so vsi primarno vgrajeni uporabniški računi odstranjeni, razen če obstaja utemeljen razlog ohranitve. Ohranitev vgrajenih uporabniških računov za organizacijo predstavlja varnostne pomanjkljivosti, saj se večina poskusov napada začne z ugibanjem kombinacij uporabniškega imena in gesla, ki so javno znana. V spodnji tabeli je prikazanih nekaj vgrajenih uporabniških računov in njihovih namenov vgraditve. Revizor dostopa do teh podatkov z izvedbo naslednje SQL–procedure:

SQL>Select Username, Password, Account_Status, Default_Tablespace, Profile from DBA_USERS
(Mookhey, 2003, str. 8).

Tabela 2: Predstavitev primarno vgrajenih uporabniških računov

UPORABNIŠKO IME	GESLO	NAMEN VGRADITVE	PRIPOROČLJIV UKREP
SYS	CHANGE_ON_INSTALL	Račun z največ pravicami; te dovoljujejo dostop do vseh objektov, ki tvorijo bazo	Zaklenitev računa
SYSTEM	MANAGER	Račun, ki se uporablja za kreiranje objektov	Menjava gesla
SCOTT	TIGER	Uporablja se za učenje SQL–jezika in testiranja mrežnih povezav baze	Odstranitev računa
DBSNMP	DBSNMP	Uporabljen za upravljanje baze na daljavo	Odstranitev računa ali sprememba gesla
TRACESVR	TRACE	Uporabljen za zbiranje informacij o učinkovitosti in uporabi virov	Menjava gesla
DEMO	DEMO	Uporaba je namenjena predstavitvi produkta	Odstranitev računa
ADAMS	WOOD	Namenjen učenju pravnih transakcij	Odstranitev računa
MTSYS	MTSYS	Podpira uporabo »Microsoft Transaction Server« in Microsoftovih demo aplikacij	Odstranitev računa
SAP	SAPR3	Uporabljen, če organizacija uporablja SAP–rešitev	Menjava gesla ali odstranitev

Mookhey, 2003, str. 8

V zgornji tabeli je predstavljenih le nekaj uporabniških računov, ki predstavljajo varnostne pomanjkljivosti v primeru neprimernega upravljanja in nastavitve baze.

Verzija 8i ali starejše vsebujejo funkcijo direktnega povezovanja v bazo »Connect Internal«, kamor se uporabnik poveže z geslom ORACLE in s tem pridobi pravice, ki mu omogočajo zagon ali zaustavitev delovanja baze. V poznejših verzijah je ta funkcija odstranjena, saj je predstavljala veliko varnostno pomanjkljivost. Pri revidiranju Oracleove baze verzije 8i ali nižjih revizor preveri obstoj te funkcije in spremembo gesla z uporabo naslednjega SQL–ukaza:

SQL>connect internal/oracle
(Mookhey, 2003, str. 9).

5.4.1 Profili uporabnikov

V zvezi z dostopi uporabnikov je treba oceniti, ali je implementirana politika gesel primerna in velja tako za lokalne uporabnike, pri katerih dostop preverja in dovoljuje Oracle, kot tudi za tiste, pri katerih Oracle zaupa preverjanje in dovoljevanje dostopa zunanjemu okolju: OS ali namenski programski opremi (KERBEROS, RADIUS) in

uporabnikom, ki dostopijo z oddaljenih lokacij. Implementacije politike gesel (glede dolžine, kompleksnosti, ponovljivosti, trajanja in zaklepanja) so v Oracleu (od verzije 8 dalje) izvedljive prek profilov uporabnikov (Javornik, 2003, str. 6).

Ob namestitvi Oracle kreira privzet profil uporabnika (DEFAULT), ki ne izpolnjuje praktično nobene restriktivne politike, če se ne spremeni njegovih parametrov, do katerih lahko revizor dostopi z izvedbo naslednje SQL–procedure:

*SQL>Select * from DBA_PROFILES*

(Mookhey, 2003, str. 9).

Rezultat poizvedbe so parametri profila in njihove vrednosti. Primarna skrb revizorja je preveriti spremembe parametrov glede na vrednosti, nastavljene pri namestitvi – privzetem profilu, preveriti pooblastila in privilegije ter njihovo skladnost s postavljenimi varnostnimi politikami in splošnimi standardi (npr: ISO 17799) (Javornik, 2003, str. 6).

V prvem delu tabele so predstavljeni parametri, ki se nanašajo na nastavitve gesel, kratek opis pomena parametrov ter privzeta in priporočena vrednost. Drugi del tabele pa opisuje omenjene nastavitve na nivoju »Kernel«[6] sistema.

