Dokument:	**PRIMER Spoznavanje IS organizacije – Maloprodajna veriga osnutek**
Ime revidiranca:	Maloprodajna trgovska veriga ABC (izmišljeni primer)
Ime revizije:	Revizija delovanja informacijskih sistemov po okviru COBIT 4.1[1]
Namen dokumenta:	Dokumentirati in razumeti vse komponente IS revidirane organizacije, ki so relevantni za izvedbo revizijske naloge[2].
Uporaba dokumenta:	Pričujoči vzorčni dokument je zasnovan ob naslednjih predpostavkah: • da je cilj načrtovane revizije učinkovitost delovanja celotnega IS revidirane organizacije, • da je revidirana organizacija del zasebnega sektorja Kot ilustrativni primer smo izbrali maloprodajno trgovsko verigo, kot tip organizacije, ki je široko znan in katerega procese si je relativno lahko predstavljati. **Vsi podatki pričujočega primera delovnega papirja so izmišljeni in ne predstavljajo dejanskega delovanja kakršnekoli resnične organizacije!** Spoznavanje IS za doseganje drugih revizijskih ciljev ali za drug tip organizacije bi potekalo drugače.
Povzetek točk:	**1. Temeljne programske rešitve organizacije 3** **2. Tehnološka infrastruktura informacijskega sistema organizacije**

[1] Kljub temu, da je že izdana različica 5 okvira COBIT, se v standardni revizijski mapi zanašamo na v slovenščino prevedeno različico COBIT 4.1. Okvir COBIT 4.1 (Kontrolni cilji za informacijsko in sorodno tehnologijo) pripravlja Inštitut za upravljanje IT (angl. IT Governance Institut ITGI™), ki pripravlja standarde v zvezi z usmerjanjem in nadzorom informacijske tehnologije v podjetjih (različico 5 pripravlja ISACA). Okvir opisuje dobre prakse celotne domene IT in procesnega okvira ter predstavlja aktivnosti na področju IT na obvladljiv in logičen način. COBIT-ove dobre prakse so usmerjene bolj na kontrolo in manj na izvajanje. Namenjene so pomoči pri optimiziranju investicij s komponento IT, pri zagotavljanju storitev IT ter pri presojanju v primerih, ko gredo stvari narobe. Kot okvir dobrih praks izvajanja domene IT jih lahko uporabljamo tudi kot vodilo priporočenega stanja procesov in kontrol na tem področju, pri čemer pa je treba upoštevati uporabnost posameznih dobrih praks v dejanskih organizacijah. Slovenski prevod COBIT 4.1 je na voljo na spletni strani http://www.isaca.si/. Gradivo je avtorsko zaščiteno ter je v pričujoče materiale vključeno izključno v izobraževalne namene.

[2] Delovni zapis je pripravljen ob predpostavki, da organizacija naroča revizijo učinkovitosti delovanja informacijskega sistema ABC po okviru COBIT 4.1. Primer je izbran ker gre za pogost tip pregleda. Dokument mora biti prilagojena zahtevam konkretne revizijske naloge.

Avtor:	Maja Hmelak, Uroš Žust

Verzija	Datum	Oseba	Opis
1.0	16.9.2013	MH, UŽ	Prva pripravljena verzija
1.1	20.10.2013	MH, UŽ	Uskladitev dokumentov na nivoju celotne mape
1.2	4.11.2013	MH, UŽ	Izboljšanje skladno s prvimi povratnimi komentarji

Razumevanje IS revidirane organizacije je ključno za načrtovanje vsake revizijske naloge oz. oblikovanje revizijskega pristopa, saj predstavlja osnovo za:

- opredelitev tveganj IS
- pripravo revizijskega programa

Usmeritve na področju spoznavanja okolja organizacije podajajo **Standardi za revidiranje informacijskih sistemov in dajanje zagotovil**[3], ki jih skupaj z njihovo interpretacijo podajava v dokumentu **1001_VODNIK_Nacrtovanje_Revizijskega_Posla_V1.1**.

