UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

IZBRANE METODOLOGIJE KOT ORODJE ZA UPRAVLJANJE INFORMATIKE

Ljubljana, september 2009 ŠPELA KERN

I Z J A V A

Študentka Špela Kern izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom dr. Aleša Groznika, in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____ Podpis:

_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

Zahteve in pričakovanja poslovnega sveta od informatike postajajo vedno bolj kompleksne, zato postaja tudi upravljanje in varovanje računalniške infrastrukture ključnega pomena. Informatika danes predstavlja celostni del mnogih organizacij, še bolj pomembna pa bo postala v prihodnosti. Prav tako mora biti tudi upravljanje informatike celostni del organizacijskega vodenja. Upravljanje informatike je ena izmed ključnih funkcij pri vodenju celotne organizacije ter organizaciji prinaša številne koristi znotraj kot tudi izven nje. Neustrezno upravljanje z informatiko lahko povzroči operativne težave, incidente in visoke stroške, ki so posledica neustreznega upravljanja s tveganji, neuspešno izvedbo projektov ter neustreznim vrednotenjem informatike.

Informacijska tehnologija v podjetjih predstavlja dragoceni vir, saj varuje sredstva pred škodami, znižuje tveganja za finančne in informacijske prevare in izboljšuje celotni upravljavski sistem z namenom odkrivanja in preprečevanja tveganj in problemov v prihodnosti. Mnogo poslovnih procesov je odvisnih predvsem od informacijske tehnologije. Vsaka organizacija, ne glede na svojo velikost, mora poskrbeti za informacijsko varnost in upravljanje informacijske tehnologije na način, da procesi znotraj organizacije potekajo nemoteno. Upravljanje informatike je odgovornost vodstva, saj morajo izvršni odbor in managerji določiti cilje in strategijo v organizaciji. Poskušati morajo vpeljati upravljavski okvir, ki ustreza strategiji in vodi do boljšega položaja v poslovnem svetu.

Številne organizacije z namenom obvladovanja tveganj iščejo načine, kako na najboljši način upravljati z informatiko. Obstaja veliko alternativnih modelov ter standardov, ki organizacijam pomagajo načrtovati, razvijati in upravljati informacijsko tehnologijo. Ti se osredotočajo predvsem na doseganje višje stopnje zrelosti ter učinkovitosti. Z uporabo najboljših praks na tem področju želijo standardizirati procese in upravljati okolja informacijske tehnologije. Metodologije in najboljše prakse so smernice, ki omogočajo oblikovanje procesov, da ustrezajo poslovnim potrebam v organizaciji. Dve izmed vodilnih metodologij na tem področju sta Kontrolni cilji za informacijske in sorodne tehnologije (angl. *Control Objectives for Information and Related Technology*, v nadaljevanju COBIT) in Zbirka napotkov za upravljanje in uvajanje storitev informacijske tehnologije (angl. *Information Tehnology Infrastructure Library*, v nadaljevanju ITIL) ter globalni standard najboljših praks za varovanje poslovnih informacij ISO/IEC 17999:2000, (v nadaljevanju ISO 17799), ki jih obravnavam v svojem diplomskem delu.

Organizacije se iz dneva v dan bolj zavedajo pomembnosti področja upravljanja z informatiko. Učinkovito delujoča informatika mora v ravnovesje postaviti tehnologijo, zaposlene, partnerje in procese, ki vplivajo drug na drugega.

Namen diplomskega dela je predstaviti področje upravljanja informatike in prikazati področja, ki jih pokrivajo posamezne izbrane dobre prakse. Cilj diplomskega dela je analizirati izbrani metodologiji ITIL in COBIT ter standard ISO 17799, jih primerjati med seboj, analizirati, katera področja prekrivajo, kje se dopolnjujejo ter preko pregleda skupnih točk predlagati, katero kombinacijo metodologij je smiselno vpeljati v organizacijo.

Diplomsko delo je razdeljeno na tri poglavja. Prvo poglavje obravnava upravljanje informatike, njen namen, koristi in definira pojma korporacijsko upravljanje in management informatike, ki sta tesno povezana z upravljanjem informatike. Opisana so ključna področja oziroma komponente upravljanja informatike ter strukturalni problemi pri upravljanju informatike. V drugem poglavju se osredotočam na analizo izbranih metodologij ITIL in COBIT ter standarda ISO 17799, katerih namen je boljše in kakovostnejše upravljanje informatike. Opisujem njihov namen ter strukturo. V zadnjem delu skušam na podlagi primerjav skupnih točk omenjenih dveh metodologij in standarda poiskati najbolj primerno oziroma učinkovito ogrodje za upravljanje informatike.

1 UPRAVLJANJE INFORMATIKE

Področje upravljanja informatike je obravnavano v mnogih znanstvenih člankih in knjigah na to temo. V nadaljevanju bom podala nekaj najpogosteje opaženih in zanimivih razlag. Na podlagi teh bom kasneje poskušala razložiti pomen upravljanja informatike ter povezanost s področjem korporacijskega upravljanja in managementa informatike, saj v praksi pogosto naletimo na mešanje omenjenih pojmov.

Pojem upravljanje informatike Symons (2005, str. 2) poenostavljeno pojasnjuje kot proces, pri katerem se odloča o investicijah v informatiko. Temeljne gradnike upravljanja informatike poveže z vprašanji, ki se nanašajo na postopek sprejemanja odločitev, odgovornosti zanje ter merjenje učinkov le-teh. Inštitut za upravljanje informacijske tehnologije (angl. *Information Technology Governance Institute*, v nadaljevanju ITGI) opredeljuje upravljanje informatike kot podmnožico korporacijskega upravljanja, saj je zanjo poleg managerjev informatike odgovorna tako uprava, kot tudi izvršno vodstvo družbe. Sestavljeno je iz vodenja ter organizacijskih struktur in procesov, ki skrbijo za to, da informatika v podjetju podpira in razširi strategije in cilje družbe.

Robinson (2005, str. 45) ugotavlja, da imajo definicije upravljanja informatike skupno točko v tem, da je cilj upravljanja informatike vzpostavitev nadzorovanega okolja, ki bo vzpodbujalo učinkovito in varno uporabo informacijske tehnologije. Nadzorovano okolje, skladno s kontrolami znotraj organizacije, tvorijo obnašanje, sposobnosti ter delovanje uprave in managementa. Kot dejavnike nadzorovanega okolja navaja verodostojnost, etične vrednote, filozofijo in stil vodenja managementa.

Upravljanje informatike kot ključna funkcija pri vodenju celotne organizacije omogoča podjetjem doseganje poslovnih uspehov, vendar pa lahko predstavlja tudi vzrok za neuspehe. Najpomembnejši dejavniki, ki organizaciji omogočajo kakovostno poslovanje, so (Groznik & Babnik, 2007, str. 150):

- usklajenost poslovne strategije celotne organizacije s strategijo informatike;
- ustrezna struktura oddelka za informatiko;
- ustrezna opredelitev funkcij vodje informatike.

Iskanje ustrezne usklajenosti informatike s poslovanjem celotne organizacije je zaradi vseh prej omenjenih dejavnikov ena izmed pomembnejših nalog najvišjega vodstva. Doseganje poslovnih ciljev organizacije ni mogoče brez strateške usklajenosti strategije informatike s strategijo celotne organizacije (Groznik & Kovačič, 2001, str. 12). Namen upravljanja informatike je (Seling & Waterhouse, 2006, str. 4):

- določati prioritete in investicije v informatiko glede na poslovanje;
- upravljati, vrednotiti, postavljati prioritete, vlagati, meriti in spremljati zahteve za storitve informacijske tehnologije;
- odgovorno upravljati vire in premoženje;
- zagotoviti, da so storitve zagotovljene v skladu z načrti, proračunom in obvezami;
- vzpostaviti odgovornost in pravico do odločanja (jasno opredeliti vloge in pooblastila);
- aktivno upravljati tveganja, spremembe in nepredvidene dogodke;
- izboljšati delovanje, usklajenost s predpisi in zrelost organizacije ter razvoj zaposlenih,
- izboljšati poslovanje s strankami.

Učinkovito upravljanje informatike je ključno za uspešnost poslovanja in nudi naslednje koristi (Seling & Waterhouse, 2006, str. 4):

- oblikuje pregled in odgovornost nad informacijsko tehnologijo z namenom zagotavljanja bolj učinkovitega in etičnega vodenja;
- izboljša planiranje, povezovanje in komunikacijo med poslovnimi področji in oddelki informatike ter znotraj oddelkov za informatiko;
- izboljša donosnost;
- pri upravljanju potreb na osnovi donosnosti naložb izboljša odločitve za analizo, razvrstitev po pomembnosti, financiranju, odobritvi in upravljanju večjih naložb v informatiko (investicije in operativni stroški);
- formalizira postopek izbire, upravljanja s pogodbami in upravljanja s pobudami dobaviteljev in zunanjih sodelavcev;
- optimizira sredstva in človeške vire;
- poveča učinkovitost in zrelost organizacije;
- z dokumentiranjem postopkov, nadzorom in odločitvenimi pravili pospeši ustreznost predpisom in revizijam.

1.1 Povezanost korporacijskega upravljanja in upravljanja informatike

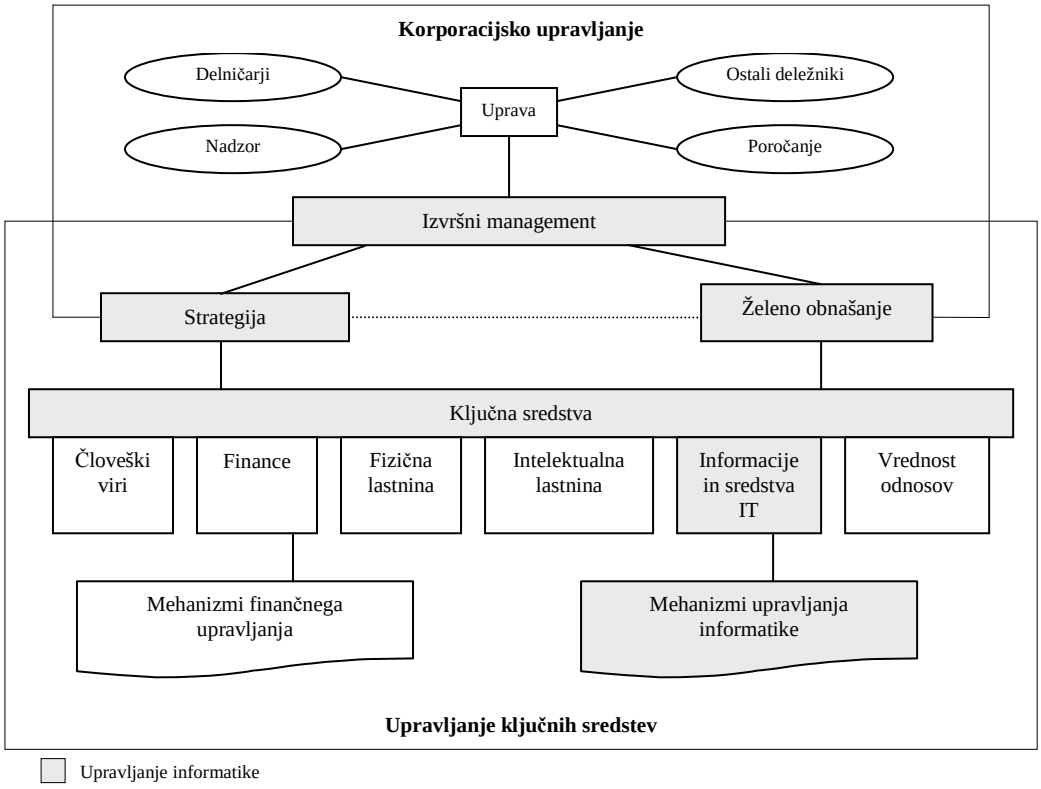
Organizacija za ekonomsko sodelovanje in razvoj *(*angl. *Organisation for Economic Co-operation and Development*, v nadaljevanju OECD*)* je leta 1999 objavila načela korporacijskega upravljanja. Temeljna opredelitev pojma se glasi (OECD, 2004, str.11): "Upravljanje korporacij (angl. *Corporate Governance*) je sistem, s pomočjo katerega se usmerjajo in nadzirajo podjetja. Struktura upravljanja korporacij določa distribucijo pravic in odgovornosti med različnimi udeleženci v podjetju, denimo managerji, člani nadzornega sveta, delničarji in preostalimi deležniki. Poleg tega izpostavlja pravila in postopke za sprejemanje odločitev o poslovnih zahtevah. S tem zagotavlja tudi strukturo, skozi katero se dosegajo poslovni cilji podjetja in sredstva za doseganje teh ciljev ter spremljanje uspešnosti."

Tudi Van Grembergen in De Haes (2008, str. 8) pojem korporacijsko upravljanje podobno pojasnjujeta kot sistem, ki usmerja in nadzoruje organizacijo. Cadbury (2002, str. 157) je definicijo korporacijskega upravljanja razširil s trditvijo, da je korporacijsko upravljanje tisto, ki drži ravnotežje med ekonomskimi in socialnimi ter individualnimi in družbenimi cilji. Tako spodbuja učinkovitost uporabe virov in zahteva nadzor nad njimi. Namen korporacijskega upravljanja vidi v povezovanju interesov posameznikov, korporacij in družbenega okolja.

Za razumevanje koncepta upravljanja informatike je pomembno poznavanje pojmov korporacijsko upravljanje in upravljanje informatike, saj sta med seboj tesno povezana. Problemi korporacijskega upravljanja zaradi odvisnosti poslovanja od informacijske tehnologije ne morejo biti rešeni brez upoštevanja informacijske tehnologije, saj informacijska tehnologija kot orodje za doseganje ciljev korporacije (Etzler, 2007, str. 12) vpliva na strateške priložnosti ter tako ključno doprinese k strateškemu planiranju. Upravljanje informatike omogoča organizacijam učinkovito izkoriščanje informacij in tako predstavlja gonilno silo upravljanja korporacije (Van Grembergen & De Haes, 2008, str. 8). Schleifer in Vishny (1997, str. 737) pojasnjujeta korporacijsko upravljanje kot način, s katerim si vlagatelji zagotovijo pozitivno donosnost naložb in potrdita dejstvo, da je poslovanje organizacije odvisno od informacijske tehnologije in da je reševanje problemov korporacijskega upravljanja nemogoče brez nje. Pokazala sta, da se problemi in izzivi korporacijskega upravljanja prenesejo v ustrezne specifične probleme upravljanja informatike.

Weill in Ross (2004, str. 5) sta prikazala povezanost načel korporacijskega upravljanja in upravljanja informatike. Področja, ki na Sliki 1 povezujejo korporacijsko upravljanje in upravljanje informatike, so sivo obarvana. Upravljanje informatike predstavlja del celostnega upravljanja organizacije in skrbi za doseganje informacijskih ciljev z izkoriščanjem sredstev (ITGI, 2003).

Slika 1: Korporacijsko upravljanje in upravljanje ključnih sredstev



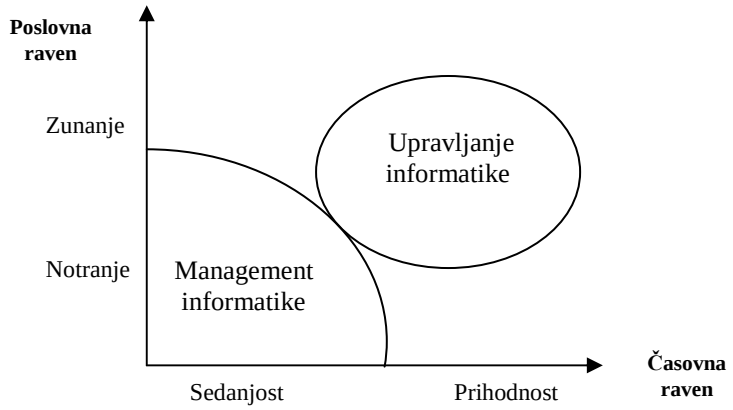
Vir: P. Weill in J. W. Ross, IT Governance, How Top Performers Manage IT Decision Rights for Superior Results, 2004, str. 5.

Mehanizmi upravljanja informatike omogočajo lažje upravljanje z informacijami in sredstvi informacijske tehnologije in tako pomagajo doseči želeno stanje v organizaciji. Uporaba informacijske tehnologije ter upravljanje z njo pomaga pri doseganju strategije organizacije.

1.2 Razlika med managementom informatike in upravljanjem informatike

Van Grembergen, De Haes in Guldentops (2004, str. 5) pojasnjujejo sedanje in prihodnje poslovne cilje kot pomembno povezavo med upravljanjem informatike in managementom informatike, kar ponazarja Slika 2. Management informatike je osredotočen na notranjo učinkovito ponudbo storitev in produktov ter na upravljanje sedanjih nalog. Upravljanje informatike je obsežnejše področje in poudarja predvsem izvrševanje in preoblikovanje postopkov v informatiki, z namenom zagotavljati sedanje in prihodnje poslovne zahteve.

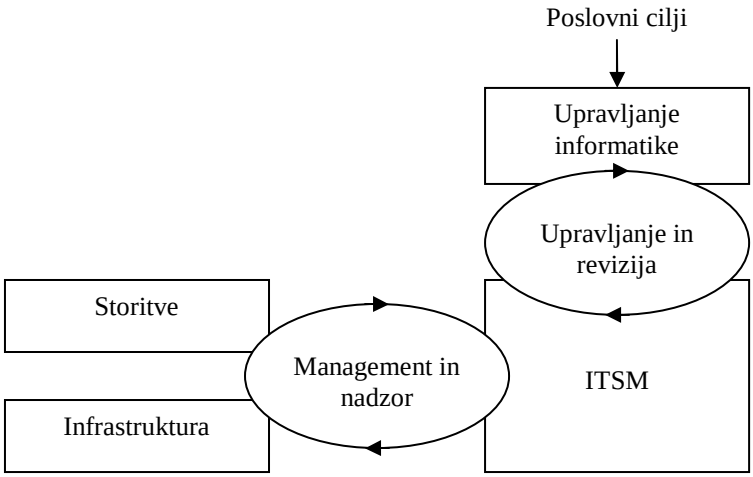
Slika 2: Položaj managementa informatike in upravljanja informatike



Vir: W. Van Grembergen, S. De Haes in E. Guldentops, Structures, Processes and Relational Mechanisms for IT Governance, 2004, str. 5.