Tabela 3: Nastavitve gesel

PARAMETER	OPIS	PRIVZETA VREDNOST	PRIPOROČENA VREDNOST
FAILED_LOGIN_ATTEMPTS	Število dovoljenih napak pri vnosu gesla, preden se uporabniški račun zaklene	Neomejena	Priporočeno 3, maksimalno dovoljeno 6
PASSWORD_LOCK_TIME	Čas, ko je uporabniški račun zaklenjen, preden se avtomatsko odklene	Neomejena	0.0006
PASSWORD_LIFE_TIME	Število dni veljavnosti gesla – po preteku obdobja geslo postane neveljavno	Neomejena	Tako, kot je določeno v politiki gesel – priporočljivo 30–60 dni
PASSWORD_GRACE_TIME	Čas (pred iztekom gesla), v katerem morajo uporabniki spremeniti geslo	Neomejena	10 dni
PASSWORD_REUSE_TIME	Število dni, ki morajo preteči, preden je enako geslo lahko spet uporabljeno	Neomejena	1800 sekund
PASSWORD_VERIFY_FUNCTION	Uporaba dodatne funkcije preverjanja kompleksnosti gesla; Oracle ima vgrajeno funkcijo (utlpwdmg.sql), ki preverja kompleksnost	NULL	VERIFY_FUNCTION (uporaba Oracleove ali svoje kode)

[6] Kernel – glavna enota računalniškega sistema, ki se shrani v glavni spomin sistema.

Tabela 4: Nastavitve na Kernel sistemu

PARAMETER	OPIS	PRIPOROČENA VREDNOST
SESSION_PER_USER	Določa število sej, ki jih uporabnik lahko vzpostavi brez prekinitve prejšnjih sej	1
CPU_PER_SESSION	Določa maksimalen čas CPU, dovoljen znotraj posamezne seje	1.000.000 sekund
CPU_PER_CALL	Določa maksimalen čas CPU, dovoljen za posamezen klic/povezavo v sistem	1.000.000 sekund
IDLE_TIME	Maksimalen dovoljen čas nedejavnosti znotraj določene seje	15
CONNECT_TIME	Maksimalen dovoljen čas povezave seje, namenjen prekinitvi povezave, če se uporabnik ne odjavi iz sistem	90 minut

Theriault, Heney, 1998, str. 352

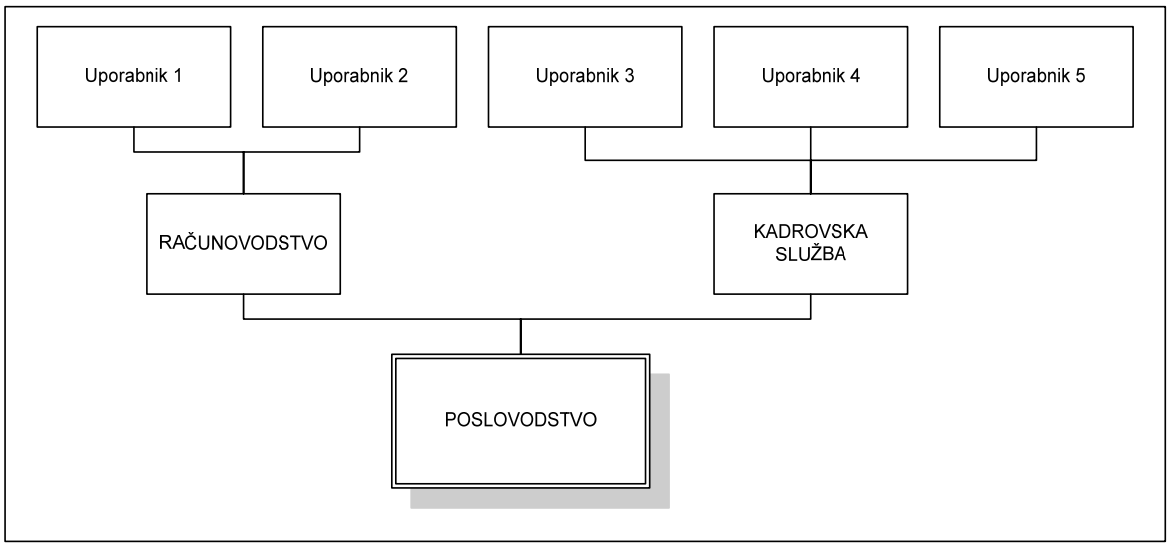
Oracle ima kodo (utlpwdmg.sql), v katero so vgrajeni priporočeni parametri. Organizacija ima tako izbiro uporabiti Oracleovo kodo in se zadovoljiti z varnostnimi nastavitvami, priporočenimi s strani Oracla, ali svojo kodo. Večina organizacij ima svojo varnostno politiko in politiko gesel, ki se razlikuje od priporočene dobre prakse, zato mora spremeniti vrednosti zgoraj opisanih parametrov glede na svoje potrebe (Mookhey, 2003, str. 10).

5.5 Vloge in pravice uporabnikov

Oracle ponuja možnost določanja pravic dostopa direktno uporabniku ali posamezni skupini (role) uporabnikov, kar prinaša velike prednosti pri administraciji uporabnikov. Uporabo bom opisal v spodnjem primeru v povezavi s pripadajočo skico.

Namesto da bi določili enake pravice dostopa vsakemu od zaposlenih v računovodstvu posebej, lahko skrbnik kreira skupino »Računovodstvo«, ji dodeli pravice dostopa, nato pa vse zaposlene na tem oddelku, ki naj bi imeli enake pravice dostopa, poveže v prej omenjeno skupino. Možna je tudi uporaba višjega nivoja združevanja, saj lahko del pravic dostopa, ki so skupne mnogim skupinam (npr: menedžmentu), shrani v novo skupino in ji pozneje dodeli vse pripadajoče podskupine, v katere so dodeljeni končni uporabniki.