[3] Do vključno 30.10.2013 so veljali Standardi, smernice ter orodja in tehnike za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT, od 1.11.2013 pa veljajo prenovljeni **Standardi za revidiranje informacijskih sistemov in dajanja zagotovil**. Le-ti so del novega **Okvira poklicnih praks za revizijo informacijskih sistemov in dajanje zagotovil ITAF** (ITAF™: A Professional Practices Framework for IS Audit/Assurance, 2nd Edition). V obdobju priprave standardne revizijske mape ti še niso prevedeni v slovenščino. V tekstu nove standarde in smernice le povzemava, posebej pa poudarjava, da pričujoči prevodi niso uradni in veljavni prevodi, temveč sva jih pripravila avtorja. **Pred izvedbo vsakega revizijskega posla mora strokovnjak za revizijo IS in dajanje zagotovil preveriti besedila veljavnih in uradno objavljenih standardov in smernic za revidiranje informacijskih sistemov in dajanje zagotovil.**

1. Temeljne programske rešitve organizacije

V prvem koraku identificiramo vse ključne programske rešitve organizacije - programske rešitve, ki so relevantne za doseg zastavljenega revizijskega cilja. Vsaka sodobna organizacija navadno uporablja vrsto različnih programskih rešitev, od katerih pa so le nekatere neposredno relevantne za doseganje organizacijskih ciljev. Navadno so to tiste programske rešitve, ki podpirajo temeljne organizacijske procese.

Za namene priprave tega delovnega papirja, je smiselno slediti Porterjevemu modelu verige vrednosti, ki vse poslovne procese organizacije deli na temeljne in podporne aktivnosti. Praviloma je vsaka opredeljena aktivnost podprta z eno ali več programskimi rešitvami, kar nam omogoča, da jih pregledno povzamemo in prikažemo.

Pri spoznavanju informacijskega okolja revidirane organizacije istočasno spoznavamo tudi temeljne kontrolne mehanizme, ki jih organizacija uporablja za nadzor nad revidiranim področjem.

POSLOVNE IN IT KONTROLE[4]

Skladno s COBIT sistem notranjih kontrol organizacije vpliva na IT na treh ravneh:

1. Na ravni izvršnega vodstva se določijo poslovni cilji in politike, sprejmejo se odločitve, kako razviti in upravljati vire organizacije za izvrševanje strategije organizacije. Uprava določi splošen pristop k upravljanju in kontroli in z njim seznani celotno organizacijo. Ti cilji in politike, določeni na najvišji ravni, usmerjajo okolje za kontrolo IT.
2. Na ravni poslovnega procesa se kontrole uporabljajo za specifične poslovne aktivnosti. Večina poslovnih procesov je avtomatiziranih in vključenih v aplikacijske sisteme IT, zaradi česar so številne kontrole na tej ravni prav tako avtomatizirane. Te kontrole so znane kot aplikacijske kontrole. Vendar pa nekatere kontrole v poslovnem procesu še vedno ostajajo v obliki ročnih postopkov, kot so pooblaščanje za transakcije, ločevanje nalog in ročno usklajevanje. Zato so kontrole na ravni poslovnih procesov kombinacija ročnih kontrol, ki jih upravlja organizacija, ter avtomatiziranih poslovnih in aplikacijskih kontrol. Opredelitev in upravljanje obeh oblik kontrol je zadolžitev vodstva, čeprav aplikacijske kontrole zahtevajo, da njihovo zasnovo in razvoj podpira IT.

[4] Povzeto po COBIT 4.1., ki ga je izdal IT Governance Institute 2007 ter prevedel Slovenski inštitut za revizijo 2009.

3. IT za podporo poslovnim procesom zagotavlja storitve IT, običajno v obliki storitve, ki si jo delijo številni poslovni procesi, saj se številni razvojni in produkcijski procesi IT zagotavljajo za celotno organizacijo. Poleg tega velik del infrastrukture IT predstavlja skupno storitev (npr. omrežja, zbirke podatkov, operacijski sistemi in shranjevanje). Kontrole, ki se uporabljajo za vse dejavnosti storitve IT, se imenujejo splošne kontrole IT. Te morajo delovati zanesljivo, da se lahko zanašamo na aplikacijske kontrole. Na primer, slabo upravljanje sprememb lahko ogrozi (namerno ali nenamerno) zanesljivost avtomatskih preverjanj celovitosti.

SPLOŠNE KONTROLE IT IN APLIKACIJSKE[5] KONTROLE

Splošne kontrole so kontrole, vključene v procese in storitve IT. Primeri vključujejo:

- kontrole varnosti dostopa (do infrastrukture, aplikacij in podatkov)
- kontrole življenjskega cikla razvoja sistemov,
- kontrole upravljanja sprememb sistemov,
- kontrole fizičnega varovanja podatkovnega centra,
- kontrole varnostnih kopij (sistemov in podatkov) ter kontrole obnovitev po nesreči
- kontrole delovanja računalnikov.

Kontrole, vključene v aplikacije poslovnih procesov, se navadno imenujejo aplikacijske kontrole. Primeri vključujejo:

- kontrole popolnosti, pravilnosti in veljavnosti,
- kontrole nad notranjim procesiranjem (ki zagotavljajo pričakovane rezultate ter da procesiranje izpolni želeni cilj)
- kontrole zagotavljanja zaupnosti poročil
- Kontrole avtorizacije in ločevanja vlog (segregacije dolžnosti).