Slika 3 prikazuje konceptualni pogled na primerjavo upravljanja informatike in upravljanja managementa. Cilji upravljanja informatike morajo biti skladni s poslovnimi cilji na korporacijskem nivoju. Iz višjih organizacijskih ciljev se izpeljejo cilji in metrike učinkovitosti, ki so potrebni za učinkovito upravljane informatike. Hkrati se uvedejo revizijski postopki, s katerimi se meri in analizira učinkovitost organizacije. Na enak način management informatike, zaposleni, procesi in tehnologija upravljajo storitve informacijske tehnologije (angl. *Information Technology Service Management*, v nadaljevanju ITSM) in infrastrukturo glede na cilje, ki so jih prejeli s strani procesa upravljanja informatike.

Slika 3: Relacijski model upravljanja informatike in upravljanja storitev informacijske tehnologije in operacij informacijske tehnologije ter storitev



Vir: S. Salle, IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing, 2004, str. 3.

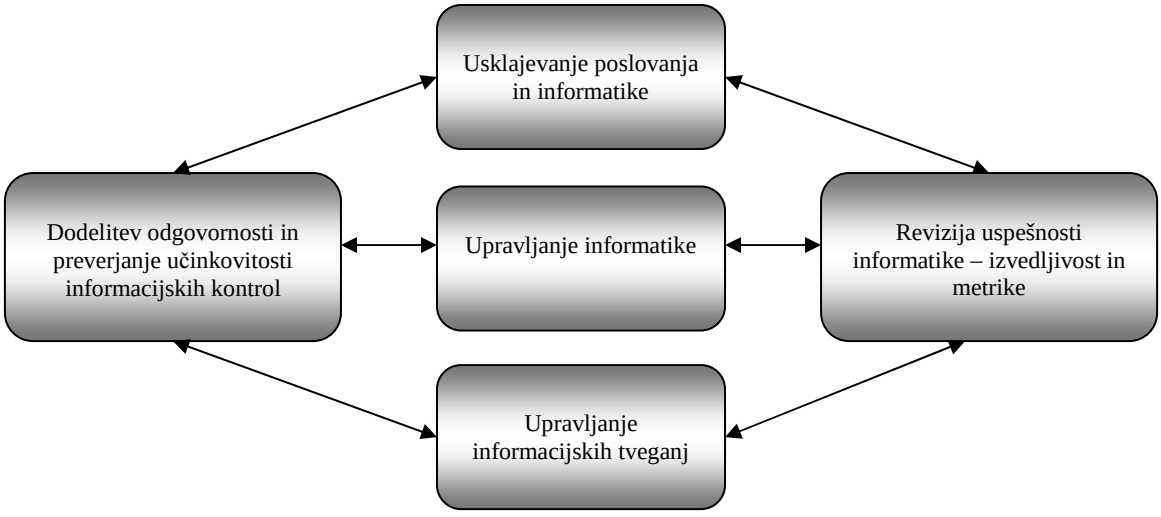
Temelj procesa upravljanja je institucionalni okvir in pristojnosti o odločanju v podjetju, kdo je pooblaščen za določene vrste odločitev in na kakšen način se odločitve sklepajo. Korporacijska raven določa, kdo je pooblaščen za odločitve o višini sredstev namenjenih vlaganjem v informatiko, managerska raven pa potrjuje višino sredstev in prioritetna področja vlaganj (Panian et al., 2007, str. 16). Wilbanks (2008, str. 61) ugotavlja, da razlika med upravljanjem informatike in managementom informatike obstaja. Če podjetje želi rasti in biti uspešno, mora poleg upravljanja informacijskih virov te vire tudi uporabiti skozi celotno podjetje kot del upravljavske strukture.

Poslovni procesi v podjetju potekajo s pomočjo informacijske tehnologije in informacijskih sistemov. Najvišja raven managementa usmerja pozornost na uskladitev ključnih poslovnih procesov z informacijsko infrastrukturo. Spremić v intervjuju revije InfoSRC (2007, str. 34) poudarja, da se morajo vodje služb za informatiko zavedati, da lahko inovativna uporaba informacijskih tehnologij prinese pozitivne spremembe poslovnih procesov, modela poslovanja in tako vpliva na konkurenčno prednost. Vodja službe za informatiko (angl. *Chief Information Officer*) mora v podjetju določiti optimalno vlogo informatike pri poslovanju, ki lahko posledično pripelje do operativne učinkovitosti, inovativnih rešitev in konkurenčne prednosti.

1.3 Komponente upravljanja informatike

Namen poglavja je opredeliti glavne komponente upravljanja informatike, ki predstavljajo izziv vodjem služb za informatiko v dinamičnem poslovnem okolju. Osnovni deli in področja koncepta korporacijskega upravljanja informatike, kot prikazuje Slika 4, so (Panian et al., 2007, str. 36):

Slika 4: Komponente upravljanja informatike



Vir: Panian et al., Korporativno upravljanje i revizija informacijskih sustava, 2007, str. 36.

Strateško povezovanje poslovanja in informatike

V sklopu strateškega povezovanja informatike se določa strateška vloga in povezanost informatike s poslovanjem ter ustvarjanje dodane vrednosti. Na tem področju je pomembno organizirati korporacijske mehanizme, ki se bodo uporabljali skladno z uvedbami odločitev o vlaganjih v informatiko, nadzor in kontrolo. Kovačič (2004, str. 10) ugotavlja, da je dandanes še vedno preveč izpostavljena uporaba informacijske tehnologije kot podpornega dejavnika pri poslovanju, zapostavlja pa se ustrezne naložbe ter strateško vlogo informatike, saj ta vpliva na poslovno uspešnost organizacije. Predlaga partnerstvo med managementom in informatiko, kar pomeni boljšo vključenost vodje službe za informatiko v strateško poslovno načrtovanje in odločanje. Tako se mora vodja službe za informatiko zavzemati za usklajenost med poslovno strategijo in strategijo informatike, kar posledično doprinese dodano vrednost informatike k poslovanju organizacije. Na drugi strani pa je za vodstvo organizacije pomembno, da gradi svoje znanje na področju informatike (Groznik & Babnik, 2007, str. 3). Ključni dejavniki, ki vplivajo na skladnost poslovnega strateškega načrta s strateškim načrtom informatike in njegovim izvajanjem, so (Groznik & Kovačič, 2001, str. 13):

- poslovna strategija;
- organizacijska struktura in procesi;
- strategija informatike;
- obstoječe rešitve na področju informatike;
- kadri.

Upravljanje informacijskih tveganj v poslovanju

Organizacije so izpostavljene različnim tveganjem (na primer poslovnim tveganjem, finančnim tveganjem, tveganju neprekinjenega poslovanja, tveganju varnosti, tveganju ugleda, raznim operativnim tveganjem, itd.), zato bi moralo to področje predstavljati sestavni del upravljanja korporacijskih tveganj. Tveganja s področja informatike se nahajajo znotraj širšega kroga poslovnih tveganj. Pomembnosti tveganj se mora zavedati predvsem najvišji management in na dnevnem nivoju skrbeti za njihovo obvladovanje. Predvsem pa mora biti prisoten pri obvladovanju le-teh, saj lahko njihova prezrtost privede do neustreznih akcij in izvajanje neustreznih investicij. Dva najpomembnejša elementa upravljanja s tveganji sta analiza in obvladovanje tveganj. Analiza tveganj na podlagi zbiranja informacij in odkrivanja tveganj omogoča sprejemanje pravih odločitev in jih primerno nadzoruje, obvladovanje tveganj pa s prikazom, vrednotenjem, analiziranjem in identificiranjem tveganj predstavlja podporo sprejemanju poslovnih odločitev (Groznik & Babnik, 2007, str. 5). Za področje upravljanja tveganj je torej potrebno izdelati načrt upravljanja s tveganji, neprenehoma spremljati nivo tveganj, njihov vpliv na poslovne procese in določiti učinkovite ukrepe z ustrezno kontrolo (Panian et al., 2007, str. 37).

Dodelitev odgovornosti in preverjanje učinkovitosti informacijskih kontrol
Kontrola je pomembna komponenta vsakega upravljanja, med drugim tudi upravljanja uporabe informacijske tehnologije v poslovnih sistemih. Upravljanje s sistemom pomeni prevzemati ustrezna določila, ki zagotavljajo, da sistem deluje na želeni način. Z ustreznim nadzorom in ukrepi lahko dosežemo cilje upravljanja. Ta komponenta predstavlja okvir, s katerim se ukrepi in koncepti upravljanja informatike razširjajo na aktivnosti v informatiki. To se predvsem nanaša na jasno nedvoumno dodelitev odgovornosti za izvedbo informacijskih aktivnosti in preverjanje učinkovitosti kontrol, vgrajenih v informacijski sistem. Doseči želimo poslovanje, ki bo lahko delovalo nemoteno, učinkovito in v skladu s pričakovanji.

Revizija uspešnosti informatike
Ta predstavlja metrike, s katerimi se kvalitativno in kvantitativno meri uspešnost izvedbe različnih informacijskih procesov ter postopek analize in preveritev njihove točnosti, učinkovitosti in zanesljivosti. Končni rezultat teh postopkov je revizijsko poročilo informacijskega sistema, katerega sestavljajo naslednji koraki:

- analiza stanja uporabe informacijskega sistema;
- ocena poslovnih tveganj;
- priporočila managementu za izboljšave stanj.

1.4 Strukturalni problemi upravljanja informatike

Razvoj in uveljavljanje upravljanja informatike zahteva tudi razumevanje organizacijskega vidika ogrodja upravljanja. Symons (2005, str. 4) opisuje štiri tipe organizacijskih struktur v informatiki. Vsaka izmed naštetih struktur vsebuje različne izzive pri uvedbi upravljanja informatike.V nadaljevanju so predstavljene naslednje organizacijske strukture:

Centralizirana
V centralizirani organizaciji sta odločanje in finančni del na enem mestu, zaradi česar ju je veliko lažje upravljati in zahtevata manj napora za organizacijo. Vodja informatike lahko prevzame razvoj upravljavskih procesov in dela neposredno s skupino izvršnih direktorjev. Izziv centraliziranih organizacij je zagotoviti, da imajo poslovne enote in operativne skupine v procesu uvedbe svoj glas, s čimer se prepreči prevelik vpliv vodstva.

Decentralizirana
Decentralizirane organizacije najbolj pogosto dosežejo razdrobljeno stanje, saj vsaka decentralizirana funkcija razvija svoje upravljavske procese, med poslovnimi enotami ali poslovnimi enotami in upravo pa formalni procesi niso določeni. Odločitve o investicijah v informatiko so lahko optimizirane na nivoju poslovnih enot, niso pa optimizirane čez celotno podjetje. To se pogosto pokaže kot podvojena infrastruktura in programska oprema

in premalo širjenja znanja. Izziv je razviti postopek upravljanja v celotno podjetje, ki organizaciji omogoča sprejemati kompromise.

Federalna

To so hibridne organizacije, ki vsebujejo tako centralizirane kot tudi decentralizirane komponente. Večina infrastrukture in aplikacij so centralizirane in vodene na nivoju organizacije, poslovne enote pa imajo nadzor nad specifičnimi aplikacijami in razvojnimi viri. Centralizirani nadzor prinaša zmanjšanje stroškov, razvoj aplikacij pri poslovnih enotah pa je ustreznejši. Izziv federalne organizacije je uravnovesiti potrebe poslovnih enot po infrastrukturnih naložbah in se hkrati prilagoditi arhitekturi in standardom podjetja.

Projektno naravnana

Projektno naravnane organizacije so relativno nov pojem. So oblika centralizirane informatike, kjer so vsi informacijski viri centralizirani in odgovarjajo vodji informatike. Razlikujejo pa se predvsem na področju razvoja aplikacij. Namesto klasične razvojne skupine je zgrajena organizacijska struktura nad razvijalci. Ta struktura se pogosto imenuje kompetenčni centri, ki so sestavljeni iz sorodnih virov. Klasični vodje so zamenjani z vodji kompetenčnih centrov, ki vodijo posamezno razvojno skupino. Učinkovitost novih vodij se meri na podlagi izkoriščenosti virov in možnosti posojanja kvalificiranih virov v zadostnem številu, kot jih zahteva nabor projektov v določenem časovnem okviru. Če želijo biti projektne organizacije učinkovite, potrebujejo močan upravljavski mehanizem zagotavljanja izbire in financiranja ključnih projektov. Izziv projektno naravnanih organizacij je postopek izbire, financiranja in razvrščanja projektov po prioritetah.

Upravljanje informatike v podjetjih je vedno bolj obsežno področje, saj sčasoma število nalog in opravil, s katerimi se upravljanje ukvarja, narašča. Pred časom je pojem upravljanja informatike predstavljal le upravljanje s programsko in strojno opremo. Danes se vse več podjetij zaveda, da je upravljanje informatike veliko več kot le to: upravljati je potrebno z ljudmi, znanji in procesi, ki se v podjetju odvijajo, ob tem pa upoštevati tveganja, ki se pojavljajo in otežujejo poslovanje, če jih pravočasno ne zaznamo in pravilno obvladamo. Na drugi strani pa je postalo tudi poslovanje podjetij bolj kompleksno, kar predstavlja dodaten problem pri želji po učinkovitem in uspešnem vodenju. Seveda pa z uporabo in razširitvijo informatike niso prišli le problemi, ampak tudi prednosti. Pogosto je prav vpeljava informatike gonilna sila pri uvedbi novih rešitev, optimizaciji postopkov in povečanju dobičkov. Zaradi ugotovljenih potreb se je pojavilo več metodologij, standardov in primerjalnih testov, ki poskušajo olajšati problematiko upravljanja informatike.

Mednarodno združenje za revizijo in kontrolo informacijskih sistemov (angl. *Information Systems Audit and Control Association*, v nadaljevanju ISACA) navaja sledeča dejstva, težave in gonila pri upravljanju informatike (ISACA, 2006):

- Informacijske tehnologije so tako razširjene in koristne, da je njihova uporaba postala ključnega pomena za poslovni uspeh podjetja.
- Z razširitvijo uporabe informacijskih tehnologij so se pojavile potrebe po novih znanjih, predvsem potreba po razumevanju in upravljanju tveganj, ki jih tehnologije prinašajo.
- Investicije v informacijske tehnologije so pogosto ključnega pomena, vendar je ob investicijah potrebno zagotoviti tudi optimiziranje vračil teh investicij.
- Vzporedno z izdatki za informatiko je potrebno zagotoviti tudi koristi.
- Potrebno je zagotoviti, da podjetje maksimizira priložnosti za uporabo informacijskih tehnologij, kar vključuje tudi najnovejše tehnologije.
- Zaradi povezanosti obstoječih procesov podjetja in informatike se pojavlja potreba po boljšem razumevanju povezave med poslovanjem in informacijsko funkcijo.
- Upravljanje informatike je novo področje, zato je zagotavljanje primernih zmogljivosti informatike pogosto težka naloga.
- Pri uporabi informacijskih tehnologij je potrebno dosegati pravno in regulativno skladnost. To se še posebej kaže v zadnjih letih, saj je vedno več področij informatike tudi pravno urejeno.
- Potrebno je poskrbeti za transparentnost postopkov in zagotoviti, da bodo zgornje zahteve dosežene.

Opisana dejstva in problemi so skupni vsem poskusom upravljanja informatike po različnih organizacijah. Zaradi potrebe po učinkovitem in preprostejšem upravljanju so se sčasoma oblikovala ogrodja ter dobre prakse, ki naj bi na preprost način olajšala in omogočila upravljanje informatike v podjetjih.

2 STANDARDI IN METODOLOGIJE ZA UPRAVLJANJE INFORMATIKE

Dandanes, ko vsaka organizacija na eni strani poskuša z uporabo informacijskih tehnologij ustvariti prednosti, na drugi strani pa upravljati z vedno bolj kompleksnimi tveganji, povezanimi z informacijsko tehnologijo, lahko učinkovita uporaba dobrih praks pomaga pri izogibanju ponovnega odkrivanja že odkritih znanj, učinkoviti rabi informacijskih virov in zmanjšanju večjih tveganj, na primer pri (http://www.itgovernance.co.uk):

- neuspelih projektih;
- slabih naložbah;
- varnostnih kršitvah;
- sesutju sistema;
- nezmožnosti razumevanja in izpolnjevanja potreb strank.

Metodologiji in standard, ki jih opisujem v nadaljevanju, se po vsem svetu uporabljajo za večanje učinkovitosti, vrednosti in nadzora nad naložbami organizacij v informatiko. Do sedaj so se o namenih in vrednosti teh standardov večinoma pogovarjali le strokovnjaki s področja informacijskih tehnologij, kar pa danes ni več dovolj. Če želi višje vodstvo učinkovito voditi svoja podjetja, potrebuje znanje o teh standardih in mora vedeti, kako se med seboj prekrivajo. Ker standardi izhajajo iz tehničnega področja, jih najbolje poznajo informacijski strokovnjaki, managerji in svetovalci, ki jih sicer lahko uvedejo in uporabljajo z dobrim namenom, vendar potencialno brez poslovnih usmeritev ali vpletenosti in podpore stranke (Hardy, 2006).

Metodologije oziroma dobre prakse so postale pomembne zaradi (ISACA, 2007, str. 9):

- potrebe po zadoščanju zakonskih zahtev glede nadzora informatike na področjih, kot sta finančno poročanje in varovanje osebnih podatkov, na primer v zdravstvu in farmaciji;
- izbire ponudnikov izvajanja storitev, zunanjega izvajanja in prevzemov;
- povečevanja zahtevnosti informacijsko povezanih tveganj, npr. omrežna varnost;
- iniciativ upravljanja informatike, ki vključujejo prevzem metodologij nadzora in dobrih praks, kar pomaga spremljati in izboljšati kritične aktivnosti, s tem pa povečati poslovno vrednost in zmanjšati poslovno tveganje;
- potrebe po optimizaciji stroškov z upoštevanjem standardiziranih pristopov, kjer je to mogoče (namesto posebej razvitih samo za ta namen);
- naraščanja zrelosti in posledično sprejetjem metodologij COBIT, ITIL, ISO standardov serije 27000, standard za vodenje kakovosti ISO 9001:2000, CMMI (angl. *Capability Maturity Model Integration*), PRINCE 2 (angl. *Projects in Controlled Environments*) in PMBOK (angl. *Project Management Body of Knowledge*), ki štejejo kot priznane in najbolj uveljavljene dobre prakse;
- potrebe družb, da ocenijo, kako upoštevajo splošno sprejete standarde glede na področje oziroma podobna podjetja.