Slika 4: Prikaz zgoraj opisanega primera združevanja skupin



Vir: Lastni vir

Prvotna naloga revizorja je preveriti skladnost dodeljenih uporabniških pravic z varnostno politiko organizacije. Revizor primerja skladnost informacij, pridobljenih iz popisa delovnih mest, kjer so naloge in pravice zaposlenih, z varnostno politiko organizacije. Ažurnost liste zaposlenih in njihovih dostopov je nujen dokument, ki ga revizor uporabi pri pregledu uporabnikov. Še posebno mora biti pozoren na tiste uporabnike, ki so zapustili organizacijo oziroma so odsotni dalj časa. Dostop do uporabniškega računa mora biti primerno zaščiten – za tiste, ki so zapustili organizacijo, pa onemogočen.

Pri nadaljnjem pregledu pravic posameznikov in skupin mora pozornost posvetiti skupinama RESOURCE in CONNECT. Prva omogoča uporabniku ustvarjanje programskih procedur in sprožilcev, medtem ko druga dovoljuje kritične privilegije ustvarjanja tabel (CREATE TABLE) in povezav (CREATE DATABASE LINK) ter omogoča povezavo v bazo. Namesto uporabe vloge CONNECT je z vidika varnosti priporočljivejša uporaba pravice SESSION (seja), ki končnemu uporabniku dovoli le začasen dostop in po poteku seje prekine povezavo z bazo (Theriault, Heney, 1998, str. 422).

Do informacij o uporabi omenjenih skupin in pravic revizor dostopi z naslednjo poizvedbo:

- za skupino RESOURCE:

*SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='RESOURCE';*

- za skupino CONNECT:

*SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='CONNECT'*

(Mookhey, 2003, str. 12).

Privilegiji se dodajajo uporabniku ali skupini z ukazom GRANT, odvzamejo pa z ukazom REVOKE.

Tabela 5: Prikaz vgrajenih privilegijev

Privilegij	Avtorizacija
Select	Prebere podatke iz tabele
Update	Spreminja podatke v tabeli
Insert	Dodaja nove podatke v tabelo
Delete	Briše podatke iz tabele
Execute	Izvaja ukaze funkcije ali procedure
Alter	Spreminja vrednosti parametrov
Read	Bere podatke iz datotečnega sistema
Reference	Naredi povezave, referenco na tabelo
Index	Naredi kazalo (index) na tabelo

(Mookhey, 2003, str. 12)

Pri pregledovanju pravic dostopa uporabnikov in skupin mora revizor pregledati dostop do skupine PUBLIC (javno), ki je vgrajena v Oracle in avtomatsko dodeli vsakega novega uporabnika tej skupini, če to ni posebej določeno. Omenjena skupina dovoljuje uporabniku dostop do kritičnih informacij, ki so v bazi, zato je zelo priporočljiva odstranitev vseh privilegijev in uporabnikov, ki ji pripadajo. Do teh informacij revizor lahko dostopi z SQL–ukazom:

*SQL>Select * from DBA_TAB_PRIVS where GRANTEE='PUBLIC'*
*SQL>Select * from DBA_SYS_PRIVS where GRANTEE='PUBLIC'*
*SQL>Select * from DBA_ROLES_PRIVS where GRANTEE='PUBLIC'*

Čeprav večina uporabnikov dostopa do podatkov z uporabo aplikacij, ki imajo vgrajene varnostne mehanizme dostopa do podatkov, obstaja nevarnost, da končni uporabnik z uporabo orodij, kot je SQL*PLUS, poskuša pridobiti podatke s svojimi SQL–ukazi, s katerimi bi brez omejitve privilegijev lahko dostopil do zaupnih podatkov, shranjenih v podatkovni bazi (Knox, 2004, str. 355).

5.6 Revizijske sledi

Oracle izdatno podpira tvorbo revizijskih sledi. Te lahko nastanejo ob izvedbi ukaza, uporabi sistemskega privilegija, na nivoju objekta ali za konkretnega uporabnika. Beleži se lahko tako uspešne kot neuspešne izvedbe. Revizijske sledi se lahko hranijo v bazi (SYS.AUD$) ali pa na nivoju datotečnega sistema zunaj baze, odvisno od nastavitev vrednosti parametra AUDIT_TRAIL v datoteki init.ora (DB – shrani v bazo, OS – shrani v datotečni sistem) (Mookhey, 2003, str. 16).

Posebno pozornost je treba posvetiti konfiguraciji beleženja sledi v »three–tier« konfiguracijah, ko do baze dostopa aplikacijski strežnik v imenu različnih uporabnikov. Od verzije 8i dalje lahko sled vsebuje tako uporabnika, ki je prijavljen (middle–tier), kot tudi uporabnika, v čigar imenu dostopa (klient, končni uporabnik). Za dodatno tvorbo revizijskih sledi in alarmiranje se lahko izkoristijo tudi sprožilniki.