Na izmišljenem primeru Maloprodajne trgovske verige ABC (Slika 1) so opredeljeni **podporni procesi:**

- Računovodstvo in finance
- Upravljanje človeških virov organizacije

[5] Poimenovane tudi aplikacijske kontrole, kontrole programskih rešitev in programske kontrole. V različnih standardih in smernicah, ki jih navaja pričujoča dokumentacija, najdemo različna poimenovanja.

- Informacijske tehnologije
- Nabava za interno uporabo
- Vzdrževanje infrastrukture
- Administracija, notranja revizija.

Podporni procesi posredno vplivajo na doseganje organizacijskih ciljev, praviloma pa ne predstavljajo ključnega elementa dodane vrednosti delovanja organizacije.

Podporni procesi so lahko v različnih organizacijah dokaj poenoteni, kljub temu da obstajajo nekatere sektorske razlike. Enotnost teh procesov omogoča razvijalcem programskih rešitev organizacijskega načrtovanja virov (angl. Enterprise Resources Planning, v nadaljevanju: ERP rešitev) pripravo standardnih programskih paketov, ki jih lahko organizacije uporabijo z minimalnim prilagajanjem. Primeri tovrstnih programskih paketov vključujejo SAP, Oracle Financials, Microsoft Dynamics (NAV in AX), slovenske iCenter, miniMax, Pantheon, SAOP, Birokrat, KOPA, MAOP, Perftech, Orkester in druge.

V 2013 in 2014 bo naraščal trend selitve nekaterih izmed standardnih rešitev iz tehnološke infrastrukture v upravljanju organizacije v tehnološko okolje t.i. oblaka oz na tehnološko infrastrukturo v najemu. Ta vidik je izjemno pomemben za pripravo in izvedbo nadaljnjih revizijskih postopkov.

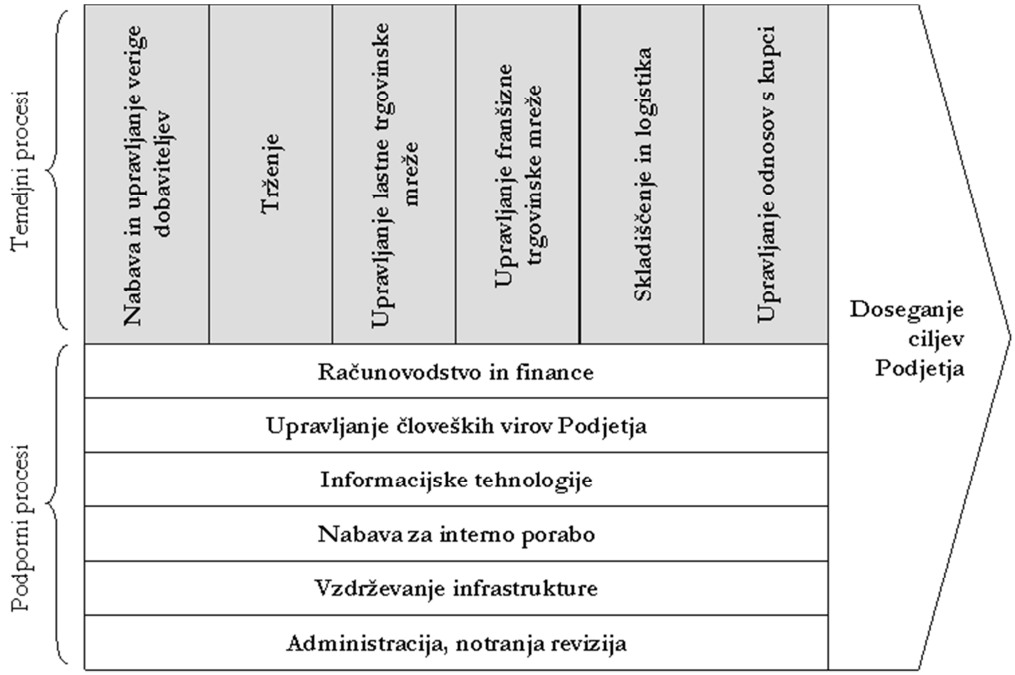
Temeljni poslovni procesi naj bi bili praviloma vir strateških prednosti organizacije in večinoma niso poenoteni niti v organizacijahznotraj enega sektorja. Programske rešitve, ki podpirajo temeljne poslovne procese so pogosto posebej razvite in prilagojene tako, da odsevajo posebne potrebe organizacij, ki jih uporabljajo. Z razvojem globalnega trga programskih rešitev se je sicer tudi na področju programskih rešitev, ki podpirajo temeljne poslovne procese posameznih sektorjev razvila določena standardizacija, vendar so tudi ti kupljeni paketi praviloma precej prilagojeni.