Razlog za rast vpeljave dobrih praks je zahteva informacijske industrije po boljšem upravljanju kakovosti in zanesljivosti informacijskih tehnologij v poslovnem svetu ter odgovor na vedno večje zakonske in pogodbene zahteve. Kljub temu pa obstaja nevarnost, da bo vpeljava sicer koristnih dobrih praks draga in ne bo ciljno usmerjena. To se lahko zgodi, če na metodologije gledamo striktno kot na tehnične smernice. Če želimo biti najbolj učinkoviti, moramo dobre prakse vpeljati s poslovnega vidika, z usmerjenostjo na področja, kjer bi njihova vpeljava podjetju prinesla največ koristi. Višje vodstvo, poslovno vodstvo, revizorji in vodje informatike bi morali sodelovati in s tem zagotoviti, da bi uporaba dobrih praks vodila k stroškovno učinkovitim in dobro nadzorovanim informacijskim izdelkom.

2.1 Metodologija COBIT

Metodologija COBIT predstavlja enega najbolj obsežnih in vsestranskih orodij za upravljanje informatike ter vsebuje dobro prakso na celotnem področju uporabe informacijske tehnologije (Žabkar & Mahnič, 2005, str. 257).

2.1.1 Namen in cilj metodologije

COBIT je orodje za kontrolo in revizijo informacijske tehnologije. Nastal je leta 1996 pod okriljem Mednarodnega združenja za revizijo in kontrolo informacijskih sistemov ISACA (angl. *Information System Audit and Control*). Je procesno orientiran model, ki zajema vsa področja upravljanja informatike ter je namenjen širokemu krogu uporabnikov, informatikom, direktorjem informatike, managementu, notranjim in zunanjim revizorjem ter uporabnikom. Managerjem pomaga uravnavati tveganja in nadzor nad njihovimi investicijami v informacijsko tehnologijo, medtem ko uporabnikom zagotavlja varnost in kontrolo storitev informatike. Revizorjem informacijskih sistemov služi za pomoč pri utemeljitvi mnenj o notranjih kontrolah pri poročanju managementu. COBIT uporabljajo tudi lastniki poslovnih procesov, glede na njihovo funkcijo odgovornosti pri kontroli informacijskih vidikov procesa. Glavni namen metodologije COBIT je razvoj postopkov za varnost in kontrolo v informatiki (ISACA, 2007, str. 25).

Glede na pomembnost informacijske tehnologije v poslovanju so se menjavali tudi cilji metodologije COBIT. Prvotno je bil COBIT usmerjen predvsem v revizijo finančnih poročil, revidiranje ciljnih poslovnih procesov ter delov informacijskega sistema. Informacijski sistemi in tehnologija so kasneje začeli igrati veliko vlogo pri poslovanju v modernih podjetjih. S tem se je izboljšala zavest o potrebi kontrole. Tako je druga verzija metodologije COBIT, ki je bila izdana leta 1998, namenila velik del prav kontroli. Obseg revizije informacijskih sistemov je kasneje postajal vse širši; od podpore reviziji finančnih poročil do današnje upravljavske vloge, kjer obseg predstavlja revizijo celotnega informacijskega sistema, tehnologije in ključnih poslovnih procesov podjetja. Danes je revizija postala samostojna svetovalna funkcija ter ključna pomoč managementu pri upravljanju informatike. Trenutna verzija COBIT-a 4.1 predstavlja okvir splošno uporabnih informacijsko tehnoloških, varnostnih in kontrolnih postopkov ter služi kot učinkovito orodje pri upravljanju informatike (Panian et al., 2007, str. 197-198).

V zadnjih raziskavah je bila metodologija COBIT v svetovnem merilu ena najbolje sprejetih metodologij in jo uporablja kar 30% organizacij, zajetih v raziskavi. Zanimiv podatek je tudi ta, da se več kot 50% organizacij zajetih v raziskavi zaveda pomembnosti vpeljave metodologije COBIT (Global Status Report, ITGI, 2008).

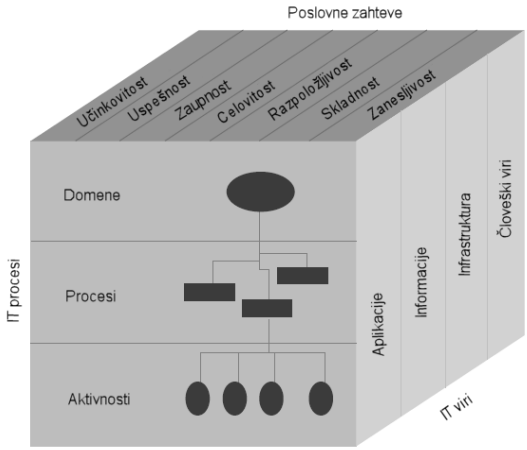
2.1.2 Struktura metodologije

Ogrodje COBIT je na najnižjem nivoju sestavljeno iz kontrolnih ciljev, kateri predstavljajo želene rezultate, ki jih dosežemo z uvedbo kontrolnih postopkov. Srednji nivo predstavljajo kontrolni procesi, ki so združitev procesov. Procesi so razporejeni v štiri področja, ta pa so sestavljena iz 34 procesov in 318 kontrolnih ciljev in smernic za revizijo za ocenitev 34 procesov. COBIT omogoča za vsakega izmed 34 procesov (Panian et al., 2007, str. 201):

- pregled procesa, ki vključuje opis procesa, njegovega cilja, pričakovanih učinkov, nosilca aktivnosti ključne prakse, metrike ali opis ciljev uporabe informacijske tehnologije in kazalnik upravljanja informatike ter uporabo informacijskih virov;
- cilje in teste učinkovitosti poslovnega procesa;
- smernice managementu, kako učinkovito upravljati s poslovnim procesom.

Strukturo modela COBIT si še najlažje predstavimo kot kocko, ki ima tri izhodišča in tri dimenzije in je prikazana na Sliki 5.

Slika 5: Kocka COBIT



Vir: ISACA, COBIT 4.1, 2007, str. 25.

Poslovne zahteve (ISACA, 2007, str. 10 in 11). COBIT na podlagi spodaj navedenih kriterijev skrbi za kakovost, zakonitost in varnost v organizaciji. Kriteriji določajo, kaj poslovni del potrebuje od informatike. Kriteriji so:

- *Uspešnost* – informacije so primerne za poslovanje; informacije so dostavljene v času, so pravilne, konsistentne in uporabne.
- *Učinkovitost* – skrb za informacije skozi optimalno porabo resursov.
- *Zaupnost* – ščiti občutljive informacije pred nepooblaščenimi razkritji.
- *Celovitost* – nanaša se na točnost, celovitost in veljavnost informacij v skladu poslovnimi vrednotami in pričakovanji.

- *Razpoložljivos*t – se nanaša na razpoložljivost informacij, ki jih zahtevajo poslovni procesi v sedanjosti in prihodnosti
- *Skladnost* – pomeni skladnost z zakonom, predpisi in pogodbenimi ureditvami.
- *Zanesljivost* – skrb za primerne informacije managementu za finančno poročanje.

Sredstva informacijske tehnologije (ISACA, 2007, str. 12) so potrebna za doseganje informacijskega kriterija. Ta sestavljajo:

- *Človeški viri* – so osebje, ki skrbi za planiranje, organiziranje, izvedbo, dostavo, podporo, spremljanje in vrednotenje informacijskih sistemov in storitev.
- *Aplikacije* – so uporabniški sistemi in procedure, ki obdelujejo informacije.
- *Infrastruktura* – predstavlja tehnologijo.
- *Informacije* – so podatki v vseh možnih oblikah, obdelani s pomočjo informacijskih sistemov.

Procesi (ISACA, 2007, str. 12) se z namenom doseganja informacijskega kriterija izvajajo s pomočjo informacijskih sredstev in obsegajo 4 domene, 34 procesov in 318 kontrolnih ciljev.

Strukturo metodologije prikazuje Slika 6 vključno s področji:

Planiranje in organiziranje

Področje opisuje, kako se skozi uporabo informacijske tehnologije poslovni cilji najbolje dosegajo. Proces upravlja področje strateških usmeritev in taktik z vidika načrtovanja, komunikacije in vodenja različnih vidikov v organizaciji.

Pridobitev in uvedba

Za izvedbo strategije morajo biti rešitve informacijske tehnologije identificirane, razvite in pridobljene, kot tudi uvedene in integrirane v poslovne procese. Pridobitev in uvedba pokriva tudi področje vzdrževanja in upravljanja sprememb obstoječih sistemov ter zagotavljanja, da rešitve še vedno ustrezajo poslovnim ciljem.

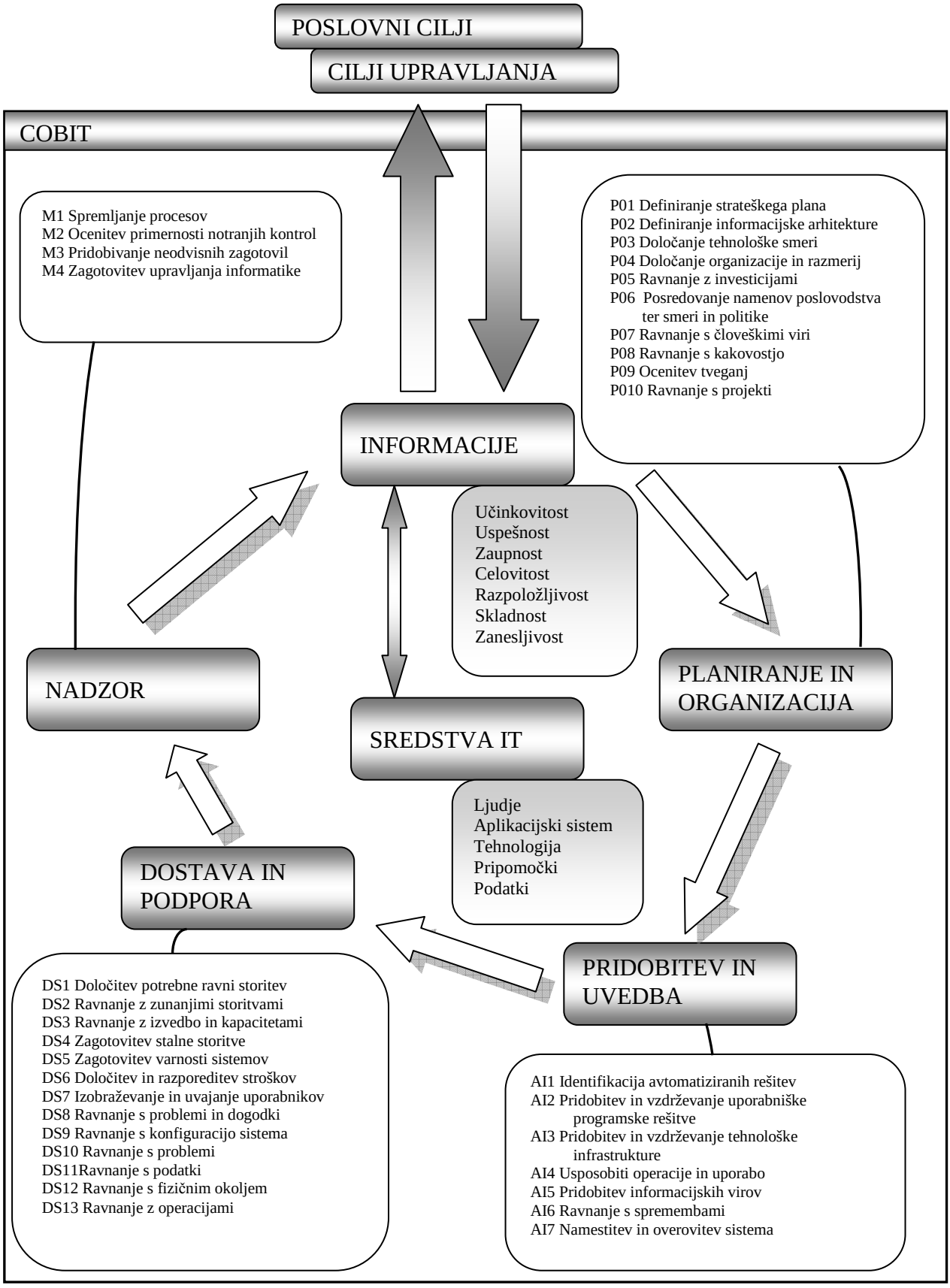
Dostava in podpora

Domena se nanaša na izvedbo dostave potrebnih storitev, kar vključuje izvedbo storitev, varnostno politiko, podporo uporabnikom in upravljanje s podatki.

Nadziranje

Vsi procesi morajo biti redno ocenjevani glede na kakovost in skladnost s kontrolnimi zahtevami. Področje se ukvarja z nadzorom procesov ter zunanjih in notranjih kontrol.

Slika 6: Struktura metodologije COBIT



Vir: ISACA, COBIT 4.1, 2007, str. 26.

2.1.3 Smernice za upravljanje poslovnih procesov

Metodologija COBIT z namenom povečevanja uspešnosti in učinkovitosti procesov predlaga nabor metrik, ki se uporabljajo pri merjenju posameznega procesa. Metrike so različne za vsak proces, kljub temu pa imajo nekaj podobnih lastnosti. Poleg metrik se za uspešno upravljanje poslovnih procesov uporabljata model zrelosti in RACI diagram. Osnovni namen smernic je omogočiti managementu, da (Guldentops, 2004, str. 281):

- meri učinkovitost (Kaj so pokazatelji visoke učinkovitosti?);
- oceni nadzor informatike (Kaj je pomembno? Kaj so ključni dejavniki uspeha nadzora?);
- poveča zavedanje (Kakšno je tveganje, da ne dosežemo postavljenih ciljev?);
- primerja organizacijo s tekmeci (Kaj počnejo drugi? Kako se lahko ocenimo in primerjamo mi?).

Metrike
Kazalniki so glavni podatki v postopku primerjave z drugimi organizacijami. Smernice za management so metrike, med katere uvrščamo ključne kazalnike ciljev, ključne kazalnike poslovanja in ključne dejavnike uspeha.

- **Ključni kazalniki ciljev** (angl. *Key Goal Indicators*) merijo, kaj mora biti narejeno, da dosežemo procesne cilje. Določajo mere, ki povejo, če smo dosegli poslovne cilje za posamezni proces in so pogosto uporabljeni za določitev cilja, ki ga je potrebno doseči. Poslovne zahteve so v splošnem izražene z:
  - razpoložljivostjo informacij, ki so potrebne za poslovne potrebe;
  - odsotnostjo neokrnjenosti in tveganja zaupnosti;
  - stroškovno učinkovitostjo procesov in obratovanja;
  - potrditvijo zanesljivosti, učinkovitosti in ustreznosti.

- **Ključni kazalniki poslovanja** (angl. *Key Performance Indicators*) določajo, v kakšni meri proces dosega cilje in kako dobro opravlja nalogo. Pri odkrivanju, ali cilj lahko dosežemo ali ne, so ti kazalniki najpomembnejši. Pogosto se uporabljajo za to, da že v zgodnjih fazah povejo, ali bodo ključni dejavniki ciljev doseženi.

- **Kritični dejavniki uspeha** (angl. *Critical Success Factors*) določajo najpomembnejše ukrepe za management, da doseže kontrolo znotraj procesov. Nakazujejo najpomembnejše stvari, ki jih mora management storiti na strateškem, tehničnem in organizacijskem nivoju.

RACI diagram

Kratica RACI pomeni "Responsible – Accountable – Consulted – Informed", slovensko "odgovoren za izvajanje – odgovoren – svetovalec – informiran". Diagram za vsak proces določa ključne vloge odgovornosti, in sicer kdo je odgovorna oseba za izvajanje, kdo mora opraviti nadzor in kontrolo, s kom se je potrebno posvetovati in koga je treba o tem obvestiti. Tako ima management jasne smernice za upravljanje s tveganji.

Zrelostni model

Zrelostni model (angl. *Maturity Model*) je upravljavsko orodje za merjenje stopnje zrelosti procesov glede na notranje kontrole. Organizaciji omogoča, da zrelost procesov oceni na lestvici od "neobstoječa" (stopnja 0) do "optimizirana" (stopnja 5). Glavna lastnost zrelostnega modela je sposobnost, da organizacija izmeri trenutno stanje procesov ter določi želeno stanje na področjih, kjer zrelost ni zadostna. Na ta način organizacija lahko odkrije praktične izboljšave v sistemu notranjih kontrol. Doseganje zrelostnih stopenj ni cilj, ampak sredstvo za ovrednotenje zadostnosti notranjih kontrol glede na poslovne cilje organizacije (Pederiva, 2003). Ocenjevalna lestvica in opis posameznih stopenj zrelosti sta prikazana v Tabeli 1.

Tabela 1: Zrelostni model

Stopnja zrelosti procesa	Opis stopnje
0 Neobstoječa	Proces upravljanja informatike na korporacijski ravni ne obstaja. Organizacija ni spoznala, da obstajajo problemi, s katerimi se je potrebno soočiti.
1 Začetna	Organizacija je spoznala, da obstajajo problemi, ki jih je potrebno obravnavati, vendar ima neformalne in slabo definirane postopke. Namesto strukturiranih postopkov obstajajo ad hoc pristopi, ki se uporabljajo individualno ali odvisno od posameznega primera. Celoten pristop do upravljanja je neorganiziran.
2 Ponovljiva	Procesi upravljanja informatike obstajajo, vendar so nekoordinirani. Pogosto se dogaja, da velika večina zaposlenih opravlja podobne naloge, saj ni nadzora, koordinacije in standardiziranih postopkov. Obstaja visoka stopnja zaupanja v znanje posameznika, zato so napake verjetne.
3 Definirana	Procesi upravljanja informatike so že standardizirani in dokumentirani; stalno se izvajajo usposabljanja. Postopki in korporacijska pravila so formalna, vendar niso zrela in prilagojena poslovanju organizacije.
4 Vodena	Procesi in aktivnosti postajajo bolj napredni. Meri in nadzoruje se njihova uspešnost. V primeru neučinkovitosti procesa se takoj reagira. Postopki so delno avtomatizirani.
5 Optimizirana	Postopki so izboljšani do nivoja najboljše prakse na osnovi stalnega izboljševanja. Vlada popolna transparentnost v upravljanju informatike, korporacijska telesa imajo formalni mehanizem za nadzor nad informatiko. Informatika se uporablja za strateške namene.

Vir: ISACA, COBIT 4.1, 2007, str. 19.

2.2 Zbirka priporočil ITIL

Britanski OGC *(*angl. *Office of Government Commerce)*, prej poznan kot Urad za trgovino britanske vlade (*CCTA* – angl. *Central Computer and Telecommunications Agency*), je v 80. letih začel z načrtovanjem in razvojem zbirke ITIL. Skupaj z britanskim inštitutom za standarde podpira britanski standard za upravljanje s storitvami informatike BS 15000. Čeprav je bila zbirka priporočil vzpostavljena za potrebe upravljanja informacijske infrastrukture v angleških vladnih ustanovah, se je hitro uveljavila tudi v gospodarskem sektorju in širše. Uporablja se za zagotavljanje in podporo informacijske tehnologije ter infrastrukture. Informacijska industrija po svetu jo je sprejela kot osnovo za uspešno upravljanje storitev informatike. Zaradi hitrih sprememb v poslovanju in razvoja tehnologije se stalno posodablja (Rudd, 2004, str. 10).