Izdatno tvorjenje revizijskih sledi negativno vpliva na odzivnost in hitrost procesiranja baze, zato je pri odločitvi o tvorbi revizijskih sledi potrebna posebna previdnost. Tvorile naj bi se le tiste revizijske sledi, ki jih predvidevajo varnostni ukrepi, izpeljani iz varnostne politike. Revizor je ena od oseb, ki so ji revizijske sledi namenjene.

Poleg pregleda sledi, ki mu pomagajo restavrirati dogajanje v sistemu, je naloga revizorja tudi, da oceni primernost in zadostnost tvorjenja revizijskih sledi predvsem v luči zagotavljanja varnosti. Ugotoviti pa mora še, ali je revizijskim sledem posvečena zadostna pozornost za arhiviranje, brisanje in pregledovanje ter ali posegi uporabnikov s posebnimi pooblastili (skrbniki) puščajo sledi, ki jih za sabo ne morejo odstraniti (Javornik, 2003, str. 8).

5.6.1 Slabosti funkcionalnosti zagotavljanja revizijskih sledi

Kompleksnost revizijskih sledi v Oracleu predstavlja eno izmed večjih slabosti baze, ki v praksi privedejo do nižjega nivoja uporabnosti informacij. Gre predvsem za zapletene nastavitve, ki zahtevajo veliko strokovnega znanja in stroškov. Slabosti so naslednje (Nelson, 2003, str. 3):

- Pripravljena poročila – Oracle nima vgrajene funkcionalnosti, ki bi avtomatsko pripravila poročila. Za dostop do podatkov je potrebna »ad–hoc« SQL–poizvedba za vsako posamezno tabelo.
- Slaba normaliziranost podatkov – Podatki so shranjeni v nenormalizirani obliki, kar otežuje pripravo poročil po različnih sortnih kriterijih. Ker gre za zapletene poizvedbe, morajo biti večinoma pripravljene s strani izkušenih programerjev. Težavo predstavljajo poizvedbe nad tabelami z nastavitvami, kjer je nujna uporaba SQL–ukazov združevanja (UNION, OUTHER JOIN …).
- Pomanjkanje varnosti dostopa do revizijskih sledi – Oracle ima slabo varovan dostop do specifičnih revizijskih sledi. Z višjezahtevnimi poizvedbami je omogočen dostop do kritičnih revizijskih sledi.
- Potreba po programiranju poročil – Za pridobitev poročil, pripravljenih iz revizijskih sledi, je potrebno dodatno programiranje.
- Učinkovitost (odzivnost in hitrost procesiranja) baze – Poizvedbe, potrebne za pripravo poročil, ki temeljijo na podatkih iz revizijskih sledi, vsakič znova analizirajo vse podatke, shranjene v revizijskih sledeh, kar negativno vpliva na učinkovitost baze.

- Uporabniku neprijazen postopek transformacije podatkov – Podatki, ki so v revizijskih sledeh, so shranjeni v nestrukturirani obliki, zato predstavlja pomanjkanje aplikativne podpore za izdelavo poročil veliko pomanjkljivost.

5.7 Varnost mrežne povezave baze

Od verzije 8i dalje je varnost mrežnih povezav z bazo izboljšana z implementacijo funkcije »napredne varnosti«, kar zagotavlja šifriranje prenosa vseh podatkov v času povezave odjemalcem na strežnik (Client–Server). Uvedba šifriranja je še posebno pomembna pri dostopu do baze zunaj lokalnega omrežja (LAN[7]), saj omogoča zaščito nad (Mookhey, 2003, str. 17):

- povezavo – napadalec izkoristi povezavo z bazo,
- vohljanjem – napadalec pride do podatkov, ki se prenašajo v omrežju, in
- zaščito celovitosti – napadalec spremeni podatke, ki se prenašajo v omrežju.

Do nastavitev, ki zagotavljajo napredno varnost, revizor dostopi z uporabo Net8 konfiguracijskega agenta prek poti (Mookhey, 2003, str. 17):

- Windows – administracija omrežja/Net8 asistent ali
- Unix – mapa $ORACLE_HOME/bin/netasst.

Nastavitve, ki jih lahko uporabi, so naslednje:

- avtentikacija (dokaz pristnosti) – preveri, ali je parameter nastavljen na vrednost Kerberos, RADIUS, NTS, SecurID, CyberSafe ali Identix,
- celovitost – MD5 ali SHA1,
- šifriranje – vključitev/izključitev opcije šifriranja (izključena le v primeru posebne zahteve),
- SSL – protokol, ki zagotavlja šifriranje podatkov med prenosom v času vzpostavljene seje (CISA Review Manual, 2005, str. 265) – revizor mora preveriti veljavnost certifikata (CA[8]) (Mookhey, 2003, str. 17).

5.8 Zagotavljanje neprekinjenosti poslovanja

Informacije so eden od ključnih dejavnikov, potrebnih za delovanje organizacije. Glede na veliko povezanost poslovanja z delovanjem IS je nerealno pričakovati daljše delovanje poslovnega sistema brez zagotovljenega delovanja IS. Moderno poslovanje se ne more izogniti tveganjem, ki prežijo nad organizacijo. Namen zagotavljanja neprekinjenosti poslovanja je preživetje in zmožnost nadaljnjega poslovanja po katastrofi (Mookhey, 2003, str. 16).