Na izmišljenem primeru Maloprodajne trgovske verige ABC (Slika 1) so opredeljeni **temeljni procesi**:

- Nabava in upravljanje verige dobaviteljev;
- Trženje;
- Upravljanje lastne trgovinske mreže;
- Upravljanje franšizne trgovinske mreže;

- Skladiščenje in logistika;
- Upravljanje odnosov s kupci.

Slika 1: Teoretičen primer prikaza temeljnih in podpornih organizacijskih procesov maloprodajne trgovske verige



V konkretnem primeru maloprodajne trgovske verige lahko sklepamo, da bo organizacija potrebovala posebne programske rešitve vsaj za podporo procesov poslovanja na nivoju lastnih podajalen (trgovinsko skladišče, blagajna,…), upravljanja franšizne mreže, upravljanja skladiščne funkcije in logistike, vodenja odnosov s kupci in programov za pospeševanje prodaje ter rešitev za upravljanje dobaviteljev.

Za učinkovito razumevanje informacijskega okolja je smiselno pripraviti preglednico ali pisni opis, ki povzema rešitve, uporabljane v podporo posameznim organizacijskim procesom ter tehnološko infrastrukturo, na kateri delujejo. Predlog tovrstnega seznama prikazuje Tabela 1.

Tabela 1: Teoretičen primer seznama ključnih programskih rešitev po procesih

Organizacijski proces	Programska rešitev	Moduli	Razvojni okvir / jezik	Baza podatkov programske rešitve	Operacijski sistem programske rešitve	Dobavitelj	Vzdrževanje

Računovodstvo in finance	SAP	FI/CO - Financials and Controlling	n/a	Oracle v 11g	Redhat Linux	IBM Slovenija	IBM Slovenija
Človeški viri	SAP	HR - Human Resources	n/a	Oracle v 11g	Redhat Linux	IBM Slovenija	IBM Slovenija
Upravljanje lastne trgovske mreže	Lastna programska rešitev - IBM host	Prodajna	pl/1	DB2	IBM Unix	Lastni razvoj	Lastni razvoj
..	..			..	..		

Primer tovrstnega seznama predstavlja tudi dokument: **103003 PREDLOGA Seznam aplikacij.**

V nekaterih primerih posamezno področje ne bo podprto s poslovno rešitvijo temveč s t.i. uporabniško razvito rešitvijo - Excel ali Access dokumentom, ki je prilagojen tako, da podpira celoten poslovni proces. Če imajo te rešitve lahko pomemben vpliv na poslovanje organizacije ali delovanje nekega področja, je potrebno te rešitve obravnavati enako kot druge programske rešitve.

Seznam lahko revidirani organizaciji pošljemo v izpolnitev že pred začetkom pregleda. Osnovne podatke o verjetnih temeljnih procesih organizacije lahko pridobimo iz spletne predstavitve organizacije, področne zakonodaje ipd.

V povezavi z vsako uporabljano programsko rešitvijo je torej smiselno postaviti vsaj naslednja vprašanja (v kolikor nanje ni odgovorov v zgornji tabeli):

- ✓ Ali je programska rešitev razvita v organizaciji, zunaj organizacije a samo za namene organizacije ali je programska rešitev generična? Do katere mere je v slednjem primeru prilagojena organizaciji?
- ✓ Kdo je lastnik materialnih avtorskih pravic programske rešitve?

Čim bolj je posamezna rešitev prilagojena organizaciji, tem težje jo je načeloma zamenjati. To omejuje možnosti menjave zunanjih dobaviteljev oz. povečuje odvisnost organizacije od njih. Običajno je, da za standardne programske rešitve – pakete (na primer MS Office) njihov kupec oziroma kupec licence za njihovo uporabo ne kupi tudi materialnih avtorskih pravic. Kadar pa nek zunanji izvajale razvija programsko rešitev prav za konkretnega kupca, pa bi morali biti v ceno všteti vnaprej tudi že stroški prenosa materialnih avtorskih pravic. Razlog za to je med drugim to, da se tudi zunanji izvajalec uči od poslovnih procesov organizacije.

- ✓ Kdaj je bila programska rešitev prvič uvedena? Kako se zagotavlja njena primernost za spremembe v tehnološkem okolju (pri starejših rešitvah)?

Starejše rešitve so pogosto slabo dokumentirane, kar omejuje možnosti za njihovo menjavo in nadgradnjo. Starejše programske rešitve pogosto manj celovito podpirajo delovanje organizacije.