ITIL ni standard, temveč okvir, oziroma zbirka znanja in veščin, katere so se do danes izkazale in potrdile v različnih okoljih in situacijah ter predstavljajo zbirko obširnih izkušenj na področju informatike v mnogih organizacijah. Avtorji strokovne literature ITIL poleg zbirke priporočil obravnavajo kot metodologijo, dobro prakso ali de-facto standard, termine pa v literaturi pogosto izmenjujejo. V nadaljevanju diplomskega dela se na zbirko priporočil ITIL sklicujem kot na metodologijo.

2.2.1 Cilj zbirke priporočil

»Eden izmed poglavitnih ciljev zbirke priporočil ITIL je pomagati ponudnikom storitev informatike, da bi izboljšali uspešnost in učinkovitost informacijske tehnologije ter zvišali kakovost svojih storitev v okviru omejenih stroškov« (Rudd, 2004, str. 8).

Metodologija ITIL služi kot orodje, ki ga je mogoče povsem prilagoditi različnim gospodarskim in negospodarskim ustanovam. ITIL vodi k optimalni izkoriščenosti virov ter na strokoven in sistematičen način upravlja informacijske sisteme. Zagotavlja optimalno delovanje, pomaga razumeti informacijski sistem in razmerja med njegovimi gradniki. Cilj metodologije ITIL je upravljanje informacijskih sistemov tako, da se skozi poslovne procese informacijski oddelki preobrazijo v profitne centre.

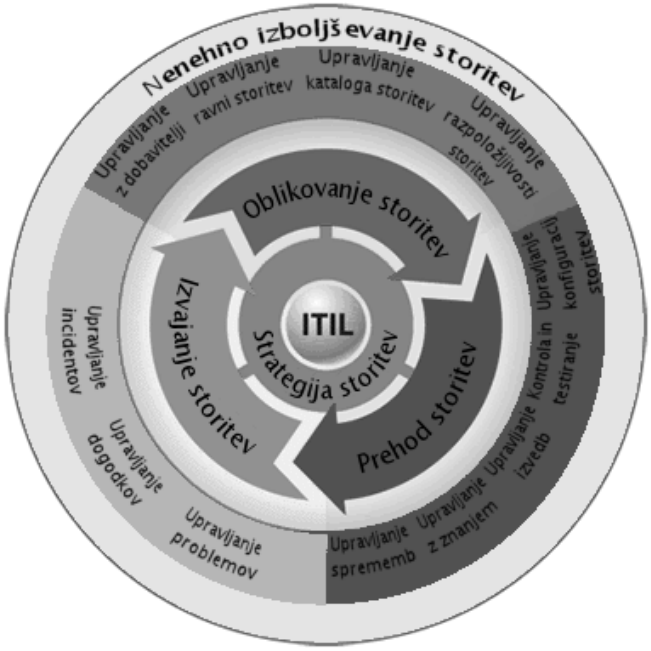
Prednosti uvedbe metodologije ITIL so (Rudd, 2004, str. 8):

- izboljševanje zagotavljanja kakovosti storitev;
- znižanje dolgoročnih stroškov zaradi višje donosnosti naložb ali nižjih skupnih stroškov lastništva;
- nazoren prikaz upravičenosti vloženih sredstev;
- boljša komunikacija in delovni odnosi;
- zmožnost hitrejšega prilagajanja spremembam z izboljšano in merljivo stopnjo uspeha;
- postopki in procesi, katerih skladnost s smernicami najboljše prakse je mogoče preveriti;

- izboljšana zmožnost za preprečevanje prevzemov, združevanj in prenosa nalog na zunanje izvajalce.

Začetna verzija metodologije ITIL obsega zbirko 31 knjig, ki zajemajo vse vidike upravljanja storitev informatike. Naslednjo verzijo tvori sedem modulov, ki so umeščeni v poslovno in tehnološko okolje. Jedro knjižnice sta modula podpora in zagotavljanje storitev, vsak od njiju vključuje discipline, katere podjetjem omogočajo prilagodljivost in stabilnost storitev.

Slika 7: Življenjski krog storitev informatike



Vir: Cartlidge et al., An Introductory Overwiev of ITIL, 2007, str. 9.

Zadnja, tretja verzija metodologije, je izšla leta 2007 in jo bom v nadaljevanju podrobneje opisala. Glavna sprememba v tej verziji je poudarjanje življenjskega kroga storitev informatike, ne pa osredotočenje na procese. Na Sliki 7 je prikazan življenjski krog storitev in spremljajoči procesi. Procesi so namreč umeščeni v življenjski krog storitev. Z namenom ohranitve ključnih načel, ki so bila uporabljena pri procesih podpore in dobavi storitvam, pri slednji niso uvajali korenitih sprememb. Procese so reorganizirali in združili v pet smiselnih sklopov (Cartlidge et al., 2007):

- strategija storitev *(*angl. *Service Strategy)*;
- oblikovanje storitev *(*angl. *Service Design);*
- prehod storitev *(*angl. *Service Transition);*
- izvajanje storitev *(*angl. *Service Operation);*
- izboljševanje storitev *(*angl. *Continual Service Improvement).*

2.2.2 Strategija storitev

Namen strategije storitev je zagotoviti planiranje strategije na osnovi obravnave skupnih poslovnih namenov in poslovnih pričakovanj. Pri vpeljavi strategija storitev upošteva različne modele storitev in strateške cilje, pri tem pa obravnava razumevanje analize in načrtovanja storitev. Pomemben cilj je zagotavljanje dodane vrednosti za stranko in dobavitelja na učinkovit način, pri tem pa izkoriščati vse zmožnosti upravljanja storitev. Za povečanje dodane vrednosti je njen bistveni del tudi zbiranje zahtev strank, na podlagi katerih se določajo strategije in politike, določijo se potrebni viri, prepoznajo omejitve in izpeljejo zadani cilji. Strategija storitev vsebuje priporočila za odločanje o naboru storitev, razvoju zmogljivosti, učinkoviti izvedbi, organizacijskih modelih ter zagotavlja obvladovanje stroškov in tveganj storitev informatike. Glavni rezultat strategije storitev pa naj bi bil strateški pogled na vsako storitev. Ta naj bi nam omogočil, da se pred implementacijo vsake storitve vprašamo, zakaj storitev potrebujemo. Šele na podlagi odgovora bi poiskali še odgovor na vprašanje, kako bomo storitev izvedli (Erzetič, 2007a, str. 10).

2.2.3 Oblikovanje storitev

Oblikovanje storitev je del procesa zamenjave celotnega poslovanja, ki ga lahko definiramo kot načrt inovativnih informacijskih storitev, ki vključuje arhitekturo, procese in dokumentacijo, njegov cilj pa je zadovoljevati obstoječe in bodoče poslovne potrebe. Po novi različici metodologije ITIL predstavlja enega pomembnejših korakov, saj predstavlja nekakšno naslednico dobave storitev iz prejšnje različice. Namen oblikovanja storitev je prenos strateških načrtov in ciljev v specifikacije in načrte, ki omogočajo prehod na nove storitve in njihovo izvajanje. Pri tem se najbolj poudarja naloge združevanja infrastrukture, aplikacij, sistemov in zunanjih dobaviteljev na način, ki bo zagotavljal upravičeno ponudbo storitev. Tudi oblikovanje storitev upošteva mnenja strank, saj na podlagi njihovih zahtev določa standarde, arhitekture in načrte rešitev (Erzetič, 2007b, str. 10).

Področje oblikovanja storitev mora zagotoviti uspešno oblikovanje tehnologije, procesov in meritev. Ugotoviti mora, kateri model dobave storitev je primernejši, zato se ukvarja z vprašanji notranjega ali zunanjega izvajanja storitev ter z vprašanji lastnega razvoja ali nakupa že izdelane ali naročene programske opreme. Postopek oblikovanja storitev informacijske tehnologije se razteza od novih poslovnih zahtev ali sprememb obstoječih do zaključka razvoja nove rešitve, ki ustreza vsem dokumentiranim poslovnim zahtevam. Rešitev, ki v tem procesu nastane, mora biti oblikovana na način, da jo je mogoče predati vpeljavi storitev, ki na njeni osnovi lahko izdela, preizkusi in namesti novo ali spremenjeno storitev. Del procesa oblikovanja storitev je tudi izvedba predaje storitve vzdrževanju in nenehni izboljšavi storitev ob koncu vpeljave storitve (Erzetič, 2007a, str. 11).

Procesi, zajeti v oblikovanju storitev, so (Cartlidge et al., 2007, str. 19 - 22):

- **Upravljanje ravni storitev** *(*angl. *SLM – Service Level Management)*

Namen procesa dogovor o ravni storitev *(*angl. *Service Level Agreement*, v nadaljevanju SLA*)* je dokumentiranje, spremljanje, merjenje, poročanje in pregled v zvezi z dogovorom o ravni storitev ter usklajevanje ciljev podpore, kot so opisani v ravni operativne podpore *(*angl. *Operational Level Agreement*, v nadaljevanju OLA*).*

- **Upravljanje razpoložljivosti storitev** *(*angl. *Availability Management)*

Cilj procesa je izdelava in vzdrževanje ažurnega načrta za razpoložljivost storitev in pomoč pri reševanju incidentov in problemov z vplivom na razpoložljivost ter zagotavljanje ukrepov v zvezi z njo.

- **Upravljanje neprekinjenosti storitev** *(*angl. *Continuity Management)*

Namen je zmanjšati obseg prekinitev poslovnih procesov, ki se zgodijo zaradi večjih incidentov in zagotavljanje, da se storitve vzpostavljajo v dogovorjenih časovnih okvirih in na dogovorjeni ravni.

- **Upravljanje varovanja informacij** *(*angl. *Information Security Management)*

Cilj procesa upravljanja varnosti je varovanje podatkov in informacijskih storitev.

- **Upravljanje kataloga storitev** *(*angl. *Service Catalog Management)*

Cilj procesa je upravljanje informacij, ki jih vsebuje katalog storitev ter zagotavljanje ažurnosti ter dejansko odražanje trenutnih podrobnosti, statusov, odnosov in odvisnosti med storitvami, ki so ali pa se bodo izvajale v operativnem okolju.

- **Upravljanje zmogljivosti** *(*angl. *Capacity Management)*

Zagotavlja stalno razpoložljivost zadostnih kapacitet skozi celoten cikel razvoja storitve. Cilj je izdelava in vzdrževanje primernega in ažurnega načrta upravljanja potrebnih kapacitet.

- **Upravljanje z dobavitelji** *(*angl. *Supplier Management)*

Proces omogoča proizvajalcem ali dobaviteljem storitev, da dosegajo želeni nivo kakovosti storitev in da delujejo v skladu s cilji izvedljivosti informacijskih storitev ter poslovnih zahtev.

2.2.4 Prehod storitev

Ključnega pomena je, da je prehod storitev usklajen s strategijo storitev. Naloga prehoda storitev je omogočiti pravilne praktične aktivnosti in pristope v toku izvajanja prenosa storitev iz faze načrtovanja in razvoja v operativno uporabo. Določiti mora načrt vpeljave storitve in poskrbeti, da bo določena rešitev izdelana in preizkušena. Prehod storitev določa tudi upravljanje sprememb in tveganj ter zagotavlja kakovost storitev. Posebno pozornost namenja področju ocene in zgodnje podpore storitvam informacijske tehnologije, upravljanju z organizacijo in spremembo kulture med prehodom. Osnovne funkcije prehoda storitev so izvedba organizacijskih in kulturnih sprememb, uvajanje znanja, vzpostavitev sistema za upravljanje znanja upravljanja storitev ter analiza in upravljanje tveganj (Erzetič, 2007a, str. 11).

Procesi prehoda storitev so (Cartlidge et al., 2007, str. 25 - 28):

- **Planiranje in podpora prehoda storitev** *(*angl. *Transition Planing and Support)*

Učinkovito planiranje in podpora prehoda storitev lahko znatno izboljša ponudnikovo zmožnost ravnanja z veliko količino sprememb in novih izdaj pri strankah.

- **Upravljanje sprememb** *(*angl. *Change Management)*

Namen upravljanja sprememb je zagotovitev učinkovitega in takojšnjega ukrepanja v primeru sprememb z uporabo standardiziranih metod, tako da so spremembe evidentirane v sistemu upravljanja konfiguracij. S tem se optimizira poslovno tveganje.

- **Upravljanje konfiguracij in sredstev storitev** *(*angl. *Service Asset and Configuration Management)*

Cilj tega procesa je nadzor komponent storitev in infrastrukture ter ohranjanje ažurnih konfiguracijskih zapisov v zvezi s tem. To organizacijam omogoča, da lažje vodijo skupne aktivnosti, nadzorujejo svoja osnovna sredstva, optimizirajo posamezne stroške, lažje upravljajo spremembe in izdaje ter hitreje rešujejo incidente in probleme.

- **Upravljanje izvedb** *(*angl. *Release and Deployment Management)*

Pokriva celotno izvedbo vpeljave novih ali spremenjenih storitev za operativno rabo. Proces upravljanja izdaj je proces planiranja in kontrola procesov upravljanja izvedbe. Zaključek tega procesa je testiranje in uvedba v produkcijsko okolje.

- **Kontrola in testiranje storitev** *(*angl. *Service Validation and Testing)*

Ključni namen tega procesa je učinkovito testiranje ter s tem omogočen razvoj storitev v skladu z zahtevami dogovora o ravni storitev.

- **Upravljanje z znanjem** *(*angl. *Knowledge Management)*

Učinkovito in kakovostno upravljanje z znanjem je pomembno za dosego kakovostnih storitev. Za doseganje visoke dodane vrednosti niso potrebna le tehnična, temveč tudi poslovna znanja.

2.2.5 Izvajanje storitev

Izvajanje storitev je v glavni meri posvečeno upravljanju infrastrukture in upravljanju aplikacij. Namen področja je upravljanje storitev, pri čemer je poudarek na upravljanju vsakodnevnih ponavljajočih aktivnosti, s tem pa tudi zagotavljanje doseganja zagotovljenih ravni storitev. Poglavje je razdeljeno na več osnovnih procesov: upravljanje dogodkov, upravljanje incidentov, izpolnitev zahtev, upravljanje problemov in upravljanje dostopov. Glede na prejšnjo različico ITIL so v tem poglavju združeni procesi, ki so bili prej opisani v poglavju podpore storitvam. Druga večja sprememba glede na prejšnjo različico je opis upravljanja incidentov, ki je po novem opisan bolj podrobno. Proces upravljanja incidentov je razdeljen na tri procese, in sicer na procese upravljanja incidentov, upravljanje dogodkov in izpolnitev zahtev.

Izvajanje storitev se praktično ukvarja s spremljanjem in nadzorom informacijskih sistemov, upravljanjem osrednjega računalnika, upravljanjem strežnikov, upravljanjem računalniškega omrežja, upravljanjem pomnilniškega prostora in arhiviranja, upravljanjem

podatkovnih zbirk, upravljanjem storitev imenikov, podporo namiznim računalnikom, podporo vmesni opremi, upravljanjem interneta in spleta, upravljanjem poslovnih prostorov in informacijske varnosti. Vse to so aktivnosti, ki so potrebne za zagotavljanje storitev. Zajete so tudi dejavnosti, ki so vezane na računske centre, kot so razporejanje dela, izdelava varnostnih dvojnikov in povrnitev podatkov iz teh, tiskanje in podobno. Področje tako pokriva večino vseh dejavnosti, ki so označene kot tipične računalniške dejavnosti. Za izvajanje storitev je predvsem pomembno vsakodnevno načrtovanje dela, ki omogoča dobavo zanesljivih storitev. Področje se torej ukvarja z upravljanjem dogodkov, tehnologijo in zahtevami iz okolja. Ker se poslovno okolje vse hitreje spreminja, pa je pomembno, da je to upravljanje čim bolj učinkovito in prilagodljivo (Erzetič, 2007a, str. 11).

Pri izvajanju storitev je prisotnih nekaj ključnih procesov, ki omogočajo učinkovito podporno strukturo (Cartlidge et al., 2007, str. 29 - 32):

- **Upravljanje dogodkov** *(*angl. *Event Management)*

Dogodek je vsak odkrit ali opažen pojav, ki vpliva na upravljanje informacijske infrastrukture in dobavo storitev. Tipični dogodki so obvestila in opozorila, ki jih ustvari storitev. Sistem upravljanja opozoril predstavlja učinkovit način avtomatskega upravljanja sistema storitev, kateri zmanjšuje vpliv na resurse.

- **Upravljanje incidentov in problemov** *(*angl. *Incident and Problem Management)*

Je proces zaznavanja, beleženja in zaključevanja incidentov. Cilj je ugotovitev incidentov in preprečitev pojavljanja v prihodnosti. Upravljanje problemov se dopolnjuje z upravljanjem incidentov na ta način, da rešuje večje incidente ter analizira pojavljanje incidentov ter preprečuje njihovo nastajanje.

- **Upravljanje z zahtevami** *(*angl. *Request Fulfilment)*

Namen upravljanja z zahtevami je omogočati uporabnikom prejem želenih storitev, informacij in dostavo storitev. Uporabniki ne prijavljajo samo napak, ampak imajo tudi nove zahteve, katere je potrebno informacijsko podpreti.

