**UNIVERZA V LJUBLJANI**
**EKONOMSKA FAKULTETA**

MAGISTRSKO DELO

# REVIZIJA INFORMACIJSKE TEHNOLOGIJE ZA PRIDOBITEV AKREDITACIJE ARSKTRP

Ljubljana, november 2004 ANA PIRC KOVAČIČ

**IZJAVA**

Študentka Ana Pirc Kovačič izjavljam, da sem avtorica tega magistrskega dela, ki sem ga napisala pod mentorstvom prof. dr. Mira Gradišarja in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, 30.11.2004

Podpis:

# KAZALO

# 1 UVOD

Slovenija je 01.05.2004 postala članica Evropske unije (v nadaljevanju: EU). Z vstopom v EU članica del svoje državne samostojnosti prenese na skupno organizacijo. EU za uresničevanje svojih ciljev uporablja skupne politike na številnih področjih. Ena od teh je tudi skupna kmetijska politika (v nadaljevanju: SKP), na katero se navezuje tematika naloge.

SKP je bila ena izmed prvih skupnih politik EU in sodi med pomembnejše skupne evropske politike. S pomočjo SKP je EU postala druga največja kmetijska sila na svetovnem trgu. Z vstopom v EU država članica v celoti prenese pristojnosti za izvajanje kmetijske politike na skupne ustanove in telesa. Slovenija s prevzemom pravnega reda EU na področju kmetijstva prevzema vse pravice, ki veljajo za države članice EU.

V zadnjem desetletju je Slovenija izpolnila vrsto nalog z namenom čim uspešnejše prilagoditve slovenskega kmetijstva razmeram v EU. Vlada Republike Slovenije je morala za pridobitev sredstev iz EU ter za izvajanje lastne kmetijske politike do pristopa v EU vzpostaviti primerne institucionalne okvire[1].

V skladu z zakonodajo EU morajo vse države članice za izvajanje ukrepov kmetijske politike ustanoviti plačilne agencije. V Sloveniji je bila plačilna agencija - Agencija Republike Slovenije za kmetijske trge in razvoj podeželja (v nadaljevanju: ARSKTRP oziroma Agencija) ustanovljena leta 1999, delovati pa je pričela leta 2000. Agencija deluje kot organ v sestavi Ministrstva za kmetijstvo, gozdarstvo in prehrano (v nadaljevanju: MKGP). Agencija izvaja naloge, ki se nanašajo na izvajanje ukrepov na področju kmetijstva. Kot evropsko naravnana organizacija mora poslovati skladno s pravili in zakonodajo EU.

Agencija mora od pristojnega organa, ki ga imenuje Vlada RS, pridobiti akreditacijo, to je zagotovilo, da ima vzpostavljene vse predpisane postopke, deluje v skladu s pravili in izvaja sistem notranjega nadzora. Akreditacijski pregled izvede pristojni organ na podlagi meril Evropske komisije za akreditacijske kriterije.

ARSKTRP je začasno akreditacijo pridobila aprila 2004. S tem je pridobila status plačilne agencije za izplačevanje sredstev Jamstvenega oddelka Evropskega kmetijsko usmerjevalnega in jamstvenega sklada za financiranje SKP kot edina tovrstna plačilna agencija v Sloveniji.

[1] Sklep Vlade RS, številka 900-10/98-31 z dne 7.1.1999.

Plačilne agencije letno izplačujejo visoke finančne zneske, zato je njihovo delovanje nenehno izpostavljeno grožnjam in tveganjem. Evropska zakonodaja določa, da morajo biti poslovni procesi plačilnih agencij ustrezno računalniško podprti. Zaradi hitrega razvoja informacijske tehnologije postaja obvladovanje poslovanja vse težje, vodilni delavci pa nosijo vedno večjo odgovornost. Zato je varnost informacijske tehnologije izrednega pomena.

Informacijski sistem ima v plačilnih agencijah, kot je ARSKTRP, določene lastnosti in posebnosti, ki zahtevajo dodatno skrb za zagotavljanje varnosti in kakovosti. V plačilni agenciji je količina dnevno obdelanih transakcij in podatkov zelo velika. Zato predstavljajo informacijska tehnologija, podatki in kakovostna programska oprema največje premoženje organizacije. Informacijski sistem mora biti varovan pred grožnjami iz okolja. Zagotavljati mora visoko razpoložljivost, stabilnost, varnost in zanesljivost pri delovanju. V primeru nepredvidljivih dogodkov je potrebno zagotoviti ponovno vzpostavitev poslovanja v najkrajšem možnem času.

Informacijski sistem mora ustrezati predpisanim kontrolnim zahtevam za izvajanje postopkov zagotavljanja varnosti informacijskih sistemov. Plačilne agencije v državah članicah EU morajo na področju informatike izpolnjevati kriterije, predpisane v Smernicah za računalniško zaščito informacijskih tehnologij plačilnih agencij[2] (v nadaljevanju: Smernice za računalniško zaščito). Smernice za računalniško zaščito so zasnovane na najboljši praksi in izkušnjah plačilnih agencij EU, ki se nanašajo na SKP. Pri tem je vsaki posamezni agenciji prepuščena odločitev o tem, na kakšen način bo zahteve izpolnila in kateremu standardu bo pri tem sledila.

Smernice za računalniško zaščito so referenčna točka za katerikoli pregled, ki ga izvaja Evropska komisija v kontekstu akreditacije ali certificiranja letnih računov (Smernice za računalniško zaščito, 1998).

Iz poročila o revizijskih pregledih plačilnih agencij držav članic EU v letu 2002 je razvidno, da je bila pri pregledu skladnosti poslovanja s Smernicami za računalniško zaščito dosežena povprečna ocena 3, pričakovana ocena pa je bila 3,41. Področja pregleda v skladu s Smernicami za računalniško zaščito so:

- splošna organizacija, upravljanje in revizija,
- fizično varovanje,
- logično varovanje,

[2] Sistemi informacijskih tehnologij plačilnih agencij: Smernice za računalniško zaščito. Dokument Evropske komisije št. VI/667/97, 2. popravek, 1998.

- razvijanje, programiranje in vzdrževanje,
- rutinske operacije,
- telekomunikacije,
- osebni računalniki,
- načrtovanje neprekinjenega poslovanja in
- aplikativne kontrole.

Več kot 30% plačilnih agencij je doseglo slabše rezultate od pričakovanega povprečja. Najmanj točk je bilo doseženih na področjih načrtovanja neprekinjenega poslovanja (kontingenčno načrtovanje) - 2,59, logične zaščite - 2,76 ter splošne organizacije in upravljanja - 2,9. Od vseh pregledanih področij je bilo najslabše ocenjeno področje načrtovanja neprekinjenega poslovanja (IT Audits in the paying agencies, Final report, 2002).

**Cilj raziskovalne naloge** je izdelati revizijski vprašalnik za pregled poslovanja v skladu s Smernicami za računalniško zaščito, ki bo obsegal vsa področja in kontrolne cilje v skladu z naslednjimi kriteriji: splošna organizacija in upravljanje, fizično varovanje, logično varovanje, razvoj programske opreme, rutinske operacije osrednjih računalnikov, telekomunikacije, mikroračunalniki, načrtovanje neprekinjenega poslovanja in aplikativne kontrole.

Tako izdelan vprašalnik lahko uporablja revizor pri revizijskem pregledu, namenjen pa je tudi vodstvu in udeležencem, zadolženim za izvajanje nalog, pri pregledu izpolnjevanja nalog v skladu s predpisanimi postopki. Vprašalnik je izdelan tako, da obsega vse kontrolne cilje, ki jih predvidevajo Smernice za računalniško zaščito. S pomočjo sistematično izdelanega vprašalnika pri pregledu obvladovanja poslovanja dobimo natančno predstavo o obstoječem stanju, urejenosti postopkov na posameznih področjih ter področjih, na katerih je potrebno postopke dopolniti oziroma izpopolniti.

V raziskovalni nalogi so kot izhodišče za izdelavo vprašalnika uporabljene Smernice za računalniško zaščito. Metodologijo za izdelavo vprašalnika je mogoče prenesti in uporabiti za izdelavo vprašalnikov za pregled kateregakoli drugega področja poslovanja.

Magistrsko delo temelji na proučevanju teoretičnih podlag ter na proučevanju in analiziranju prakse. Pri proučevanju teorije je bila uporabljena domača in tuja literatura s področja revidiranja in informacijskih tehnologij. Pri proučevanju literature in v magistrskem delu sem se osredotočila na pravne podlage, notranje revidiranje in revidiranje informacijskih sistemov. Pomagala sem si s praktičnimi izkušnjami, pridobljenimi z delom na področju informatike in revizije.

Pri izdelavi magistrskega dela sem uporabljala metodologijo znanstveno - raziskovalnega dela. Kot temeljna metoda dela je bil uporabljen analitično - teoretični pristop in proces ugotavljanja dejstev na podlagi predhodnih znanj ter metoda kompilacije (uporaba znanj in izkušenj iz tuje in domače literature). Pri prikazu praktičnega primera sem uporabila izkustveno metodo, ki izhaja iz lastnih izkušenj pri dosedanjem delu.

Magistrsko delo je razdeljeno v šest sklopov, ki obsegajo uvod, pregled pravnega reda EU, pregled informacijskih tehnologij, revidiranje, revidiranje informacijskih sistemov, predstavitev slovenske plačilna agencije ter zaključek. Uvod povzema problematiko in namen magistrskega dela, cilje ter metode dela. V poglavju o pregledu pravnega reda so predstavljene institucije in zakonodaja EU ter pregled SKP. V nadaljevanju je predstavljeno financiranje SKP in vloga plačilnih agencij pri izplačevanju finančnih sredstev EU. V poglavju o informacijskih tehnologijah je predstavljena vloga oddelka za informacijsko tehnologijo, metodologije razvoja informacijskih sistemov ter pomen varovanja in zaščite informacij in informacijskih sistemov. V nadaljevanju so predstavljeni postopki revidiranja, posebnosti pri revidiranju informacijskih sistemov, pomen notranjih kontrol, standard za varovanje informacij in informacijskih tehnologij, metodologija za obvladovanje informacijskih tehnologij ter smernice EU, iz katere izhajajo kontrolne zahteve za računalniško zaščito (Smernice za računalniško zaščito). V zadnjem delu je predstavljena plačilna agencija v Sloveniji in izdelan revizijski vprašalnik z vsemi ključnimi kontrolnimi točkami. Sklep obsega ključne ugotovitve magistrskega dela.

# 2. PRAVNI RED EU IN SKP

## 2.1 Pravni red EU

Začetek evropskega združevanja predstavljajo tri skupnosti:
- Evropska skupnost za premog in jeklarstvo, ki je bila ustanovljena leta 1951 s Pariško pogodbo;[3]
- Evropska gospodarska skupnost (v nadaljevanju: EGS), ki je omogočila oblikovanje skupnega trga za industrijske izdelke in kmetijske pridelke, uresničevanje prostega pretoka blaga, delavcev, storitev in kapitala;
- Evropska skupnost za jedrsko energijo (EJS oziroma Euratom). EGS in Evropska skupnost za jedrsko energijo sta bili ustanovljeni leta 1957 v Rimu z Rimsko pogodbo[4].

Skupnosti so se z leti širile in poglabljale. Iz treh Evropskih skupnosti je bila leta 1987 oblikovana Evropska skupnost (v nadaljevanju: Skupnost oziroma ES). Po podpisu Pogodbe o ustanovitvi EU[5] leta 1992 se je delovanje ES razširilo na področje ekonomske in denarne unije, kar je privedlo do uvedbe skupne valute. Pogodba o ustanovitvi EU je uvedla delitev na tri stebre. EU je skupni izraz za vse tri stebre. Prvi, najpomembnejši in najmočnejši steber predstavljajo Evropske skupnosti. V prvem stebru se sprejema zakonodaja in politike EU. Drugi steber obsega področje skupne zunanje in varnostne politike, tretji steber pa predstavlja področje pravosodja in notranjih zadev.

S podpisom Amsterdamske pogodbe[6] oktobra 1997 so države članice EU podrobneje določile carinsko poslovanje, ukrepe za spodbujanje gospodarskega razvoja in socialne zaščite. Države članice so decembra 2001 podpisale Pogodbo iz Nice, s katero je bila omogočena širitev EU. Po širitvi leta 1995 je EU sestavljalo 15 držav, od 01.05.2004 pa

[3] Pariška pogodba je pričela veljati 23.07.1952. S Pariško pogodbo so bile odpravljene ovire, ki so omejevale prosto trgovino s premogom in jeklom med podpisnicami pogodbe. Veljati je prenehala leta 2002.

[4] Rimska pogodba je splošen dokument, v katerem so zapisani temeljni okviri delovanja skupnosti. Vsebuje pravne podlage za poglabljanje združitvenih procesov v zahodni Evropi.

[5] Pogodba o ustanovitvi EU ali Maastrichtska pogodba je bila podpisana 7. februarja 1992 v Maastrichtu. Veljati je pričela novembra 1993. Pogodba opredeljuje temeljne cilje delovanja EU, ki so spodbujati uravnotežen gospodarski razvoj, uvedba državljanstva EU, sodelovanje na področju pravosodja in notranjih zadev, zagotavljanje učinkovitega delovanja institucij EU ter oblikovanje enotnega evropskega trga in denarne unije.

[6] Z Amsterdamsko pogodbo je bila delno spremenjena vsebina vseh treh stebrov. Temelji cilji opredeljujejo skupno sodelovanje držav članic pri reševanju brezposelnosti v EU in oblikovanju demokratične Evrope. Izpostavlja spoštovanje človekovih pravic in demokratičnih načel v državah EU. Dopolnjuje področje pravosodja in notranjih zadev ter področje prostega pretoka oseb.

EU sestavlja 25 držav. Od 1. januarja 2002 je uradna valuta v vseh državah članicah nova skupna evropska valuta – evro.

Temelj evropskega povezovanja predstavljajo štiri svoboščine: prost pretok blaga, kapitala, storitev in oseb.

## 2.2 Delovanje EU

EU je skupna organizacija držav članic. Deluje na pravno obvezujočih pogodbah. EU nima mednarodnopravnega značaja, ki med drugim pomeni tudi sposobnost sklepanja (mednarodnih) pogodb. Pogodbe se sklepajo v imenu Evropskih skupnosti. Z vstopom v EU članica del svoje državne samostojnosti prenese na EU. Temeljni cilji združevanja v EU so dvig blaginje prebivalstva, pospeševanje gospodarske rasti ter utrjevanje miru in svobode. Zakonodaja EU je veljavna v vseh državah članicah (Cunder et al., 1997, str. 11).

### 2.2.1 Institucije EU

EU izvaja odločanje in pristojnosti preko naslednjih institucij:
- Evropska komisija,
- Evropski parlament,
- Evropski svet,
- Svet Evropske unije ali Svet ministrov,
- Evropsko sodišče oziroma Sodišče Evropskih skupnosti,
- Računsko sodišče.

#### 2.2.1.1 Evropska komisija

Evropska komisija (v nadaljevanju: Komisija) je samostojna in neodvisna strokovna institucija, ki zastopa interese EU kot celote. Odgovorna je za predlaganje in izvrševanje zakonodaje EU. Predstavlja celotno javno upravo EU, katere osrednji del so generalni direktorati (imenovani s francosko kratico DG – directorate général) in njihovi oddelki. Generalnih direktoratov je 24. Komisijo sestavljajo komisarji, ki jih predlagajo države članice in jih potrdi Evropski parlament (v nadaljevanju: EP). Komisarji morajo delovati v splošnem interesu EU. Vsaka država članica ima vsaj enega komisarja, večje članice dva.

Evropska komisija opravlja tri temeljne naloge:
- pripravlja predloge zakonodajnih aktov. O predlogih odločata EP in Svet EU;

- opravlja izvršilno funkcijo izvajanja zakonodaje ter sprejema podzakonske akte EU;
- nadzoruje proračun EU.

Komisija zagotavlja uresničevanje ustanovitvenih pogodb. V imenu držav članic EU se pogaja z državami nečlanicami o širitvi EU. Komisija za svoje delo odgovarja Evropskemu parlamentu. Ena od nalog Komisije je zagotavljati, da države članice pravilno uvajajo zakonodajo EU.

#### 2.2.1.2 Evropski parlament

Evropski parlament zastopa interese državljanov EU. V zakonodajno institucijo EU se je razvil iz posvetovalnega telesa Evropske skupnosti. Sedež EP je v Strasbourgu. Po sprejetju Maastrichtske pogodbe so se njegove pristojnosti razširile. Skupaj s Svetom EU soodloča o zakonodaji s področja skupnega trga na približno 35-ih področjih. Odloča tudi o vstopu novih članic v EU. EP daje soglasje pri sprejemanju evropskega proračuna in nadzoruje njegovo porabo. Poslanci EP so izvoljeni na neposrednih splošnih volitvah v državah članicah vsakih pet let. Vsaka država članica ima v EP določeno število predstavnikov.

#### 2.2.1.3 Evropski svet in Svet EU

**Evropski svet** je najvišje politično telo EU. Ustanovljen je bil leta 1974. Njegov status je bil določen z Maastrichtsko pogodbo. Sestavljajo ga predsedniki držav ali vlad članic ter predsednik Evropske komisije. Njegova najpomembnejša vloga je določanje skupne zunanje in varnostne politike. Oblikuje splošne politične smernice za pospeševanje razvoja EU in definira politične opredelitve.

**Svet EU** sestavljajo vlade držav članic. Temeljna naloga Sveta EU je sprejemanje zakonodaje EU. Sprejema pravne akte, med katerimi so najpomembnejše uredbe. Vsaka država članica EU predseduje Svetu EU šest mesecev.

#### 2.2.1.4 Evropsko in računsko sodišče

**Evropsko sodišče** je najvišje pristojno sodišče za zakonodajo EU. Njegova naloga je zagotavljati, da se zakonodaja znotraj skupnosti uresničuje na enak način. Pristojno je za pravilno tolmačenje in izvajanje zakonodaje EU. Na področjih, ki jih zakonodaja EU ne pokriva, nima pristojnosti. Ureja tudi spore med državami članicami in daje mnenja k mednarodnim sporazumom.

**Evropsko računsko sodišče** nadzoruje finančno poslovanje in porabo sredstev EU. Ustanovljeno je bilo leta 1977. Evropsko računsko sodišče ima po enega predstavnika iz vsake države članice. Mandat traja šest let in ga je mogoče podaljšati.

### 2.2.2 Zakonodaja EU

Evropski pravni red[7] je sestavljen iz primarne in sekundarne zakonodaje. **Primarno zakonodajo** predstavljajo ustanovitvene pogodbe, predvsem Rimska in Maastrichtska pogodba, dopolnitve ustanovitvenih pogodb, pristopne pogodbe ter pogodbe med Skupnostjo in tretjimi državami. Posamezne ustanovitvene pogodbe predstavljajo pravni temelj za ustanovitev in delovanje posameznih skupnosti. **Sekundarno zakonodajo** predstavljajo pravni predpisi, ki urejajo predvsem delovanje skupnega trga[8]. Ti pravni akti so uredbe, direktive oziroma smernice, odločitve, priporočila, mnenja in resolucije. Vsak od pravnih aktov ima drugačen vpliv na pravni sistem držav članic. Podlaga za sprejem vsakega od navedenih aktov je primarna zakonodaja.

Sekundarni pravni viri so:

- **Uredbe** (Regulation) so najvišja oblika sekundarnih pravnih predpisov. So zavezujoče, hierarhično nad zakonodajo držav članic in veljajo neposredno kot zakon. Uredbe postanejo pravno zavezujoče za vse države članice z dnevom objave v Uradnem listu EU. Države članice jih morajo neposredno prenesti v svojo zakonodajo. Države članice se uredbam ne prilagajajo, temveč jih izvajajo.
- **Direktive** oziroma smernice (Directive) so obvezujoč pravni predpis in države članice zavezuje, da ga vgradijo v svoj zakonodajni sistem. Državam članicam je prepuščena odločitev o tem, na kakšen način bodo zahteve iz direktiv uresničile.
- **Odločitve** (Decision) so zavezujoče za posamezne primere in imajo takojšen učinek za tistega, na katerega se nanašajo. Prilagoditev nacionalne zakonodaje ni potrebna.
- **Priporočila** (Recommendation) predlagajo določen način ravnanja.
- **Mnenja** (Opinion) ocenjujejo trenutni položaj ali določena dejstva v EU ali v državi članici. Priporočila in mnenja niso pravno zavezujoča in evropskim institucijam omogočajo, da sprejmejo stališča brez pravnih obveznosti za države članice oziroma državljane.
- **Resolucije** sprejemata EP in Svet EU kot odraz politične želje po ukrepanju na posameznem področju. Resolucije niso pravno zavezujoče.

[7] Pravni red tvorijo predpisi, politične usmeritve, prakse in obveznosti, ki so nastale v procesu razvoja EU.

[8] Z izrazom skupni trg se označuje Evropska skupnost oziroma njena predhodnica EGS.

## 2.3 Skupna kmetijska politika

EU za uresničevanje svojih ciljev uporablja številne skupne politike. Ena izmed prvih skupnih politik EU je bila SKP. SKP sodi med pomembnejše skupne evropske politike. Temelji na ciljih in načelih iz Rimske pogodbe. Cilji kmetijske politike se vse od nastanka do današnjih dni niso spreminjali. S pomočjo SKP je EU postala druga največja kmetijska sila na svetovnem trgu. Uresničevanju SKP namenja EU skoraj polovico proračunskega denarja.

### 2.3.1 Temelji in razvoj SKP

SKP je nastajala postopno. Leta 1962 je bil sprejet predpis o ustanovitvi posebnega Evropskega kmetijsko usmerjevalnega in jamstvenega sklada za financiranje SKP - EKUJS[9] (v nadaljevanju: Sklad). Sklad je finančno orodje SKP od leta 1965. SKP je zaživela leta 1968.

#### 2.3.1.1 Cilji in načela SKP

Temeljni cilji SKP, določeni v Rimski pogodbi, so:
- povečanje kmetijske pridelave,
- zagotovitev spodobne življenjske ravni kmetijskih skupnosti, posebno s povečanjem individualnih zaslužkov ljudi, ki delajo v kmetijstvu,
- stabiliziranje kmetijskih trgov in
- zagotovitev dostopnosti ponudbe po razumnih cenah.