V primeru katastrofe lahko organizacija utrpi naslednje posledice:

- nezmožnost nadaljevanja poslovanja,
- izguba prihodkov,

[7] LAN – Local Area Network – lokalno omrežje.
[8] CA – Certified Authority –organizacija, pooblaščena za izdajo, vzdrževanje in preklic digitalnih certifikatov

- izguba konkurenčne prednosti,
- izguba zaupanja v podjetje in
- sankcije.

Organizacija mora izdelati natančno analizo tveganj, kjer identificira področja tveganja in na podlagi rezultatov analize določi dejavnosti, ki bi zmanjšale izgube v primeru katastrofe. Stroški predlaganih rešitev ne smejo presegati koristi rešitve. Neprekinjenost poslovanja zajema področja celotnega poslovanja, pri čemer je največja pozornost namenjena reševanju ljudi in podatkov. V naslednjih dveh točkah bom opisal le pomembnosti, ki se navezujejo na varnost podatkovne baze (Mookhey, 2003, str. 16).

5.8.1 Zagotavljanje fizične zaščite

Zagotavljanje fizične zaščite je z vidika baz podatkov povezano na nivoju zaščite prostora, kjer je strežnik, na katerem je nameščena baza podatkov. Priporočila pri zagotavljanju fizične zaščite so:

- zaščita na dveh nivojih — z uporabo magnetne identifikacijske kartice (kar imaš) in PIN–kode (kar veš),
- primerna zaščita prostora pred nesrečami, kot so požar (senzor za dim in temperaturo), poplave (strežniki so dvignjeni od tal) in napake na električnem omrežju (priporočena uporaba UPS[9] in generatorjev),
- nadzor sistemske sobe in povezava z varnostnokomunikacijskim centrom (Mookhey, 2003, str. 16).

5.8.2 Zagotavljanje varnostnih kopij in okrevanja

Organizacija, ki ima poslovanje podprto z računalniško tehnologijo, mora zagotavljati neprekinjenost poslovanja. Ta je lahko dosežena s podvojenostjo kapacitet na različnih lokacijah, podvojenim procesiranjem, podvojenimi komunikacijami in podvojenim hranjenjem podatkov (Andolšek, Javornik, 2001, str. 1).

Zaradi nevarnosti, ki prežijo na informacijski sistem (naravne katastrofe, človeške napake, napake strojne ali programske opreme), mora organizacija skrbeti za primerno in pravočasno izdelavo varnostnih kopij, ki bi omogočale obnovitev podatkov v stanje pred prekinitvijo/katastrofo. S pravo frekvenco in obsegom arhiviranja si mora zagotoviti povrnitev prvotnega stanja sistema in podatkov. Točke, ki se navezujejo na revizijo podatkovne baze z vidika zagotavljanja varnostnih kopij podatkov, so:

- obstoj primerne varnostne kopije (obseg in frekvenca arhiviranja),
- primerno določene odgovornosti in naloge oseb, odgovornih za varnostne kopije,
- beleženje izdelave varnostnih kopij,
- frekvenca rotiranja trakov – nevarnost izbrisa nearhiviranih podatkov,
- zaščita prostora, kjer so shranjeni trakovi z varnostnimi kopijami,
- obstoj zunanje lokacije, kamor se shranjuje trake z varnostnimi kopijami,

[9] UPS – Uninterruptible Power Supply - vir energije v primeru izpada električne energije

- obstoj testiranja trakov varnostnih kopij,
- kompatibilnost informacijske opreme z varnostnimi kopijami,
- vsebina shranjena na trakove in
- ažurnost načrta okrevanja (CISA Review Manual, 2005, str. 336).

V planu za neprekinjeno poslovanje morajo biti opredeljene kritične in vitalne poslovne funkcije. Slednje morajo biti zaščitene pred večjimi nesrečami in katastrofami. Kritičnost poslovnih funkcij se določi na podlagi analize tveganj, ki vključuje po prioriteti razvrščene kritične sisteme v skladu s časovno občutljivostjo, kritičnostjo in neobhodno potrebo za nadaljevanje poslovanja, ki sledi nesreči (Andolšek, Javornik, 2001, str. 2).

6 Sklep

Prihod novih tehnologij je povzročil spremembe tudi na področju revizije, saj je večina informacij, potrebnih za izvedbo revizije računovodskih izkazov, v informacijskih sistemih organizacije. Naloga revizorja informacijskih sistemov je oceniti varnost sistema in primernost vanj vgrajenih notranjih kontrol, saj je to pomembno pri zanašanju na pravilnost podatkov, pridobljenih iz sistema. V tem delu gre za revizijo informacijskih sistemov kot podporno vejo revizije računovodskih izkazov, ki potrebuje mnenje o ustreznosti delovanja notranjih kontrol sistema. Revizijo informacijskih sistemov pa lahko obravnavamo tudi povsem ločeno, kjer je namen ugotoviti pravilnost procesov, ki jih podpira sistem z vidika zagotavljanja celovitosti, zaupnosti, razpoložljivosti, skladnosti in zanesljivosti informacij.