- **Upravljanje dostopov** *(*angl. *Access Management)*

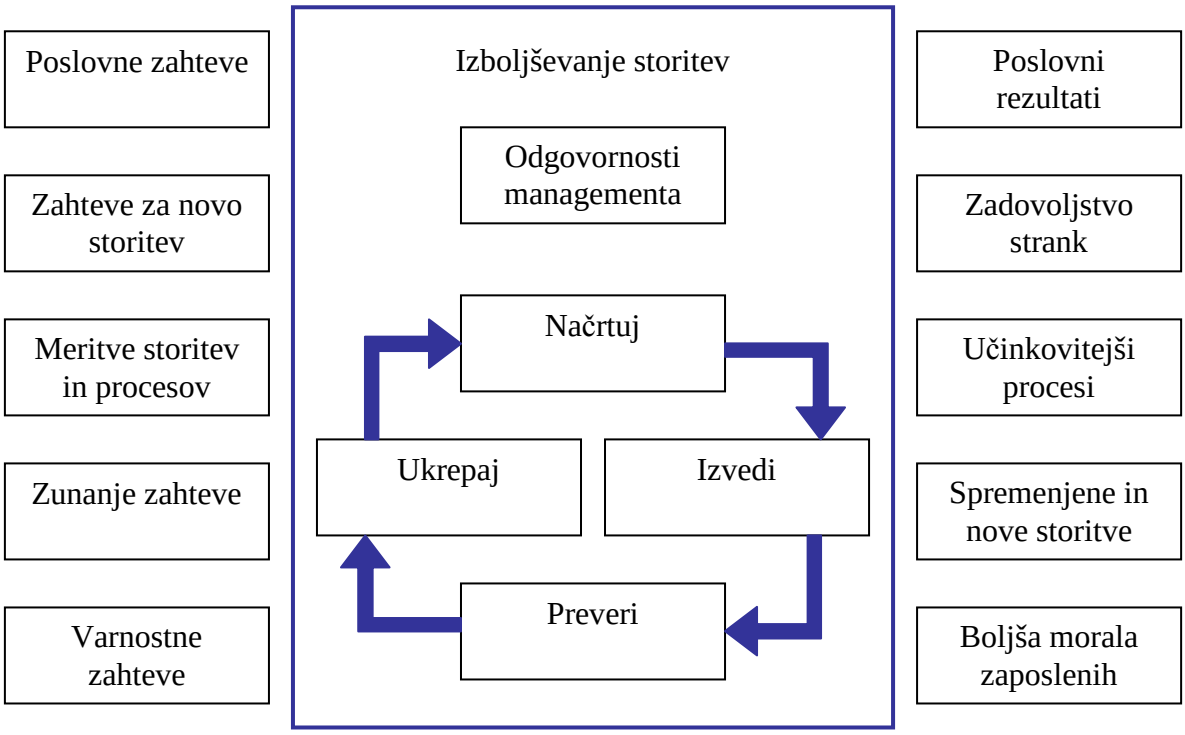
Proces upravljanja dostopov uporabnikom zagotavlja pravice dostopa do določenih storitev in podatkov. Glavni cilj procesa je omogočanje uporabe informacijskih storitev na način, ki ga predpisuje varnostna politika in politika uporabe storitev.

2.2.6 Izboljševanje storitev

Področje nenehnega izboljševanja storitev obravnava strategije storitev, ki vplivajo na celotno izvedbo vseh dejavnosti, in kot tako ni neposredno povezano le s posamezno fazo življenjskega kroga storitve. Eno izmed osnovnih priporočil ITIL je zagotavljanje stabilnosti v stalno spreminjajočem se okolju. Obstaja nevarnost, da zagotovljena stabilnost prinese kot stranski učinek tudi vztrajanje na doseženi ravni ali celo stagnacijo. Na nivoju stabilnosti vsaka sprememba namreč samodejno prinaša tudi nevarnost in tveganje, da bo s spremembo stanje slabše, kot je bilo pred njo. Ravno iz tega razloga ITIL vpeljuje načelo

stalnih izboljšav, ki ga imenujejo Demingov krog. Ideja Demingovega kroga je, da z uvajanjem nenehnih izboljšav dolgoročno dosežemo boljše storitve. Demingov krog predpisuje uvajanje izboljšav po načelu PDCA (angl. *"Plan – Do – Check – Act"*, slovensko "Načrtuj – izvedi – preveri – ukrepaj"), ki pomeni: odloči se, kaj želiš, to izvedi, preveri, če deluje, izboljšaj tisto, kar ne deluje, in začni vse skupaj znova. Ta model je del upravljavskega pristopa k razvoju, implementaciji ter izboljševanju učinkovitosti sistemov in storitev. Demingov krog je sestavni del vseh procesno usmerjenih standardov (Zupan, 2006, str. 4).

Slika 8: Demingov krog - prilagojen izboljševanju storitev



Vir: OGC, Continual Service Improvement, 2007, str. 112.

Slika 8 prikazuje Demingov krog, ki je prilagojen izboljšavam storitev. Izboljšave so možne na celotnem področju upravljanja storitev, torej na samih storitvah in tudi na procesih, funkcijah ter vlogah. Zato procesi tega področja vplivajo tudi na vsa druga področja. Glavni namen področja izboljševanja storitev je zagotoviti, da bo storitev prinašala največjo korist. Poleg tega pa omogočiti, da se bo korist storitve lahko merilo skozi celoten življenjski krog in na podlagi meritev predlagalo in izvedlo izboljšave storitve. Področje obravnava prepoznavanje poslovnih in tehničnih gonil za izboljšave in določa načela za ugotavljanje upravičenosti izboljšav ter njihove poslovne in organizacijske koristi. Odgovornost področja je splošno stanje upravljanja storitev ter upravljanje zrelosti in razvoja praks upravljanja storitev (OGC, 2007, str. 112).

S področjem izboljševanja storitev se glavna vsebina priporočil okvira ITIL zaključuje. Priporočila vključujejo še dodatno dokumentacijo, ki opisuje študijske primere, konkretne primere poslovnih priložnosti, predloge ter vnaprej pripravljene primere za vpeljavo. Dodatna dokumentacija ni več splošna, kot je glavna vsebina ITIL, ampak se osredotoča na posamezne dejavnosti, industrije in tehnologije (Erzetič, 2007a, str. 12).

2.3 Mednarodni standard za varovanje informacij ISO/IEC 27001:2005

Ob vedno večji odvisnosti od informacijskih tehnologij in povečanem pretoku informacij se moramo vse bolj zavedati tudi pomembnosti varovanja le-teh. Živimo v informacijski dobi, kjer se poslovanje nenehno spreminja, saj je podvrženo različnim poslovnim zahtevam. Z uporabo sodobnih informacijskih tehnologij pa ogroženost informacij narašča. Iz želje po poenotenju razmer v organizaciji na področju informacijske varnosti je nastal standard za upravljanje varovanja informacij.

Uporaba standarda ni odvisna od pojavne oblike informacije, ki je lahko v pisni, elektronski ali ustni obliki. Ko informacijo spoznamo za potrebno varovanja, postane predmet sistema upravljanja informacij. Zagotavljanje varnosti informacij zahteva celovit pristop, saj se zaradi njenih pojavnih oblik ne da rešiti izključno s tehničnimi ukrepi, ampak jih je potrebno dopolnjevati še s standardi in politikami (http://www.housing.si/).

Pod pritiski regulative so organizacije primorane oblikovati učinkovit sistem varovanja informacij, če želijo slediti sodobnim trendom, kar pa še zdaleč ni enostavna naloga (Brezavšček & Zupan, 2006, str. 1). Na spletni strani podjetja Housing Co., d.o.o. poudarjajo, da zagotavljanje varovanja informacij zahteva mnogo več kot le postavitev požarnega zidu, uporabo gesel ali izdelavo varnostnih kopij, temveč je potrebno upoštevati tudi naravne katastrofe, tatvine in človeški faktor (http://www.housing.si/).

2.3.1 Predstavitev standarda

Standard ISO/IEC 27001:2005 poznamo po predhodni izdaji mednarodno uveljavljenega standarda BS 7799:1995, ki se je prvič pojavil v Veliki Britaniji leta 1995 kot kodeks varovanja informacij. Opisuje posamezne elemente sistema vodenja varovanja informacij in proces vzpostavitve sistema v praksi. S posodobitvijo leta 1999 sta bila objavljena dva dela standarda za upravljanje informacijske varnosti. Prvi BS 7799-1:1999, imenovan Kodeks varovanja informacij, in drugi nov standard BS 7799-2:1999, imenovan Specifikacija za sisteme za upravljanje informacijskih standardov. Slika 9 nazorno prikazuje izvor in razvoj standarda za varovanje informacij.

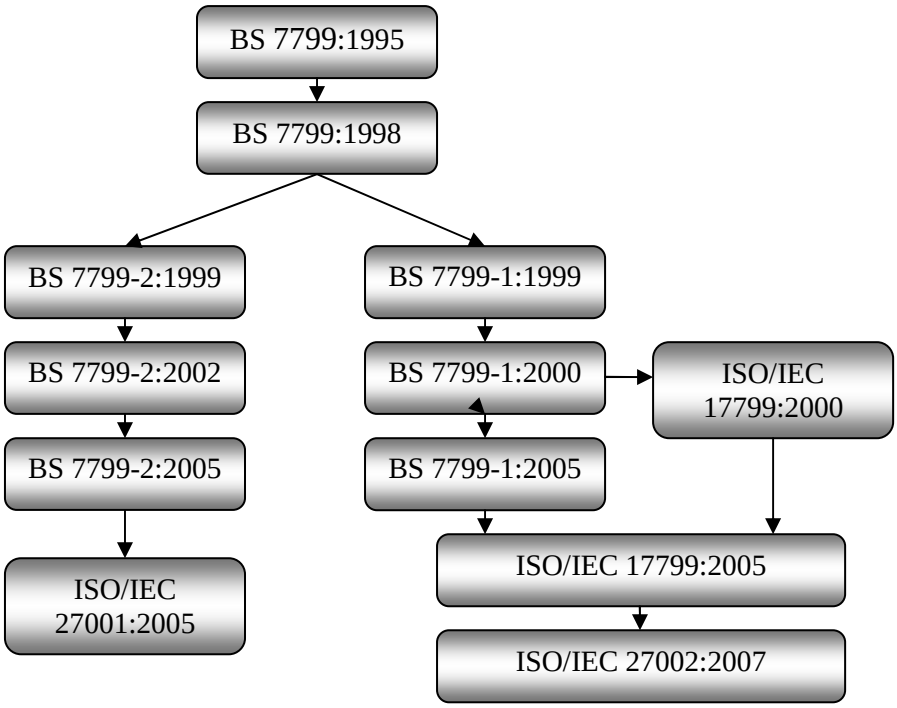
Dosedanjo verzijo standarda BS sestavljata dva dela (Brezavšček & Zupan, 2006, str. 3):

- **ISO/IEC 17799:2005 oziroma 27002:2007** je kodeks varovanja informacij, ki obsega priporočila in nabor nadzorstev, ki predstavljajo najboljšo prakso na področju

zagotavljanja informacijske varnosti. Standard je torej namenjen varovanju dobrin informacijskega sistema.

- **BS ISO/IEC 27001:2005** je specifikacija za sisteme za upravljanje informacijskih standardov (v nadaljevanju SUIV), je drugi del standarda, ki predstavlja zbirko lastnosti, katerim mora SUIV v organizaciji ustrezati. Sledi modelu PDCA.

Slika 9: Razvoj standarda za varovanje informacij



Vir: A. Vujović in Z. Krivokapić, ISO 27001 and ISO 20000, Basis for Organizational Profit, 2007, str. 2.

Z namenom omogočanja konsistentnega in integriranega delovanja upravljavskih sistemov je bil drugi del standarda usklajen z upravljavskima standardoma ISO 9001:2000 za vodenje kakovosti in ISO 14001:1996, ki je mednarodni standard o sistemih okoljskega varovanja (Palsit, 2005, str. 2).

Osnovni cilji nadzorstev, ki jih BS ISO/IEC 17799:2005 predlaga, so zagotavljanje (Zupan & Brezavšček, 2006, str. 59):

- **zaupnosti** - občutljive informacije so dostopne samo pooblaščenim uporabnikom;
- **celovitosti** - informacije oziroma druge dobrine informacijskega sistema niso bile nepooblaščeno spremenjene; informacije kakor tudi postopki za njihovo obdelavo so točni in popolni;
- **razpoložljivosti** - informacije oziroma druge dobrine informacijskega sistema so dostopne pooblaščenim uporabnikom, kjerkoli in kadarkoli jih le-ti potrebujejo.

Vsi ti cilji igrajo bistveno vlogo pri ohranjanju konkurenčnosti, denarnih tokov, dobičkonosnosti, usklajenosti z zakonom ter uspešnim poslovanjem na dolgi rok (Računalniške novice, 18.5.2006).

Standard ISO/IEC 17799:2005 je prilagodljiv, zato ga uporabljajo številne organizacije. Organizacije si prizadevajo bolje upravljati z informacijami, zato morajo določiti, kaj je njihov primarni cilj varovanja in prilagoditi uporabo standarda glede na svoje cilje. Tabela 2 prikazuje primarne cilje in uporabo standarda glede na velikost organizacije po številu zaposlenih (Saint - Germain, 2005, str. 62).

Tabela 2: Uporaba standarda ISO/IEC 17799

Velikost organizacije	Primarni cilj	Uporaba standarda
Manjša podjetja in organizacije (do 200 zaposlenih)	Povečanje zavedanja upravljanja varovanja informacij	ISO 17799 vsebuje poglavja o varovanju, ki naj bi bila uporabljena kot temelj informacijske varnosti
Srednje velika podjetja in organizacije (med 200 in 2000 zaposlenih)	Ustvarjanje kulture podjetja na področju izvajanja varovanja	Standard vsebuje prakse, ki so potrebne za izdelavo politike informacijske varnosti
Velika podjetja in organizacije (več kot 2000 zaposlenih)	Pridobitev varnostnega potrdila	Uporaba standarda BS7799-2 za vpeljavo, vzdrževanje, preverjanje in izboljšanje sistema za upravljanje varovanja informacij

Vir: R. Saint - Germain, Information Security Management Best Practice Based on ISO/IEC 17799, 2005, str. 62.

Organizacije ne uporabljajo standarda le za vzpostavitev varnostnega ogrodja, temveč tudi za pridobivanje varnostnih potrdil in v revizijske namene (Myler & Broadbent, 2006, str. 44).

2.3.2 Struktura standarda

Standard ISO/IEC 27001:2005 sestavlja 15 poglavij, 36 ciljev in 134 kontrol. Uvodno poglavje obravnava področje varovanja dobrin informacijskega sistema, ocenjevanje varnostnih tveganj, poda izhodišča varovanja informacij ter obrazloži kritične dejavnike uspeha. Dalje struktura standarda navaja definicije pojmov, ki obravnavajo prej omenjeno področje. Standard za varovanje informacij je razdeljen na enajst sledečih poglavij (Palsit, 2005):

Varnostna politika
Poglavje predpisuje vzpostavitev informacijske varnostne politike. Po standardu se to doseže s tem, da se izdela in objavi dokument informacijske varnostne politike v

organizaciji. Skrbnik varnostne politike mora biti jasno določen. Varnostno politiko je potrebno periodično pregledovati in ocenjevati na podlagi vnaprej definiranega procesa pregledovanja in ocenjevanja.

Organiziranje informacijske varnosti
Za organiziranje informacijske varnosti je potrebno vzpostaviti varnostno infrastrukturo v organizaciji. Organiziramo jo tako, da določimo skupino, ki izvaja varovanje ter razporeja odgovornosti za varovanje. Poglavje obravnava odobritveni proces za naprave, neodvisne preglede varovanja in sodelovanje tretjih strank.

Razvrstitev in kontrola sredstev
Poglavje obravnava lastnino organizacije. Najprej je potrebno popisati sredstva in določiti stopnjo zaščite za sredstva informacijske tehnologije. Obravnava smernice za klasifikacijo informacij.

Varovanje človeških virov
Prvo področje varovanja človeških virov je vzpostavitev nadzora nad procesom zaposlovanja. Predpisuje varnostne obveze v opisih del, preverjanje ozadja prosilcev za delo, uporabo izjave o varovanju poslovnih skrivnosti ter uporabo pogodb o zaposlitvi z določili odgovornosti pri varovanju informacij. Preostali področji predpisujeta usposabljanje iz področja informacijske varnosti in dosledno odzivanje na incidente.

Fizična zaščita in zaščita okolja
Področje se ukvarja z varovanjem poslovnih prostorov, zaščito opreme pred nevarnostmi in nadzorom dostopa do informacij in lastnine. Za področje varovanja prostorov svetuje razdelitev na varnostna področja, načrtovanje področij, uporabo nadzornih mehanizmov dostopa in določen način dostopa do varnostnih področij. Opremo je potrebno varovati, zaščititi, vzdrževati, nadzorovati njeno uporabo ter uničenje ob zaključku življenjske dobe.

Upravljanje komunikacij in obratovanja
Točka 6 natančno obravnava upravljanje sistemov za obdelavo informacij in je eno najobsežnejših določil standarda. Za to področje svetuje vzpostavitev operativnih postopkov, katere je potrebno ustrezno dokumentirati in nadzorovati spremembe v sistemu. Standard prav tako priporoča vzpostavitev postopkov za upravljanje z incidenti na področju varovanja informacij, kar omogoča tudi pravilnost podatkov. Obravnava opravilne postopke, zaščito mrežne infrastrukture, določa postopke proti zlonamerni programski opremi ali vdorom v sistem. Opozarja na dve pomembni problematiki možnega uhajanja informacij nepooblaščenim osebam, nadzor nad računalniškimi mediji, ki se povezujejo s podatkovnimi sistemi, in prenos podatkov izven matične organizacije. Predpisuje mehanizme za varovanje, nadzor in upravljanje s prenosnimi mediji, s fizičnim prenosom podatkov, z elektronskim poslovanjem, z zunanjimi komunikacijami, javnimi informacijskimi sistemi in elektronskimi pisarniškimi zbirkami.

Obvladovanje dostopov

Obvladovanje dostopov do informacij je ključnega pomena, zato je tudi ustrezno poglavje standarda obširno. Potrebno je odgovorno določiti in razdeliti dostopne pravice, preprečiti možnosti nepooblaščenega dostopa ali dostopa do nedovoljenih virov, vsak dostop je potrebno ustrezno nadzorovati, spremljati in beležiti v dnevniške datoteke. Dnevniške datoteke je potrebno redno pregledovati in ugotavljati, če so uporabljeni mehanizmi varovanja zadostni in ni prišlo do nepooblaščenih dostopov. Poleg konkretnih predlogov pa standard predvideva spodbujanje odgovornosti pri uporabi aplikacij, informacijskih sistemov in opreme zaposlenih.

Nabava, razvoj in vzdrževanje informacijskega sistema

Standard se ukvarja tudi z razvojem in vzdrževanjem informacijskih sistemov. Določa, da je najprej potrebno ugotoviti zahteve po varnosti, nato pa jih moramo vgraditi v aplikacijske sisteme. Zaščititi je potrebno sistemske datoteke in ustrezno nadzorovati izvajanje razvoja novih funkcionalnosti, nadgradenj in podpore. Predpisuje določitev politike šifriranja in uporabo le-te v praksi. Cilj poglavja je doseganje varnih sistemov, ki onemogočajo zlorabo informacij in izgubo podatkov. Zagotavljajo njihovo avtentičnost, zaupnost in neoporečnost.