Po Rimski pogodbi temelji SKP na treh glavnih načelih:

- **Načelo enotnosti trga.** To načelo utemeljuje skupni kmetijski trg, na katerem se izvaja prost pretok kmetijskih proizvodov med članicami EU brez carinskih ali necarinskih ovir. Enotnost trga pomeni, da lahko obstaja le enotna tržno-cenovna politika.
- **Načelo prednosti skupnosti.** Drugo načelo ščiti EU pred poceni uvozom (uvozne dajatve, izvozne subvencije). Domači pridelki in živila imajo prednost pred uvoženimi.
- **Načelo finančne solidarnosti**. To načelo pomeni financiranje stroškov SKP iz skupnega proračuna. Izvaja se preko Sklada.

9 FEOGA (Fond Europeen d'Orientation et de Garantie Agricole) – evropski kmetijski usmerjevalni in jamstveni sklad (EKUJS).

SKP sestavljajo pravila in ukrepi, s katerimi dosega zastavljene cilje. Predpisani so s tržnimi redi. Tržni red predstavlja skupno ime za uredbe, pravila in ukrepe, ki jih sprejme zakonodajno telo EU. Tržni redi veljajo za posamezne kmetijske pridelke, kot so žita, meso, mleko, sadje in drugi. Med seboj se razlikujejo po vsebini in intenzivnosti tržne zaščite za posamezen pridelek.

Mehanizmi podpor se delijo na:
1. tržno - cenovne podpore in
2. strukturne ukrepe za razvoj podeželja.

1. tržno - cenovne podpore vplivajo na trg in cene. Mednje sodijo naslednje skupine ukrepov:
   - zunanjetrgovinski ukrepi (uvozne dajatve in podpore za izvoz);
   - intervencije na notranjem trgu (javni nakupi, podpore skladiščenju, podpore porabi). Z intervencijskimi nakupi se ustvarja dodatno povpraševanje. Ta mehanizem se uporabi, če cene na skupnem trgu padejo pod raven določenih zaščitnih (intervencijskih) cen;
   - omejevanje ponudbe (proizvodne kvote);
   - neposredna plačila (plačila na hektar kmetijske površine ali glavo živine).

2. strukturni ukrepi in ukrepi za razvoj podeželja so vsi netržni ukrepi v podporo kmetijstvu. Mednje sodijo:
   - okoljski ukrepi in izravnalna plačila za območja z omejenimi možnostmi za kmetijsko pridelavo;
   - podpore naložbam v kmetijska gospodarstva;
   - podpore za zgodnje upokojevanje, za mlade prevzemnike in za delovno usposabljanje;
   - podpore za izboljšave v predelavi in trženju kmetijskih proizvodov;
   - podpore gozdarstvu in podpore za strukturne prilagoditve ter razvoj podeželskih območij (interna gradiva MKGP, 2003).

#### 2.3.1.2 Razvoj SKP

V skladu z zastavljenimi cilji SKP sta se do 70. let storilnost kmetijskih gospodarstev in kmetijska pridelava zelo povečala. V 70. letih pa so se kmetijski pridelki pričeli kopičiti. Pojavljali so se veliki presežki sladkorja, vina, govedine in žit. Zaradi zaščite trga so bile cene kmetijskih pridelkov v EU dvakrat ali celo do trikrat višje od cen na svetovnem trgu, zaradi česar je bil onemogočen normalen izvoz. Presežke je bilo potrebno uničevati oziroma z visokimi izvoznimi spodbudami izvoziti. Izdatki EU za kmetijstvo so se v dveh desetletjih delovanja SKP za nekajkrat povečali in so še naraščali. Zaradi visoke kmetijske intenzivnosti je v okolju pričela nastajati velika

škoda. SKP ni uresničila cilja zagotavljanja spodobne življenjske ravni vsem zaposlenim v kmetijstvu.

Težave SKP so se reševale z reformami kmetijske politike. Cilj reform je bil reševanje proračunskih težav, povečanje konkurenčnosti kmetijstva EU na svetovnih trgih, zmanjšanje presežkov zaradi zniževanja stroškov, ohranjanje družinskih kmetij in zmanjševanje škode v okolju.

**Reforme SKP:**

- **Leta 1984** so bili uvedeni kontingenti oziroma kvote za pridelavo mleka. Proračunski izdatki so najhitreje naraščali pri mleku. Nemški kmetijski minister Joseph Ertl je predlagal uvedbo proizvodnih kontingentov[10] oziroma kvot. S to reformo je bila uspešno omejena rast pridelave mleka in proračunskih izdatkov.
- **Leta 1988** je bil zaradi nadaljnjega naraščanja proračunskih izdatkov sprejet stabilizacijski paket za omejevanje poljščin, ki je vključeval tudi program prahe[11]. Omenjena reforma ni izpolnila pričakovanj.
- EU je **leta 1992** izvedla temeljitejše spremembe SKP. Najpomembnejši razlogi za prenovo SKP so bili veliki presežki žit in govedine ter naraščanje proračunskih izdatkov. V okviru t.i. MacSharry-eve[12] reforme so uvedli postopno zniževanje intervencijskih cen[13] pridelkom, obvezno vključitev v program prahe in različne spremljevalne ukrepe. Reforma je pomenila preobrat v kmetijski politiki EU in prenos proračunskih podpor kmetijstvu na davkoplačevalce.
- **Leta 1997** je Evropska komisija predstavila dokument Agenda 2000. Namen reforme je bil stabilizacija kmetijskih trgov z zmanjševanjem tržno cenovnih podpor na račun povečevanja neposrednih proračunskih plačil. Spremenila je način zaščite in financiranja kmetijstva.

Evropska komisija je leta 2003 objavila predlog reforme SKP. Predlog Komisije vsebuje načrt kmetijske politike EU do leta 2013. Cilji reforme so večja konkurenčnost evropskega kmetijstva ter preprostejše in preglednejše razdeljevanje sredstev SKP.

Glavni elementi predlagane reforme so uveljavitev enotnega plačila, pogojenost plačila s spoštovanjem okoljskih zahtev, varnostjo in kvaliteto hrane, blaginjo živali, higienskimi standardi in standardi varstva pri delu ter ohranjanje kmetijskega zemljišča v dobrem stanju. Več sredstev naj bi bilo namenjenih razvoju podeželja, neposredna

[10] Vsaka država članica lahko uveljavlja polno zaščitno ceno mleka, tako imenovane nacionalne proizvodne kontingente. Ti se delijo na mlekarne ali na posameznega rejca. Če pride do količinskih presežkov, proizvajalec plača visoko dajatev. S kontingiranjem država uravnava delovanje trga in pravzaprav zavira njegovo spontano delovanje.

[11] Uvedba podpor oziroma nadomestil za opuščanje pridelave na delu zemljišč.

[12] Tedanji komisar za kmetijstvo.

[13] Zaščitne cene.

plačila pa naj ne bi bila več vezana na količino pridelave, temveč na zaščito okolja (interna gradiva MKGP, 2003).

### 2.3.2 Financiranje SKP

Financiranje SKP določa Uredba Sveta (ES) o financiranju SKP. Izdatki za vodenje SKP se financirajo preko Sklada. Za izvrševanje proračuna Skupnosti je odgovorna Komisija. Komisija mora preveriti pogoje, pod katerimi se izvajajo plačila in preverjanja upravičenosti izplačil. Skupnost financira le izdatke, ki jih izvedejo akreditirane plačilne agencije držav članic. Zato morajo države članice akreditirati plačilne agencije (Uredba Sveta (ES) o spremembah Uredbe o financiranju SKP, 1995).

Države članice morajo v skladu z nacionalnimi predpisi preverjati naslednje:
- da so transakcije, financirane iz Sklada, dejansko in pravilno izvršene,
- da so nepravilnosti obravnavane in preprečene,
- da je zagotovljeno vračilo preveč izplačanih zneskov, ki so bili izplačani zaradi nepravilnosti ali malomarnosti (Uredba Sveta o financiranju SKP, 1999).

Izdatki Skupnosti so pod natančnim nadzorom. **Za nadzor izdatkov** Skupnosti so primarno odgovorne države članice, preverjanja pa opravljajo tudi uradniki Skupnosti. Komisija financira izdatke le, če obstajajo vsa potrebna in zadostna jamstva glede skladnosti poslovanja s predpisi Skupnosti. Komisija določi skupne izdatke v breme jamstvenega dela Sklada na podlagi zadostnih zagotovil o ustreznosti in preglednosti državnega nadzora ter zagotovil, da plačilne agencije preverjajo zakonitost in pravilnost zahtevkov za izplačila.

#### 2.3.2.1 Vloga Sklada

Ukrepi SKP se financirajo iz Sklada. Temelji za ustanovitev in delovanje Sklada so zapisani v Rimski pogodbi. Za **upravljanje** Sklada je odgovorna Komisija (Uredba Sveta (ES) o financiranju SKP, 1999).

Sklad je del splošnega proračuna Skupnosti in je največji od strukturnih skladov, saj mu pripada skoraj polovica celotnega proračuna Namenjen je financiranju **tržnocenovne politike** (jamstveni oddelek) in programov **strukturne politike** (usmerjevalni oddelek). Tržnocenovni politiki je namenjen večji del sredstev iz proračuna in obsega stroške, povezane z izvajanjem tržnih redov. Jamstveni oddelek podpira okolju prijazno kmetovanje ter spodbuja k trajnostnemu gospodarjenju s podeželskimi območji in naravnimi viri. Usmerjevalni del Sklada zagotavlja sredstva za izboljšanje konkurenčnosti kmetijskega in živilskega sektorja. Podlage za črpanje sredstev iz tega

dela Sklada so opredeljene v Enotnem programskem dokumentu (interna gradiva MKGP, 2003).

**1. Jamstveni del** Sklada financira:

- izvozna nadomestila za izvoz v tretje države,
- intervencije za stabilizacijo kmetijskih trgov,
- ukrepe za razvoj podeželja,
- posebne veterinarske ukrepe v veterinarstvu, kot so inšpekcijski ukrepi in programi za izkoreninjenje in nadziranje bolezni živali ter fitosanitarne ukrepe,
- ukrepe za informiranje o SKP,
- neposredna plačila (plačila na hektar kmetijske površine ali glavo živine).

**2. Usmerjevalni del** Sklada financira izdatke za nekatere ukrepe za razvoj podeželja.

Iz Sklada se ne financirajo izdatki upravnih stroškov. Ti stroški so breme države članice in prejemnikov pomoči Sklada.

### 2.3.3 Plačilne agencije

Skupnost lahko **financira** le izdatke, ki jih izplačajo akreditirane plačilne agencije držav članic. Zato morajo države članice plačilne agencije akreditirati.

Glavne naloge plačilne agencije so:

1. **odobritev izplačil:** predstavlja določitev zneska za izplačilo upravičencu v skladu s pravili Skupnosti;
2. **izvajanje izplačil:** obsega izdajanje navodil plačilnemu organu za izvedbo izplačila odobrenega zneska upravičencu ali njegovemu pooblaščencu;
3. **računovodstvo izplačil:** predstavlja evidentiranje plačil izdatkov EKUJS-a v posebne računovodske evidence, pripravo periodičnih povzetkov izdatkov ter pošiljanje mesečnih in letnih poročil Evropski komisiji (Uredba Komisije (ES) o določitvi podrobnih pravil za uporabo Uredbe Sveta (ES) št. 729/70 v zvezi s postopkom za potrditev obračuna Jamstvenega oddelka EKUJS, 1995).

Agencija mora nuditi zadostna jamstva, da v zvezi z izplačili, za katera je odgovorna, izvaja naslednje postopke:

- pred odobritvijo izplačil se preveri dopustnost odobritve izplačil in skladnost s pravili Skupnosti,

- izvršena plačila so pravilno in v celoti evidentirana v ustreznih evidencah,
- potrebna dokumentacija je predložena v roku in v obliki, kot to predpisujejo pravila Skupnosti.

Vsaka država članica določi omejeno število akreditiranih plačilnih agencij. Pred akreditiranjem plačilne agencije mora pristojni organ opraviti pregled, kjer ugotovi, ali upravna in računovodska ureditev agencije vsebuje jamstva, ki jih določi država članica, pristojni organ pa uporabi za akreditacijo. Pri tem upošteva smernice za merila za akreditacijo plačilne agencije (Uredba Sveta (ES) o spremembah Uredbe o financiranju SKP, 1995).

Predakreditacijski pregled zajema pregled usposobljenosti plačilne agencije za odobritev in izvrševanje plačil, zaščito finančnih sredstev, varnost računalniških sistemov, vodenje računovodskih evidenc, delitev nalog ter ustreznost notranjih in zunanjih kontrol v zvezi z izplačili, ki jih financira Jamstveni oddelek Sklada.

Akreditacijski akt je pisna potrditev, da agencija izpolnjuje kriterije za akreditacijo. Akt se pošlje Komisiji. Akreditacija se lahko glede na resnost težav dodeli za začasno obdobje. Kadar akreditirana plačilna agencija več ne izpolnjuje enega ali več pogojev za akreditacijo, se akreditacijo umakne, razen če agencija ne uresniči potrebnih sprememb v določenem časovnem obdobju. Če se akreditacija odvzame, država članica določi drugo plačilno agencijo ter zagotovi neprekinjenost izplačil upravičencem (Uredba Komisije (ES) o določitvi podrobnih pravil za uporabo Uredbe Sveta (ES) št. 729/70 v zvezi s postopkom za potrditev obračuna Jamstvenega oddelka EKUJS, 1995).

#### 2.3.3.1 Smernice za merila za akreditacijo

Smernice za merila za akreditacijo plačilne agencije (v nadaljevanju: Merila za akreditacijo) so priloga Uredbe Komisije (ES) št. 1663/95 o določitvi podrobnih pravil za uporabo Uredbe Sveta (EGS) št. 729/70 v zvezi s postopkom za potrditev obračuna Jamstvenega oddelka EKUJS. Uredba se uporablja neposredno. Plačilne agencije morajo izvajati vse točke uredbe in izpolniti vse pogoje, navedene v Merilih za akreditacijo. V skladu z Merili za akreditacijo mora agencija zagotavljati delovanje sistema notranjih kontrol.

Organizacijska struktura agencije mora zagotavljati ločitev izvajanja nalog tako, da se naloge odobritve, izvajanja in računovodstva izplačil izvajajo v ločenih organizacijskih enotah. Odgovornosti posameznih enot morajo biti opredeljene v organizacijski shemi.

Vsaka plačilna agencija mora vzpostaviti naslednje postopke:

- Določiti je potrebno podrobne pisne postopke za sprejem, evidentiranje in obdelavo zahtevkov. Postopki morajo vključevati opise vseh dokumentov v postopku.
- Noben uradnik ne sme biti odgovoren za več kot eno od področij odobritve, izplačevanja ali računovodstva izplačil (delitev nalog). Delo vsakega uradnika mora nadzirati drug uradnik.
- Odgovornosti vsakega uradnika morajo biti pisno določene.
- Vzpostavljen mora biti ustrezen sistem izobraževanja zaposlenih.
- Za zaposlene na občutljivih delovnih mestih mora veljati postopek rotacije oziroma povečan nadzor nad njihovim delom.
- Vsak uradnik, odgovoren za odobritev izplačil, mora izvesti ustrezna preverjanja in potrditi, da so bila ta preverjanja izvedena. Delo uradnika mora pregledati nadrejeni in to potrditi.
- Zahtevek za izplačilo se odobri šele po zadostnih preverjanjih, da je zahtevek v skladu z zahtevami Skupnosti.
- Postopki morajo zagotavljati, da se izplačilo izvede samo upravičencu oziroma pooblaščeni osebi na njegov bančni račun. Uvesti je potrebno postopke, ki zagotavljajo, da se vsa neizvršena plačila ponovno knjižijo v dobro Sklada. Gotovinska plačila niso dovoljena.
- Dostop do računalniškega sistema in podatkov mora biti ustrezno zaščiten. Računalniški sistem mora biti ustrezno nadziran.
- Vsaka sprememba predpisov Skupnosti mora biti evidentirana. Navodila in podatkovne baze je potrebno pravočasno posodabljati.

V svojem nadaljnjem poslovanju mora Agencija delovati v skladu z vzpostavljenimi postopki. Nadzor nad delovanjem agencije izvajajo Služba za notranjo revizijo, državni organi in organi Skupnosti. Namen pregledov je pregled delovanja kontrolnega sistema ter učinkovitosti upravljanja in porabe sredstev EU.

# 3 INFORMACIJSKA TEHNOLOGIJA

## 3.1 Upravljanje informacijskih sistemov

**Z vidika ravni upravljanja** delimo informacijske sisteme (v nadaljevanju: IS) na strateški informacijski podsistem, taktični informacijski podsistem in operativni informacijski podsistem.

- **Na strateški ravni** se določijo osnovni cilji in usmeritve delovanja sistema za doseganje zastavljenih ciljev ter opredelijo dolgoročne usmeritve in način delovanja.
- **Na taktični ravni** se načrtuje kdo, kako in kdaj naj opravi posamezne naloge za doseganje zastavljenih strateških ciljev.
- **Operativno upravljanje** predstavlja aktivnosti oziroma naloge, ki jih je potrebno izvesti za uresničitev nalog, zastavljenih na taktični ravni (Bobek, Lesjak, 1993, str. 56).

### 3.1.1 Naloge oddelka za informacijsko tehnologijo

Temeljne naloge oddelka za informacijsko tehnologijo so (Turban et al., 2003, str. 45):

- razvoj programskih rešitev,
- integracija računalniških sistemov,
- usposabljanje končnih uporabnikov,
- zasnova strateškega IS,
- načrtovanje, razvoj in nadziranje infrastrukture,
- uvajanje elektronskega in Internetnega poslovanja,
- podpora končnim uporabnikom,
- sodelovanje z vodstvom organizacije,
- sodelovanje pri prenovi poslovnih procesov organizacije,
- sodelovanje z dobavitelji in ostalimi organizacijami s področja informatike.

### 3.1.2 Podatki in informacije

Informacije nastopajo v različnih oblikah. Lahko so v pisni obliki, natisnjene ali v elektronski obliki. So izgovorjene, oziroma se pošiljajo po pošti ali elektronskih kanalih. Kakovost podatkov in informacij je za organizacije ključnega pomena.

**Kakovost informacije** določajo:
- **dostopnost:** informacija je uporabniku na voljo takrat, ko jo potrebuje;

- **točnost:** točnost informacije je odvisna od stopnje zanesljivosti;
- **pravočasnost:** povezana je s stopnjo odzivnosti IS in dostopnostjo;
- **popolnost:** informacija daje uporabniku vse potrebne elemente za sprejemanje odločitev;
- **zgoščenost:** predstavlja kratkost in jedrnatost informacije, ki nudijo uporabniku le podrobnosti, ki jih potrebuje;
- **ustreznost:** pove, do kakšne mere je informacija prilagojena potrebam uporabnika;
- **razumljivost:** informacija mora biti pripravljena tako, da jo bo uporabnik zlahka razumel in uporabil;
- **objektivnost:** pomeni odražanje realnega stanja (Gradišar, Resinovič, 2001, str. 61).

### 3.1.3 Delitev IS

IS se v osnovi delijo na **centralizirane in decentralizirane.**

Struktura **centraliziranega IS** je takšna, da je ves informacijski potencial organizacije – strokovnjaki, naprave, metode in podatki - centraliziran. Uporaba centraliziranega informacijskega sistema omogoča standardizacijo postopkov in podatkov. Vsak podatek se v skupno bazo evidentira le enkrat, zaradi česar ne prihaja do podvajanja podatkov. Tak sistem zagotavlja visoko stopnjo varnosti, kontrole in zaščite podatkov. Zaradi kompleksnosti se tak sistem težko prilagaja novim informacijskim potrebam, težje okvare računalniške opreme pa vplivajo na celotno poslovanje organizacije. Stroški vzdrževanja takšnega sistema so visoki.

V **decentraliziranem IS** se celoten proces generiranja informacij izvaja neposredno pri uporabniku. Vsak informacijski podsistem vzdržuje lastno podatkovno bazo in izvaja lokalno obdelavo podatkov. Tak sistem je cenejši od centraliziranega, vendar obstaja nevarnost podvajanja podatkov (Gradišar, Resinovič, 2001, str. 350-351).

**Osnovne sestavine** IS so:
- informacijska tehnika,
- informacijska tehnologija (v nadaljevanju: IT),
- ljudje,
- podatki ter
- metode in načini njihovega usklajevanja in povezovanja.

**Osnovne značilnosti** sodobno organiziranega IS so:
- **kompleksnost**;
- **integriranost:** informacijski sistem je sestavljen iz več podsistemov, vendar deluje kot celota;

- **dinamičnost**: IS se je sposoben nenehno prilagajati notranjim in zunanjim spremembam procesov;
- **samoorganiziranost**;
- **odprtost** in
- **usmerjenost k upravljanju** (Bobek, Lesjak, 1993, str. 23 - 27).

### 3.1.4 Načrtovanje IS

Za uspešen začetek razvoja IS je pomembno načrtovanje IS, ki naj temelji na strateških usmeritvah organizacije. Razvoj IS je skupek nalog, potrebnih za izgradnjo programske rešitve za določen poslovni problem.

Pri načrtovanju in razvoju IS je potrebno upoštevati naslednje (Natek, 1990, str. 6):
- **odzivnost sistema**: čas od naročila do prejema podatkov;
- **razpoložljivost podatkov**: verjetnost, da bo podatek na voljo, ko ga bodo uporabniki potrebovali;
- **natančnost:** verjetnost, da so podatki, ki jih IS zagotavlja, skladni z izvornimi podatki;
- **posredovanje podatkov**: uporabniku so posredovani samo podatki, ki jih potrebuje;
- **dostopnost podatkov**: način, kako uporabnik dostopa do podatkov;
- **zagotavljanje sledi uporabe podatkov**: možnost ponovitve vseh postopkov;
- **varnost podatkov:** zadostna zagotovila, da nepooblaščene osebe ne bodo imele dostopa do podatkov oziroma možnosti spreminjanja podatkov;
- **zanesljivost IS:** zagotovljeno neprekinjeno delovanje IS ter onemogočeno nenadzorovano spreminjanje;
- **standardiziranost:** usklajenost s standardi in načeli dobre prakse na področju razvoja IS.

Nekatere od **tehnik načrtovanja IS so:**
- **stopnja rasti;**
- **SCF**. Metoda je sestavljena iz štirih korakov, in sicer analize osnovnega poslanstva organizacije, določitve kritičnih dejavnikov uspeha, kot sta organizacijska struktura in tržna strategija, določitve informacijskih potreb in načrtovanje izboljšanja informacijske podpore za posamezne dejavnike;
- **analiza strategije naložb;**
- **načrtovanje poslovnih sistemov** (BSP);
- **prenova poslovnih procesov**.