- ✓ Ali je programska rešitev kakovostna - ali podpira vse elemente organizacijskega procesa in izpolnjuje potrebe uporabnikov? Kaj so najpogostejše pripombe uporabnikov glede programske rešitve?

Pogled informatikov in pogled uporabnikov na uporabnost določene programske rešitve se pogosto razlikujeta. Pri pregledu je smiselno upoštevati oba vidika.

- ✓ Katero bazo podatkov uporablja programska rešitev in kdo je odgovoren za njeno administracijo? Na katerem operacijskem sistemu deluje aplikativni strežnik, na katerem operacijskem sistemu deluje podatkovni strežnik programske rešitve? Kdo je odgovoren za njihovo administracijo?
- ✓ Ali ima organizacija vpeljan sistem spremljanja sprememb programskih rešitev? Ali so bile vse spremembe v programskih rešitvah odobrene in dokumentirane? Ali ima organizacija enake postopke uvajanja sprememb za vse spremembe ali ločuje kompleksnost postopkov glede na potencialni vpliv spremembe?

Postopki uvajanja sprememb v programsko opremo predstavljajo enega izmed najbolj tveganih področij upravljanja informacijskih sistemov organizacije. Neprimerno strukturirani postopki sprememb produkcijske različice programov lahko:

- povzročijo napake v delovanju programskih rešitev, ustavitve in motnje produkcijskega delovanja rešitev ter celo odpoved programskih rešitev,
- omogočijo prevare in zlorabe.

Nekatera ključna vprašanja v povezavi z uvajanjem sprememb v programsko opremo so tako:

- ✓ Katere pomembnejše spremembe / razvojne naloge so se izvedele v povezavi s programsko rešitvijo v obdobju, ki ga opazujemo?
- ✓ Ali je organizacija v opazovanem obdobju izvedla pomembnejše nadgradnje / spremembe baze podatkov, na kateri je zasnovana

programska rešitev (prehod na novo verzijo baze, pomembnejši poseg v strukturo baze, menjava baze podatkov, ...)?

Podobno kot postopki uvajanja sprememb v programske rešitve predstavljajo tudi postopki sprememb baz podatkov tveganje za delovanje programskih rešitev, ki črpajo podatke iz njih. Tipični posegi v baze podatkov so spremembe strukture baze in spremembe definicije podatkov ter nadgradnje in popravki orodij za upravljanje baz podatkov. V nekaterih primerih je potrebo tudi neposredno posegati v transakcijske podatke in jih spremeniti ali dopolniti. Postopki uvajanja sprememb v baze podatkov naj bi pokrivali vse zgoraj naštete primere, po potrebi pa tudi področje verzioniranja baze podatkov, kopiranja produkcijskih podatkov za namene preizkušanja sprememb baz podatkov ipd.

2. Tehnološka infrastruktura informacijskega sistema organizacije

Programske rešitve delujejo na tehnološki infrastrukturi, ki smo jo deloma spoznali že skozi vprašanja o programskih rešitvah organizacije. Nekatera ključna vprašanja za spoznavanje tehnološke infrastrukture organizacije so:

- ✓ Kakšno strežniško arhitekturo uporablja organizacija? Ali je strežniška infrastruktura organizacije centralizirana (na eni lokaciji) ali decentralizirana?
- ✓ Kako je zasnovano komunikacijsko omrežje organizacije znotraj glavne procesne lokacije (npr. sedeža organizacije)? Kako je zasnovano prostrano omrežje organizacije (pri več lokacijah delovanja)? Kako je organiziran oddaljen dostop do omrežja organizacije in katere tipe naprav (prenosni računalniki, mobilne telekomunikacijske naprave, ..) podpira? Katere rešitve organizacija uporablja za upravljanje elektronske pošte? Na kakšen način se zagotavlja varnost pred zunanjimi vdori v notranje omrežje organizacije?

Za namene razumevanja komunikacijskega omrežja je smiselno zaprositi za diagram prostranega omrežja ter diagram komponent omrežja (požarna pregrada, demilitarizirana cona ipd.)

- ✓ Ali organizacija uporablja koncept standardne delovne postaje? Kaj je standardna konfiguracija npr. za trgovsko blagajno?