Ravnanje ob uresničitvi grožnje varnosti

Upravljanje z varnostnimi incidenti vključuje določitev postopkov za poročanje o incidentih, poročanje o ugotovljenih varnostnih pomanjkljivostih, določitev postopkov za hitre in učinkovite odgovore na incidente, izdelavo orodij za določanje vrste, količine in stroškov posameznih skupin incidentov in določitev postopkov za hranjenje sledi o zabeleženih varnostnih incidentih.

Načrtovanje neprekinjenega delovanja

Poglavje obravnava neprekinjeno poslovanje na podlagi celotne organizacije. Z načrtovanjem neprekinjenega poslovanja lahko preprečimo prekinitev postopkov in obnavljamo aktivnosti ter zagotavljamo informacije na zahtevani ravni in v zahtevanem času po prekinitvi ključnih poslovnih procesov.

Usklajenost

V zadnji točki standard priporoča zagotavljanje skladnosti vseh aktivnosti informacijskega sistema z zakonskimi določili. Posveča se usklajenosti varovanja informacij oziroma delovanja z domačimi in mednarodnimi zakoni ter standardi (npr.: zakonodaja, avtorske pravice, varovanje osebnih podatkov in podobno).

2.3.3 Prihodnost standarda

Standard BS7799 se je razvil v družino mednarodnih standardov ISO/IEC 27000. Odbor ISO/IEC si je za prihodnost naložil delo pri razvoju nove družine standardov za sisteme upravljanja z varnostjo podatkov. Nova družina standardov 27000 obsega naslednje objavljene standarde (http://www.iso27001security.com/):

- ISO/IEC 27001 - je najbolj razširjen standard upravljanja informacijskih sistemov, ki nadomešča starejši standard BS7799-2 (izšel leta 2005).
- ISO/IEC 27002 - je naslednik standarda BS7799-1. Namen novega standarda je vzdrževanje sodobnosti in skladnosti priporočenih dobrih praks s trendi na področju varovanja informacij (izšel leta 2007).
- ISO/IEC 27005 - obravnava tveganja, povezana s sistemom za upravljanje informacijske varnosti (izšel leta 2008).
- ISO/IEC 27006 - daje smernice za certificiranje (izšel leta 2007).

Spodaj navedeni standardi so še v pripravi in so že bili potrjeni s strani odbora ISO/IEC:

- ISO/IEC 27000 - standard bo obsegal temeljne principe in pojmovnik.
- ISO/IEC 27003 - bo dal napotke za vzpostavitev sistema za upravljanje informacijske varnosti.
- ISO/IEC 27004 - bo ponujal smernice in merila za merjenje učinkovitosti implementacije sistema za upravljanje informacijske varnosti.
- ISO/IEC 27007 - bo dal smernice za revizijo sistema za upravljanje varovanja informacij.
- ISO/IEC 27008 - bo obsegal smernice za revizijo upravljanja varovanja informacij ter bo osredotočen na varnostne kontrole.
- ISO/IEC 27011 - bo obsegal smernice upravljanja varovanja informacij za telekomunikacije.

3 PRIMERJAVA IZBRANIH METODOLOGIJ IN STANDARDA

V diplomskem delu skušam primerjati standarde in metodologije za upravljanje informatike, ki so danes na trgu. Informatika postaja čedalje bolj kompleksna, pojavlja se vse več metodologij, ki so načeloma v pomoč direktorjem službe za informatiko. Ker število metodologij narašča, bom poiskala primerjave, ki mi bodo potencialno dale odgovor, ali obstaja najboljša metodologija. Med seboj jih bom primerjala in potegnila vzporednice med njimi.

V naslednjih poglavjih diplomskega dela bom podala temeljne izsledke primerjav med metodologijami. Metodologije, ki jih primerjam, so podrobneje opisane v drugem poglavju. V primerjavah bom upoštevala naslednje različice metodologij:

- ITIL verzija 2;
- COBIT verzija 3;
- ISO 17799.

Posamezne metodologije obstajajo že v nadgrajenih različicah (npr. ITIL verzija 3, COBIT verzija 4.1), vendar sem za potrebe primerjave izbrala različice, ki se v praksi najbolj pogosto uporabljajo (Cartlidge et al., 2007, str. 8).

V primerjavah sem se osredotočila predvsem na področja informatike, ki jih posamezne metodologije pokrivajo, kar pa niso vsa področja informatike. Primerjave so opisne, saj metrike, po katerih bi bilo mogoče oceniti nivo pokrivanja posameznega področja, ne obstajajo. Pri primerjavah sem se oprla na temeljne vire in že obstoječe primerjave.

Pri primerjavah bom izhajala iz metodologije ITIL ter jo primerjala z metodologijo COBIT in standardom ISO 17799 ter na koncu poglavja potegnila vzporednice med njimi. Izsledke primerjav metodologij bom predstavila v več skupinah, kjer bom metodologije primerjala po parih. Najprej bom primerjala ITIL in COBIT, nato ITIL in ISO 17799. Na koncu poglavja bom podala izsledke primerjav med vsemi tremi metodologijami hkrati.

3.1 Primerjava metodologij ITIL in COBIT

V zadnjem desetletju je opaziti pojav in sprejemanje metodologij, zlasti ITIL in COBIT. Nekateri so prepričani, da je uporaba dveh orodij alternativni pristop za dosego enakega cilja, drugi menijo, da sta medsebojno izključujoči. Dejansko pa sta ogrodji za upravljanje storitev informatike in upravljanje informatike pravzaprav komplementarni in skupaj skrbita za doseganje večje vrednosti, kot če bi uporabljali le eno izmed njiju. Čeprav ITIL zagotavlja odlično dokumentacijo procesnih tokov, ni popolno orodje, saj nima posebnega sistema merjenja, ki bi pripomoglo k izboljšanju procesov. COBIT načrtuje oziroma definira cilje, kaj je treba narediti, da dosežemo želeni rezultat, ITIL pa nam pomaga priti do ciljev.

Ko primerjamo ITIL in COBIT, moramo identificirati njuno medsebojno skladnost. Kar nas najprej lahko zmede je, da z različnimi besedami opisujeta pomensko enako stvar. Na primer pri upravljanju z incidenti ne moremo najti nobene povezave med metodologijama COBIT in ITIL, vendar to še ne pomeni, da COBIT upravljanja incidentov ne pokriva. Namesto tega ga pokriva v ostalih delih ogrodja oziroma z drugačnim pristopom, kot vidimo v Tabeli 3.

Kot navajajo smernice analitskega podjetja Gartner (Mingay & Bittinger, 2002, str. 3) je kar nekaj procesov COBIT izpeljanih iz ITIL procesov podpore storitvam in zagotavljanja storitvam, na primer DS1, DS3, DS4, DS6, DS8, DS9 in DS10. Opisi procesov so razvidni

iz Slike 6 v drugem poglavju. Omenjeni procesi COBIT se prekrivajo z enim ali več procesi ITIL, in sicer nivojem storitev, upravljanjem konfiguracij, upravljanjem problemov, upravljanjem incidentov, upravljanjem izdaj, upravljanjem razpoložljivosti in finančnim upravljanjem storitev. Na preostalih treh področjih metodologije COBIT je neposrednega prekrivanja z metodologijo ITIL manj, kljub temu pa k njim prispeva s svojo ozko usmeritvijo na upravljanje storitev informatike. Na primer ITIL poudarja dosledno komunikacijo in sodelovanje uporabnikov. Podobno so COBIT-ova načela upravljanja kakovosti skladna z metodologijo ITIL, ki je grajena na kakovostnem pristopu. ITIL se ne dotika vodenja projektov, tako kot COBIT (P10), vendar to OGC pokriva z metodologijo upravljanja projektov PRINCE. Prav tako se COBIT-ov proces AI6 odlično prekriva s procesom upravljanja sprememb in podpornim procesom upravljanje izdaj metodologije ITIL.

V nadaljevanju je na podrobnejši način prikazano prekrivanje izbranih metodologij in dopolnjevanje metodologij v življenjskem ciklu upravljanja informatike. Pri primerjavi izhajam iz procesov ITIL, vsebina Tabel 3 in 4 pa je obrazložena v celotnem poglavju.

3.1.1 Prekrivanje procesov ITIL podpore storitev in zagotavljanja storitev ter procesov COBIT

Podporo uporabnikom imata obe metodologiji dobro pokriti. ITIL v obliki storitvenega centra nudi storitve uporabnikom ter se ukvarja z reševanjem incidentov ter sprejemanjem zahtevkov. Na drugi strani COBIT podporo uporabnikom rešuje s svetovanjem in pomočjo uporabnikom. Dodatno s kontrolnimi cilji skrbi za razvoj in vzdrževanje postopkov, pripravo navodil za uporabnike, operativnih navodil in navodil za usposabljanje.

Tabela 3: Prekrivanje procesov podpore storitev v ITIL in procesov COBIT

ITIL	COBIT (primarno)	COBIT (sekundarno)
Storitveni center	DS8 Pomoč in svetovanje strankam	AI 4 Razvijanje in vzdrževanje postopkov DS7 Izobraževanje in uvajanje uporabnikov
Upravljanje incidentov	DS10 Upravljanje problemov in incidentov	
Upravljanje problemov	DS10 Upravljanje problemov in incidentov	DS8 Pomoč in svetovanje strankam
Upravljanje konfiguracij	DS9 Upravljanje s konfiguracijo sistema	AI6 Upravljanje sprememb DS10 Upravljanje problemov in incidentov
Upravljanje sprememb	AI6 Upravljanje sprememb	AI3 Pridobitev in vzdrževanje tehnološke infrastrukture DS9 Upravljanje s konfiguracijo sistema
Upravljanje izdaj		AI6 Upravljanje sprememb DS9 Upravljanje s konfiguracijo sistema

Vir: J. Wallhoff, Combining ITIL and COBIT with 17799, 2005, str. 7.

Vzpostavitev normalnega delovanja vsakdanjih nalog in storitev pokrivata področji upravljanje incidentov in problemov. Obe metodologiji se teh področij lotevata celovito. Sistem upravljanja s problemi zagotavlja, da so vsi incidenti, problemi in napake evidentirani, analizirani in pravočasno razrešeni. Uvedeni so postopki za reševanje problemov, ki jih razvrščajo po stopnji rešljivosti. Sistem za upravljanje problemov naj bi zagotavljal zadostne mehanizme beleženja dogodkov, ki omogočajo sledenje od incidenta do razloga zanj.

Upravljanje konfiguracij kot osnova za upravljanje storitev skrbi za nadzor in evidenco celotnega inventarja informacijskega sistema ter podpira vse ostale procese. Obe metodologiji dobro pokrivata področje upravljanja konfiguracij in predpisujeta uporabo podatkovne zbirke upravljanja konfiguracij. COBIT predpisuje mehanizme, s pomočjo katerih omogoča beleženje, upravljanje s podatkovno zbirko in nepooblaščeno spreminjanje konfiguracij. Obe metodologiji priporočata beleženje revizijske sledi reševanja incidentov.

Tako ITIL kot COBIT uvajata procese za uspešno in učinkovito upravljanje s spremembami, saj se oba zavedata, da je to področje zelo pomembno za uspešno delovanje katerekoli organizacije. ITIL svetuje, da se spremembe spremlja in upravlja od začetka do zaključka, rezultat tega je načrtovan časovni razpored sprememb. COBIT priporoča, da za vsako spremembo ocenimo njen vpliv, ob spremembi ustrezno ažuriramo dokumentacijo in postopke, vodenje verzij pa mora biti nadzorovano v okviru predpisane politike. Upravljanje sprememb tehnološke infrastrukture obravnava v ločenem poglavju, kjer se ukvarja z vprašanji vzdrževanja, namestitve in sprememb sistemske, programske in strojne opreme.

Tabela 4: Prekrivanje procesov zagotavljanja storitev ITIL in procesov COBIT

ITIL	**COBIT (primarno)**	**COBIT (sekundarno)**
Upravljanje ravni storitev	DS1 Določitev potrebne ravni storitev	AI 4 Razvijanje in vzdrževanje postopkov DS2 Upravljanje z zunanjimi storitvami DS4 Zagotovitev stalne storitve DS6 Določitev in razporeditev stroškov M3 Pridobivanje neodvisnih zagotovil
Finančno upravljanje za storitve informatike	DS6 Določitev in razporeditev stroškov	M2 Spremljanje procesov
Upravljanje zmogljivosti	DS3 Upravljanje izvedbe in kapacitet	
Upravljanje neprekinjenosti delovanja storitev	DS4 Zagotovitev stalne storitve	AI6 Upravljanje sprememb
Upravljanje razpoložljivosti	DS3 Upravljanje izvedbe in kapacitet	AI2 Pridobitev in vzdrževanje uporabniške programske rešitve

Vir: J. Wallhoff, Combining ITIL and COBIT with 17799, 2005, str. 7.

Proces upravljanja izdaj skrbi za upravljanje in izdajo potrjene strojne in programske opreme ter za točno vsebino knjižnice potrjene programske opreme. Primarno COBIT ne pokriva upravljanja izdaj. Področje pokriva z upravljanjem sprememb in konfiguracijo sistema.

Obe metodologiji predpisujeta uporabo dogovora o ravneh storitev in omogočata upravljanje celotnega življenjskega cikla ravni storitev. V praksi to pomeni, da spremljata skladnosti in opredelitve dogovorov, zbirata in analizirata podatke o izvedbi izboljšav ponujenih storitev ter poskušata zagotoviti, da so pričakovanja dosežena ali presežena. COBIT ima metrike, s katerimi se določajo kriteriji za dogovor o ravni in operativni ravni storitev. Sekundarno pokriva področja razvijanje in vzdrževanje postopkov, upravljanje z zunanjimi storitvami, zagotavljanje neprekinjenih storitev, določitev in razporeditev stroškov ter pridobivanje neodvisnih zagotovil.

Metodologiji z namenom podpore aplikacijam in procesom upravljanja ravni storitev finančno upravljanje informacijskih storitev rešujeta tako, da ugotavljata stroške, povezane z zagotavljanjem storitev, kot zahteva dogovor o ravni storitev. ITIL z namenom podpore upravljanja zmogljivosti dodatno zagotavlja, da bodo izdatki načrtovanih, zahtevanih in napovedanih zmogljivosti preverjeni glede na zagotovljena sredstva. Zagotavlja tudi, da bodo vse primerne informacije, ki so povezane s funkcijami upravljanja storitev, kot jih določa ITIL, na voljo za analizo v zbirki upravljanja konfiguracij.

V poglavju upravljanja zmogljivosti se obe metodologiji popolnoma prekrivata. Vsebujeta mehanizme za spremljanje komponent infrastrukture, povezavo z zbirko upravljanja konfiguracij in poslovnimi storitvami, storitvenim centrom, upravljanjem ravni storitev, rešitvami sprememb in izdaj. Zagotavljata izdelavo poročil o zmogljivosti in časovnih razporedih.

Pri neprekinjenosti poslovanja je pomembno, da je zagotovljen dostop do podatkov v zbirki upravljanja konfiguracij iz vseh ključnih področij ITIL-a: upravljanja konfiguracij, storitvenega centra in upravljanja incidentov, upravljanja sprememb, upravljanja razpoložljivosti in zmogljivosti, upravljanja ravni storitev in upravljanja infrastrukture. Pomembno se je povezati z rešitvijo upravljanja ravni storitev in zagotoviti, da so dogovorjene storitve ponovno vzpostavljene in na voljo znotraj časovnih okvirov, ki so določeni v dogovoru o ravni in operativni ravni storitev in podpornih pogodbah.

Upravljanje razpoložljivosti odlično pokrivata obe metodologiji. COBIT poleg tega predvideva, da naj bi do podatkov v zbirko upravljanja konfiguracij imele dostop tudi vse ključne funkcije upravljanja storitev. Predvideva tudi zagotovitev ponovne vzpostavitve dogovorjenih storitev.

COBIT je osnovan na že obstoječih metodologijah kot so CMM *(*angl. *Capability Maturity Model)*, ISO 17799, ISO 9000 in najpomembnejše v tem kontekstu, metodologije ITIL. Kot dopolnjevalec združuje neskladne dobre prakse v eno in jih povezuje s strateškimi poslovnimi cilji. COBIT je namenjen uporabi na najvišjem nivoju upravljanja informatike. Oskrbuje celoten okvir upravljanja na visokonivojskem procesnem modelu in je tako primeren za mnoge organizacije.

Organizacije, ki želijo vpeljati metodologijo ITIL, potrebujejo učinkovito upravljanje informatike in kontrolni okvir za uspešno izvedbo. COBIT je obsežno upravljavsko ogrodje, ki vsebuje smernice za pomoč organizacijam pri poslovnih zahtevah. Deluje tudi kot mehanizem za merjenje zmogljivosti organizacije; ljudi, procesov in tehnologije za dosego uspešnega rezultata in poslovnih zahtev ter merjenje izvedljivosti. Čeprav je COBIT usmerjen na procese, ne vsebuje procesnih korakov in nalog. Procesi so osredotočeni na poslovne zahteve in navodila, kako jim zadostiti. Na drugi strani ITIL definira najboljše prakse za upravljanje storitev informatike in se osredotoča na metode ter jih definira bolj obsežno kot COBIT. ITIL je kot nekakšen vodič za gradnjo procesov. ITIL in COBIT omogočata organizacijam dosego treh ciljev (Hill & Turbitt, 2006, str. 1):

- Uvajata preizkušene dobre prakse upravljanja procesov storitev informatike s poslovnega vidika in dajeta smernice za doseganje poslovnih ciljev.
- Urejata procesne cilje, ki temeljijo na organizacijskih poslovnih ciljih in delujeta kot sredstvo za merjenje razvoja procesov.
- Zagotavljata učinkovito upravljanje in kontrolo na procesnem nivoju.

ITIL in COBIT sta odlična kombinacija, ki organizaciji omogočata upravljati informatiko s poslovnega vidika. ITIL predstavlja smernice najboljših praks procesov ITSM skladnih s poslovnimi zahtevami. COBIT pomaga organizaciji oblikovati procese ITIL za poslovne potrebe in cilje organizacije. Organizaciji pomaga pri vzpostavitvi začetne in končne točke. To pomeni, da določa, v kakšnih okoliščinah je organizacija oziroma kje želi biti. Če poznamo cilje informatike, lahko aktiviramo poslovne cilje. Prav tako predstavlja učinkovit mehanizem za upravljanje in merjenje razvoja vpeljave procesov ITIL, tako da meri razvoj in pomaga pri izvrševanju ciljev. COBIT specifično določa področje upravljanja, ima pod kontrolo informacije in procese v podjetju, spremlja izvrševanje in cilje organizacije, spremlja izvedljivost znotraj procesov informatike ter primerja dosežke v organizaciji. Organizacije bi morale izkoristiti priložnosti in prednosti, ki jih ponujata vpeljavi obeh standardov (Hill & Turbitt, 2006, str. 4).