### 3.1.4 Metodologija razvoja IS

Obstajajo različne metode razvoja IS:
- **Metoda razvoja življenjskega cikla** (Systems Development Life Cycle - SDLC).
- **Tradicionalni pristop**. Razvoj računalniške rešitve ne poteka po formalnem postopku. Dokumentacija k rešitvi nastaja ob snovanju rešitve. Dokumentacija je velikokrat nepopolna.
- **Metoda prototipa**. Ta metoda se uporablja pri načrtovanju rešitev za osebne računalnike. Pri tej metodi se najprej izgradi začetna prototipna rešitev, ki se jo izpopolnjuje do končne sprejemljive rešitve.
- **Razvoj s strani končnih uporabnikov**. Uporabniki sami razvijejo preproste računalniške rešitve za določeno področje.
- **Uporaba programskih paketov**. Nakup že razvitih programskih rešitev.

Najbolj uporabljena metoda za razvoj obsežnejših IS je metoda razvoja življenjskega cikla (Gradišar, Resinovič, 2001, str. 422).

#### 3.1.4.1 Metoda razvoja življenjskega cikla

Metoda predstavlja klasičen pristop k razvoju IS. Primerna je za razvoj obsežnejših projektov. Sestavljena je iz naslednjih faz (Turban et al., 2003, str. 464-471, Ruthberg et al., 1991, str. 1-1):

1. **Pobuda za projekt.** Pobudo navadno podajo uporabniki, ki se pri delu srečajo z določeno težavo. V tej fazi se izvede študija izvedljivosti, ki da odgovor na vprašanje o izvedljivosti projekta. Študija mora zajeti tehnologijo, stroške/koristi, možna tveganja, sprejemljiva odstopanja in upoštevanje zakonskih predpisov.
2. **Sistemska analiza.** Definiranje uporabniških zahtev.
3. **Razvoj**. V tej fazi se načrtuje vhode, izhode, obdelavo, podatkovne baze, telekomunikacije, potrebne kontrole in varnost.
4. **Programiranje ali nakup rešitve.** Razvoj IS ali nakup že obstoječega programskega paketa.
5. **Testiranje.** Namenjeno je preizkušanju delovanja razvitega IS in odkrivanju napak v posamezni fazi razvoja. Sintaktične napake je lažje odkriti, ker program napako javi. Težje je odkriti logične napake, katerih rezultat je napačno delovanje programa.
6. **Uvajanje in uporaba sistema.** Uvedba nove rešitve v delovanje. Eden od mogočih načinov implementacije je uvedba, kjer »stara« in »nova« rešitev nekaj časa delujeta vzporedno. Mogoča je tudi takojšnja uvedba nove rešitve in ukinitev stare, kar pa predstavlja večje tveganje. V tej fazi je pomembno usposabljanje uporabnikov.
7 **Delovanje.** Delovanje in uporaba rešitve.

8. **Vzdrževanje.** V celotni življenjski dobi razvitega IS je potrebno skrbeti za vzdrževanje. Sistem je potrebno tudi nadgrajevati oziroma dodati nove funkcionalnosti.

Omenjena metoda omogoča fazni razvoj in zgodnje odkrivanje napak. Pri razvoju IS je pomembno dejstvo, da je napake potrebno odkriti čim prej. Nepravočasno odkrite napake je težje odpraviti, stroški za odpravo teh napak pa so višji. Ena od slabosti metode SDLC je ta, da je dokaj toga, razvoj pa je drag in dolgotrajen. Že definirane uporabniške zahteve je težko spremeniti.

#### 3.1.4.2 Metodologija vodenja projektov v državni upravi

V državni upravi je uveljavljena metoda razvoja projektov na osnovi metodologije PRINCE (PRoject IN a Controled Environment). Metodologija je bila prvotno namenjena le vodenju projektov na področju informacijske tehnologije, vendar jo danes uporabljajo na vseh strokovnih področjih. PRINCE kot eno od standardnih metodologij za vodenje projektov uporablja tudi EU (Metodologija vodenja projektov v državni upravi, 1997).

Osnovni elementi metodologije so:
- **organizacija:** razporeditev odgovornosti in nalog pri projektu;
- **načrti:** stalne aktivnosti pri kateremkoli projektu so načrtovanje, pregled izdelanega in ponovno načrtovanje. Pripravijo se načrti projekta, načrt faze projekta in podrobnejši načrt aktivnosti. V primeru odstopanj se pripravi izredni načrt;
- **nadzor**: zagotavljanje pravočasnosti izvedbe projekta, nadzor stroškov in kakovosti izdelane rešitve;
- **izdelki**: izdelek se opredeli že na začetku projekta.
- **postopki za izvedbo**.

## 3.2 Telekomunikacijska tehnologija

Bistvo računalniških mrež je izmenjava informacij ali **komuniciranje** (Simič, 1988, str. 13). Komuniciranje je proces posredovanja informacij med oddajnikom in sprejemnikom. Informacije se med njima posredujejo v obliki **sporočil**. Oddajnik (oseba, računalnik) sporočilo pošlje, sprejemnik (oseba, računalnik) pa ga sprejme. Sporočilo potuje po **komunikacijskem mediju.**

Pri telekomunikaciji se sporočilo v kakršnikoli obliki prenaša na daljavo. Sporočila se prenašajo po žičnih, svetlovodnih ali radijskih napravah. Primer takšnih sporočil je telefonski pogovor, elektronska pošta in podobno (Gradišar, Resinovič, 2001, str. 265).

**Telekomunikacije potekajo** po telekomunikacijskih mrežah. Posamezna naprava v mreži se imenuje vozlišče. Vozlišče je lahko računalnik, telefon in podobno. Med vozlišči potujejo podatki, ki predstavljajo promet mreže. Podatke je pred pošiljanjem potrebno preoblikovati v obliko, ki je primerna za prenos. Omenjeni postopek se imenuje **kodiranje**. Po prejemu podatkov se sporočilo pretvori v prejemniku razumljivo sporočilo, kar se imenuje **dekodiranje**. Postopek kodiranja in dekodiranja se izvaja z **modemom**.

**Telekomunikacijska omrežja** se glede na vrsto delijo na:
- telefonska omrežja,
- radio in televizija; brezžični in kabelski prenos podatkov in
- računalniške mreže.

## 3.3 Računalniške mreže

**Računalniška mreža** je »omrežje, v katero sta povezana dva ali več računalnikov ter ki omogoča izmenjavo sporočil pa tudi souporabo sredstev, npr. računalniških programov, tiskalnikov in podatkov« (Turk, 2002, str. 357).

Računalniške mreže se v osnovi delijo na:
- LAN (Local Area Network) - lokalne računalniške mreže,
- WAN (Wide Area Network) - razprostrto računalniško omrežje.

Preko **lokalnega računalniškega omrežja** omejeno število uporabnikov izmenjuje velike količine informacij z veliko hitrostjo na omejenih razdaljah. Posebna oblika lokalnih mrež so mestne mreže, ki pokrivajo določeno območje, med seboj pa so povezane v razprostrta računalniška omrežja (CISA Review Manual, 2003, str. 135-139).

**Razprostrta računalniška omrežja** povezujejo krajevno oddaljene točke. Prenos podatkov lahko poteka preko žic (koaksialni, optični, stekleni kabel) ali brezžično (po zraku), kjer fizična povezava ni potrebna (sateliti, mikrovalovi, laserski žarki, radijski valovi).

**Računalniško izmenjavanje podatkov** poteka preko elektronske pošte, zvočne pošte, telefaksa in telekonference. Največje omrežje, ki omogoča izmenjavo elektronske pošte, je Internet.

**Internet** je omrežje, ki med seboj povezuje druga računalniška omrežja. Dostop v Internet je možen preko ponudnikov Internetnih storitev (ISP - Internet Service Provider). Za uporabo Interneta je potrebna dobra telekomunikacijska infrastruktura. Delovanje omrežij, ki sestavljajo Internet, omogočajo ponudniki omrežnih storitev (NSP – Network Service Provider).

Pri prenosu po telekomunikacijskih omrežjih je posebnega pomena **varnost in zaščita** omrežij ter varovanje podatkov, da med prenosom ne pridejo v roke nepooblaščenim osebam.

## 3.4 Varovanje in zaščita informacij in IS

IT postaja temeljno premoženje organizacij, poslovanje organizacij pa je od delovanja informacijske tehnologije vse bolj odvisno. Zato postajajo vse pomembnejša zagotovila, da so IS v uporabi varni in zanesljivi. IS mora biti varovan pred najrazličnejšimi grožnjami iz okolja.

**Ključni dejavniki** za delovanje internega kontrolnega sistema varovanja IS so:
- varnostna politika,
- implementirane interne kontrole,
- delovanje internega kontrolnega sistema,
- prepoznavanje, razumevanje in ovrednotenje tveganj ter
- usposabljanje zaposlenih (Javornik, 2000, str.7).

Proces varovanja v organizaciji je potrebno izgraditi, nadzorovati, spremljati in o delovanju poročati. V organizaciji morajo biti varovane in zaščitene vse informacije, ki se pojavljajo v različnih oblikah, npr. zapisi na papirju, informacije za zbirke podatkov, filme, prosojnice, modele, magnetne trakove, diskete in druge.

Varovanje in zaščita informacij in IS vsebuje naslednje značilnosti:
- **zaupnost** (confidentiality): zagotovitev, da so pomembne informacije na voljo le pooblaščenim osebam in da so zaščitene pred nepooblaščenim prestrezanjem ali razkritjem;
- **neoporečnost** (integrity): varovanje točnosti (accuracy) in popolnosti (completeness) informacij in programske opreme;
- **razpoložljivost** (availability): zagotovilo, da so informacije in osnovne storitve uporabnikom na voljo takrat, ko jih potrebujejo (Kodeks varovanja informacij, 1997).

### 3.4.1 Ogroženost IS

IT je ogrožena iz mnogih vidikov. Ogrožajo jo **nevarnosti, nesreče** in razne oblike **računalniškega kriminala.**

**Nevarnosti, ki ogrožajo IS:**

- **Nedokončani projekti**. Velik odstotek projektov izgradnje IS je neuspešen. Največja nevarnost je v tem, da so v projekt vložena obsežna finančna sredstva, končni rezultat pa ne dosega načrtovanega.

Največje nevarnosti so:
- projekti niso pravočasno dokončani;
- projekti presegajo načrtovane stroške;
- nove rešitve ne ustrezajo potrebam uporabnikov;
- pri delovanju razvitih rešitev se pojavljajo napake;
- uporabniki so dejavni samo pri testiranju;
- slabo sodelovanje med uporabniki in oddelkom informatike;
- pri projektu sodelujejo neizkušeni sodelavci;
- kontrolne funkcije se v sistem vgrajujejo šele po pričetku delovanja sistema (Drobnič, 1996, str. 24).

Gradišar in Resinovič k temu dodajata še naslednje:
- projekt nima dovolj podpore s strani vodstva oziroma se zdi predrag;
- zapletene zahteve za definiranje oziroma sistem ni tehnično izvedljiv;
- pomanjkljivo sodelovanje med uporabniki in razvijalci;
- uporabniki razvitega sistema ne želijo uporabljati;
- sistem preverjanja pravilnosti podatkov in delovanja ni dovolj dobro izdelan;
- sistem deluje počasi oziroma ni dovolj učinkovit;
- sistem ne ustreza spremenjenim poslovnim potrebam (Gradišar, Resinovič, 2001, str. 448).

**Ostale nevarnosti, ki ogrožajo IT:**

- **nesreče:**
  - napačno ravnanje operaterja: nepozornost, neupoštevanje organizacijskih predpisov, dogovorov itd.;
  - okvare strojne opreme;
  - okvare programske opreme;

  - napake v računalniških programih;
  - **napačni podatki**; podatki se večinoma vnašajo ročno, kar predstavlja veliko verjetnost za nastanek napak;
  - neprimerne tehnične karakteristike: te se odražajo tako, da z razpoložljivo računalniško opremo ni mogoče izvesti zahtevanih nalog;
  - neodgovornost.
- **računalniški kriminal in zlonamerne škode**: sabotaže, kot na primer puščanje skrivnih vrat, skozi katera sistemski inženirji nenadzorovano dostopajo do sistema, trojanski konji, virusi, logične bombe in podobno;
- **uporabniške napake;**
- **težave z električnim napajanjem;**
- **vohunstvo;**
- **prevare;**
- **kraje, tatvine;**
- **naključne napake in druge odpovedi** (Laudon, 2000, str. 499).

**Vnos podatkov** je najbolj kritičen za nastanek napačnih podatkov. Primeri vnosnih napak so:
- napačno prebrani izvorni podatki,
- zamenjava številk,
- napačno vnesena šifra (oziroma koda) oziroma šifra ni vnesena,
- podatek je vnesen v napačno polje,
- okrajšave.

Pri vnosu podatkov preko internetnih aplikacij se verjetnost napak še poveča (Eckerson, 2002, str. 8-12).

### 3.4.2 Varnostna politika

Zaradi vsega navedenega je potrebno informacije in IS primerno varovati. Pomembna naloga vodstva je varovanje vseh sredstev organizacije. To še posebej velja za informacije in podatke ter informacijsko in telekomunikacijsko tehnologijo. Nevarnosti, ki ogrožajo IT, je potrebno ustrezno predvideti in z njimi upravljati. V nasprotnem primeru lahko popolnoma ohromijo poslovanje organizacije.

Varovanje IS se zagotavlja z vzpostavitvijo politik, postopkov in ukrepov, s katerimi se preprečuje nepooblaščen dostop, spreminjanje, kraja ali fizično poškodovanje IS (Laudon, 2000, str. 502).

Navodila in pravila za ravnanje s tveganji se zapišejo v dokument, ki se imenuje »Varnostna politika« (Security Policy) in je ključnega pomena za učinkovito varovanje sredstev organizacije. Metodologija za vzpostavitev varnostne politike v organizaciji temelji na oceni tveganja. V dokumentu se natančno opredeli postopke ravnanj v primeru težav, kršitev in podobno. Vodstvo organizacije z objavo dokumenta »Varnostna politika« opredeli usmeritev, podporo in zavzetost za varovanje informacij in sredstev organizacije. Dokument mora biti na voljo vsem zaposlenim, ki so odgovorni za varovanje informacij. Dokument je potrebno redno vzdrževati.

**Ključne sestavine dokumenta varnostna politika so:**
- varovanje in kontrola dostopa do informacij,
- usklajenost z zakoni in predpisi,
- ustrezno usposabljanje zaposlenih z namenom povečevanja zavedanja o pomembnosti varovanja informacij in sredstev organizacije,
- kazni zaradi neskladnosti (Derek, 2002, poglavje 3, str. 1).

Kodeks varovanja informacij k temu dodaja še naslednje:
- politika preprečevanja in odkrivanja virusov,
- načrtovanje neprekinjenega poslovanja,
- opredelitev odgovornosti in
- opredelitev postopkov poročanja ob sumu varnostnih incidentov (Kodeks varovanja informacij, 1997, str. 16).

# 4 REVIDIRANJE

Temeljna naloga revidiranja je preverjanje kontrolnega sistema in je izpolnjena tedaj, če funkcija revidiranja sistematično presoja vsa pomembna poslovna področja z vidika postavitve in delovanja sistema notranjih kontrol (Brečko, 2001, str. 5).

Namen revidiranja je prepoznati slabosti v sistemu in pomagati vodstvu zmanjšati ali odstraniti potencialna tveganja.

## 4.1 Opredelitev revidiranja

Taylor in Glezen povzemata definicijo revidiranja, ki jo je opredelila AAA[14]. Revidiranje je po AAA sistematičen postopek nepristranskega pridobivanja in vrednotenja dokazov v zvezi z uradnimi trditvami o gospodarskem delovanju in dogodkih za ugotavljanje stopnje skladnosti teh uradnih trditev z uveljavljenimi sodili. Vključuje poročanje o izsledkih zainteresiranim uporabnikom (Taylor in Glezen, 1996, str. 32).

Turk opredeljuje **revidiranje** kot pretežno popravljalno, poznejše nadziranje, ki je zasnovano na izvedenskem obnavljanju. Na podlagi revidiranja se oblikuje sodba o pravilnosti revidiranega procesa ali stanja. Obsega oblikovanje in ovrednotenje dokazov o trditvah v zvezi s predmetom nadziranja ter poročanje o ugotovitvah pristojnim za ukrepanje. Razlikuje se od kontroliranja in inšpiciranja (Turk, 2000, str. 644; Turk, 2002, str. 379).

**Revizija** je »posamezen posel revidiranja pri posamezni organizaciji, ki naj bi vodil do izsledkov« (Turk, 2002, str. 380).

## 4.2 Razvrstitev revidiranja

### 4.2.1 Razvrstitev revidiranja glede na povezanost posameznika ali skupine

**Glede na povezanost posameznika ali skupine**, ki opravlja revizijo, se revidiranje deli na:
- zunanje revidiranje,
- notranje revidiranje in
- državno revidiranje (Taylor in Glezen, 1996, str. 35).

[14] AAA – American Accounting Association, Sarasota, Florida, 1973, str. 2.

**Zunanje revidiranje** izvajajo zunanji revizorji, ki niso uslužbenci organizacije, ki je predmet revidiranja.

**Notranje revidiranje** je neodvisno in nepristransko dajanje zagotovil in svetovanje z namenom povečevanja koristi in izboljšanja delovanja organizacije. Organizaciji pomaga pri uresničevanju ciljev s spodbujanjem premišljenega in urejenega načina vrednotenja in izboljševanja uspešnosti postopkov ravnanja s tveganji ter obvladovanjem in upravljanjem s tveganji (Standardi notranjega revidiranja, 2003).

**Državno revidiranje** je revidiranje različnih organizacijskih funkcij. Izvajajo ga državni uslužbenci (Taylor in Glezen, 1996, str. 36). V Sloveniji to področje urejajo Usmeritve za državno notranje revidiranje[15], ki opredeljujejo notranje revidiranje v sistemu notranjega nadzora javnih financ. Temeljijo na standardih notranjega revidiranja in so namenjene notranjim revizorjem pri revidiranju proračunskih uporabnikov[16].

**Naloga** tako notranjega kot zunanjega revizorja je »preverjanje in ocenjevanje kvalitete delovanja sistema notranjih kontrol«. Pri tem ugotavlja, ali sistem notranjih kontrol deluje tako, kot je bil oblikovan, ali je ustrezno zasnovan glede na tveganja ter preverja stroške izvajanja glede na koristi sistema. Revizor o svojih ugotovitvah pripravlja revizijska poročila s priporočili. Revizor ne sme biti del operativnega delovnega postopka in ne sme odrejati korekcijskih akcij (Turk, 2001, str. 2-4).

### 4.2.2 Razvrstitev revidiranja glede na cilje delovanja

**Glede na cilje delovanja** se revidiranje deli na:
- revidiranje računovodskih izkazov,
- revidiranje skladnosti s predpisi in
- revidiranje poslovanja (Taylor in Glezen, 1996, str. 33).

**Revidiranje računovodskih izkazov** (Financial Statement Audit) je zbiranje dokazov o uradnih trditvah v računovodskih izkazih podjetja ter uporabljanje teh dokazov za preverjanje njihove skladnosti s splošno sprejetimi računovodskimi načeli.
Notranje revidiranje računovodstva je naknadno presojanje pravilnosti sistema računovodskega kontroliranja podatkov in zanesljivosti delovanja. Revidiranje naj

[15] Usmeritve za državno notranje revidiranje, 2003.
[16] Proračunski uporabnik je v skladu s 34. in 65. členom Zakona o javnih financah odgovoren za obe strani proračuna, tako za prejemke kot izdatke.

zagotovi pravilnost podatkov, ki vstopajo in se obdelujejo v informacijskem podsistemu ter pravilnost informacij, ki iz podsistema izstopajo (Hočevar in Igličar, 1995, str. 214).

**Revidiranje skladnosti s predpisi** (Compliance Audit) je ugotavljanje, ali zaposleni oziroma podjetje delujejo v skladu s predpisi, zakoni, usmeritvami in drugimi predpisi. Večina državnih revizorjev izvaja tovrstno revidiranje.

**Revidiranje poslovanja** (Operational and Performance Audit) sodi v širše pojmovanje revidiranja. Namen revidiranja je ocenitev strukture notranjih kontrol na določenem področju.

Ratliff in Reding (2002, str. xviii) k navedenemu dodajata tudi:
- revidiranje IS in
- revidiranje prevar.

## 4.3 Notranje revidiranje in postopki revidiranja

Temeljna sestavina in obveznost vodstva pri vodenju organizacije je nadziranje izvajanja delovnih nalog. V manjših organizacijah opravlja nalogo notranje revizije vodstvo z izvajanjem neposrednega nadzora. V večjih organizacijah nadzor izvaja notranjerevizijska služba.

**Cilji nadziranja so:**
- zagotoviti gospodarno, učinkovito in uspešno poslovanje organizacije;
- zagotavljanje varovanja sredstev organizacije pred izgubo zaradi malomarnosti, zlorab, slabega gospodarjenja, napak in poneverb ter drugih nepravilnosti;
- zagotavljanje skladnosti poslovanja organizacije z zakonskimi in drugimi predpisi, notranjimi pravili in navodili vodstva;
- zagotavljanje zanesljivih računovodskih in drugih podatkov in informacij ter resnično in pošteno prikazovanje teh podatkov in informacij v poročilih (Standardi notranjega revidiranja, 2003, str. 4).

Vzpostavitev funkcije notranjega revidiranja je za nekatere organizacije tudi zakonsko predpisana. V Sloveniji to velja za banke[17] in zavarovalnice[18] ter za vse neposredne uporabnike državnega in občinskega proračuna[19], ravno tako pa tudi za prejemnike finančnih sredstev EU.

[17] Zakon o bančništvu, 1999.
[18] Zakon o zavarovalništvu, 2004.
[19] Zakon o javnih financah, 1999.

**Cilj notranjega revidiranja** je pomagati vodstvu organizacije pri učinkovitem opravljanju vodstvenih nalog. Notranjerevizijska služba to nalogo izvaja z dajanjem strokovnih ocen stanja in podajanja priporočil za izboljšave. To izvaja s presojanjem učinkovitost neposrednih in posrednih notranjih kontrol v organizaciji. Pri tem mora upoštevati načelo gospodarnosti, torej da koristi revidiranja presegajo stroške, ki z revidiranjem nastanejo (Standardi notranjega revidiranja, 2003, str. 5).