Implementacija informacijskega sistema zahteva vrsto postopkov, ki morajo biti izpolnjeni v pravilnem časovnem zaporedju s strani visokokvalificiranih strokovnjakov, da sistem pozneje prinaša dodano vrednost organizaciji. Naloga poslovodstva je zagotoviti ustrezno raven kontrol. Te bodo zmanjšale tveganja, ki se pojavljajo pri poslovanju in izhajajo iz zunanjega ali notranjega okolja organizacije. Novejši informacijski sistemi imajo vgrajene funkcionalnosti, ki ob pravilnih nastavitvah omogočajo zanesljivo delovanje v informacijski sistem vgrajenih notranjih kontrol. Ker prevelik obseg notranjih kontrol znižuje učinkovitost organizacije, saj v veliki meri zahteva dodatno preverjanje, je odvisno od organizacije same, kakšno stopnjo kontrol želi implementirati. Poslovodstvo mora pretehtati stroške implementacije sistema notranjih kontrol v primerjavi z njegovimi koristmi, ki se lahko odražajo v finančnih rezultatih ali zagotavljajo višjo stopnjo varnosti.

Varnost podatkov je odvisna od mnogih elementov, ki tvorijo celoten sistem. Poglavitni del informacijskega sistema je zagotovo podatkovna baza, kjer so shranjeni podatki organizacije, katere poslovni proces poteka ob pomoči informacijskega sistema. Organizacija mora tako varnost svojih podatkov – baze podatkov zagotoviti na vseh nivojih, kjer je možen dostop do njih, na fizičnem in logičnem nivoju. Fizični nivo zaščite

se v prvi meri nanaša na varnost strežnikov v sistemski sobi, kjer stoji podatkovna baza, torej zaščita dostopa do sistemske sobe, medtem ko predstavlja logični nivo zaščite predvsem omejitve pri razpolaganju s podatki in pravicami dostopa do njih.

Glede na tendenco naraščanja števila prevar v organizaciji in nepooblaščenih vdorov v informacijski sistem bodo morale organizacije vse več sredstev nameniti področjem, ki bodo zagotavljala večje stopnje zaščite. Informacijski sistem sicer lahko v danem trenutku zagotavlja visoko stopnjo varnosti, kar pa ob hitrem razvoju tehnologije zagotovo ne velja na dolgi rok. Poslovodstvo mora vlagati v redno nadziranje delovanja sistema, vzdrževanje in nadgradnje, posebno ko se nanašajo na varnost sistema, ter slediti standardom, smernicam razvoja in dobrim praksam.

Vse omenjeno bo v prihodnosti še povečalo vlogo revizorja informacijskih sistemov, ki naj bi z rednimi pregledi ugotovil trenutno stanje sistema in njegove pomanjkljivosti ter na podlagi ugotovitev svetoval organizaciji o potrebnih izboljšavah sistema ali vzpostavitvi dodatnih notranjih kontrol, ki bi povečale varnost poslovanja.

Literatura

1. Brečko Vlasta: Sistem notranjih kontrol. Gradivo za izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor. Ljubljana : Slovenski inštitut za revizijo, 2001. 15 str.
2. Brumen Boštjan, Welzer Tatjana: Dostopnost in zaščita podatkov na relacijski podatkovni bazi Oracle. Uporabna informatika, Ljubljana :02(1998), 2, 39 str.
3. Damij T., J.Grad, J.Jaklič: Izbrane teme iz informacijske tehnologije. Učbenik. Ljubljana: Ekonomska fakulteta, 1995. 316 str.
4. Damij Talib: Informacijski sistemi – teorija in metodologija. Učbenik. Ljubljana : Ekonomska fakulteta, 1993. 32 str.
5. Grad Janez, Dacar France: Podatkovne strukture, osnove baze podatkov in njene uporabe. Ljubljana : Ekonomska fakulteta Borisa Kidriča, 1985. 164 str.
6. Javornik Boža: Revidiranje v okolju AOP in revidiranje kontrol delovanja informacijskega sistema. Gradivo za izobraževanje za pridobitev strokovnega naziva revizor. Ljubljana : Slovenski inštitut za revizijo, 2005, str. 43–80
7. Karnet Igor, Tajnik Franci: Pripravljalni seminar za pripravo na izpit CISA. Ljubljana : Slovenski inštitut za revizijo, 2003. 140 str.
8. Knox David: Effective Oracle Database 10g Security by Design. Electronic book. Oracle Press. California : 2004.
9. Lešnik Korbar Boža: Postopki notranjega revidiranja. Gradivo za izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor. Ljubljana : Slovenski inštitut za revizijo, 2001. 62 str.
10. Mark L. Nelsen: Providing continuous audit to Oracle applications. California: Information system control journal, 3(2000), 2, str. 28–31
11. Mookhey K. K.: Oracle Security and Auditing. India : Network Intelligence India Pvt. Ltd. 2003. 28 str.
12. Odar Marjan: Razvoj revizijske stroke in drugih strok, povezanih s kakovostjo revidiranja v Sloveniji – Revizija prinaša dodano vrednost. Zbornik referatov: 10. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo. 2002. str. 7–20.
13. Odar Marjan: Vloga revizorja na trgih kapitala. Zbornik referatov 29. simpozija o sodobnih metodah v računovodstvu in poslovnih financah. Ljubljana : Koordinacijski odbor Zveze ekonomistov Slovenije ter Zveze računovodij, finančnikov in revizorjev Slovenije, 1997. str. 349–346.
14. Oliver Derek J.: Pregledni seminar za pripravo na izpit CISA. Ljubljana : Slovenski inštitut za revizijo, 2002. 122 str.
15. Perše Zoran: Izvedba revizije informacijskih sistemov. Organizacija. Ljubljana, 33(2000), 2, str. 142–145.
16. Pete Finningan: Introduction to simple Oracle auditing. Information system control journal. USA, 2(2003), 3, str. 36-48.