- ✓ Katere baze podatkov (poleg baz, neposredno povezanih s ključnimi programskimi rešitvami za računovodsko poročanje) uporablja organizacija? Kdo jih administrira?
- ✓ Ali je organizacija v opazovanem obdobju izvedla večje spremembe/nadgradnje tehnološke infrastrukture (npr. menjavo strežnikov, menjavo omrežne opreme, ...)? Kako je bila menjava zasnovana in nadzorovana?
- ✓ Ali organizacija v bližnjem prihodnjem obdobju načrtuje večje spremembe/nadgradnje tehnološke infrastrukture (npr. menjavo strežnikov, menjavo omrežne opreme, ...)?
- ✓ Ali je organizacija v opazovanem obdobju doživela večje izpade delovanja tehnološke infrastrukture? Katere? Kako so vplivali na finančno relevantne obdelave?
- ✓ Kako je organizacija zasnovala neprekinjeno poslovanje in postopke okrevanja po katastrofi?

Vse organizacije bi morale načrtovati neprekinjenost poslovanja (tako računalniške podpore poslovanja kot poslovnih postopkov), še posebej pa tiste organizacije, ki morajo biti razpoložljive tudi v obdobju naravnih in drugih nesreč.

3. Politike in postopki informacijske funkcije

Ker so informacijske tehnologije kompleksne in imajo velik potencialni vpliv na delovanje organizacije, naj bi bila temeljna načela njihovega upravljanja in delovanja opredeljena z internimi pravilniki. Vprašanja, povezana z internimi pravilniki in politikami so:

- ✓ Ali ima organizacija opredeljene:
  - o Krovno varnostno politiko
  - o Politiko nadgrajevanja in uvajanja sprememb.

Relevantna in ažurna dokumenta Krovna varnostna politika in Politika nadgrajevanja in uvajanja sprememb sta temeljna dokumenta, ki naj bi jih imela vsaka organizacija, saj naslavljata največja tveganja, povezana z informacijskimi tehnologijami. Krovna varnostna politika naj bi povzemala načela primernega in varnega ravnanja vseh uporabnikov IT v organizacij. Politika nadgrajevanja in uvajanja sprememb naslavlja tveganja, ki izhajajo iz nenadzorovanih sprememb programske opreme, podatkovnih baz oziroma ostale opreme, kar lahko povzroči napake ali celo prevare ter s tem pomembno napačne navedbe v računovodskih izkazih.

Poleg omenjenih politik ima večina organizacij še druge politike in druge dokumente posameznih področij na primer politika:

- dodeljevanja in odvzema uporabniških dostopov in pravic, vključno z zunanjimi dostopi,
- varovanja opredmetenih informacijskih tehnologij,
- varnosti elektronskega poslovanja,
- zagotavljanja revizijske sledi,
- upravljanja gesel,
- upravljanja varnostnih incidentov,
- projektnega vodenja,
- razvoja internih programskih rešitev,
- varnostnih popravkov in nadgrajevanja operacijskih sistemov,
- arhiviranja podatkov,
- zagotavljanja neprekinjenega poslovanja in okrevanja po katastrofi,
- klasifikacije podatkov,
- zagotavljanja zaupnosti podatkov,
- varnega uničevanja elektronskih nosilcev podatkov,
- varovanja pred zlonamerno programsko kodo,
- varovanja omrežja,
- postopkov »čiste« mize in »čistega« ekrana,
- kriptografskih tehnologij,
- …

4. Umeščenost in organizacija podpore informacijskim tehnologijam

Podpora informacijskih tehnologijam organizacije je navadno organizirana v obliki posebnega oddelka. Del podpore informacijskim tehnologijam se praviloma izvaja zunaj organizacije. Primeri vprašanj, povezanih z organizacijo informacijske funkcije so:

- ✓ Kako je organiziran oddelek/sektor informacijske podpore? Koliko podsektorjev in koliko zaposlenih ima?

Priporočljivo je pridobiti organigram organizacije in razumeti njeno organiziranost:

- ✓ Ali organizacija zaposluje varnostnega inženirja?
- ✓ Ali ima organizacija notranjega revizorja, ki je strokovno usposobljen revidirati informacijske tehnologije?
- ✓ Katere storitve podpore informacijskim tehnologijam se izvajajo izven organizacije? Kako je pogodbeno dogovorjeno izvajanje storitev zunanjih izvajalcev? Kdo je odgovoren za nadzor nad njihovim delom in kako se le ta izvaja? Ali imajo zunanji izvajalci informacijskih storitev zunanji dostop do notranjih virov organizacije? Kako se ta dostop nadzira?

Navadno večina organizacij deluje z enim ali več zunanjimi izvajalci. Le ti večinoma izvajajo naloge razvoja in nadgradnje programskih rešitev, pogosto pa tudi storitve postavitve in nadzora nad komunikacijskim omrežjem, administracije baz podatkov in druge storitve. Pogosto imajo zunanji izvajalci IT storitev zunanji dostop do notranjih virov organizacije, npr. za namene izrednih posegov in popravkov. Ti zunanji dostopi so včasih slabše nadzorovani kot uporabniški dostopi internih uporabnikov.