**Temeljni cilji notranjega revidiranja so:**
- revidiranje skladnosti poslovanja z zakonskimi predpisi, smernicami, načrti in postopki,
- varovanje sredstev organizacije,
- gospodarna in učinkovita uporaba virov sredstev,
- doseganje zastavljenih ciljev in nalog (Kodeks notranjerevizijskih načel, 1998).

Notranji revizor poroča neposredno vodstvu. Delo opravlja v skladu s standardi notranjega revidiranja, ki obsegajo:
- neodvisnost in nepristranskost,
- poklicno strokovnost,
- področje dela,
- opravljanje revizijskega dela in
- vodenje notranjerevizijske službe (Majič, 2001, str. 2).

Neodvisnost in nepristranskost se zagotavljata tako, da je notranjerevizijska služba organizirana kot samostojna organizacijska enota. Notranji revizor se mora izogibati navzkrižju interesov. Pri svojem delu mora biti nepristranski in neodvisen ter brez predsodkov. Pri opravljanju dela svojega mnenja ne podreja presoji drugih.

**Namen notranjerevizijskih načel in temeljna notranjerevizijska načela:**
- Načela so notranjemu revizorju v pomoč pri opravljanju nalog. Opredeljujejo nadziranje in cilj notranjega revidiranja. Notranji revizor ne sme imeti glede revidiranega področja nobenih pristojnosti. Delovati mora v skladu s standardi notranjega revidiranja in kodeksom poklicne etike notranjega revizorja.

**Načela o strokovnosti in neodvisnosti:**
- Dolžnost vsakega revizorja je primerna strokovna usposobljenost in obvladovanje poklicnih veščin. Pri opravljanju svojega dela mora pozornost posvetiti odkrivanju namernih prevar, napak, neučinkovitosti, škode, neuspešnosti in sporov zaradi koristi. O sumu prestopkov mora obveščati osebo, odgovorno za revidirano področje (Kodeks notranjerevizijskih načel, 1998).

### 4.3.1 Organiziranost službe za notranjo revizijo

Listina o ustanovitvi notranjerevizijske službe (Audit charter), ki jo odobri predstojnik organizacije, je temeljna listina o delovanju notranjerevizijske službe. Opredeljuje namen in način delovanja, pooblastila in odgovornosti (Standardi notranjega revidiranja, Navodila za postopke, 2003, str. 1).

Služba za notranjo revizijo opravlja dve temeljni nalogi, in sicer dajanje zagotovil in svetovanje, z namenom povečevanja koristi in izboljševanja delovanja organizacije. Revizor pri dajanju zagotovil poda nepristransko in neodvisno mnenje o preiskovanem področju v obliki pisnega poročila. Pri svetovalni dejavnosti revizor ustno svetuje vodstvu.

**Dajanje zagotovil obsega:**
- ovrednotenje kontrolnih postopkov za posamezne poslovne procese,
- primerjava doseženih rezultatov z načrtovanim,
- analiza učinkovitosti uporabe določenih virov,
- dajanje zagotovil skladnosti poslovanja z zakonodajo,
- raziskava prevar,
- skrbni pregled poslovanja.

**Svetovanje obsega:**
- svetovanje vodstvu,
- pomoč vodstvu pri sprejemanju odločitev,
- odpravljanje napak in sodelovanje v različnih projektnih skupinah (Nemec, 2003, str. 9).

### 4.3.2 Izvedba revizijskega pregleda

**Koraki revizijskega pregleda** so naslednji:
- opredelitev vsebine revizijskega pregleda,
- priprava na revizijski pregled,
- revizijski pregled,
- priprava revizijskega poročila (Turk, 2001, str. 15-17).

Notranja revizija mora biti načrtovana in odobrena. Za vsako revizijsko nalogo je potrebno izdelati revizijski načrt. Podatke in informacije je potrebno preveriti in ovrednotiti. O izsledkih je potrebno poročati ter spremljati izvajanje predlaganih ukrepov.

**Opravljanje revizijskega dela obsega:**

1. **Načrtovanje revizijskega pregleda.**
   Načrtovanje mora biti dokumentirano. Načrtovanje revizijskega pregleda obsega:
   - določitev ciljev, obsega in vsebine pregleda ter izdelava načrta dela;
   - oblikovanje revizijske skupine;
   - priprava revizijskega programa;
   - najava pregleda revidirani enoti;
   - pregled revizijskega poročila in dokumentacije predhodnega revizijskega pregleda;
   - izdelava poteka pregleda (Turk, 2003, str. 2).
2. **Zbiranje, proučevanje in ovrednotenje informacij ter dokumentiranje izsledkov.**
3. **Izdelava končnega revizijskega poročila.**
4. **Nadaljnje spremljanje** (Kodeks notranjerevizijskih načel, 1998, Standardi notranjega revidiranja, 2003).

Rezultat revizijskega pregleda je **revizijsko poročilo**. Revizijsko poročilo mora biti nepristransko, jasno, zgoščeno in pravočasno. Vsebovati mora:
- uvod,
- cilje in področje revidiranja,
- revizijske izsledke,
- priporočila, predloge za izboljšavo ali potrdilo o zadovoljivem delovanju (Lešnik Korbar, 2001, str. 10).

# 5 Revidiranje IS

Za zbiranje, shranjevanje in obdelovanje informacij se danes v večini organizacij uporabljajo zmogljivi računalniški sistemi. Za uspešno poslovanje organizacij so informacije temeljnega pomena. Posledice napačnega delovanja IS lahko privede do napačnih poslovnih odločitev, zlorab oziroma prevar, nezakonitega poslovanja in podobno.

Ker je danes večina poslovnih procesov odvisnih od delovanja IS, praktično vse revizije vključujejo tovrstno revidiranje. Revidiranje IS preiskuje zanesljivost (reliability) IS in neoporečnost (integrity) informacij kot izhodov iz sistema (Ratliff in Reding, 2002, str. xxi).

Pri revidiranju IT se preverja skladnost poslovanja s predpisi (zakoni, pravili, standardi) in dobrimi navadami na področju IT. Revizor mora pridobiti zadostna zagotovila o obstoju notranjih kontrol, njihovi učinkovitosti in stalnosti (Mugerle, 1995, str. 70).

Namen revidiranja IS je ocenjevanje obstoja, ustreznosti in zadostnosti splošnih in aplikativnih kontrol. Pri revidiranju IS je pomembno razumevanje računovodskih in drugih internih kontrol v sistemu, s tem povezanih tveganj ter način izvedbe testiranja delovanja kontrol (Javornik, 2001, str. 4).

Revidiranje IS je preizkušanje kakovosti delovanja IS z izbranimi sodili in oblikovanje načinov za preprečevanje oziroma odpravljanje njenih nepravilnosti. Revidiranje IS je presojanje računalniškega obravnavanja podatkov (Turk, 2001, str. 125).

Pri svojem delu revizor deluje v skladu z mednarodno sprejetimi standardi za revidiranje IS. Standardi opredeljujejo revizorjevo odgovornost, neodvisnost, pristojnosti, stalno izpopolnjevanje in izobraževanje, načrtovanje in izvedbo dela, poročanje in ponovno izvedbo pregledov (IS Standards, Guidelines and Procedures for Auditing and Control Professionals, 2002).

V organizaciji mora biti področje izvajanja revizij s področja IT jasno določeno. Ponavadi je opredeljeno v ustanovni listini o delovanju notranje revizijske službe.

**Načrtovanje in izvedba pregleda**

Revizor IS opravlja svoje delo v skladu s postopki, opisanimi v poglavju »Revidiranje«. Pri izvajanju revizijske naloge opazuje procese, pregleduje dokumentacijo, izvaja intervjuje, išče in preverja podatke in izvaja preglede uporabniških aplikacij z namenom

ugotovitve zadostnega obstoja notranjih kontrol za preprečevanje, odkrivanje in zmanjševanje učinkov tveganj (Uratnik, 2002, str. 265).

Ena od nalog revizorja IS je zagotoviti, da je revizijski pregled načrtovan in v skladu s poslovnimi cilji. Revizije IS je mogoče izvajati kot samostojne preglede ali hkrati z rednimi notranjerevizijskimi pregledi (Silltow, Internet, 2004).

**Pri izvedbi revizijskega pregleda mora revizor izvesti naslednje:**
- **Priprava na pregled**: Pregled seznama zaposlenih v oddelku za informatiko ter opisa del in nalog; priprava pregleda celotne IT in seznama vseh aplikacij.
- **Pregled predhodnih revizijskih poročil:** Pregled, ali je vodstvo ukrepalo v skladu s priporočili.
- **Priprava in izpolnjevanje vprašalnika o notranjih kontrolah:** Pregled upravljanja IT; pregled strateških dokumentov; pregled kontingenčnega načrtovanja; pregled razvoja IS in programiranja; pregled delovanja računalnikov.
- **Priprava revizijskega poročila** (Ray, Internet, 1999).

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

## 5.1 Tveganja in notranje kontrole

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

ISACA povzema definicijo tveganja po Smernicah za upravljanje varnosti IT, ki jih je izdala Mednarodna organizacija za standardizacijo[20]. Tveganje opredeljuje kot verjetnost, da bo grožnja povečala ranljivost sredstev organizacije, kar lahko privede do izgub ali poškodb sredstev (CISA Review Manual 2003, str. 28-30).

[20] Information Technology - Guidelines for the Management of IT Security. International Organization for Standardization/IEC TR 13335-1, 1996.

Pri poslovanju vedno obstaja 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).

Organizacija naj bi izvedla oceno tveganj ter pripravila in izvajala ukrepe za zmanjševanje ali preprečevanje tveganj na sprejemljivo raven (Hajtnik, 2002, str. 2).

Izbira ustreznih kontrol temelji na primerjavi stroškov vzpostavitve kontrol v primerjavi s koristmi, ki bi jih imela organizacija od vzpostavitve kontrol ter na odločitvi o nivoju tveganja, ki ga je vodstvo pripravljeno sprejeti (Derek, 2003, str. 2-6).

Opredelitev in zmanjševanje tveganj je naloga vodstva podjetja. Ovrednotenje in ocenjevanje sistema upravljanja s tveganji izvajajo revizorji.

**Ravnanje s tveganji** je proces ugotavljanja, ovrednotenja in upravljanja s tveganji. V procesu ravnanja s tveganji se opredeli:
- vrste tveganja, ki bi lahko vplivalo na varnost poslovanja organizacije in določanje verjetnosti pojava,
- vpliv na poslovanje,
- ukrepe za ublažitev učinkov posameznega tveganja (ISACA Review Manual 2003, str. 29 in 374).

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

Nekatere od **posledic neuspešnega obvladovanja tveganj** so:
- izguba prihodkov,
- napačno poročanje,
- zmanjšanje ali izguba konkurenčne prednosti in izguba ugleda,
- zmanjšanje produktivnosti zaradi neobvladovanja procesa,
- izgube zaradi izgubljenih poslovnih priložnosti,
- kršitve zakonov in drugih predpisov (Javornik, 2001, str.4).

Tveganja pri računalniško podprtem poslovanju so tako tveganja, ki se pojavljajo pri ročnem izvajanju nalog kot tudi tveganja, ki so značilna samo za informacijsko podprte poslovne procese. Ta tveganja so:
- nepravilna uporaba IT,
- nesposobnost obvladovanja IT,
- nesposobnost prevesti uporabniške zahteve v tehnične specifikacije,
- nesposobnost hitrega reagiranja,
- kopičenje in ponavljanje napak,
- nepravilen vnos podatkov,
- kopičenje podatkov (Ruthberg, Fisher, Lainhart, 1991, str. 1-5).

Organizacije morajo tveganja prepoznati in vzpostaviti kontrole, ki bodo zmanjševale škode, povezane z morebitnim nastankom neželjenega dogodka. Izbira kontrol je povezana s stroški in stopnjo zanesljivosti.

### 5.1.1 Kontrolno okolje

Vodstvo organizacije mora vzpostaviti **kontrolno okolje**, s katerim dosega zastavljene cilje poslovanja. Najpomembnejše kontrole, ki jih je potrebno vzpostaviti v organizaciji, morajo biti vzpostavljene na podlagi zakonodaje in predpisov, ali pa morajo predstavljati splošno priznano dobro prakso.

**Kontrole** so politike, postopki, dobra praksa in organizacijske strukture, vzpostavljene z namenom zagotavljanja razumnih zagotovil, da bodo poslovni cilji doseženi ter da bodo neželjeni dogodki preprečeni oziroma zaznani in popravljeni (metodologija COBIT[21] povzema definicijo po COSO Report - Internal Control – Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission, 1992) (Vallabhaneni, 1998, str. 3).

**Temeljne interne kontrole** so:
- skladnost (compliance) poslovanja z zakonodajo in predpisi,
- gospodarnost, učinkovitost in uspešnost poslovanja,
- zanesljivost informacij,
- preprečevanje prevar in korupcij,
- varovanje sredstev in informacij (Javornik, 2000, str. 7).

[21] COBIT je sistemski okvir oziroma metodologija kontrol v informacijski tehnologiji.

### 5.1.2 Sistem notranjih kontrol

Notranje kontrole so sestavni del upravljanja in vodenja organizacij. Pravilnost in zanesljivost podatkov in izvajanja poslovnih nalog sta odvisna od pravilnosti delovanja notranjih kontrol. Namen vzpostavitve kontrol nad poslovnimi dogodki je zagotoviti preprečevanje prevar in napak.

**Notranje kontrole** so politike, predpisi, postopki, običaji in organizacijske strukture, ki zagotavljajo razumno zagotovilo, da bodo poslovni cilji doseženi in da bodo nezaželjeni dogodki oziroma morebitne napake preprečene, zaznane in popravljene.

**Sistem notranjih kontrol** so notranji mehanizmi, ki jih vodstvo vzpostavi z namenom:
- varovanja osnovnih sredstev organizacije,
- zagotavljanja točnosti in zanesljivosti zapisov,
- zagotavljanja učinkovitosti postopkov,
- zagotavljanja skladnosti s politikami in zunanjimi predpisi (Hudoklin, 1996, str. 390).

Notranje kontrole delujejo na vseh nivojih organizacije z namenom zmanjševanja izpostavljenosti poslovanja različnim tveganjem. Notranje kontrole so lahko:
- ročne ali avtomatizirane,
- preventivne ali detektivne ter
- formalne ali neformalne.

Za izgradnjo učinkovitega sistema notranjih kontrol organizacije in pravilnost poslovanja je odgovorno vodstvo organizacije (CISA Review Manual, 2003, str. 30).

**Cilji notranjih kontrol** so zagotavljanje:
- **popolnosti:** vsi poslovni dogodki so evidentirani in ostanejo popolni na vsaki stopnji obdelave;
- **točnosti:** poslovni dogodki so pravilno obdelani;
- **odobritve**: zagotovljena je obdelava samo odobrenih poslovnih dogodkov.

Interne kontrole se delijo na:
- **notranje računovodske kontrole** (Internal accounting controls). Njihov namen je zagotavljanje varovanja sredstev in zagotavljanje razpoložljivosti finančnih zapisov;
- **administrativne kontrole** (Administrative controls). Predstavljajo uveljavljene standarde, pravila in postopke. Najpomembnejše administrativne kontrole so: delitev nalog, pisni postopki in pravila in nadzor;

  - **delitev nalog:** naloge zaposlenih se ne smejo prekrivati. S to kontrolo se zmanjša možnost napak in namernih prevar;
  - **pisni postopki in politike**: s pisnimi postopki in politikami se opredelijo standardi za izvajanje kontrole. Postopke in politike mora odobriti vodstvo organizacije. Odgovornosti morajo biti jasno opredeljene.
  - **nadzor:** Namen nadzora je preverjati, ali se predpisani kontrolni postopki izvajajo. Vsak kontrolni sistem, tudi če je zelo kvaliteten, je brez ustreznega nadzora mogoče obiti.
- **kontrole pri obdelavi podatkov** (Operational controls). Zagotavljajo, da so rezultati obdelav v skladu s cilji (Karnet in Tajnik, 2003, str. 9).

**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 presoja tveganja in predlagajo izboljšave (Brečko, 2001, str. 1-3).

### 5.1.3 Delitev kontrol

Interni kontrolni sistem varovanja IS sestavljajo:
- varnostna politika,
- implementiranje in delovanje internih kontrol ter
- prepoznavanje in ravnanje s tveganji (Javornik, 2000, str. 7).

Temeljna naloga revizorja IS je prepoznati slabosti pri poslovanju in vodstvu pomagati pri zmanjševanju ali odstranjevanju izpostavljenosti tveganjem in nevarnostim. To izvaja z ocenjevanjem stopnje tveganja in razvrščanjem napak glede na težo posledic za poslovanje. Z namenom zmanjševanja tveganj se v sistem vgrajujejo kontrole. Pri odločitvi o izbiri ustreznih kontrol je potrebno 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. Kontrole morajo uporabnikom predstavljati korist in ne smejo biti dražje od koristi. Za učinkovito delovanje sistema notranjih kontrol večinoma ne zadostuje le ena kontrola, temveč je potrebna kombinacija več kontrol ali uvedba dopolnilnih kontrol.

V osnovi se kontrole delijo na **splošne** in **aplikativne.**

**Splošne kontrole** predstavljajo politike in postopki, ki pomagajo zagotavljati kontinuirano in pravilno delovanje IS. Splošne kontrole podpirajo delovanje aplikativnih kontrol. Med splošne kontrole sodijo postopki, zapisniki, dnevniki, poročila ter zakonodaja, poslovniki, pravilniki, navodila in standardi.

**Splošne računalniške kontrole - splošni kontrolni okvir:**
- strategija in načrtovanje IS,
- splošna organizacija in vodenje,
- fizično in logično varovanje IS,
- dostop do podatkov in programske opreme,
- razvoj programske opreme in upravljanje z verzijami,
- odnosi s proizvajalci in dobavitelji,
- sistemska programska oprema in tehnična podpora,
- podpora strojne opreme,
- načrt neprekinjenega poslovanja in okrevalni načrt,
- omrežna tehnologija in telekomunikacije,
- razvoj in vzdrževanje podatkovnih baz (CISA Review Manual, 2003, str. 32; Podgoršek, 2003, str. 6).

**Aplikativne kontrole** so kontrole, vgrajene v aplikacije. Aplikativne kontrole so kontrole, ki dajejo zagotovila, da bodo aplikacije delovale v skladu z zahtevami in da bodo podatki točni, pravočasni in popolni. Delijo se na ročne in avtomatizirane. Aplikativne kontrole delujejo tako, da se odzovejo takoj, če se podatki ne ujemajo. Če so splošne kontrole nezadostne, tudi aplikativne kontrole ne zadoščajo, ker te predpostavljajo, da sistem deluje pravilno (Sawyer, 2003, str. 591).

Ročne kontrole niso računalniške kontrole, lahko pa se izvajajo s pomočjo računalniških izpisov. Podpirajo zagotavljanje točnosti, pravilnosti, popolnosti, pravočasnosti in pooblaščenosti.

**Aplikativne kontrole** se delijo na:
- vhodne kontrole (kontrole vnosa),
- kontrole obdelave,
- izhodne kontrole,
- kontrole funkcionalnosti (Laudon, 2000, str. 509).

**Kontrole vhodnih podatkov** se zagotavljajo s kontrolo popolnosti in točnosti vhodnih podatkov ter kontrolo veljavnosti poslovnih dogodkov. Pri tem je pomembno, da je vsak poslovni dogodek:
- evidentiran,
- računalniško obdelan,

- evidentiran samo enkrat,
- da je razkrito podvajanje poslovnih dogodkov.

Pomembno je, da IS sprejme vse poslovne dogodke. Vedeti pa moramo, kateri poslovni dogodki so bili zavrnjeni.

**Kontrole obdelav zagotavljajo:**
- da se obdelujejo samo točni in popolni podatki,
- da obdelavo sproži pooblaščena oseba.

**Kontrole izhodnih podatkov** dajo zagotovila:
- da so rezultati obdelav točni,
- da je dostop do podatkov dovoljen samo pooblaščenim osebam,
- da so podatki na voljo pravočasno (Drobnič, 1996, str. 38-42).

**Kontrole se po času delovanja delijo na:**

- **Preprečevalne** (Preventive Control): njihov namen je odkriti težavo, preden se pojavi. Preprečujejo nastanek nezaželjenih 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 nezaželjenih dogodkov. Primeri kontrol odkrivanja so izvajanje notranje revizijskega pregleda, dvakratno preverjanje izračunov, avtomatična sporočila o napaki itd.).
- **Korektivne (popravljalne) kontrole** (Corrective Control): kontrole, ki se uporabljajo po nastanku nezaželjenih dogodkov. Uporabljajo se za zmanjševanje vpliva posledic in ugotavljanje vzroka težav. Primer popravljalnih kontrol je načrt neprekinjenega poslovanja (Contingency planning) (CISA Review Manual, 2003, str. 33).

**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, s 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 od rezultatov testa skladnosti. Z njim se testira dejansko izvajanje progama (Karnet in Tajnik, 2003, str.15).

## 5.2 Kontrolni okvir za upravljanje IT

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 nalogi sta predstavljena naslednja:

- **PSIST BS 7799:1995** – Kodeks varovanja informacij (posodobljen na ISO/IEC 17799:2000) (v nadaljevanju: Kodeks varovanja informacij) 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** (**C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology, v nadaljevanju COBIT) je priročnik, ki definira 34 kontrolnih ciljev na najvišjem nivoju in 318 kontrol, ki so predstavljene v štirih področjih. COBIT predstavlja model oziroma metodologijo za upravljanje IT.

Kot navaja sistemski okvir COBIT metodologije, trenutno obstajata dve skupini kontrolnih modelov, in sicer poslovno 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 ostali standardi za upravljanje IS (COBIT Framework, 2000, str. 13).

Obe metodologiji vsebujeta primere kontrol za obvladovanje posameznih tveganj na področju IT. Pri izbiri kontrol je potrebno upoštevati, da vse kontrole niso primerne za vsak IS ali okolje in jih je potrebno prilagoditi oziroma po potrebi razviti nove kontrole.

## 5.3 Standardi in metodologije

### 5.3.1 COBIT

COBIT ponuja uporabne rešitve kontrolnega modela za IT, ki podpira poslovne procese organizacije. Priročnik COBIT je bil prvič izdan leta 1996[22]. Vseboval je izhodišča za zaščito oziroma varnost in kontrolne mehanizme v IT. Leta 2000 je izšla tretja,

[22] Izdala ga je ISACF – Information Systems Audit and Control Foundation.

posodobljena verzija, ki jo je izdal IT Governance Institute, ki ga je leta 1998 ustanovila ISACA[23].