17. Podgoršek, Urška, Revizijsko poročilo – kako zagotoviti vodstvu njegovo sporočilnost. 12. Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2004. str. 229–240.
18. Pohorec Damjan: Revizija informacijskih sistemov s praktičnim primerom podjetja "X". Diplomsko delo. Maribor : Ekonomsko–poslovna fakulteta, 2006. 59 str.
19. Potočnik Konrad, Franci Tajnik: Uporaba modela COBIT za načrtovanje in poročanje o njej. 11. Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2003, str. 105–123
20. Potočnik Konrad: Kaj lahko ponudi revizija uporabniških rešitev in česa ne more jamčiti?. Zbornik referatov 9. mednarodne konference o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2001, str. 153–171.
21. Rajiv Sinha: A Security Checklist for Oracle9i: An Oracle white paper. Redwood Shores, USA: 2001. 10 str.
22. Sawyer L. et al.: The Practice of Modern Internal Auditing. Altamonte Springs : The Institute of Internal Auditors, 2003. 1446 str.
23. Simson Garfinkel, Spafford Gene.: Practical UNIX & Internet Security (Druga izdaja). Electronic book. USA : O'Reilly, 1996. 984 str.
24. Skitek Mitja: Revizorjevo poročilo o kakovosti računalniškega informacijskega sistema. 33. Simpozij o sodobnih metodah v računovodstvu, financah in reviziji. Ljubljana : Zveza ekonomistov Slovenije in Zveze računovodij, finančnikov in revizorjev Slovenije, 2001, str. 289 – 309.
25. Theriault Marlene, Heney William: Oracle Security. California: O'Reilly, 1998. 446 str.
26. Turk Ivan et al.: Notranje revidiranje poslovanja. Ljubljana : Slovenski inštitut za revizijo in Zveza računovodij, finančnikov in revizorjev, 1994. 282 str.
27. Turk Ivan: Pojmovnik računovodstva, financ in revizije. Ljubljana : Zveza računovodij, finančnikov in revizorjev Slovenije, 2000. 1082 str.
28. Vrešnik Čemas Nina: Posebnosti revizije računalniško podprtih informacijskih sistemov v borzno posredniških družbah. Magistrsko delo. Maribor : Ekonomsko–poslovna fakulteta. 2002. 121 str.

Viri

1. Andolšek Irena, Javornik Boža: Pomembnost plana za neprekinjeno poslovanje za organizacije. [URL:www.drustvo–informatika.si/dogodki/arhiv/dsi2001/sekcija_d/andolsek_javornik.doc], 1.7.2006.
2. CISA Review Manual 2005/2003/2000. Information system audit and control association (ISACA) USA, 2005. 559 str.
3. COBIT–Governance, Control and Audit for Information and Related Technology 4rd Edition. IT Governance Institute, 2005. 194 str.
4. Deloitte & Touche Methodology, 2005 (Audit support).
5. Inštitut za revizijo – ISACA. [URL: www.si–revizija.si/isaca/revizija_IS.php], 22.6.2006.
6. Javornik Boža. Revizijske sledi (online). [URL: www.si–revizija.si/isaca/slo/datoteke/rev_sled_0503.ppt], 27.11.2005.
7. Javornik Miro: Revizija podatkovne baze Oracle. [URL: www.sioug.si/sioug2003/attachments/MiroJavornik_RevidiranjeDBOracleSIOUG2003.doc], 2003.
8. Javornik Miro: Revizija podatkovne baze Oracle. [URL: www.si–revizija.si/isaca/datoteke/revizija–oracle04–2003.ppt], 2003a.
9. Mednarodni revizijski standardi. Ljubljana : Zveza računovodij, finančnikov in revizorjev Slovenije, 1994. 313 str.
10. Mednarodni standardi revidiranja in mednarodna stališča o revidiranju (MSR). Ljubljana : Zveza Slovenski inštitut za revizijo, 1997.
11. Moškon Stane: Revizija in varnost informacijskih sistemov. 109 str. [URL: ecenter.fov.unimb.si/Studenti/Predmeti/Prezentacije/Microsoft%20PowerPoint%20–%20ISACA%20univerza%20FOV.pdf], 2006.
12. Oracle v Sloveniji, [URL: http://www.oracle.com/global/si/index.html], 2006.
13. Publikacija SRC.SI Info. 2002, [URL: www.src.si/library_si/pdf/infosrc/InfoSRC.SI%20–%202002–34.pdf], 2002
14. Technical comparison of Oracle database vs. IMB DB2 – Focus on security: An Oracle white paper. 32 str. [URL: www.oracle.com/technology/deploy/security/oracle9ir2/pdf/CWP_9IVSDB_SECURITY.PDF], 2002.
15. Zakon o revidiranju (Uradni list RS, št. 11/20).