5. Delovanje podpore informacijskim tehnologijam

- ✓ Ali se podatki iz ene programske rešitve prenašajo tudi v druge programske rešitve in kako? Kdo je razvil vmesnike oz. druge oblike prenosa? Ali pri prenosih podatkov kdaj prihaja do napak? Ali jih sistem zazna avtomatsko? Kdo jih razrešuje?
- ✓ Kdo je odgovoren za vodenje matičnih podatkov (šifrantov) in nadzor nad njihovim poenotenjem?
- ✓ Kako se znotraj programske rešitve zagotavlja pravilnost izvrševanja velikih obdelav, npr. velikih obračunov?
- ✓ Kdo je odgovoren za načrtovanje poročil in predvidevanje drugih informacijskih potreb?

6. Varovanje informacijskih virov

Vprašanja, ki si jih lahko zastavimo so med drugim[6]:

- ✓ Ali je organizacija v zadnjem obdobju doživela pomembnejši varnostni incident? Kako se ga je obravnavalo?
- ✓ Kdo je odgovoren za dodeljevanje dostopa do informacijskih virov organizacije (omrežnih virov, baz podatkov, programskih rešitev, ...)
- ✓ Kdo je odgovoren za razvoj, prilagajanje in nadgradnjo programske rešitve? Kako je razvoj pogodbeno urejen?

Vzdrževanje in nadgrajevanje vpeljanih programskih rešitev lahko predstavljata pomemben strošek. Le ta je redko vnaprej predviden že v postopku (javnega) naročanja, kar ustvarja neenakopraven odnos med ponudniki, hkrati pa potencialno neučinkovito rabo sredstev.

- ✓ Kako je programska rešitev zaščitena pred nepooblaščenim dostopom?

Med ključne metode varovanja informacijskih virov spadajo gesla, pametne kartice, ...

- ✓ Kako je znotraj organizacije organizirano dodeljevanje dostopa in uporabniških pravic v uporabniški rešitvi? Kako se zagotavlja spoštovanje načela ločevanja vlog skozi uporabniške pravice v programski rešitvi?

Ločevanje uporabniških vlog je izjemno pomembno področje, zato so se sčasoma razvile standardne dobre prakse ločevanja vlog. Dobra praksa upravljanja s človeškimi viri na primer zahteva, da je kadrovska funkcija (osebje, ki upravlja z evidenco zaposlenih in njihovimi plačami), ločena od funkcije izplačevanja plač. Ločevanje vlog je eden ključnih mehanizmov za preprečevanje prevar, saj je izvedba prevare precej težja, če mora biti vanjo vključenih več oseb.

Neustrezno razvite ali konfigurirane programske rešitve pa lahko standardno ločevanje vlog v poslovnih procesih popolnoma zaobidejo. Programske rešitve so navadno razvite tako, da določen poslovni proces podpirajo od prvega do zadnjega koraka in če želimo, da določeni zaposleni nekaterih korakov ne

[6] Kljub temu, da izven javnega sektorja ta dokument ni zavezujoč si pri presoji ustreznosti ravnanja organizacije na področju informacijske varnosti lahko pomagamo z dokumentom *Priporočila informacijske varnostne politike javne uprave,*ki je bil izdan in pripravljen na podlagi Uredbe o upravnem poslovanju (Uradni list RS, št. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07 , 31/08, 35/09, 58/10, 101/10 in 81/13) in določa vse temeljne elemente zagotavljanja informacijske varnosti v javni upravi. Kot tak je primeren tudi za pripravo različnih podrobnih revizijskih programov. Dostopen je na spletni strani Ministrstva za notranje zadeve:

http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/JAVNA_UPRAVA/DIES/IVPJU_01.pdf.

morejo izvajati, jim moramo to pravico odvzeti. Brez ustrezne pretvorbe kontrolnih mehanizmov standardnih delovnih procesov v mehanizme uporabniške rešitve lahko porušimo kontrolne aktivnosti za preprečevanje prevar, ki so obstajale pred uvedbo rešitve, saj jih je sedaj možno zaobiti.

Osnovni sistem, ki ga imajo na voljo programske rešitve za podporo ločevanju vlog v poslovnih procesih, je sistem uporabniških vlog (ki je hkrati osnovna preprečevalna kontrola). Uporabniška vloga je vnaprej določen nabor standardnih funkcionalnosti sistema, ki se lahko dodeli uporabnikom na osnovi delovnih nalog, ki jih opravljajo skladno z dobrimi praksami poslovnih procesov. Uporabniške vloge morajo ustrezati delovnim mestom zaposlenih. Oblikovane morajo biti po načelu najmanjšega možnega dostopa. Organizacije morajo sistem uporabniških vlog pravilno načrtovati že ob uvedbi programskih rešitev.