COBIT je metodologija za obvladovanje IT. Temeljni koncept COBIT metodologije je ta, da se k kontroli IT pristopi s poudarkom na informacijah, potrebnih za podporo poslovnemu procesu. Za zadovoljitev poslovnih ciljev mora informacija ustrezati določenim kriterijem. COBIT je sestavljen iz **seznama kontrol**, ki je namenjen lastnikom poslovnih procesov oziroma odgovornim za izvedbo določenih poslovnih procesov. Lastniki poslovnih procesov v organizaciji so namreč polno odgovorni za poslovne procese in oblikovanje kontrolnih mehanizmov.

Za varnost celotnega premoženja organizacije je odgovorno vodstvo organizacije. Organizacije morajo poskrbeti za svoje podatke, za vsa sredstva, s katerimi razpolagajo ter za kvaliteto in varnost sredstev. Vodstvo je odgovorno za uravnoteženo uporabo razpoložljivih človeških virov, naprav, tehnologije, uporabniških sistemov in podatkov. Vsaka kontrolna aktivnost mora biti jasno določena.

**Metodologija COBIT je namenjena:**

- **Vodstvu.** Vodstvu je metodologija v pomoč pri odločitvi glede investiranja v varnost in kontrolo IT ter uravnoteženju tveganj in nadzoru investicij.
- **Uporabnikom sistemov.** Uporabnikom sistemov daje zagotovila, da so v sistem vgrajene zadostne kontrole in da je zagotovljena varnost IS.
- **Revizorjem informacijskih sistemov** služi kot sistemska podlaga in pomoč pri utemeljitvi mnenj o zadostnem obstoju notranjih kontrol ter o varnosti IS.

#### 5.3.1.1 Okvir COBIT metodologije

COBIT sestavlja šest delov:
- Uvod (Executive Summary);
- Sistemski okvir (Framework);
- Kontrolni cilji (Control Objectives);
- Smernice za poslovodstvo (Management Guidelines);
- Smernice za revidiranje (Audit Guidelines);
- Orodje za implementiranje (Implementation Tool Set).

**Sistemski okvir** sestavlja 34 kontrolnih ciljev na najvišjem nivoju za vsakega od postopkov, ki so združeni v štiri področja: planiranje in organizacija, nabava in vzdrževanje, dobava in podpora ter nadzor. Vsebuje tudi smernice za upravljanje IT.

[23] Information Systems Audit and Control Association.

Sistemski okvir je lastnikom poslovnih procesov v pomoč pri vzpostavljanju sistema notranjih kontrol za IT. Z uporabo kontrolnih ciljev na najvišjem nivoju lastniki poslovnih procesov zagotavljajo, da je za IT vzpostavljen ustrezen kontrolni sistem.

**Kontrolni cilji** s skupno 318 kontrolnimi cilji za izbrane IT procese so zbrani iz 41-ih mednarodnih standardov.
**IT kontrolni cilj**[24] je definiran kot »rezultat ali namen, ki ga nameravamo na področju IT doseči z uvedbo določenih kontrolnih postopkov« (COBIT Framework, 2000, str. 12).

**Smernice za poslovodstvo** so namenjene vodstvu kot pomoč pri učinkovitem upravljanju IT. Predstavljajo smernice za vzpostavitev kontrol nad poslovnimi in informacijsko podprtimi procesi organizacije, za nadziranje doseganja ciljev organizacije, za nadziranje informatiziranih procesov in za izdelavo primerjav (benchmarking). Namenjene so tudi izdelavi zrelostnega modela procesa (Maturity Model) s petimi stopnjami zrelosti.

**Smernice za revidiranje.** Glede na 34 kontrolnih ciljev smernice revidiranja zagotavljajo pregled IT procesov za vsakega od 318-ih podrobnih **kontrolnih ciljev**, ki dajo vodstvu zadostna zagotovila o učinkovitosti notranjih kontrol in/ali nasvet za izboljšanje.

**Orodje za implementiranje** navaja primere za hitro in uspešno uvedbo COBIT metodologije v poslovno okolje organizacije.

#### 5.3.1.2 Načela sistemskega okvirja COBIT

**COBIT merila so opredeljena na dveh nivojih:**

Na prvem nivoju opredeljujejo informacijske kriterije, ki so:
- **zahteva po kakovosti**: kakovost, stroški, izdelki;
- **zahteva po zanesljivosti**[25]: uspešnost in učinkovitost operacij, zanesljivost informacij, skladnost z zakonodajo in predpisi;
- **zahteve po varnosti**[26]: zaupnost, celovitost in razpoložljivost.

[24] Metodologija COBIT povzema definicijo po SAC poročilu (Systems Auditability and Control report, The Institute of Internal Auditors Research Foundation, 1991 and 1994).
[25] COBIT metodologija je povzela COSO poročilo in ne spreminja obstoječih definicij učinkovitosti, uspešnosti, zanesljivosti in skladnosti. Definicijo zanesljivosti je razširila tako, da se nanaša na vse informacije, ne samo na finančne.
[26] COBIT metodologija povzema v svetovnem merilu uveljavljene elemente zahtev po varovanju informacij - zaupnost, celovitost in razpoložljivost.

Na drugem nivoju opredeljuje naslednje samostojne, medsebojno povezane **informacijske kriterije**:

- **Uspešnost** (effectiveness). Informacije, pomembne za podporo poslovnemu procesu, naj bodo pravočasne, pravilne in uporabne.
- **Učinkovitost** (efficiency). 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.
- **Razpožljivost** (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.

**Viri za delovanje informacijskega sistema[27]:**

- **Človeški viri:** znanja, osveščenost in sposobnost zaposlenih za načrtovanje, organiziranje, nabavo, dobavo, podporo in nadzor informacijskih sistemov in storitev.
- **Aplikacije oziroma informacijski sistemi:** skupek ročnih in programiranih postopkov.
- **Tehnologija:** strojna oprema, operacijski sistemi, sistemi za upravljanje z bazami podatkov, mrežni sistemi in podobno.
- **Kapacitete:** vsi viri za uporabo in fizično razpolaganje ter podporo IS.
- **Podatki:** podatkovni objekti v najširšem smislu, tako notranjega kot zunanjega izvora.

COBIT razvršča **IT procese** v štiri **področja**:

- **Planiranje in organizacija.** To področje pokriva strategije in taktike ter načine, na katere lahko IT najbolje prispeva k doseganju poslovnih ciljev. Za uresničitev strateške vizije mora biti ta načrtovana, izvedena in upravljana z različnih vidikov.
- **Nabava in uvedba**. Za uresničitev IT strategije je potrebno definirati IT rešitve, jih razviti ali nabaviti ter implementirati in integrirati v poslovne procese. To področje pokriva tudi področje vzdrževanja obstoječih sistemov.
- **Dobava in podpora.** Področje obravnava dobavo zahtevanih storitev, kot so varnostne zahteve, načrt neprekinjenega poslovanja, izobraževanje in podobno. Z

[27] COBIT metodologija povzema v svetovnem merilu sprejete vire za delovanje IS.

namenom zagotavljanja storitev mora biti vzpostavljen ustrezni podporni proces. Vključuje tudi obdelavo podatkov v aplikacijah.
- **Nadzor.** Vse IT postopke je potrebno v določenem časovnem obdobju spremljati ter ocenjevati z vidika kakovosti in skladnosti s kontrolnimi zahtevami.

Vse navedene IT postopke je mogoče uvesti na različnih nivojih znotraj organizacije, na primer na področju informatike, pri lastnikih poslovnih procesov in podobno.

**Upravljanje informacijskih virov** poteka na treh nivojih.

- na najnižjem nivoju se izvajajo **naloge in aktivnosti**, potrebne za doseganje merljivih rezultatov. Aktivnost traja skozi nek življenjski cikel, medtem ko so naloge ciljno usmerjene. Kontrolno okolje aktivnosti se razlikuje od kontrolnega okolja nalog;
- **postopki** so na višjem nivoju in so definirani kot skupina združenih aktivnosti ali nalog s kontrolnimi presledki;
- na najvišjem nivoju se postopki združujejo v **področja**.

**Preglednica kontrolnih ciljev,** predstavljena v nadaljevanju**,** prikazuje skupno preglednico COBIT metodologije. Prikazuje informacijske kriterije, ki podpirajo podrobne kontrolne cilje ter povezavo z IT procesi in IT sredstvi. Namenjena je revizorjem IS kot pomoč pri osredotočanju na kriterije in IT sredstva glede na cilje revizijskega pregleda (Karnet, 2003, str. 14)

Preglednica 1: Pregled kontrolnih ciljev.

| PODROČJA | | PROCESI | INFORMACIJSKI KRITERIJI | | | | | | | IT SREDSTVA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | uspešnost | učinkovitost | zaupnost | celovitost | razpoložljivost | skladnost | zanesljivost | človeški viri | aplikacije | tehnologija | kapacitete | podatki |
| Planiranje in organizacija | PO1 | Določanje strateškega plana IT | P | S | | | | | | x | x | x | x | x |
| | PO2 | Določanje informacijske arhitekture | P | S | S | S | | | | | x | | | x |
| | PO3 | Določanje tehnoloških smernic | P | S | | | | | | | | x | x | |
| | PO4 | Določitev organizacije in smernic | P | S | | | | | | x | | | | |
| | PO5 | Upravljanje investicij | P | P | | | | | S | x | x | x | x | |
| | PO6 | Predstavitev ciljev in usmeritev vodstva | P | | | | | S | | x | | | | |
| | PO7 | Ravnanje s človeškimi viri | P | P | | | | | | x | | | | |
| | PO8 | Zagotovitev skladnosti z zunanjimi zahtevami | P | | | | | P | S | x | x | | | x |
| | PO9 | Ocena tveganja | P | S | P | P | P | S | S | x | x | x | x | x |
| | P10 | Upravljanje projektov | P | P | | | | | | x | x | x | x | |
| | P11 | Upravljanje kakovosti | P | P | | P | | | S | x | x | x | x | |
| Nabava in uvedba | AI1 | Prepoznavanje avtomatiziranih rešitev | P | S | | | | | | | x | x | x | |
| | AI2 | Nabava in vzdrževanje aplikativne programske opreme | P | P | | S | | S | S | | x | | | |
| | AI3 | Nabava in vzdrževanja tehnološke infrastrukture | P | P | | S | | | | | | x | | |
| | AI4 | Razvoj in vzdrževanje postopkov | P | P | | S | | S | S | x | x | x | x | |
| | AI5 | Namestitev in akreditiranje sistema | P | | | S | S | | | x | x | x | x | x |
| | AI6 | Upravljanje sprememb | P | P | | P | P | | S | x | x | x | x | x |
| Dobava in podpora | DS1 | Opredelitev in upravljanje nivoja storitev | P | P | S | S | S | S | S | x | x | x | x | x |
| | DS2 | Upravljanje storitev zunanjih izvajalcev | P | P | S | S | S | S | S | x | x | x | x | x |
| | DS3 | Upravljanje zmogljivosti in kapacitet | P | P | | | S | | | | x | x | x | |
| | DS4 | Zagotovitev neprekinjenega poslovanja | P | S | | | P | | | x | x | x | x | x |
| | DS5 | Zagotovitev varnosti sistema | | | P | P | S | S | S | x | x | x | x | x |
| | DS6 | Določitev in razporejanje stroškov | | P | | | | | P | x | x | x | x | x |
| | DS7 | Izobraževanje in usposabljanje uporabnikov | P | S | | | | | | x | | | | |
| | DS8 | Pomoč in svetovanje strankam | P | P | | | | | | x | x | | | |
| | DS9 | Upravljanje konfiguracij | P | | | | S | | S | | x | x | x | |
| | DS10 | Upravljanje s težavami in nepredvidenimi dogodki | P | P | | | S | | | x | x | x | x | x |
| | DS11 | Upravljanje podatkov | | | | P | | | P | | | | | x |
| | DS12 | Upravljanje z napravami | | | | P | P | | | | | | x | |
| | DS13 | Upravljanje operacij | P | P | | S | S | | | x | x | | x | x |
| Nadzor | M1 | Nadzor procesa | P | P | S | S | S | S | S | x | x | x | x | x |
| | M2 | Ocena primernosti notranjih kontrol | P | P | S | S | S | P | S | x | x | x | x | x |
| | M3 | Pridobitev neodvisnega zagotovila | P | P | S | S | S | P | S | x | x | x | x | x |
| | M4 | Zagotovitev neodvisne revizije | P | P | S | S | S | P | S | x | x | x | x | x |

P[28] – primarno
S[29] – sekundarno □ - prazno polje x – možnost uvedbe

Vir: COBIT Framework, str. 20.

[28] določen kontrolni cilj v celoti vpliva na informacijski kriterij.
[29] kontrolni cilj le delno ali posredno vpliva na informacijski kriterij.

### 5.3.2 Kodeks varovanja informacij

Standard **PSIST BS 7799:1995** - Kodeks varovanja informacij (posodobljen na ISO/IEC 17799:2000) je kodeks dobre prakse in osnova za varnostne standarde na področju upravljanja varovanja in zaščite informacij v organizaciji. Namenjen je vodstvu oddelka za informatiko in zaposlenim, zadolženim za področja varovanja informacij, kot podlaga za upravljanje in uvajanje varnostnih standardov v IS.

Zasnovan je bil zaradi naraščajočih nevarnosti, ki pretijo IT in omrežjem. Organizacije so odvisne od zanesljivosti delovanja IS. Razpoložljivost, neoporečnost in zaupnost podatkov so bistvene za varno poslovanje organizacije. Vzpostavitev in izpolnjevanje postopkov za varovanje in zaščito IS je zaradi naraščajočih groženj in nevarnosti, računalniškega kriminala in drugih morebitnih nesreč, katerim so IS vedno bolj izpostavljeni, temeljna naloga vsake organizacije.

V zvezi z uvajanjem kontrol na področju varovanja IS velja, da je ceneje uvesti kontrole preprečevanja, kot pa popravljalne. Nastanek nepričakovanega in neobvladanega dogodka lahko povzroči veliko več škode, kot je cena, ki jo je potrebno plačati za uvedbo preventivnih ukrepov. Včasih so lahko posledice tako resne, da je ogroženo poslovanje in nadaljnji obstoj organizacije.

Kodeks varovanja informacij je razdeljen na deset poglavij. V vsakem od poglavij so navedene kontrole in primeri dobre prakse, ki temeljijo na varnostnih ukrepih. Kontrole niso primerne za vsako okolje in jih je potrebno uporabljati glede na okoliščine.

**Ključne kontrole,** ki predstavljajo osnovo za vzpostavitev varovanja in zaščite informacij v organizaciji:
- dokument o varnostni politiki,
- organiziranost varovanja informacij,
- izobraževanje in usposabljanje za varovanje informacij,
- poročanje o varnostnih incidentih,
- obvladovanje računalniških virusov,
- načrtovanje neprekinjenega poslovanja,
- obvladovanje kopiranja avtorsko zaščitene programske opreme,
- varovanje zapisov,
- zaščita podatkov,
- usklajenost z varnostno politiko.

#### 5.3.2.1 Varovanje informacij

Informacije v organizaciji pomenijo premoženje, ki ga je potrebno na primeren način varovati. Ustrezno varovanje informacij ščiti informacije pred različnimi grožnjami in nevarnostmi z namenom, da se zagotovi nemoten potek poslovanja in da se ob morebitni uresničitvi katere od groženj škoda zmanjša na najmanjšo možno mero.

Namen varovanja informacij je »zagotavljanje neprekinjenega poslovanja in omejevanja poslovne škode na najmanjšo možno mero s preprečevanjem in zmanjševanjem učinkov varnostnih incidentov« (Kodeks varovanja informacij, 1995, str. 5).

**Varovanje informacij** pomeni zagotavljanje in ohranjanje naslednjih značilnosti:
- zaupnost,
- celovitost – neoporečnost,
- razpoložljivost.

#### 5.3.2.2 Varnostne zahteve in ocena tveganj

Za učinkovito delovanje sistema notranjih kontrol sta pomembna vgrajevanje pravih kontrol in ustrezna stopnja prilagodljivosti vse od načrtovanja IS naprej. BS 7799 opredeljuje tri vidike varnostnih zahtev:

1. **Splet varnostnih tveganj**. To predstavlja ogrožanje sredstev in njihova ranljivost ter možni učinki teh nevarnosti na poslovanje. Večino tovrstnih tveganj se lahko razreši in uspešno odpravi, če se postopa v skladu s kodeksom.
2. **Splet zakonskih in /ali pogodbenih zahtev**, ki jih morajo zadovoljiti organizacije. Namen kodeksa je, da bi služil kot osnovno vodilo pri tovrstnih zahtevah.
3. **Splet načel, ciljev in zahtev za obravnavanje podatkov** za podporo poslovanju organizacije. Z vidika konkurenčnosti je pomembno, da varnostna politika podpira te zahteve. Uvajanje ali odsotnost varnostnih kontrol ne smeta ovirati učinkovitosti poslovanja.

Organizacija mora za vsa tri področja pripraviti oceno tveganj. Ta se izvede na nivoju celotne organizacije ali samo za posamezna področja.

**Ocenjevanje varnostnih tveganj** obsega oceno o:
- višini poslovni škode, ki bi verjetno nastala kot posledica napake ali vdora v varnostni sistem IT. Pri tem je potrebno upoštevati posledice kršitev načel zaupnosti, neoporečnosti in razpoložljivosti informacij ter drugega premoženja.

- oceni verjetnosti, da bi do vdora prišlo ob upoštevanju nevarnosti in groženj in pri že vzpostavljenih kontrolah.

Na osnovi ocene tveganja se ugotovi, kje je potrebnih več kontrol.

### 5.3.3 Smernice za računalniško zaščito

Nadzor računalniškega sistema plačilnih agencij je prvotno določala točka (vi) Smernic za merila za akreditacijo plačilne agencije (Uredba Komisije (ES) o določitvi podrobnih pravil za uporabo Uredbe Sveta (ES) št. 729/70 v zvezi s postopkom za potrditev obračuna Jamstvenega oddelka EKUJS, 1995).

Pri računalniški obdelavi zahtevkov je potrebno dostop do IS varovati na naslednji način:
- vsi vneseni podatki morajo biti pravilno potrjeni;
- zagotovljeno naj bo odkrivanje in popravljanje vnosnih napak;
- podatke smejo vnašati, spreminjati ali potrjevati le pooblaščene osebe z ustreznimi gesli;
- istovetnost osebe, ki vnaša ali spreminja podatke, naj se evidentira v dnevnik delovnih operacij;
- gesla je potrebno redno spreminjati;
- računalniški sistemi naj bodo pred nepooblaščenim dostopom zaščiteni s fizičnim nadzorom;
- podatke je potrebno shranjevati na varnostne kopije, ki naj se hranijo na posebnem mestu;
- vnos podatkov se z namenom odkrivanja nedoslednosti preverja z logičnimi preverjanji.

Z Uredbo Komisije (ES) št. 2025/2001[30] je bila točka (vi) - Nadzor računalniškega sistema Priloge k smernicam za merila za akreditacijo v celoti spremenjena:

"Zaupnost, celovitost in dostopnost vseh računalniških podatkov je treba zagotoviti z ukrepi, ki upoštevajo upravno strukturo, kadrovsko strukturo in tehnološko okolje posamezne plačilne agencije. Finančni in tehnološki napor mora biti sorazmeren z dejansko nastalimi tveganji.

Vsak računalniški sistem mora vključevati ustrezne postopke za:

[30] Uredba Komisije (ES) št. 2025/2001 ureja spremembe Uredbe (ES) št. 1663/95 o podrobnih pravilih za uporabo Uredbe Sveta (EGS) št. 729/70 glede postopka potrditve obračunov Oddelka za jamstva EKUJS.

(a) splošno organizacijo, upravljanje in revizijo,
(b) fizično varnost,
(c) logično varnost,
(d) razvijanje, programiranje in vzdrževanje,
(e) rutinske operacije,
(f) telekomunikacije,
(g) osebni računalniki,
(h) načrtovanje neprekinjenega poslovanja,
(i) aplikativne kontrole."

Smernice za računalniško zaščito pojasnjujejo smernice za merila za akreditacijo plačilne agencije v točki, ki se nanaša na postopke za računalniško zaščito. Predstavljajo referenčno točko za katerikoli pregled, ki ga izvaja Evropska komisija za potrebe akreditacije in certifikacije letnih računov. V smernicah so navedeni temeljni kontrolni cilji, ki jih mora plačilna agencija izpolniti ter možni pristopi k rešitvi. Načini in pristopi za izpolnitev kontrolnih ciljev so prepuščeni plačilni agenciji.

**Pregled kontrolnih ciljev Smernic za računalniško zaščito:**

**a) Splošna organizacija, upravljanje in revizija**
Strategija razvoja IT plačilne agencije naj bo skladna s cilji posamezne plačilne agencije. Vzpostavitev in posodobitev strategije upravljanja IT je odgovornost vodstva. Varnost in zaščita računalniških sistemov naj bo del strategije. Obstajati morata dolgoročni in kratkoročni strateški načrt razvoja IT, ki naj bosta skladna s splošnimi načrti organizacije.
Aktivnosti naj bodo zasnovane na politikah, standardih in postopkih. Status oddelka za informatiko mora zagotavljati njegovo neodvisnost od ostalih oddelkov. Vodstvo mora zagotavljati primerno ločitev funkcij znotraj poslovne enote ter med poslovnimi enotami.

**b) Fizična varnost**
Namernemu ali nenamernemu fizičnemu uničenju namestitve računalniške opreme naj bi se izognili z izvajanjem preventivnih ukrepov in odkrivanjem v zgodnji fazi z namenom zaščite pred možnimi posledicami. To obsega fizični dostop, zaščito pred požarom, zaščito pred iztekom tekočine in zaščito ob izpadu električne energije.

**c) Logična varnost**

Dostop do podatkov naj bo omejen le na tiste posameznike, ki imajo pooblastilo za dostop. Nadzor nad dostopi se izvaja s sledmi za nadzor. Področje zajema logično zaščito dostopov, logično zaščito do programske opreme, logično zaščito za zaposlene, logično zaščito podatkov in logično zaščito za sistemsko programsko opremo.

**d) Razvijanje, programiranje in vzdrževanje**

Metoda razvoja in vzdrževanja programske opreme mora zagotavljati učinkovito in zmogljivo programsko opremo ter zagotavljati zaščito podatkov v smislu zaupnosti, celovitosti, razpoložljivosti in sledljivosti. To zajema projektno vodenje, standarde za razvoj programske opreme, postopke pri posameznih stopnjah projekta in upravljanje sprememb (change management).