Priloge

Priloga 1: Slovar angleških strokovnih izrazov in kratic

KRATICA	RAZLAGA
Ad–hoch	Poivedovanje po potrebi
CISA	(Certified Information System Auditor) – Preizkušeni revizor informacijskih sistemov (http://www.si–revizija.si/isaca/predstavitev.php)
CISM	(Certified Information System Manager) – Preverjeni vodja informacijske varnosti (http://www.si–revizija.si/isaca/predstavitev.php)
COBIT	(Control Objectives for Information and related Technology) – Kontrolni cilji informacijske tehnologije: ogrodje dobrih praks, ki se ukvarjajo s kontrolami poslovnih procesov, podprtih z informacijsko tehnologijo – Standard, ki ga je izdala ISACA.
DBA	(Database Administrator) - Skrbnik baze podatkov
DEFAULT	Tovarniško vgrajene nastavitve
DES	(Data Encryption Standard) – Obširno uporabljen šifrirni algoritem na svetu. Algoritem je bil pripravljen z namenom šifriranja in dešifriranja blokov podatkov velikosti 64 bitov in sicer s 64 bitnim ključem, katerega morata poznati tako pošiljatelj kot prejemnik (http://sl.wikipedia.org/wiki/DES)
ERP	(Enterprise Resource Planning) - Sistemi za načrtovanje virov - skupaj z manjšimi aplikacijami, ki podpirajo le del poslovnega procesa, tvorijo celoten informacijski sistem
FGAC	(Fine Grained Access Control) – Opcija Oracle podatkovne baze, ki omogoča izvajanje varnostne politike nad podatki na nivoju zapisa (vrstice) v tabeli
IS	Informacijski sistem
ISACA	Slovenski odsek ISACA (mednarodnega Združenja za revizijo in kontrolo informacijskih sistemov). Cilj organizacije je promovirati dobre rešitve pri zaščitah delovanja informacijskih sistemov, kot tudi visoke kvalitete izvajanja revidiranja delovanja kontrol v informacijskem sistemu. (http://www.si–revizija.si/isaca/predstavitev.php)
ISO 17799	Britanski standard o informacijski varnosti, ki ga je izdala Internacionalna organizacija za standardizacijo
IT	informacijska tehnologija
KERBEROS	Internetni standard, ki se ukvarja s področji avtentikacija – prepoznavanja
KERNEL	Glavna enota računalniškega sistema, ki se shrani v glavni spomin sistema (http://www.monster–isp.com/glossary/Kernel.html)
LAN	(Local area network) - Lokalna računalniška mreža
MD5	(Message–Digest algorithm 5) – Znan kot pogosto uporabljana kodirna funkcija z 128–bitnim izhodom. Po internetnem standardu (RFC 1321), je bil MD5 priznan in uporabljen v velikem številu aplikacij za izboljšanje varnosti. (http://sl.wikipedia.org/wiki/Algoritem_MD5)
RADIUS	(Remote Authentication Dial–in User Services) – Internetni standard za

	prepoznavanje oddaljene prijave uporabnika
RC2	(Block Cipher) – Algoritem uporabljen pri šifriranju
RLS	(Row Level Security) – Zaščita na nivoju posamezne vrstice
SHA1	(US Secure Hash Algorithm) – Standard šifriranja – uporabi sporočilo, ki je krajše od 264 bitov in naredi 160bitni razpoznavni odtis potrdila (http://authors.phptr.com/morris/glossary.html)
SQL	(Structured Query Language) - Strukturiran poizvedovalni jezik
SSL	(Secure Socket Layer) – Protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem
UPS	(Uninterruptible Power Supply) - vir energije v primeru izpada električne energije
USER	Uporabnik sistema
VPD	(Virtual Private Database) – Gre za podatkovne baze iz sistema Oracle9i, ki zagotavljajo varnost posameznikovega dela v primeru skupinskega dela. (http://www.oracle.com/global/si/corporate/press/24092001c.html)
VPN	(Virtual Private Network) - Navidezno lokalno omrežje - VPN vam omogoča, da se preko VPN vmesnika, ne glede na to, kje se nahajate, z uporabo modema ali obstoječega omrežja, direktno povežete na domače računalniško omrežje

Priloga 2: Primer init.ora datoteke

Vrednosti nastavitvenih parametrov

db_name = "dbora"
db_domain = home.si
instance_name = dbora
control_files=("D:\oracle\oradata\dbora\control01.ctl",
"D:\oracle\oradata\dbora\control02.ctl", "D:\oracle\oradata\dbora\control03.ctl")
…
db_file_multiblock_read_count = 8
db_block_buffers = 19600
shared_pool_size = 64000817
large_pool_size = 614400
java_pool_size = 20971520
log_checkpoint_interval = 10000
log_checkpoint_timeout = 1800
audit_trail = true # če želimo revizijsko sled
db_block_size = 8192
remote_login_passwordfile = exclusive
os_authent_prefix = ""
remote_os_authent = True – nastavitev za oddaljen dostop
(Javornik, 2003a)