Vpeljava kombinacije ITIL in COBIT vsekakor ni vsakdanja naloga, saj se mora organizacija vpeljave lotiti na treh področjih: infrastrukturi, procesih ITIL in kontrolnih ciljih COBIT.

3.1.2 Primerjava metodologij z vidika upravljanja informatike

Kljub temu, da se ITIL neposredno ne ukvarja z upravljanjem informatike ampak z upravljanjem storitev, nekatera področja ITIL-a lahko pozitivno dopolnjujejo metodologijo COBIT pri doseganju ciljev upravljanja informatike.

Tabela 5: Prekrivanje življenjskega cikla upravljanja informatike z metodologijama ITIL in COBIT

Življenjski krog upravljanja informatike			
Področja upravljanja informatike	**Cilji**	**Komponente, ki jih podpira COBIT**	**Komponente, ki jih podpira ITIL**
Usklajenost poslovanja in informatike	USMERJANJE Zmožnost spodbujanja sposobnosti potrebnih za ustvarjanje poslovnih vrednosti	Ključni kazalniki ciljev	Zagotavljanje storitev Planiranje vpeljave upravljanja storitev
Zagotavljanje vrednosti	USTVARJANJE Uspešno zagotavljanje poslovne vrednosti	Ključni kazalniki učinkovitosti procesov Kritični dejavniki uspeha Kontrolni cilji Kontrolne prakse	Podpora storitvam Upravljanje infrastrukture informacijsko komunikacijskih tehnologij Upravljanje aplikacij Upravljanje z viri programske opreme
Upravljanje tveganj	VAROVANJE Ugotavljanje tveganj in blaženje tveganj za zavarovanje vrednosti		Upravljanje varovanja informacij Upravljanje neprekinjenosti storitev
Upravljanje virov	DELOVANJE Vzpostavljanje storitev informatike za poslovne potrebe	Zrelostni model Kritični dejavniki uspeha Kontrolni cilji Kontrolne prakse	Upravljanje razpoložljivosti storitev Upravljanje zmogljivosti Upravljanje financ za storitve informatike
Vrednotenje	SPREMLJANJE Spremljanje delovanja in po potrebi spreminjanje življenjskega kroga upravljanja informatike	Sistem uravnoteženih kazalnikov (angl. *Balanced Scorecard*) Zrelostni model Smernice za nadzor in revizijo	Upravljanje ravni storitev Storitveni center

Vir: E. Šimkova, Service level management and its link to COBIT's DS1 (Define and Manage Service Levels) and to DS2 (Manage Third – Party Services) Processes, 2005, str. 73.

Tabela 5 (Šimkova, 2005, str. 73) prikazuje življenjski cikel upravljanja informatike, kot ga določa COBIT in je dopolnjena z gradniki ITIL-a, ki pri doseganju ciljev lahko pomagajo. Povezavo med ogrodjema prikazuje na visokem nivoju, zato jo lahko uporabimo le kot smernico, težje pa kot navodilo, kako dopolniti posamezne procese. ITIL zagotavlja dobro osnovo za same procese, COBIT pa ustvarja trdne temelje za spremljanje učinkovitosti in nadzor.

3.2 Primerjava metodologije ITIL s standardom ISO 17799

Standard ISO 17799 je namenjen varovanju informacij, manj pa reševanju problemov, s katerimi se sooča informatika. Iz tega lahko sklepamo, da je skladnost z metodologijo ITIL manjša kot pri metodologijah ITIL in COBIT. Na primer ISO 17799 nima nobene skladnosti z metodologijo ITIL pri upravljanju problemov in konfiguracij, četudi ima upravljanje konfiguracij velik vpliv na okolje informacijske tehnologije in bi moralo to področje poskrbeti za varnost. Varnost pri standardu ISO 17799 pomeni predvsem ohranitev osnovnih ciljev nadzorstev, kot so zagotavljanje zaupnosti, celovitosti in razpoložljivosti. Z vidika metodologije ITIL razpoložljivost obsega vidik kakovosti, ki vključuje zanesljivost, vzdrževanje, sposobnost izvajanja storitev in fleksibilnost (Shibudin, Sharifi & Ayat, 2008, str. 752). Naslednja pomembna primerjava metodologij in standarda se dotika področja financ, ki v standardu ISO 17799 niso obravnavane, medtem ko se ITIL ukvarja s financami in alokacijo stroškov za zagotavljanje storitev informatike.

3.2.1 Prekrivanje procesov ITIL podpore storitev in zagotavljanja storitev ter standarda ISO 17799

ISO 17799 storitvenega centra ne predpisuje, zato ga primarno ne pokriva, kot ga pokriva ITIL. Kljub temu pa se področja dotika s poglavjem, kjer svetuje, da zaposleni v storitvenem centru poročajo o vseh varnostnih grožnjah ter informacijskih varnostnih slabostih in pomanjkljivostih, kot je razvidno iz Tabele 6.

ISO 17799 razvija postopke, ki upravljajo z vsemi tipi varnostnih incidentov in postopke, ki obvladujejo izpade ali prenehanje delovanja storitev. Skrbi za popolnost in pravilnost podatkov.

Tabela 6: Primerjava med podporo storitev ITIL in standardom ISO/IEC 17799:2000

ITIL	ISO/IEC 17799:2000 (primarno)	ISO/IEC 17799:2000 (sekundarno)
Storitveni center		6.3.2. Poročanje varnostnih pomanjkljivosti
Upravljanje incidentov	8.1.3 Postopki upravljanja incidentov	6.3 Odziv na varnostne incidente in slabo delovanje
Upravljanje problemov		
Upravljanje konfiguracij		
Upravljanje sprememb	10.5.1 Postopki kontrole sprememb	4.2.2 Varnostne zahteve in zunanje pogodbe 8.1.2 Kontrole operativnih sprememb 8.3.1 Kontrole proti zlonamernim programski opremi
Upravljanje izdaj		10.4.1 Kontrole operativne programske opreme 10.5.2 Tehnična ocena sistemskih sprememb

Vir: J. Wallhoff, Combining ITIL and COBIT with 17799, 2005, str. 8.

Področji upravljanje problemov in konfiguracij med standardom ISO 17799 in metodologijo ITIL nista primerljivi. Standard ISO 17799 se namreč s tema področjema ne ukvarja.

Spremembe strojne in programske opreme standard ISO 17799 upravlja s postopki kontrole sprememb. Predpisuje uporabo ločenih okolij za potrebe testiranja, razvoja in produkcije. Na drugem nivoju pogodbeno predpisuje dostop tretjim osebam in kontrole v primeru operativnih sprememb. Standard predpisuje tudi implementacijo kontrol za zaščito sistema, in sicer za odkrivanje in preprečevanje zlonamerne programske opreme.

Upravljanja izdaj ISO 17799 primarno ne pokriva, predpisuje pa nadzor nad nameščanjem programske opreme na operativnih sistemih in vzpostavitev dnevnika vseh sprememb na operativnih programskih knjižnicah. Ob vsaki spremembi operacijskega sistema priporoča preveritev in testiranje aplikacijskih sistemov ter na koncu podajo tehnične ocene (http://www.praxiom.com/).

ITIL kot dobro prakso upravljanja ravni storitev priporoča dogovora OLA in SLA. Vodilo standarda ISO 17799 je imeti pogodbo, s katero omejimo dostop tretjim osebam. Iz Tabele 7 je razvidno, da ISO 17799 upravljanja ravni storitev ne pokriva tako široko, temveč se dotika področja le z varnostnega vidika tako, da predpisuje pogodbo, ki jo je potrebno skleniti z zunanjimi izvajalci. Pogodba določa nadzorovano uporabo in dostop do informacijskih virov in informacij v podjetju.

Tabela 7: Primerjava med zagotavljanjem storitev ITIL in standardom ISO/IEC 17799:2000

ITIL	ISO/IEC 17799:2000 (primarno)	ISO/IEC 17799:2000 (sekundarno)
Upravljanje ravni storitev		4.2.2 Varnostne zahteve in zunanje pogodbe
Finančno upravljanje za storitve IT		
Upravljanje zmogljivosti	8.2.1 Planiranje zmogljivosti	8.2.2 Sistemsko planiranje in sprejemljivost
Upravljanje neprekinjenosti delovanja storitev	11. Upravljanje neprekinjenega poslovanja	
Upravljanje razpoložljivosti		4.3.1 Varnostne zahteve in pogodbe za zunanje izvajanje 8.2 Sistemsko planiranje in sprejemljivost 8.5.1 Nadzor omrežja 8.7.4 Varnost elektronske pošte 9.5.5 Uporaba sistemskih orodij 12.1.7.3 Kakovost in popolnost beleženja dogodkov

Vir: J. Wallhoff, Combining ITIL and COBIT with 17799, 2005, str. 8.

ITIL na področju varovanja upravljanja infrastrukture informacijske tehnologije vsebuje prakse, ki so povezane s standardom ISO 17799. Prvi korak pogodbe o dogovorjeni ravni storitev obravnava fazo načrtovanja, ki temelji na oceni poslovnega tveganja. Stephenson in Kampman (2004, str. 4) ugotavljata, da ta proces zvesto sledi standardu ISO 17799, ki

se konča z izbiro ustreznih varnostnih kontrol, na podlagi prej identificiranih nevarnosti in pomanjkljivosti. Kontrole se uvedejo med fazo uvajanja s pomočjo ustreznih orodij in procesov, preostanek procesa pa obsega neprekinjeno ocenjevanje in pregledovanje varnostne politike ter njene ustreznosti glede na spreminjajoče se poslovne pogoje, vzdrževanje politike in na koncu pripravo poročil, s katerimi se ocenjuje izpolnjevanje zahtev v pogodbah o dogovorjeni ravni storitev.

V točki upravljanja zmogljivosti se ITIL in ISO 17799 zelo dobro prekrivata. ISO 17799 priporoča spremljanje potreb po procesni moči in kapacitet za shranjevanje informacij, identificiranje le-teh ter razvijanje načrtov za njihovo izpolnitev. Proces po ITIL-u je z vidika načrtovanja zmogljivosti podobno opisan. Opisuje, katere komponente je potrebno nadgraditi, kdaj je potrebno nadgrajevati in koliko sredstev je potrebno vložiti v nadgradnjo. ITIL upošteva stroškovni vidik, medtem ko ga ISO 17799 ne.

ITIL področje neprekinjenosti delovanja storitev široko obravnava in z učinkovito odpravo incidentov vzpostavlja storitve v dogovorjenih časovnih okvirih in na dogovorjeni ravni. Z rednim izvajanjem različnih analiz zagotavlja usklajenost načrtov s spreminjajočimi se poslovnimi zahtevami (Rudd, 2004, str. 15). ISO 17799 se z upravljanjem neprekinjenosti delovanja storitev poglobljeno ne ukvarja, opredeljuje le najbolj osnovne dele. Proces načrtovanja neprekinjenosti poslovanja obravnava v petih fazah (Zupan & Pestotnik, 2006, str. 7):

- Vključitev informacijske varnosti v načrtovanje neprekinjenega poslovanja.
- Opredelitev možnega vpliva in tveganj različnih katastrof na poslovne dejavnosti.
- Razvoj in uvedba načrtov neprekinjenega poslovanja oziroma dokumentiranje dogovorjenih postopkov in procesov.
- Postavitev ogrodja neprekinjenega poslovanja.
- Preverjanje, vzdrževanje in ponovna evalvacija načrtov.

ISO 17799 predpisuje pogodbe za pravne in varnostne zahteve, katere je potrebno pregledati in narediti načrt, kako jim zadostiti v prihodnosti. Nadzor omrežja vključuje vzpostavljanje varnosti omrežja, nadzor nad varnostjo informacij, zaščito pred nepooblaščenimi vdori in vzpostavitev postopkov za varovanje sistemov. Na področju varovanja elektronske pošte ISO 17799 razvija politiko uporabe le-te. Skrbi tudi za kakovost beleženja dogodkov, zaščito sledov vsakih dejanj v sistemu ter uporabo sistemskih orodij.

3.3 COBIT, ITIL in ISO 17799

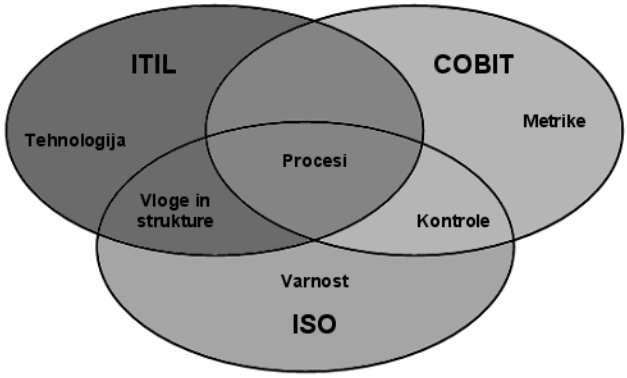
Obravnavani metodologiji in standard predstavljajo dober vir navdiha vodjem informatike, ki z namenom zmanjševanja operativnih stroškov poskušajo optimizirati sisteme in upravljanje storitev. Te najboljše prakse so najbolj znane, ker so se v preteklosti izkazale

za najbolj učinkovite. Ker en sam vir informacij morda ni dovolj, se bo združevanje gradnikov naštetih ogrodij izkazalo v izboljšanju upravljanja storitev in procesov (Garbani, 2005, str. 95).

Garbani (2005, str. 95) meni, da največjo oviro pri vpeljavi dobrih praks predstavljajo zaposleni in organizacije, saj so organizacijske strukture neprimerne, ljudje pa niso naklonjeni spremembam in se jim upirajo. Dobra stran uvajanja dobrih praks oziroma metodologij v poslovno okolje je neomejevanje organizacij na eno samo prakso. Neredko so primorane uvesti več kot eno samo dobro prakso ali več delov različnih praks, če želijo v skladu s smernicami učinkovito upravljati procese. Začetne faze vpeljave dobrih praks vsekakor zahtevajo pridobivanje informacij in primerjav med njimi. Vodje, ki so zadolženi za vpeljavo, se le redko zavedajo slabe strani uvedbe več dobrih praks, saj se pogosto preveč ukvarjajo s primerjavami kot pa z doseganjem svojih ciljev (Dubie, 2006, str. 28). Greenfield (2007, str. 38) meni, da ITIL z metodologijo COBIT in standardom ISO 17799 z združevanjem procesov, zaposlenih in tehnologij nudi priporočeno ogrodje za upravljanje operacij.

Slika 10 prikazuje ključna področja prekrivanja metodologij ITIL, COBIT in standarda ISO 17799.

Slika 10: Prekrivanje ključnih področij metodologij in standarda



Vir: J. P. Garbani, Building Blocks of Process and Innovation, 2005, str. 95.

V nadaljevanju so opisane glavne prednosti in slabosti vsake metodologije (Garbani, 2005, str. 95):

- ISO 17799 predpisuje varnostne kontrole. Ne predpisuje smernic za njihovo implementacijo in se ne ukvarja z umestitvijo teh procesov v celoten proces upravljanja informatike. Prednost standarda je zagotavljanje varnosti na vseh organizacijskih nivojih.
- ITIL je močan pri procesih zagotavljanja in podpore storitvam. Opisuje, kako lahko strukturiramo operativne procese, vendar je šibak na področju varnostnih kontrol in procesov.

- COBIT se osredotoča na kontrole in metrike. Prav tako mu manjka varnostna komponenta, vendar ponuja bolj univerzalen pogled na procese informatike pri organizacijskem upravljanju informatike kot ITIL.

Ob pogledu na vse tri metodologije na Sliki 10 pridemo do zaključka, da se medsebojno dopolnjujejo. Moč ITIL-a v operativnih procesih informatike se dopolnjuje s kritičnimi dejavniki uspeha in ključnimi kazalniki izvedljivosti COBIT-a, oba pa lahko koristno uporabita varnostne procese in kontrole, ki jih določa ISO. Violino (2006, str. 46) ugotavlja, da standard in obravnavani metodologiji ne pokrivajo v celoti varovanja informacij. Obravnava jih kot delce sestavljanke, ki se med seboj dopolnjujejo, ne pa kot obsežno varnostno ogrodje.

Dopolnjevanja med metodologijami ITIL, COBIT in ISO 17799 so (Garbani, 2005, str. 95):

- Upravljanje incidentov. V ITIL-u je določen kot proces podpore storitvam, v ISO 17799 kot varnostni incidenti, v COBIT-u kot zagotavljanje in podpora storitvam.
- Upravljanje problemov. Poglavje zagotavljanje in podpora storitvam v COBIT določa upravljanje incidentov in problemov, kar se v ITIL dopolnjuje s procesom upravljanja problemov.
- Upravljanje sprememb, konfiguracij in izvedb. Ti procesi ITIL-a imajo neposredno povezavo s COBIT-om v upravljanju sprememb in konfiguraciji sprememb, kot tudi z operativno kontrolo sprememb, kontrolami proti virusom in varnostnimi zahtevami tretjih oseb pri ISO 17799.
- COBIT in ISO 17799 zagotavljata usmeritve, ključne kazalnike in kontrole za določitev dogovora o ravni storitev, načrtovanja kapacitet, upravljanja razpoložljivosti in neprekinjenega poslovanja, ki se dopolnjujejo s procesi zagotavljanja storitev v ITIL-u.

Organizacijam ustrezen izbor najprimernejše metodologije v podjetje ter zaporedje uvedbe pogosto predstavlja težavo. Najprej potrebujejo učinkovit upravljavski okvir, ki bo omogočal konsistenten pristop k doseganju ciljev organizacije. Izbira modela je vsekakor odvisna od poslovnih ciljev organizacije, zrelosti organizacije, regulativnih zahtev ter pričakovanj trga (Zupan & Pestotnik, 2006, str. 1). Ker so področja dobrih praks, ki jih obravnavam v diplomskem delu, med seboj tesno povezana, ne moremo vpeljati zgolj enega področja. Samo metodologija COBIT obravnava celoten spekter procesov upravljanja informatike z vidika poslovne perspektive višjega managementa, s poudarkom na nadzoru in reviziji. Ostala ogrodja nekatere procese obravnavajo bolj natančno; na primer ITIL procese za upravljanje storitev in ISO 17799 za informacijsko varnost. V Tabeli 8 so splošno predstavljene ključne točke, ki ponazarjajo primerjavo metodologij in standarda.