**e) Rutinske operacije**

Viri IT naj bodo nadzorovani tako, da bo zagotovljena njihova učinkovita uporaba. Podatkovne datoteke morajo biti zavarovane pred izgubo. Zagotovljeno mora biti vzdrževanje računalniške opreme, delitev in izmenjava dolžnosti, izvajanje in razporejanje obdelav, nadzor dejavnosti, nadzor knjižnic in razdeljevanje rezultatov obdelav.

**f) Telekomunikacije**

Vzpostaviti je potrebno primerne postopke za zaščito telekomunikacijskih omrežij.

**g) Osebni računalniki**

Obstajati morajo postopki definiranja zahtev za nabavo računalniške in programske opreme ter uporabo in varnost osebnih računalnikov.

**h) Načrtovanje neprekinjenega poslovanja**

Obstajati morajo preizkušeni načrti za varnostno shranjevanje podatkov in za ponovno vzpostavitev prvotnega stanja zaradi nepredvidenih prekinitev.

Zagotavljanje neprekinjenega poslovanja je proces obvladovanja tveganj, katerih posledica bi lahko bile prekinitve in večje težave pri poslovanju. Temeljne sestavine načrta neprekinjenega poslovanja so:

- opredeliti skupine posameznikov in njihove odgovornosti,
- pripraviti seznam ključnih dobaviteljev strojne in programske opreme,
- pripraviti scenarije za posamezne vrste prekinitev,
- izbrati, pripraviti in opremiti nadomestno lokacijo,
- zagotoviti redundantnost sistema in shranjevanje varnostnih kopij podatkov na oddaljeni lokaciji,

- zavarovati strojno in programsko opremo organizacije,
- predvideti kritične čase okrevanja (Kljajić Žebeljan, 2002, str. 315-318).

**i) Aplikativne kontrole**

Vhodne podatke je potrebno pravilno odobriti in preveriti. Vzpostaviti je potrebno postopke za obravnavanje napak. Obdelava podatkov mora biti nadzorovana. Preprečiti je potrebno nepooblaščeno dodajanje, odstranjevanje ali spreminjanje podatkov. Izhodni podatki morajo biti pravočasno razdeljeni in pregledani. Dostop do stalnih podatkov (na primer podatki o strankah) mora biti nadzorovan.

# 6. PLAČILNA AGENCIJA V SLOVENIJI

## 6.1 Kmetijska politika

Iz zgodovinskega vidika sta znana dva koncepta kmetijske politike.

- Bimodalna agrarnopolitična strategija je bila značilna za jugoslovanski model kmetijske politike, ki je zaviral razvoj tradicionalnega zasebnega kmetijstva (Cunder et al., 1997, str. 158). Zanemarjala je razvoj kmetij in spodbujala razvoj novih proizvodnih in poslovnih oblik kmetijstva.
- Slovenska kmetijska politika se je začela oblikovati po razpadu bivše Jugoslavije. V letih 1990-1993 je bil oblikovan strateški dokument, ki je določil temeljne usmeritve in cilje kmetijske politike. Leta 1993 je bila sprejeta Strategija razvoja slovenskega kmetijstva (MKGP, 1993), ki je strateško opredelila usmeritev v eko-socialno kmetijstvo. Temeljni cilji, zapisani v strateškem dokumentu, so bili:
    - stabilna pridelava kakovostne in čim cenejše hrane,
    - ohranjanje poseljenosti in kulturne krajine,
    - trajno povečanje konkurenčne sposobnosti kmetijstva in
    - zagotavljanje dohodka nadpovprečno produktivnim pridelovalcem.

Med leti 1995-1997 so se v Sloveniji oblikovali ključni instrumenti kmetijske politike. Po letu 1995 se je pričelo obdobje prilagajanja EU. Od takrat je postala temeljna naloga čim uspešnejša prilagoditev slovenskega kmetijstva razmeram v EU.

S prevzemom SKP EU je velik del pristojnosti za vodenje kmetijske politike prešel v pristojnost skupnih organov EU. Na oblikovanje kmetijske politike bo Slovenija v prihodnosti imela malo vpliva (Cunder et al., 1997, str. 15).

Z namenom izvajanja ukrepov kmetijske politike oziroma prilagajanje SKP EU je bila leta 1999 ustanovljena ARSKTRP, preko katere slovensko kmetijstvo in živilsko predelovalna industrija koristita sredstva EU.

## 6.2 Predstavitev Agencije

ARSKTRP je bila ustanovljena z Zakonom o spremembah in dopolnitvah zakona o organizaciji in delovnem področju ministrstev (Uradni list RS, št. 60/99). Delovati je pričela leta 2000. Agencija je bila ustanovljena z namenom izvajanja ukrepov kmetijske politike oziroma prilagajanja SKP EU na področju izvajanja tržnih redov, zunanje trgovinske politike, intervencij na trgu, sistema plačil in strukturnih ukrepov ter izvedbo programa predpristopne pomoči SAPARD (Special Accession Programme for Agriculture and Rural Development, v nadaljevanju: SAPARD).

Agencija je organizirana po vzoru plačilnih agencij v državah članicah EU. Deluje kot organ v sestavi MKGP in je izrazito evropsko organizirana ustanova. Agencijo vodi direktor (direktorica), ki je odgovoren (odgovorna) za pravočasno, zakonito in pravilno opravljanje nalog in je odgovoren (odgovorna) ministru za kmetijstvo.

Naloge Agencije določa 99. člen Zakona o kmetijstvu. Temeljne naloge agencije so:
- izvajanje ukrepov kmetijsko tržno-cenovne in strukturne politike;
- vzpostavitev in izvajanje integriranega administrativnega kontrolnega sistema (v nadaljevanju: IAKS);
- pripravljanje ustreznih poročil in analiz;
- vzpostavitev in izvajanje tržno-informacijskega sistema;
- vodenje drugih zbirk podatkov;
- izvajanje ukrepov notranje kontrole in notranje revizije ter
- izvajanje nalog promocije kmetijskih pridelkov oziroma živil (Uradni list RS, št. 54/00).

### 6.2.1 Notranja organiziranost Agencije

Agencija izvaja temeljne naloge odobritve, izvrševanja in računovodstva plačil. Naloge se izvajajo ločeno v notranje organizacijskih enotah. Vsako od nalog opravlja odgovorni delavec v notranji organizacijski enoti, pristojni za izvedbo naloge.

Organizacijsko strukturo in sistemizacijo delovnih mest agencije, način dela in splošna določila določa Pravilnik o notranji organizaciji in sistemizaciji delovnih mest (Ur. list RS, št. 011-7/00).

V Agenciji se naloge izvajajo v štirih sektorjih in petih službah. Vodje sektorjev in služb za svoje delo odgovarjajo neposredno direktorju agencije.

**SLUŽBA ZA NOTRANJO REVIZIJO** opravlja naloge preverjanja obstoja in delovanja notranjih kontrol, preverja skladnost postopkov z uredbami, izvaja notranje-revizijske postopke v skladu z internimi akti in standardi notranjega revidiranja, sodeluje z zunanjimi revizorji ter pripravlja poročila za vodstvo.

Služba notranje revizije Agencije mora preverjati, ali so vzpostavljeni postopki Agencije skladni s predpisi Skupnosti. Preverjati mora točnost, popolnost in pravočasnost obračunov. V obdobju petih let mora pregledati vsa pomembna področja, vključno z oddelki za odobritev izplačil. Delovati mora v skladu z mednarodno sprejetimi standardi in izsledke evidentirati v delovnih dokumentih. Vodstvu agencije mora podajati poročila in priporočila (Uredba komisije (ES) o določitvi podrobnih

pravil za uporabo Uredbe Sveta (ES) št. 729/70 v zvezi s postopkom za potrditev obračuna Jamstvenega oddelka EKUJS, 1995).

**SLUŽBA ZA INFORMIRANJE IN EU ZADEVE** izvaja naloge s področja informiranja javnosti in koordinacije dela z institucijami EU. Temeljne naloge so stiki z javnostmi ter organizacija in izvajanje aktivnosti na področju akreditacije postopkov, ki se nanašajo na izplačila Jamstvenega sklada EKUJS in SAPARD ukrepov.

**SEKTOR ZA KMETIJSKE TRGE** izvaja naloge v štirih oddelkih, in sicer v oddelku za zunanjo trgovino, oddelku za intervencijske ukrepe – rastlinski del, oddelku za intervencijske ukrepe – živalski del in oddelku za tržno informacijski sistem. Sodeluje pri pripravi carinskih, zunanjetrgovinskih in deviznih predpisov, izvaja uvozno – izvozne režime (licence, izvozna nadomestila, carinske kvote), varščine, ureja uvozne in izvozne licence ter izvozna nadomestila, (intervencijski nakup, podpora skladiščenju, umik s trga), izvaja ukrepe intervencijskega nakupa in prodaje, upravlja z mlečnimi kvotami ter opravlja druge naloge s področja tržnih ureditev.

**SEKTOR ZA NEPOSREDNA PLAČILA** izvaja naloge v oddelkih za neposredna plačila – rastlinski in živalski del, v oddelku za okoljske programe in manj razvita območja ter v oddelku za tehnično pomoč. Temeljna naloga sektorja je sodelovanje pri pripravi predpisov in izvajanje ukrepov s področja dela, odobravanje in izvajanje neposrednih plačil, izvedba javnih razpisov in izvajanje postopkov administrativnih kontrol.

**SEKTOR ZA RAZVOJ PODEŽELJA** izvaja naloge v dveh oddelkih, in sicer v oddelku za prestrukturiranje kmetijstva, živilstva, gozdarstva in ribištva ter oddelku za razvoj podeželja. Izvaja strukturne ukrepe investicij v kmetijska gospodarstva, investicij v živilsko predelovalno industrijo ter ukrepe na področju gozdarstva in ribištva. Skozi ukrepe infrastrukture, ekonomske diverzifikacije podeželja, obnove vasi, priprave razvojnih in inovativnih programov in promocije izvaja programe celostnega razvoja podeželja in razvojnih programov podeželja.

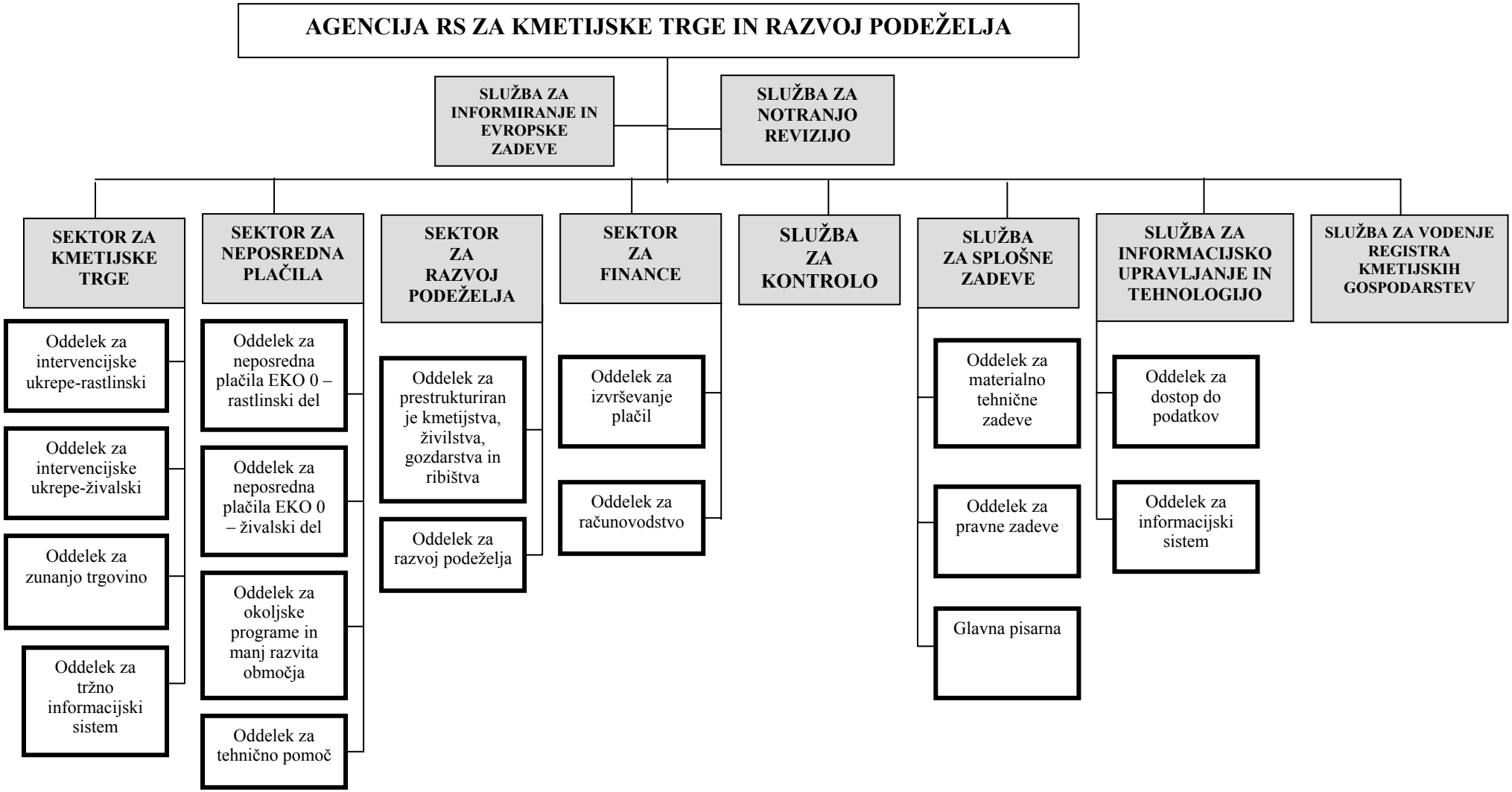
**SEKTOR ZA FINANCE** izvaja naloge v oddelku za izvrševanje plačil ter v oddelku za računovodstvo. Temeljne naloge sektorja so pripravljanje navodil za izvedbo in izvajanje finančnih postopkov, načrtovanje in izvajanje proračunske porabe agencije, načrtovanje in spremljanje likvidnosti in vračil ter izvrševanje plačil. Oddelek za računovodstvo vodi glavno knjigo po nacionalnih in EU standardih ter obračunava izplačila iz naslova dela. Sektor je odgovoren za pripravljanje analiz in ocen učinkov ukrepov kmetijske politike, pripravljanje izhodišč za programiranje ukrepov v naslednjih letih ter pripravljanje poročil.

**SLUŽBA ZA KONTROLO** izvaja kontrolo v skladu z nacionalnimi in EU predpisi, izvaja kontrole na kraju samem (on the spot controls) ter daje navodila in nadzoruje delo organov, ki jim je delegirana naloga izvajanja kontrole na kraju samem. Izdeluje in izvaja analize tveganj ter ocenjuje rezultate izvedbenih kontrol. Rezultati kontrol se upoštevajo pred izplačilom zahtevka za izplačilo.

**SLUŽBA ZA SPLOŠNE ZADEVE** izvaja naloge v oddelku za materialno tehnične zadeve, oddelku za pravne zadeva in v glavni pisarni. Naloge službe so planiranje in nabava sredstev za delo, planiranje potrebnih finančnih sredstev za delo agencije, vodenje javnih naročil, evidentiranje in vzdrževanje sredstev agencije in vodenje kadrovskih zadev, priprava predpisov z vseh področij dela agencije, pripravljanje pravnih poročil, mnenj in drugih gradiv, razlaga pomembnih evropskih in državnih predpisov, pripravljanje predlogov mnenj, pojasnil in stališč o pravnih vprašanjih z delovnega področja agencije ter upravljanje pisarniškega poslovanja agencije.

**SLUŽBA ZA INFORMACIJSKO UPRAVLJANJE IN TEHNOLOGIJO** (v nadaljevanju: SIUT) opravlja naloge v oddelku za informacijski sistem in oddelku za dostop do podatkov.

**Slika 1: Organizacijska shema Agencije RS za kmetijske trge in razvoj podeželja**




Vir: Interna gradiva ARSKTRP, 2003

### 6.2.2 Naloge SIUT

SIUT je organizirana kot ločena organizacijska enota znotraj agencije. Temeljna naloga SIUT je vzpostavitev in upravljanje IS Agencije na takšen način, da se je sposoben prilagajati organizacijskim spremembam, da zagotavlja visoko razpoložljivost, stabilnost in dostopnost podatkovnih in programskih struktur ter standardizirano povezljivost z organi v okviru in izven državne uprave. Naloge izvaja v oddelku za informacijski sistem in oddelku za dostop do podatkov (interna gradiva ARSKTRP, 2003).

**Temeljne naloge oddelka za informacijski sistem:**
- priprava metodoloških in tehnoloških podlag za izvedbo razvoja IS;
- razvoj IS agencije;
- sodelovanje z izvajalci razvoja;
- sodelovanje z drugimi organizacijami v zvezi z usklajevalnimi nalogami.

**Temeljne naloge oddelka za dostop do podatkov:**
- izvedba javnih razpisov za nabavo informacijske opreme;
- zagotavljanje fizične in logične varnosti IS;
- izvajanje izobraževanje s področja računalništva in informatike;
- urejanje in dodeljevanje dostopov do namenske programske opreme in podatkov;
- vzpostavitev in vzdrževanje sistema kontingenčnega načrtovanja;
- tehnična podpora končnim uporabnikom;
- vzdrževanje in arhiviranje baz podatkov agencije.

### 6.2.3 IS Agencije

IS Agencije je zastavljen kot sistem z enotno, centralno upravljano relacijsko bazo podatkov. Standardizirana povezljivost z organi državne uprave je zagotovljena z dostopom v zasebno prostrano omrežje državnih organov – HKOM in z uporabo standardizirane programske opreme državne uprave.

**Razvoj IS**

Razvoj IS poteka v skladu z metodologijo PRINCE in Metodologijo vodenja projektov v državni upravi za področje IT (MVPDU-IT)[31]. Nosilec razvoja IS je oddelek za informacijski sistem. Izvedbene naloge izvajajo zunanji izvajalci. Pri razvoju sodelujejo vsebinski nosilci posameznih funkcij in uporabniki Agencije.

[31] slovenska priredba PRINCE metodologije, ki jo je pripravil in jo vzdržuje Center vlade za informatiko.

Razvoj IS se izvaja z Oraclovimi orodji. Oracle je centralno upravljana relacijska podatkovna baza, ki zagotavlja razpoložljivost, stabilnost in dostopnost podatkovnih in programskih struktur. Operacijski sistem baznega in aplikacijskega strežnika je Unix. Operacijski sistem delovnih postaj uporabnikov je Windows 95/98/2000/ME/Windows NT (Interna gradiva ARSKTRP, 2002). Strojna oprema v okviru vladnih služb RS je standardizirana s strani Centra Vlade za informatiko.

Za podporo procesom, kjer je veliko netipiziranih dokumentov, se uporabljajo programske rešitve v okolju Lotus Notes. Lotus Notes je standardno okolje za podporo pisarniškemu poslovanju v slovenski državni upravi.

### 6.2.4 Zagotavljanje varnosti IS

Ena od pomembnejših nalog SIUT je zagotavljanje varnosti IS Agencije. Varnostni sistem je zgrajen na več nivojih (Interna gradiva ARSKTRP, 2003).

**Fizična varnost IS** Agencije je zagotovljena na naslednji način:

- Dostop do sistemskega prostora, kjer se nahajajo strežniki, je možen samo na podlagi pisnega pooblastila. Ključavnice na vratih v sistemski prostor so kodirane. Dostopi v sistemski prostor se beležijo v dnevnik dostopov. V sistemskem prostoru je vzdrževana primerna temperatura. V prostoru ni nikakršnih vnetljivih snovi. Dostop v poslovno stavbo in do poslovnih prostorov ARSKTRP je centralno nadziran z video nadzorom in 24 urno varnostno službo.
- Strežniki so pred izpadom električnega toka varovani s povezavo na naprave za neprekinjeno napajanje in na centralni generator za proizvodnjo električnega toka.
- Sistemski prostor je ločen od ostalih prostorov s protipožarnimi vrati. V sistemskem prostoru je gasilni aparat in naprava za javljanje požara. Temperatura prostora je regulirana s klimatsko napravo. V prostoru ni vnetljivih snovi. Vzpostavljeni so postopki za ravnanje v primeru požara. Požarni izhodi so vidno označeni.

**Logična varnost IS** Agencije je zagotovljena na naslednji način:

- Navodila opredeljujejo natančen način dodeljevanja pooblastil za dostop do podatkov in računalniških programov, ki jih uporabniki potrebujejo za opravljanje dela.
- Nastavitve programske opreme omogočajo centralno upravljanje uporabniških pravic dostopa do podatkov. Po 5-minutah neuporabe računalnika le-ta samodejno preide v stanje nedelovanja in uporabnik se mora za nadaljevanje dela ponovno prijaviti v sistem. Uporabniška gesla se dodeljujejo na podlagi pisnih pooblastil. Uporabniki se morajo držati predpisanega postopka za menjavo uporabniškega gesla za prijavo v lokalno računalniško omrežje Agencije s priporočili za izbiro gesla v skladu z

varnostnimi zahtevami za varovanje IS. Vzpostavljen je sistem za odvzem gesel uporabnikom, ki z delom na Agenciji prenehajo oziroma ki zamenjajo delovno mesto znotraj Agencije.
- Z Novellovim orodjem ZEN Works se centralno nadzirajo in administrirajo nastavitve pri uporabnikih. Z nastavitvami mrežne programske opreme je zagotovljeno centralno upravljanje konfiguracij delovnih postaj in vzpostavljanje mrežnih povezav med uporabniki.
- Protivirusni program se enkrat mesečno nadgrajuje z novimi različicami. Računalniški sistem je pred vdorom računalniških virusov zaščiten s protivirusnim programom.

**Zagotavljanje varnosti pri uporabi osebnih računalnikov**

Na delovnih postajah uporabnikov je nameščen operacijski sistem Windows 2000. Uporabniki nimajo možnosti spreminjanja nastavitev programske opreme in shranjevanja podatkov na lokalni disk. Datoteke s podatki uporabnikov se shranjujejo samo na uporabnikovem delu mrežnega diskovnega polja, do katerega lahko dostopajo z uporabniškim imenom in geslom. Geslo je potrebno enkrat mesečno spremeniti. Posebna skupina skrbi za tehnično podporo uporabnikom v primeru težav pri delu z IT.