V stvarnosti je to področje zelo redko ustrezno urejeno. Upravljanje uporabniških vlog se prepušča informatikom, ki pa nimajo dovolj znanja o poslovnih procesih, da bi lahko sami presojali, katere funkcionalnosti morajo biti razdružene, če naj bi podpirale ločevanje vlog v poslovnih procesih.

Drug pomemben nadzorni mehanizem za preprečevanje prevar je omejevanje avtorizacij – omejevanje števila zaposlenih, ki imajo pomembna pooblastila. Primeri avtorizacijskih mehanizmov so:

- Kontrola štirih oči – kontrola, ki se najpogosteje izvaja na procesih izplačil in je tehnično podprta z vgraditvijo dveh setov potrditev transakcij
- Kontrola progresivne avtorizacije – kontrola, ki se izvaja na procesih plačil, prodaje in nabave; zaposleni z različnimi nivoji pooblastil lahko odobrijo transakcijo v različni višini.

7. Strategija informacijske podpore in korporativno upravljanje

Čeprav je revizijski pregled načeloma "zgodovinske narave", saj vedno opazujemo okolje informacijskih tehnologij za obdobje priprave podatkov za računovodsko poročanje, je pri revidirancih, kjer bomo delovali več let smiselno pregledati tudi strategije informacijske podpore. Vprašanja, povezana s strategijo okolja IT so:

- ✓ Ali ima organizacija strategijo razvoja informacijske podpore ter kako je povezana s celostno strategijo organizacije?

- ✓ Kako bo organizacija v prihodnosti zagotavljala, da bo informacijska podpora kar najbolj ustrezala njenim organizacijskim potrebam?
- ✓ Katere večje projekte trenutno izvaja organizacija ter kakšen je njihov status?
- ✓ Kako organizacija vodi IT projekte ter ali so zadnji večji IT projekti dosegli predvidene cilje?

Korporativno upravljanje IT je podzvrst korporativnega upravljanja. Tako kot korporativno upravljanje je tudi korporativno upravljanje IT definirano na vrsto različnih načinov, stična točka definicij pa je uskladitev strategije IT, načrtov IT, postopkov IT in upravljanja IT s strategijo, načrti, postopki in upravljanjem celotne organizacije.

Funkcija IT je v tem pogledu posebnost, saj je skoraj edina organizacijska funkcija, ki potrebuje poseben upravljavski okvir, če naj bi delovala v skladu z interesi organizacije. Razloge gre iskati v kombinaciji velike odvisnosti od funkcije IT znotraj organizacije ter v hkratnem omejenem razumevanju te funkcije. To informatikom daje določeno, na specialnih znanjih temelječo avtoriteto ter neodvisnost. Vprašanja, povezana s korporativnim upravljanjem IT so:

- ✓ Kako je poslovodstvo prevzelo odgovornost za korporativno upravljanje IT in kaj pod tem razume?
- ✓ Do katere mere je poslovodstvo vpleteno v IT odločitve?
- ✓ Kako se sprejemajo odločitve o temeljni tehnološki usmeritvi organizacije, o IT projektih ter o uvedbi tehnoloških rešitev?

Brez ustreznega korporativnega upravljanja IT organizacije pri odločitvi za določeno programsko rešitev včasih ne upoštevajo celotnih stroškov njenega lastništva, kar naj bi poleg samih stroškov rešitve vključevalo najmanj še stroške:

- uvedbe,
- morebitnih prilagoditev potrebam organizacije,
- tehnološke infrastrukture, na kateri deluje,
- določenega obdobja vzdrževanja ter
- razvojnih ur za morebitne prihodnje nadgradnje.

- ✓ Kako organizacija upravlja nabavo IT rešitev?

Enako kot vselej pri nabavni funkciji, lahko tudi pri IT nabavah prihaja do nakupov, ki niso usklajeni z dejanskimi potrebami organizacije ter tudi do klasičnih nabavnih prevar. Tveganje nepotrebnih nabav opreme IT lahko pomembno zmanjšamo z opredelitvijo temeljnih tehnoloških usmeritev ter konsistentno uporabo ustreznih nadzornih mehanizmov nabave, ki so navadno del korporativnega upravljanja kot celote. Tudi tveganje nepotrebnih IT storitev, zlasti različnih storitev svetovanja lahko zmanjšamo z nadzorom v okviru korporativnega upravljanja, poleg tega pa je za vse svetovalne pogodbe potrebno utemeljiti skladnost z veljavnimi IT strateškimi ali taktičnimi načrti.