**Kontingenčno načrtovanje**

Varnostne kopije podatkov se izdelujejo vsak dan. Hranijo se na oddaljeni lokaciji. Postopki za vzpostavitev prvotnega stanja po morebitni odpovedi računalniškega sistema so vzpostavljeni.

100% razpoložljivost in varnost sistema za varnostno shranjevanje kritičnih računalniških aplikacij in za ponovno vzpostavljanje predhodnih storitev zaradi nepredvidenih prekinitev je zagotovljena s tehnologijo clusteringa, in sicer sta 2 enaka strežnika povezana z enim zunanjim diskovnim poljem tehnologije RAID 5.

**Varnost telekomunikacij**

Vsa omrežja so zaščitena pred zunanjim nepooblaščenim dostopom. IS je povezan v zasebno omrežje državnih organov HKOM, ki je od javnega omrežja ločeno s požarnimi stenami (Firewall). Klicni dostopi v sistem se preverjajo preko dvonivojskega sistema enkratnih gesel.

#### 6.2.4.1 Varnostna politika

V skladu z zahtevami EU mora IS Agencije zagotavljati varnost in zanesljivost ter dolgoročno stabilnost in dostop do podatkovnih in programskih struktur.

Temeljni dokument za zagotavljanje varnosti je Varnostna politika (Varnostna politika, 2003). Z Varnostno politiko Agencije so določena naslednja področja varovanja in zaščite:

- Varnostna politika se nanaša na celotno informacijsko infrastrukturo Agencije, vključno s podatki, programsko in strojno opremo, nosilci podatkov, sredstvi, komunikacijsko opremo in zaposlenimi na ARSKTRP.
- IS Agencije smejo zaposleni uporabljati le v službene namene.
- Za uvajanje varnostne politike na svojem delovnem področju in prenašanje politike na zaposlene so odgovorni vodje služb/sektorjev.
- Za doseganje varnostnih ciljev IS je zadolženo vodstvo Agencije.
- Zaposleni posameznik odgovarja za strojno in programsko opremo, ki mu je dodeljena v uporabo.
- Vzpostavljeni so postopki za fizično in logično varovanje IS.
- Uporaba nelicenčne programske opreme ni dovoljena.
- Postopkom varovanja se posveča pozornost vse od nastopa zaposlitve na delovnem mestu v Agenciji naprej. Uporabniki se pred pričetkom uporabe IT udeležijo ustreznega usposabljanja.
- Razvoj IS je ustrezno upravljan in nadzorovan.
- Ravnanje z osebnimi podatki in osnovnimi sredstvi je predpisano.
- Zagotavljanje neprekinjenega poslovanja.
- Dokumentiranje postopkov in izvajanje nadzora skladnosti s postopki.

## 6.3 Načrtovanje revizijskega pregleda - mogoč pristop

Revidiranje IT se izvaja po enakem postopku kot ostale revizije. Pregled je mogoče opraviti kot revidiranje poslovanja, kjer se sistematično pregleda posamezno področje s poudarkom na upravljanju računalniške zaščite IT plačilnih agencij. Na tem področju obstajajo natančne smernice za plačilne agencije, zapisane v dokumentu Smernice za računalniško zaščito. Namen pregleda je pridobitev zadostnih zagotovil o obstoju ustreznih kontrol, ki zagotavljajo skladnost z usmeritvami in postopki za zagotavljanje varnosti.

V nadaljevanju je predstavljen revizijski vprašalnik kot podlaga za izvedbo revizijskega pregleda. Vprašanja so izoblikovana na podlagi kontrolnih ciljev Smernic za računalniško zaščito. Med samim izvajanjem revizijskega pregleda revizor zbere dokazno gradivo in pripadajočo dokumentacijo. Rezultat revizijskega pregleda je revizijsko poročilo s priporočili. Temelje zakonske podlage za izvedbo revizijskega pregleda so:

- Uredba Komisije (ES) št. 1663/1995 o določitvi podrobnih pravil za uporabo Uredbe Sveta (ES) št. 729/70 v zvezi s postopkom za potrditev obračuna Jamstvenega oddelka EKUJS;
- Uredba Komisije (ES) št. 2025/2001 z dne 16.10.2001, ki spreminja uredbo št. 1663/1995;
- Smernice za računalniško zaščito.

Revizijski pregled se izvede po naslednjih korakih:

- (revizijski pregled je načrtovan z letnim načrtom dela notranjerevizijske službe);
- seznanitev s področjem revidiranja;
- začetek revizijskega pregleda;
- napoved revizijskega pregleda revidirani enoti in določitev okvirnih rokov;
- izdelava revizijskega programa z revizijskimi cilji;
- priprava vprašalnika;
- testiranje in preizkušanje;
- osnutek revizijskega poročila;
- končno revizijsko poročilo.

Revizijo je mogoče izvesti kot notranjerevizijski pregled ali pregled s strani zunanjih revizorjev, zato je načrtovanje revizijskega pregleda zapisano v oklepaju. Revizor se najprej seznani s področjem revidiranja ter preveri, kako so Smernice za računalniško zaščito prenesene v poslovanje.

**Izdelava revizijskega vprašalnika**

Pri načrtovanju in izvedbi revizijske naloge je pomembna opredelitev revizijskih ciljev. Na osnovi zastavljenih revizijskih ciljev je vprašalnik enostavno izdelati. Za pregled posameznih področij poslovanja je vedno potrebno izdelati drugačen vprašalnik, ki se izdela glede na zastavljene revizijske cilje. Če so revizijski cilji primerno zastavljeni, predstavljajo podlago za vprašalnik, ki ga je potrebno ustrezno prilagoditi.

Informacije, pridobljene med izvedbo revizijskega pregleda, morajo biti zadostne, zanesljive, primerne in uporabne. Ugotovitve morajo temeljiti na analizi in ovrednotenju, kar je zelo pomembno za pripravo revizijskega poročila. Zbrane informacije je potrebno primerjati in primerno ovrednotiti ter dokumentirati ter o izsledkih poročati vodstvu.

Priprava revizijskega vprašalnika je pomembna za pridobitev zanesljivih informacij. Pri izdelavi vprašalnika je pomembno, na kakšen način in kako so oblikovana vprašanja. V skladu z oblikovanimi vprašanji bodo tudi prejeti odgovori. Slabo pripravljeni vprašalniki ne dajejo prave slike o obstoječem stanju.

Informacije, zbrane s pomočjo vprašalnika, so podlaga za pripravo revizijskega poročila. Vprašanja v vprašalniku so lahko odprtega ali zaprtega tipa. Prednost vprašalnika z zaprtimi vprašanji je v tem, da je na vprašanja mogoče hitro odgovoriti, odgovori pa ne morejo biti dvoumni. Če želimo odgovore primerjati, je bolje postavljati vprašanja zaprtega tipa (Galloway, Internet, 1997).

**Zakaj revizija v skladu s Smernicami za računalniško zaščito?**

Smernice za računalniško zaščito predstavljajo okvirno podlago za revidiranje varnosti IT. Podajajo smernice za upravljanja varnosti na področju IT in ne predpisujejo, kako rešitve izvesti.

Smernice za računalniško zaščito so namenjene vodstvu informatike kot podlaga za organizacijo in upravljanje IT. Vsebujejo temeljne cilje, ki naj jih vodstvo z upravljanjem IT doseže in mogoč pristop k izvedbi. Hkrati predstavljajo temeljne podlage - kontrolne cilje za revidiranje IT. Poslovanje v skladu s Smernicami za računalniško zaščito je ena od temeljnih zahtev EU, ki jih morajo izpolnjevati plačilne agencije. Smernice za računalniško zaščito predstavljajo referenčno točko za katerikoli pregled, ki ga izvaja Evropska komisija v kontekstu akreditacije in certificiranja letnih računov.

Revizijski pregled v skladu s **Smernicami za računalniško zaščito** da izhodiščne informacije za načrtovanje bodočih revizij na področju IT. Na podlagi pregleda se pridobi vpogled v obstoječe stanje na področju upravljanja IT in ugotovi, katera področja je potrebno revidirati najprej.

**Sestava vprašalnika:**
- podrobni kontrolni cilj;
- oblikovana vprašanja v skladu s kontrolnim ciljem;
- mnenje o izpolnitvi: v to rubriko se označi, ali je zahteva izpolnjena delno ali v celoti;
- opis: v to rubriko se podrobno opiše, kako je zahteva iz kontrolnega cilja izpolnjena.

Vprašalnik je izdelan tako, da so iz kontrolnih ciljev Smernic za računalniško zaščito oblikovana vprašanja. Iz vsakega kontrolnega cilja je oblikovanih več vprašanj. Na podlagi oblikovanega vprašalnika se v nadaljevanju izdela seznam dokumentov, ki jih mora imeti oddelek za informatiko v skladu s Smernicami za varnostno zaščito.

Vprašalnik zajema bistvene kontrolne točke in se uporablja za preizkušanje delovanja sistema notranjih kontrol. Vprašalnik vsebuje kratka in nedvoumna vprašanja o področjih, ki vplivajo na uspešnost, učinkovitost in dosežke poslovanja ter so umerjena

k ciljem revidiranj. Rezultati vprašalnika služijo za začetno oceno delovanja notranjih kontrol.

### 6.3.1 Revizijski vprašalnik

Preglednica 2: Revizijski vprašalnik (1)

**1. SPLOŠNA ORGANIZACIJA, UPRAVLJANJE IN REVIZIJA**

**1.1 Strategija in upravljanje IT**

**Kontrolni cilj:** Strategija upravljanja IS plačilne agencije naj bo skladna s cilji plačilne agencije. Oddelek za informatiko mora vzpostaviti in posodabljati strategijo razvoja IS.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| Ali obstaja strategija za vzpostavitev in upravljanje IS plačilne agencije? | | | |
| Ali se strategija informatizacije plačilne agencije sklada s poslovnimi cilji plačilne agencije? | | | |
| Ali je varnostna politika del strategije informatizacije plačilne agencije? | | | |
| Ali obstajajo kratkoročni in dolgoročni načrti upravljanja IT? | | | |
| Se kratkoročni in dolgoročni načrti skladajo z načrti poslovanja plačilne agencije? | | | |
| Ali strategijo odobri najvišje vodstvo agencije? | | | |
| Ali strateški načrt obsega obdobje dveh do treh let? | | | |
| Ali strateški načrt obsega programsko in strojno opremo? | | | |

**1.2 Politike, standardi in postopki**

**Kontrolni cilj:** Aktivnosti IT naj temeljijo na politikah, standardih in postopkih.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| Ali so aktivnosti IT zasnovane na politikah, standardih in postopkih? | | | |
| Ali vodstvo določi in spremlja standarde in postopke za sistemski razvoj in programiranje, sistemsko dokumentacijo, zaščito IS in upravljanje s podatki na osnovi politik? | | | |
| Ali so politike in standardi v skladu z nacionalno in evropsko zakonodajo in se ravnajo po mednarodno sprejetih standardih? | | | |
| So odgovornosti uporabnikov in zaposlenih v oddelku za informatiko natančno opredeljene? | | | |

Nadaljevanje preglednice 2: Revizijski vprašalnik (2)

**1.3 Ločitev funkcij**

**Kontrolni cilj:** Oddelek za informatiko mora biti organizacijsko ločen od ostalih organizacijskih enot. Vodstvo naj zagotavlja ustrezno ločitev funkcij znotraj organizacijskih enot in med organizacijskimi enotami.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| Ali status oddelka za informatiko v organizacijski strukturi agencije zagotavlja njegovo neodvisnost od ostalih oddelkov? | | | |
| Ali status oddelka za informatiko v organizacijski strukturi agencije zagotavlja doseganje ciljev organizacije? | | | |
| Ali vodstvo zagotavlja primerno ločitev funkcij znotraj in med poslovnimi enotami? | | | |
| Ali ima oddelek za informatiko neodvisno mesto v organizaciji in jasno določeno organizacijsko strukturo? | | | |
| Ali ima strokovno osebje za področje informatike dovolj visok nivo znanja? | | | |
| Ali ima oddelek za informatiko na voljo dovolj finančnih virov za nakup ustrezne opreme? | | | |
| Ali je zagotovljena razmejitev nalog med uporabniki, razvojnim oddelkom in oddelkom za sistemsko podporo? | | | |

**1.4 Kadrovska politika**

**Kontrolni cilj:** Vodstvo bi moralo obravnavati kadrovske vidike računalniške zaščite.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| Ali kadrovska politika določa odgovornosti za varovanje informacij? | | | |
| Ali se zaposleni izobražujejo s področja varovanja informacij in ali se zavedajo pomembnosti tega področja? | | | |

**1.5 Revidiranje IT**

**Kontrolni cilj:** Neodvisna funkcija notranjega nadzora naj bi imela zadostno tehnično pristojnost (oziroma možnost sodelovanja z zunanjimi strokovnjaki) in pooblastila za raziskovanje in poročanje o IT kontrolah ter za predlaganje priporočil za izboljšave.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| Je revidiranje IS predvideno v listini o revizijski službi? | | | |
| Ali načrt revidiranja IS ter poročila odobri in nadzira najvišje vodstvo? | | | |
| Ali imajo revizorji IS znanja in izkušnje s področja informacijskih tehnologij agencije? | | | |

Nadaljevanje preglednice 2: Revizijski vprašalnik (3)

**2. FIZIČNA VARNOST**

**Kontrolni cilj:** Namernemu ali nenamernemu fizičnemu uničenju nameščene IT opreme naj bi se izognili z izvajanjem preventivnih ukrepov in odkrivanjem v zgodnji fazi z namenom zaščite pred možnimi posledicami.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| **2.1 Fizični dostop** | | | |
| Je fizični dostop v poslovno zgradbo centralno nadziran? | | | |
| Je fizični dostop do prostorov, kjer se nahaja vitalna oprema (strežniki in podobno), omejen na pooblaščene osebe? | | | |
| Je dostop nepooblaščenih oziroma nezaposlenih oseb do teh prostorov evidentiran? | | | |
| **2.2 Preprečitev in odkrivanje požarov ter protipožarna zaščita** | | | |
| Je računalniški center oddaljen od področij, kjer so shranjene vnetljive snovi? | | | |
| So vse vnetljive snovi shranjene izven računalniške sobe? | | | |
| Je osebje seznanjeno s tem, da v računalniški sobi ni dovoljeno jesti, piti in kaditi? | | | |
| Je centralni računalniški sistem v prostorih, ki so ločeni od ostalih prostorov? | | | |
| So v računalniškem centru nameščeni detektorji za ogenj, dim ali vročino? | | | |
| So v prostoru avtomatski ali ročni sistemi za gašenje? | | | |
| So vzpostavljeni postopki za ravnanje v sili in v primeru požara? | | | |
| So opisi postopkov za ravnanje v sili ali v primeru požara v računalniškem centru vidnem mestu? | | | |
| Se gasilske vaje redno izvajajo? | | | |
| So požarni izhodi označeni? | | | |
| **2.3 Preprečevanje in odkrivanje vdora vode** | | | |
| Je računalniški center nameščen stran od področij, ki so izpostavljena poplavam? | | | |
| So v talnih odprtinah nameščeni detektorji vode ter oprema za črpanje in odstranjevanje vode? | | | |
| **2.4 Zaščita električnega napajanja** | | | |
| Je za izvajanje ustreznega zaustavljanja kritičnih sistemov nameščen brezprekinitveni vir napajanja (UPS) ali rezervni generator, ki je redno preizkušan (vsaj enkrat letno)? | | | |

Nadaljevanje preglednice 2: Revizijski vprašalnik (4)

**3. LOGIČNA VARNOST**

**Kontrolni cilj:** Dostop do podatkov naj bo omejen le na tiste posameznike, ki imajo pooblastilo za dostop. Nadzor nad dostopi je zabeležen s sledmi za nadzor.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| **3.1 Logična zaščita – varnost** | | | |
| So dostopi do podatkov omejeni le na pooblaščene posameznike? | | | |
| Ali obstajajo formalni postopki za izdajanje dostopnih pravic? | | | |
| Se vsi dostopi v računalniški sistem beležijo v log datoteko v obliki sledi za nadzor? | | | |
| Ali se log datoteke redno pregledujejo? | | | |
| **3.2 Logična zaščita – programi** | | | |
| Ali se produkcijske knjižnice vzdržujejo ločeno od razvojnih in testnih knjižnic? | | | |
| **3.3 Logična zaščita – osebje** | | | |
| Ali je zagotovljeno, da uporabniki ne uporabljajo enakih gesel ter da si gesel medsebojno ne izmenjujejo? | | | |
| Ali so gesla tajna, imajo vsaj minimalne kakovostne zahteve in se spreminjajo v rednih časovnih obdobjih? | | | |
| Se vse operacije uporabnikov beležijo v obliki sledi za nadzor? | | | |
| Se sledi za nadzor redno pregledujejo? | | | |
| **3.4 Logična zaščita – podatki** | | | |
| Ali se vse vnosne podatke kontrolira logično in vsebinsko? | | | |
| **3.5 Logična zaščita-sistemska programska oprema** | | | |
| Je zaščita operacijskega sistema, omrežja in programske opreme ustrezno nameščena? | | | |
| So na voljo revizorske sledi za nadzor vseh sprememb nastavitev sistemske programske opreme? | | | |

Nadaljevanje preglednice 2: Revizijski vprašalnik (5)

**4. RAZVIJANJE, PROGRAMIRANJE IN VZDRŽEVANJE IS**

**Kontrolni cilj:** Metoda razvoja in vzdrževanja IS bi morala zagotavljati učinkovite in zmogljive sisteme ter zagotavljati zaščito podatkov z vidika zaupnosti, celovitosti, razpoložljivosti in sledljivosti.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| **4.1 Projektno vodenje** | | | |
| Je pristojno telo za odločanje, ki zagotavlja, da se prioritete določi v skladu s cilji organizacije, najvišje vodstvo agencije? | | | |
| **4.2 Standardi za razvoj sistemov** | | | |
| Se za razvoj aplikacij in programiranje z namenom povečanja zmogljivosti in učinkovitosti razvoja in vzdrževanja IS uporabljajo uveljavljeni standardi? | | | |
| **4.3 Postopki pri posameznih fazah projekta** | | | |
| **4.3.1 Začetek projekta** | | | |
| Je cilj razvoja IS jasno določen pred pričetkom izvajanja projekta? | | | |
| **4.3.2 Študija izvedljivosti** | | | |
| Je za vsak nov IS ali sistem, ki se bo spreminjal, jasno določen potek dogodkov? | | | |
| Se študija tehnološke izvedljivosti ter stroški in koristi vsakega predloga pregledajo? | | | |
| So opredeljena tveganja in ustrezne interne kontrole? | | | |
| Je pripravljen načrt za nadzor in upravljanje stroškov, ki bodo nastali med izvajanjem projekta? | | | |
| **4.3.3. Analiza in načrtovanje** | | | |
| So sistemske zahteve jasno določene in vključene v specifikacije za načrtovanje IS? | | | |
| So vhodne in izhodne specifikacije ter specifikacije za podatkovne strukture ter kontrole jasno opredeljene? | | | |
| So sledi za nadzor vključene v sistem? | | | |
| **4.3.4. Izgradnja, preizkušanje in implementacija** | | | |
| So cilji za programiranje definirani, programerske naloge dodeljene, priročniki in standardi za testiranje pripravljeni in kriteriji za sprejem izdelani? | | | |

**4.4. Upravljanje sprememb**

**Kontrolni cilj:** Vse spremembe strojne in programske opreme naj bi bile pred implementacijo testirane, načrtovane in odobrene.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| So postopki za nadzor sprememb vseh delujočih IS vzpostavljeni? | | | |
| Je zagotovljeno hranjenje izvorne in izvajalne kode? | | | |
| So vzpostavljeni postopki, ki zagotavljajo vzpostavljanje predhodnega stanja v primeru neuspešnih sprememb? | | | |
| Je zagotovljena ločitev razvojnega in produkcijskega okolja? | | | |

**5. RUTINSKA DELA OSREDNJIH RAČUNALNIKOV**

**Kontrolni cilj:** IT naj bi bila nadzorovana tako, da se zagotovi učinkovita uporaba. Podatkovne datoteke bi morale biti zavarovane pred izgubo. Vzpostavljene bi morale biti ustrezne sledi za nadzor.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| **5.1 Vzdrževanje opreme** | | | |
| Je preventivno vzdrževanje opreme časovno načrtovano v skladu z navodili in garancijami proizvajalca? | | | |
| **5.2 Delitev in izmenjava dolžnosti** | | | |
| Je delo operaterjev nadzirano? | | | |
| Ali sta vsaj dva zaposlena usposobljena za izvajanje katerekoli kritične naloge? | | | |
| **5.3 Operaterjevo delo** | | | |
| Ali so vsi postopki, ki jih izvaja operater, dokumentirani? | | | |
| **5.4 Izvajanje in načrtovanje obdelav** | | | |
| Se parametri za nadzor produkcijskih obdelav hranijo v zaščiteni knjižnici? | | | |
| So dopolnitve / spremembe programskih knjižnic nadzorovane? | | | |
| **5.5 Nadzor dejavnosti** | | | |
| So vzpostavljeni postopki za izvajanje in nadzor kritičnih obdelav? | | | |
| **5.6 Revizijska sled** | | | |
| Se vsi administratorjevi postopki beležijo v log datoteke? | | | |
| Se revizijske sledi redno pregledujejo? | | | |
| **5.7 Nadzor knjižnic** | | | |
| So trakovi in ostali mediji shranjeni v zaprti knjižnici z omejenim dostopom? | | | |

Nadaljevanje preglednice 2: Revizijski vprašalnik (7)

**6. TELEKOMUNIKACIJE**

**Kontrolni cilj:** Vzpostavitev ustreznih postopkov za zaščito telekomunikacijskih omrežij.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| So vsa omrežja zavarovana pred nepooblaščenim zunanjim dostopom? | | | |
| Je klicni dostop v omrežje opremljen s »call back« funkcijo (povratni klic)? | | | |
| Je dostop do Interneta zaščiten (požarni zid)? | | | |
| Je pošiljanje podatkov izven omrežja zagotovljeno preko najetih ali zaščitenih linij oziroma šifriranje podatkov? | | | |
| Je zagotovljeno preverjanje identitete pošiljatelja? | | | |
| Je zagotovljeno ohranjanje integritete podatkov pri prenosu? | | | |
| Je zagotovljeno, da v primeru napačnega vnosa sistem vnos zavrne in nadaljnje delo ni mogoče? | | | |
| So uvedeni ustrezni ukrepi proti zlonamernim dejanjem (virusi,... )? | | | |

**7. MIKRORAČUNALNIKI**

**Kontrolni cilj:** Obstajali naj bi postopki definiranja zahtev za nabavo opreme, uporabo in nadzor osebnih računalnikov in pripadajoče programske opreme.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| Je strojna in programska oprema agencije standardizirana? | | | |
| Je zagotovljeno, da uporabniki programske opreme ne morejo nameščati sami? | | | |
| Je zagotovljeno, da uporabniki ne uporabljajo programske opreme brez predhodne odobritve? | | | |
| Ali so vzpostavljeni postopki za varnostno shranjevanje ključnih podatkov in programske opreme ? | | | |
| Ali je zagotovljeno varnostno shranjevanje kopij podatkov na oddaljeni lokaciji? | | | |
| Je poskrbljeno za ustrezno fizično in logično zaščito podatkov na osebnih računalnikih? | | | |
| So podatki na prenosnih računalnikih, dlančnikih in podobno zaščiteni? | | | |
| Je vzpostavljena politika za zaščito pred zlonamernimi programi (virusi in podobno), ki vključuje zavedanje uporabnikov, preventivne in detektivne ukrepe ter odstranjevanje okuženih programov? | | | |

Nadaljevanje preglednice 2: Revizijski vprašalnik (8)

**8. NAČRTOVANJE NEPREKINJENEGA POSLOVANJA**

**Kontrolni cilj:** Obstajali naj bi preizkušeni načrti za varnostno shranjevanje kritičnih računalniških aplikacij in za ponovno vzpostavljanje predhodnih storitev na področju IT zaradi nepredvidenih prekinitev.

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| Ali obstaja ustrezen okrevalni načrt (Disaster recovery plan) za vzpostavitev predhodnega stanja za ključne aplikacije v primeru večje okvare strojne ali programske opreme oziroma začasne ali trajne prekinitve delovanja IT? | | | |
| Ali okrevalni načrt temelji na oceni tveganja, ki vključuje tako IT kot končne uporabnike in je odobren s strani najvišjega vodstva? | | | |
| Se načrt preizkusi vsaj enkrat letno? | | | |
| Se varnostne kopije podatkov (back-up), sistemske programske opreme, aplikacijske programske opreme, dokumentacije in delovnih navodil izvajajo redno? | | | |
| Se varnostne kopije podatkov, sistemske programske opreme, aplikacijske programske opreme, dokumentacije in delovnih navodil shranjujejo na oddaljeni lokaciji? | | | |
| Je prevoz varnostnih kopij na oddaljeno lokacijo varovan? | | | |

**9. APLIKATIVNE KONTROLE**

| **Nadzorni postopki, uporabljeni za ugotavljanje izpolnitve kontrolnega cilja** | **MNENJE O IZPOLNITVI** | | **OPIS** |
|---|---|---|---|
| | v pripravi | izvedeno | |
| **9.1 Vnos podatkov** | | | |
| So vhodni podatki pred vnosom ustrezno potrjeni? | | | |
| Ali se pred vnosom podatkov preveri popolnost podatkov? | | | |
| Se podatke preverja med procesom vnosa? | | | |
| So vzpostavljeni postopki za obravnavanje napak, da se zagotovi pravočasno in pravilno popravljanje podatkov? | | | |
| **9.2 Obdelava podatkov** | | | |
| Ali obstajajo kontrole nad obdelavo podatkov, z namenom preprečevanja nepooblaščenega dodajanja, brisanja ali spreminjanja podatkov? | | | |
| **9.3 Izhodni podatki** | | | |
| So rezultati obdelave pravočasno razdeljeni pooblaščenim osebam, ki pregledajo rezultate in ustrezno pravočasno ukrepajo? | | | |
| **9.4 Stalni podatki** | | | |
| Ali je dostop, spreminjanje in uporaba stalnih podatkov (ime, priimek, številka bančnega računa, …), ki se uporabljajo v različnih procesih in aplikacijah, ustrezno nadzorovan? | | | |
| Ali se takšne podatke občasno preverja z usklajevanjem ali navzkrižnim sklicevanjem na neodvisne podatke? | | | |

Vir: lasten, 2003.

# ZAKLJUČEK

Vstop v EU je prinesel novim državam članicam veliko novosti. Po vstopu v EU morajo države članice delovati v skladu s pravnim redom EU in v skladu z evropsko zakonodajo. Slovenija je z vstopom v EU za izvajanje SKP prevzela pravni red EU na področju kmetijstva ter vse pravice, ki na tem področju veljajo za države članice EU. S tem pa se je tudi zavezala k izpolnjevanju novih obveznosti ter poslovanju v skladu s pravili in zakonodajo EU.

V skladu z zahtevami EU morajo vse države članice za izvajanje ukrepov SKP EU ustanoviti plačilne agencije. Koriščenje finančnih sredstev EU je skrbno nadzorovano in v skladu s tem mora država članica vzpostaviti vrsto postopkov in se podvreči mnogim pravilom, ki jih na tem področju narekuje EU. Pri koriščenju finančnih sredstev EU je pomembno izvajanje finančnega nadzora, ki ga EU izvaja z namenom nadziranja pravilnosti porabe finančnih sredstev.

Agencija mora od pristojnega organa pridobiti akreditacijo, to je zagotovilo, da ima vzpostavljene vse predpisane postopke, da deluje v skladu s pravili in izvaja sistem notranjega nadzora. V ta namen se je Agencija spoprijela z zahtevno nalogo, saj je bilo potrebno vzpostaviti organizacijo in postopke na vseh področjih delovanja Agencije. Postopke je bilo potrebno vzpostaviti v skladu z zakonodajo EU in ravno tako v skladu s slovensko zakonodajo. V celoti je bilo potrebno vzpostaviti tudi IS Agencije.

Novost je bila tudi izpolnjevanje zahteve po povečanem izvajanju nadzora s strani predstavnikov EU in domačih organov. Vse ustanove, ki izplačujejo finančna sredstva EU, morajo poleg zagotavljanja poslovanja v skladu z zakonodajo in predpisi EU vzpostaviti tudi ustrezne sisteme notranjega in zunanjega nadzora z namenom zagotavljanja preglednosti porabe finančnih sredstev. EU zahteva preglednost poslovanja in vzpostavitev nadzora porabe finančnih sredstev z namenom zaščite koriščenja sredstev evropskega proračuna, ki lahko brez izvajanja ustreznega nadzora postane nepregledno in predstavlja nevarnosti za pojavljanje nepravilnosti, prevar in goljufij.

Pri izvajanju postopkov mora Agencije v celoti poslovati v skladu z Uredbo Komisije (ES) št. 1995/63 o določitvi podrobnih pravil za uporabo Uredbe Sveta (EGS) št. 729/70 v zvezi s postopkom za potrditev obračuna Jamstvenega oddelka EKUJS in smernicami za merila za akreditacijo plačilne agencije, ki so priloga uredbe. Plačilne agencije morajo izpolniti vse pogoje, navedene v Merilih za akreditacijo. Vsi postopki morajo biti pregledni, delovanje poslovnih procesov in IS pa mora biti preverjeno, kontrolirano in ponovljivo.

Na področju računalniške zaščite morajo biti postopki vzpostavljeni v skladu z uredbo št. 1663/95 in v skladu s Smernicami za računalniško zaščito. Cilj naloge je bil izdelati revizijski vprašalnik v skladu s Smernicami za računalniško zaščito. Vprašalnik predstavlja podlago za izvedbo revizijskega pregleda v skladu s Smernicami za računalniško zaščito IS. Pregled na podlagi Smernic za računalniško zaščito predstavlja oceno o izpolnjevanju temeljnih zahtev v skladu z varnostjo in zaščito IS. Vprašalnik pa je lahko hkrati podlaga odgovornim pri pregledu izpolnjevanja temeljnih kontrolnih ciljev v skladu z varovanjem IS. Opisano metodologijo izdelave vprašalnika je mogoče uporabiti pri katerem koli revizijskemu pregledu oziroma pri izvajanju delovnih nalog kot delovni pripomoček, namenjen pregledu izvedbe nalog.

Pomembna vloga priprave in uporabe vprašalnika je v tem, da ga je mogoče na sistematičen način izdelati in uporabiti med samim postopkom izvajanja in obvladovanja nalog na podlagi predpisanih pravil. Na ta način so na enem mestu zbrane vse kontrolne točke, na katere moramo biti pri izgradnji pozorni.

# LITERATURA


1. Bobek Samo, Lesjak Dušan: Informatika za ekonomiste. Maribor : Ekonomsko poslovna fakulteta, 1993. 325 str.
2. Brečko Vlasta: Sistem notranjih kontrol. Gradivo za izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor. Ljubljana : Slovenski inštitut za revizijo, 2001, str. 1-15.
3. Cunder Tomaž et al.: Slovensko kmetijstvo in Evropska unija. Ljubljana : ČZD Kmečki glas, 1997. 439 str.
4. Damij Talib: Poslovna informatika. Ljubljana : Ekonomska fakulteta, 2002. 204 str.
5. Donald H. Taylor, G. William Glezen: Revidiranje - zasnove in postopki. Ljubljana, Slovenski inštitut za revizijo, 1996. 1078 str.
6. Derek J. Oliver: Pregledni seminar za pripravo na izpit CISA. Ljubljana : Slovenski inštitut za revizijo, 2002.
7. Drobnič Nada et al.: Revidiranje v razmerah računalniškega obdelovanja podatkov. Ljubljana : Slovenski inštitut za revizijo, 1996. 166 str.
8. Eckerson W. Wayne: Data Quality and the Bottom Line. Achieving Business Success through a Commitment to High Quality Data. The Data Warehousing Institute, 2002. 33 str.
9. Galloway Alison: Questionnaire Design & Analysis Workbook. [URL: http://www.tardis.ed.ac.uk/~kate/qmcweb/qcont.htm], 1997.
10. Gradišar Miro, Resinovič Gortan: Informatika v organizaciji. Maribor : Univerza v Mariboru, Fakulteta za organizacijske vede Kranj, 1998. 472 str.
11. Gradišar Miro, Resinovič Gortan: Informatika v poslovnem okolju. Ljubljana : Ekonomska fakulteta, 2001. 508 str.
12. Hajtnik Tatjana: Priporočila za pripravo informacijske varnostne politike. Ljubljana : Center Vlade za informatiko, 2002. 228 str.
13. Hočevar M., Igličar A.: Osnove računovodstva. Ljubljana : Ekonomska fakulteta, 1995. 268 str.
14. Hudoklin Alenka: Varnost računalniško podprtega informacijskega sistema. Kranj : Organizacija in kadri, 1991, str. 604-609.
15. Hudoklin Alenka, Stadler Alenka: Audit in an EDI environment. Ninth International Conference on EDI – IOS. Kranj : Moderna organizacija, 1995, str. 389-397.
16. Karnet Igor, Franci Tajnik: Pripravljalni seminar za pripravo na izpit CISA. Ljubljana : Slovenski inštitut za revizijo, 2003.
17. Javornik Boža: Organiziranje notranje revizijske službe – izhodišča za postavitev revidiranja informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2000. 11 str.
18. Javornik Boža: Informacijska podpora notranjemu revidiranju in revidiranje v okolju računalniško podprtih informacijskih sistemov. Gradivo za izobraževanje za

pridobitev strokovnega naziva preizkušeni notranji revizor. Ljubljana : Slovenski inštitut za revizijo, 2001. str. 1-18.
19. Kljajić Žebeljan Tatjana: Plan neprekinjenega poslovanja. Zbornik referatov 10. mednarodne konference o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2002, str. 315-324.
20. Laudon Kenneth C., Laudon Jane Price: Information Systems - a problem solving approach. Orlando : The Dryden Press, 1995. 254 str.
21. Laudon Kenneth C., Laudon Jane Price: Management Information Systems : Organization and Technology in the Networked Enterprise. London : Prentice Hall International, 2000. 588 str.
22. Lešnik Korbar Boža: Postopki notranjega revidiranja. Gradivo za izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor. Ljubljana : Slovenski inštitut za revizijo, 2001. 62 str.
23. Majič Mojca: Obvladovanje bančnih tveganj. Gradivo za izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor. Ljubljana : Slovenski inštitut za revizijo, 2001. 12 str.
24. Mugerle Franci: Revizija računovodstva in revizija informacijskih sistemov. Zbornik posvetovanja dnevi slovenske informatike. Ljubljana : Slovensko društvo informatika, 1995, str. 68-73.
25. Natek Srečko: Razvijanje poslovnega informacijskega sistema. Vojnik : Mitos, 1990, 252 str.
26. Nemec Anica: Notranja revizija v industrijskem podjetju. Ljubljana : Slovenski inštitut za revizijo, 2003. 27 str.
27. Podgoršek Marjan: Revidiranje MFERAC – rediviranje aplikativnih kontrol. Program izobraževanja in certificiranja državnih notranjih revizorjev. Ljubljana : Center za razvoj financ, 2003. 21 str.
28. 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.
29. Ratliff R., Reding K: Introduction to Auditing: Logic, Principles, and Techniques. Altamonte Springs : The Institute of Internal Auditors, 2002. 531 str.
30. Ray Deborah: Data center review audit program. [URL: http://www.auditnet.org/docs/data_ctr.txt], 28.7.1999.
31. Ruthberg Zella G., Fisher Bonnie T., Lainhart IV John W.: System Development Auditor. Oxford : Elsevier Science Publishers, 1991. 490 str.
32. Sawyer L. et al.: The Practice of Modern Internal Auditing. Altamonte Springs : The Institute of Internal Auditors, 2003. 1446 str.
33. Silltow John: IT Audit Planning. [URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5566], 15.11.2004.
34. Simič Slobodan: Spoznajmo lokalne računalniške mreže. Ljubljana : Mikroračunalniški center ŠKD Forum, 1988. 196. str.

35. Več avtorjev: CISA Review Manual 2003. Illinois : Information Systems Audit and Control Association, Inc. 2003. 474 str.
36. Taylor D., Glezen W: Revidiranje zasnove in postopki. Ljubljana : Slovenski inštitut za revizijo, 1996. 1078 str.
37. Turban Efraim et al.: Information Technology for Management : Making Connections for Strategic Advantage. New York : J. Wiley, 1999. 791 str.
38. Turban Efraim et al.: Introduction to Information Technology. New York : J. Wiley, 2001. 526 str.
39. Turk Ivan et al.: Notranje revidiranje poslovanja. Ljubljana : Slovenski inštitut za revizijo in Zveza računovodij, finančnikov in revizorjev Slovenije, 1994. 282 str.
40. Turk Ivan: Pojmovnik računovodstva, financ in revizije. Ljubljana : Slovenski inštitut za revizijo, 2000. 1082 str.
41. Turk Ivan: Kaj razumemo z informacijskim sistemom? Zbornik referatov 9. mednarodne konference o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2001, str. 117-129.
42. Turk Ivan: Pojmovnik uporabniške informatike. Ljubljana : Slovenski inštitut za revizijo, 2002. 713 str.
43. Turk Meta: Organiziranje in vodenje notranjerevizorske službe. Gradivo za izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor. Ljubljana : Slovenski inštitut za revizijo, 2001. 20 str.
44. Turk Meta: Tehnike notranjega revidiranja. Program izobraževanja in certificiranja državnih notranjih revizorjev. Ljubljana : Center za razvoj financ, 2003. 42 str.
45. Uratnik Janko: Zagotavljanje kakovosti programske opreme in njeno revidiranje v finančnih ustanovah. Zbornik referatov 10. mednarodne konference o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2002, str. 249-269.
46. Valenčič Iztok: Postavitev in uvedba dobre varnostne politike. Zbornik referatov 8. mednarodne konference o revidiranju in kontroli informacijskih sistemov. Ljubljana : Slovenski inštitut za revizijo, 2000, str. 165-177.
47. Vallabhaneni S. Rao: CISA Examination Textbooks. Volume 1: Theory. Illinois. SRV Professional Publications, 1998. 1113 str.

## VIRI

1. CAP reform - a long-term perspective for sustainable agriculture. [URL: http://europa.eu.int/comm/agriculture/capreform/index_en.htm], 15.7.2004.
2. Commission Regulation (EC) No 1663/1995 of 7 July 1995 laying down detailed rules for the application of Council Regulation (EEC) No. 729/70 regarding the procedure for the clearance of the accounts of the EAGGF Guarantee Section (Offical Journal of the European Communities, No. 158/95).

3. Commission Regulation (EC) No 2025/2001 of 16 October 2001 amending Regulation (EC) No 1663/95 laying down detailed rules for the application of Council Regulation (EEC) No 729/70 regarding the procedure for the clearance of the accounts of the EAGGF Guarantee Section (Official Journal, No. 274).
4. Council Regulation (EC) No 1258/1999 of 17 May 1999 on financing of the common agricultural policy (Official Journal, No. 160).
5. Council Regulation (EC) No 1287/95 of 22 May 1995 amending Regulation (EEC) No 729/70 on the financing of the common agricultural policy (Official Journal, No. 125).
6. Interna gradiva Agencije Republike Slovenije za kmetijske trge in razvoj podeželja.
7. Interna gradiva Ministrstva za kmetijstvo, gozdarstvo in prehrano.
8. Information Systems Audit and Control Foundation, IT Governance Institute. Rolling Meadows : COBIT 3rd Edition, 2000.
9. IS Standards, Guidelines and Procedures for Auditing and Control Professionals. Rolling Meadows : Information Systems Audit and Control Association, 2002. 89 str.
10. IT Audits in the paying agencies – Final Report. Paris : European Commission, DG.AGRI-J1, 2002.
11. Kodeks notranjerevizijskih načel. Ljubljana : Slovenski inštitut za revizijo, 1998. 7 str.
12. Kodeks poklicne etike notranjega revizorja. Ljubljana : Slovenski inštitut za revizijo, 1998. 5 str.
13. Metodologija vodenja projektov v državni upravi. Ljubljana : Vlada Republike Slovenije, 1997. 277 str.
14. Načrt razvoja podeželja 2000-2006. Ljubljana : Ministrstvo za kmetijstvo, gozdarstvo in prehrano, 2000. 85 str.
15. Paying Agencies' I.T. Systems; Computer Security Guidelines No VI/661/97, rev. 2. Brussels : European Commission Directorate-General VI Agriculture, 1998. 10 str.
16. Pravilnik o notranji organizaciji in sistemizaciji delovnih mest (Uradni list RS, št. 011-7/00).
17. Pravni red skupnosti. [URL:http://evropska-unija.si/pages/evropska_unija/vodic/pravni_red_skupnosti.html], 1.9.2004.
18. Program reforme kmetijske politike 1999-2002. Ljubljana : Ministrstvo za kmetijstvo, gozdarstvo in prehrano, 1998. 25 str.
19. PSIST BS 7799, Kodeks varovanja informacij. Ljubljana : Urad Republike Slovenije za standardizacijo in meroslovje pri Ministrstvu za znanost in tehnologijo, 1997. 135 str.
20. Sklep Vlade Republike Slovenije, številka 900-10/98-31 z dne 7.1.1999.
21. Standardi notranjega revidiranja. Ljubljana : Slovenski inštitut za revizijo, 2003. 170 str.
22. Uredba o akreditacijskih pogojih za delovanje Agencije Republike Slovenije za kmetijske trge in razvoj podeželja (Uradni list RS, št. 78/2000).

23. Uredba o splošnih akreditacijskih pogojih plačilnih Agencij Republike Slovenije za uporabo finančnih sredstev Evropske unije (Uradni list RS, št. 107/99).
24. Usmeritve za državno notranje revidiranje. Ljubljana : Ministrstvo za finance, Služba za nadzor proračuna, 2003. 42 str.
25. Večletni sporazum o financiranju med Komisijo evropskih skupnosti in Vlado Republike Slovenije. Bruselj : Evropska komisija, 2001. 50 str.
26. Zakon o bančništvu (Uradni list RS, št. 07/99).
27. Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/00).
28. Zakon o javnih financah (Uradni list RS, št. 79/99).
29. Zakon o kmetijstvu (Uradni list RS, št. 54/00).
30. Zakon o spremembah in dopolnitvah zakona o organizaciji in delovnem področju ministrstev (Uradni list RS, št. 60/99).
31. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 59/99).
32. Zakon o zavarovalništvu (Uradni list RS, št. 13/00, 50/04).
33. Zgodovina. [URL http://www.evropska-unija.si/pages/evropska_unija/vodic/zgodovina_eu.html], 1.9.2004.

# SLOVARČEK SLOVENSKIH PREVODOV TUJIH IZRAZOV

| | |
|---|---|
| accuracy | točnost |
| audit guidelines | smernice za revidiranje |
| availability | razpoložljivost |
| backup | varnostna kopija podatkov |
| benchmarking | primerjava |
| call back | povratni klic |
| change management | upravljanje sprememb |
| completeness | popolnost |
| compliance audit | revidiranje skladnosti s predpisi |
| compliance test | test skladnosti |
| confidentiality | zaupnost |
| contingency planning | načrtovanje neprekinjenega poslovanja |
| control objective | kontrolni cilj |
| data integrity | varovanje podatkov |
| decision | odločitev |
| detective control | kontrola odkritja |
| directive | smernica |
| directorate général | generalni direktorat |
| disaster recovery plan | okrevalni načrt |
| effectiveness | uspešnost |
| efficiency | učinkovitost |
| feasibility study | študija izvedljivosti |
| financial statement audit | revidiranje računovodskih izkazov |
| hardware | strojna oprema |
| inherent risk | obstoječe tveganje |
| integrity | neoporečnost |
| internal accounting controls | notranje računovodske kontrole |
| internet service provider (ISP) | ponudnik Internetnih storitev |
| local area network (LAN) | lokalna računalniška mreža |
| network service provider (NSP) | ponudniki omrežnih storitev |
| on the spot control | kontrolni pregled na kraju samem |
| operational and performance audit | revidiranje poslovanja |
| opinion | mnenje |
| preventive control | kontrola preprečevanja |
| reliability | zanesljivost |
| residual risk | preostalo tveganje |
| risk | tveganje |
| rsk based audit | revidiranje, zasnovano na tveganjih |
| risk management | ravnanje s tveganji |

| | |
|---|---|
| security | varnost |
| security policy | varnostna politika |
| software | programska oprema |
| substantive test | primerjalni test |
| system development life cycle (SDLC) | življenjski cikel razvoja sistemov |
| traffic | promet |
| wide area network (WAN) | razprostrto računalniške omrežje |