Tabela 8: Splošni pregled metodologij COBIT in ITIL ter standarda ISO 17799

	COBIT	ITIL	ISO 17799
IZDAJATELJ	ISACA	OGC	ISO odbor in IEC
OBSEG	Procesi: Planiranje in organiziranje Pridobitev in uvedba Dostava in podpora Nadziranje	Glavna področja: Zagotavljanje storitev Podpora storitvam Upravljanje infrastrukture informacijsko komunikacijskih tehnologij Načrtovanje implementacije upravljanja storitev Upravljanje aplikacij Poslovna perspektiva Upravljanje varnosti	Področja: Varnostna politika Organiziranje informacijske varnosti Razvrstitev in kontrola sredstev Varovanje človeških virov Fizična zaščita in zaščita okolja Upravljanje komunikacij in obratovanja Obvladovanje dostopov Nabava, razvoj in vzdrževanje informacijskih sistemov Ravnanje ob uresničitvi grožnje varnosti Načrtovanje neprekinjenega delovanja Usklajenost
POUDAREK	Upravljanje informatike in nadzor (revizijska funkcija)	Upravljanje storitev informatike (izvedbena funkcija)	Upravljanje varovanja informacij (varnostna funkcija)
PREDNOSTI	Kontrole in metrike	Strukturiranost procesov	Varnostne kontrole
SLABOSTI	Ne pokriva dovolj področja varnosti	Ne ukvarja se poglobljeno s področjem varnosti in nadzora	Omejen na področju procesov upravljanja informatike
PREKRIVANJA	ISO 17799 se prekriva z metodologijo COBIT v vseh procesih metodologije COBIT, najbolj v procesu dostava in podpora ter najmanj v procesu nadziranja.	ITIL in COBIT se prekrivata v procesu nabava in uvedba, dostava in podpora ter delno v procesu planiranja in organiziranja.	ITIL dopolnjuje standard ISO 17799 na področju finančnega upravljanja storitev, upravljanja s problemi in upravljanja konfiguracij.
DOPOLNJEVANJA	COBIT in ISO 17799 sta komplementarna in ju lahko uporabljamo skupaj. COBIT pokriva področja upravljanja informatike, medtem ko ISO bolj poudarja informacijsko varnost in se ukvarja s pridobivanjem potrdil na tem področju.	COBIT dopolnjuje metodologijo ITIL v procesu nadziranja.	ISO 17799 dopolnjuje ITIL na področju varnosti.
CILJNI UPORABNIKI	Vse organizacije	Ponudniki storitev informatike	Vse organizacije

Forrester (Symons, 2006, str. 9) predlaga vpeljavo obravnavanih metodologij in standarda v naslednjem vrstnem redu; najprej COBIT, ker je dostopen managerjem ter strokovnjakom s področja informacijske tehnologije in omogoča orodja in dokumentacijo, ki olajšajo vpeljavo in osvojitev metodologije. Po implementaciji COBIT-a spodbujajo vpeljavo metodologije ITIL, saj obe metodologiji omogočata postavitev močnega upravljavskega ogrodja in izboljšujeta operativne učinke. Kot zadnje pa priporočajo uvedbo standarda ISO 17799, ki se prav tako dopolnjuje s procesi metodologije COBIT.

Vpeljava dobrih praks mora tako sovpadati z ogrodjem upravljanja in nadzora tveganj podjetja, ki je organizaciji primerno, ter se integrirati z ostalimi metodami dela in praksami, ki se že uporabljajo. Učinkovite politike vodstva in postopki brez dvoma pomagajo zagotoviti, da upravljanje informatike postane vsakodnevno rutinsko opravilo. Vpeljava standardov in dobrih praks pomaga omogočiti hitro vpeljavo dobrih postopkov in se izogniti dolgim zakasnitvam in usklajevanju pristopov. Standardi in metodologije ne odpravljajo vseh problemov, njihova učinkovitost pa je odvisna od načina vpeljave in vzdrževanja. Najbolj so uporabni takrat, kadar jih uporabimo kot nabor načel in kot osnovo za oblikovanje specifičnih postopkov. Vodstvo in zaposleni morajo razumeti, kaj je potrebno narediti, kako to narediti in zakaj je to pomembno, sicer dobre prakse postanejo le črka na papirju.

SKLEP

Informatika v podjetju predstavlja eno najmočnejših funkcij pri poslovanju v sedanjem času. Njeno upravljanje predstavlja povezovalni člen med usklajevanjem strategije informatike in poslovnimi cilji organizacije. Skozi čas se je spreminjala tudi njena vloga. Informatika je najprej predstavljala le orodje za hitrejšo obdelavo podatkov. Iz tega obdobja so sicer nastali številni tehnološki predpisi in standardi, ki so bili usmerjeni izključno v uporabo tehnologije, vendar so se le redko dotaknili poslovnih problemov. Kasneje je informatika postala sredstvo za povezovanje poslovanja, saj je z uporabo standardov in metodologij pripomogla k boljšemu upravljanju in kakovosti storitev. Danes upravljanje informatike s poslovnim pristopom in uporabo ustreznih metodologij in standardov deluje kot strateški partner pri poslovanju. Poslovni procesi potekajo z uporabo informacijske tehnologije in informacijskih sistemov. Inovativna uporaba informacijske tehnologije neposredno vpliva na konkurenčno prednost ter pokrije ključno področje upravljanja informatike, upravljanje s tveganji. Nov način standardizacije je omogočil razvoj v smeri informatike kot procesnega in strateškega partnerja pri poslovanju.

Najpogosteje uporabljeni informacijski standardi in metodologije, ki preko merljivih ciljev usklajujejo informatiko in poslovanje, so ITIL, COBIT in ISO 17799 in so bili tudi predmet obravnave v mojem diplomskem delu. V diplomskem delu sem analizirala izbrani metodologiji in standard ter na podlagi primerjav skušala poiskati tisto prakso, ki bi najbolje zadostila potrebam upravljanja informatike v podjetju. Na podlagi analize dobrih praks sem ugotovila, da so predstavljene metodologije izredno kompleksne in s tem povezana tudi njihova uporabnost. Uporabnost dobrih praks je determinirana z velikostjo in dejavnostjo podjetja ter razvitostjo informatike v podjetju. Dobre prakse omogočajo vzpostavitev učinkovitega upravljavskega okvira in le na ta način omogočajo konsistenten pristop k zagotavljanju ciljev podjetja.

V diplomskem delu sem ugotovila, da je brez analize podjetja nemogoče vnaprej napovedati, katera metodologija ali standard podjetju najbolj ustreza. Zato je izbira dobrih praks vsekakor odvisna od poslovnih ciljev in zrelosti podjetja. Poudarjam, da je težko vpeljati le eno funkcijo, saj so upravljanje, nadzor in varovanje informacij med seboj tesno povezane. Ugotovila sem, da se prakse med seboj prekrivajo ter dopolnjujejo, kar sem podrobneje opisala v tretjem poglavju.

Prikaz ključnih točk primerjav metodologij in standarda bo omogočal vodjem informatike izbiro za vpeljavo najprimernejše dobre prakse v podjetje, glede na dejavnost s katero se podjetje ukvarja. Torej bo pregled omogočal bližnjico do odgovorov, ki si jih zastavi vsak vodja informatike, ki želi vpeljati dobro prakso v podjetje.

LITERATURA IN VIRI

1. Brezavšček, A. & Zupan, L. (2006). Standardi in priporočila na področju informacijske varnosti. Elektronski vir. *Zbornik posvetovanja Dnevi slovenske informatike*. Portorož: Slovensko društvo informatika.
2. Cadbury, A. (2002). *Corporate Governance and Chairmanship: a personal view*. Oxford: Oxford University Press.
3. Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. (2007). An Introductory Overwiev of ITIL V3. Najdeno 3. decembra 2008 na spletnem naslovu http://www.itsmfbooks.com/Media/SampleFiles/itSMF_ITILV3_Intro_Overview.pdf
4. Dubie, D. (2006). Better management through best practices. *Network World*, 23 (2), 28.
5. Erzetič, A. (2007a). Tretji krog ITILa. *Sistem*, (september), str. 10-12.
6. Erzetič, A. (2007b). Sedem procesov oblikovanja storitev. *Sistem*, (december), str. 10-11.
7. Etzler, J. (2007). IT Governance According to Cobit – How does the IT Performance within one of the Largest Investment Banks in the World Compare to COBIT? Najdeno 2. maja 2009 na spletnem naslovu http://www.ee.kth.se/ php /modules / publications / reports/2007/XR-EE-ICS_2007_014.pdf
8. Garbani, J.P. (2005). Building Blocks of Process and Innovation. *Optimize*, 4 (11), 93-95.
9. Greenfield, D. (2007, 10. december). IT by the Book. *Information Week*, str. 35-38.
10. Groznik, A. & Babnik, L. (2007). Ključna področja vodenja informatike kot izzivi vodjem služb za informatiko. *Uporabna informatika*, 15 (3), 150-159.
11. Groznik, A. & Kovačič, A. (2001). Skladnost poslovanja strateškega načrta s strateškim načrtom informatike. *Uporabna informatika*, 9 (1), 12-15.
12. Guldentops, E. (2004). Strategies for Information Technology Governance. Van Grembergen. W. (ur.), *Governing Information Technology through COBIT* (str. 269 – 309). Hershey: Idea Group Publishing.
13. Hardy, G. (2006). Guidance on Aligning COBIT, ITIL and ISO 17799. Najdeno 15. maja 2009 na spletnem naslovu http://www.itgi.org/ Template.cfm? Section= Home & Template=/ContentManagement/ContentDisplay.cfm&ContentID=30690
14. Hill, P. & Turbitt, K. (2006). Combine ITIL and COBIT to Meet Business Challenges. Najdeno 12. aprila 2008 na spletnem naslovu http://documents.bmc.com/products/ documents/17/09/61709/61709.pdf
15. ISACA, (2007). COBIT 4.1 Executive Summary and Framework. Najdeno 29. decembra 2008 na spletnem naslovu: http://www.isaca.org/AMTemplate.cfm? Section =Downloads&Template=/ Content Management/ ContentDisplay. cfm&ContentID = 34172
16. *ISO 27001 Security*. Najdeno 13. marca 2009 na spletnem naslovu http://www.iso27001security.com/

17. *ISO/IEC 17799:2000 Information security standard*. Najdeno 5. decembra 2008 na spletnem naslovu http://www.praxiom.com/iso-17799-2000-outline.htm
18. IT Governance, (2005). Aligning CobiT, ITIL and ISO 17799 for Business Benefit. Najdeno na spletnem mestu 1. decembra 2008 http://www.itgovernance.co.uk / files / ITIL-COBiT-ISO17799JointFramework.pdf
19. ITGI, (2003). Board Briefing on IT Governance, 2nd Edition. USA. Najdeno 20. decembra 2008 na spletnem naslovu http://www.isaca.org/ ContentManagement / ContentDisplay.cfm?ContentID=49995
20. ITGI, (2008). IT Governance Global Status Report. Najdeno 5. maja 2009 na spletnem naslovu http://www.itgi.org/ template_ITGI.cfm?template=/ContentManagement / ContenDisplay.cfm&ContentID=40584
21. Kovačič, A. (2004). Izziv za management?. *Sistem*, (september), str. 10-11.
22. Mingay, S. & Bittinger S. (2002). *Combine COBIT and ITIL for Powerful IT Governance*, Tactical Guidelines, TG-16-1849: Gartner Research.
23. Myler, E. & Broadbend, G. (2006). ISO 17799: Standard for Security, *Information Management Journal*, 40 (6), 43-52.
24. OECD, (2004). Principles of Corporate Governance. Najdeno 13. decembra 2008 na spletnem naslovu http://www.oecd.org/dataoecd/32/18/31557724.pdf
25. Office of Government Commerce, (2007). Continual Service Improvement. London: TSO.
26. Panian, Ž. & Spremić, M. (2007). *Korporativno upravljanje i revizija informacijskih sustava*. Zagreb: Zgombič & Partneri – nakladništvo i informatika d.o.o.
27. Pederiva, A. (2003, 1.maj). The COBIT Maturity Model in a Vendor Evaluation Case. *Information system control journal.* Najdeno 20. avgusta 2009 na spletnem naslovu http://www.isaca.org/ Template.cfm?Section=Home&Template= /ContentManagement /ContentDisplay.cfm&ContentID=15925
28. *Pomembna je podpora menedžmenta in uporabnikov*. Najdeno na 20. januarja 2009 na spletni strani http://www.src.si/library_si/pdf/infosrc/2007-51/InfoSRC.SI-2007-51.pdf
29. *Prevod standarda. BS ISO/IEC 27001:2005, Information Technology, Security Techniques, Information Security, Management Systems, Requirements. Informacijska tehnologija - varnostne tehnike - sistemi za upravljanje, varovanje informacij - zahteve.* (2005). Šempeter pri Gorici: Palsit d.o.o.
30. *Prvi certifikat ISO 27001 pri nas*. Najdeno 27. marca 2009 na spletnem naslovu http://www.racunalniske-novice.com/novice/dogodki-in-obvestila/prvi-certifikat-iso-27001-pri-nas.html
31. Robinson, N. (2005). IT Excellence Starts with Governance. *The Journal of Investment Compliance*, 6 (3), 45-49.
32. Rudd, C. (2004): An Introductory Overwiev of ITIL. Najdeno 28. marca 2008 na spletnem naslovu http://www.itsmf.com/publications/ITIL%20Overview.pdf
33. Sahibudin, S., Sharifi, M. & Masarat, A. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to Design a Comprehensive IT Framework in Organizations.

Second Asia International Conference on Modelling & Simulation (AMS) (str. 749 - 753). Washington, DC: IEEE Computer Society.

34. Saint - Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal*, 39 (4), 60 - 66.
35. Sallé, M. (2004). IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing. Najdeno 2. maja 2009 na spletnem naslovu http://www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf
36. Seling, G.J. & Waterhouse, P. (2006). IT Governance – An Integrated Framework and Roadmap: How to Plan, Deploy and Sustain for Competitive Advantage. Najdeno 1. februarja 2009 na spletnem naslovu https://ca.com/Files/ WhitePapers /it_governance _ whitepaper.pdf
37. Shleifer, A., & Vishny, W. (1997). A Survey on Corporate Governance. *The Journal of Finance*, 52 (2), 737 - 783.
38. *Standardi sistemov za upravljanje varovanja informacij*. Najdeno 12. aprila 2009 na spletnem naslovu http://www.housing.si/ docs/ Vzorci_varnostnih_politik/ Standardi_ ISMS.pdf
39. Stephenson, M. & Kampman, J. (2004). Delivering Best Practices for Complex IT Environments. Najdeno 20. aprila 2009 na spletnem naslovu http://i.i.com.com/cnwk.1d/html/itp/Delivering_Best_Practices.pdf
40. Symons, C. (2005). *IT Governance Framework: Structures, Processes and Communication.* Forrester Research, Inc.
41. Symons, C. (2006). Cobit Versus Other Frameworks: A Road Map to Comprehensive IT Governance. Najdeno 20. marca 2008 na spletnem naslovu http://www.michlik.at/ it_prozesse/ COBIT_Versus_Other_Frameworks.pdf
42. Šimkova, E. (2005). Service Level Management and its link to CobiT's DS1 (Define and Manage Service Levels) and to DS2 (Manage Third – Party Services) Processes. Najdeno 30. junija 2009 na spletnem naslovu http://www.cssi.cz /cssi / system /files/ all/ SI_05_2_simkova.pdf
43. Van Grembergen, W., De Haes, S. & Guldentops, E. (2004). Strategies for Information Technology Governance. Van Grembergen. W. (ur.), *Structures, Processes and Relational Mechanisms for IT Governance* (str. 136). Hershey: Idea Group Publishing.
44. Van Grembergen, W. & De Haes, S. (2008). *Implementing Information Technology Governance: Models, Practices, and Cases*, Hershey, New York, London: IGI Global.
45. Violino, B. (2006). Sorting The Standards. *Computerworld*, 40 (16), 46.
46. Vujović, A. & Krivokapić, Z. (2007). ISO 27001 and ISO 20000, basis for organizational profit. Najdeno 29. marca 2009 na spletnem naslovu http://www.kvalis.info/dmdocuments/ISO%2027001%20I%20ISO%2020000%20OSNOV%20ZA%20ORGANIZACIONE%20DOBITI.pdf
47. Wallhoff, J. (2004). Combining ITIL with COBIT and ISO/IEC 17799:2000. Najdeno 10. marca 2008 na spletnem naslovu http://www.scillani.se/assets/pdf/EN%20 Whitepaper%20Combining%20ITIL%20with%20Cobit%20and%2017799.pdf

48. Weill, P. & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press.
49. Wilbanks, L. (2008). IT Management and Governance in Equal Parts. *IT PRO,* 10 (1), 60-61.
50. Zupan, L. (2005). Uporaba orodij pri vzpostavitvi sistema za upravljanje in varovanja informacij (ISMS) v skladu s standardom BS7799:2-2002. *Zbornik posvetovanja Dnevi slovenske informatike* (str. 263-270). Portorož: Slovensko društvo informatika.
51. Zupan, L. & Brezavšček, A. (2006). Novosti, ki jih prinašajo spremembe standarda BS 7799. *Organizacija*, 39 (1), 58-66.
52. Zupan, L. & Pestotnik, A. (2006). Sinergija informacijske varnosti in organizacijske učinkovitosti. Elektronski vir. *Zbornik posvetovanja Dnevi slovenske informatike* (str. 263-270). Portorož: Slovensko društvo informatika.
53. Žabkar, N. & Mahnič, V. (2005). Uporaba modela COBIT pri razvoju programske opreme. *Zbornik posvetovanja Dnevi slovenske informatike* (str. 257-262). Portorož: Slovensko društvo informatika.

SEZNAM UPORABLJENIH KRATIC

CCTA	Central Computer and Telecommunications Agency
COBIT	Control Objectives for information and related technology
CIO	Chief Information Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
IEC	International Electrotechnical Commision
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
ITGI	Information Technology Governance Institute
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
OECD	Organisation for Economic Co-operation and Development
OGC	Office of Government Commerce
OLA	Operational Level Agreement
PDCA	Plan-Do-Check-Act
PRINCE	Projects in Controlled Environments
PMBOK	Project Management Body of Knowledge
RACI	Responsible – Accountable – Consulted – Informed
SLA	Service Level Agreement
SLM	Service Level Management

SLOVAR IZRAZOV

Tuji izraz	Slovenski prevod
Access Management	Upravljanje dostopov
Availability Management	Upravljanje razpoložljivosti storitev
Balanced Scorecard	Sistem uravnoteženih kazalnikov
Capacity Management	Upravljanje zmogljivosti
Change Management	Upravljanje sprememb
CCTA	Osrednja agencija za računalništvo in telekomunikacije
CIO	Vodja službe za informatiko
CMM	Zmožnostno zrelostni model
CMMI	Poenoten zmožnostno zrelostni model
COBIT	Kontrolni cilji za informacijske in sorodne tehnologije
Continual Service Improvement	Nenehno izboljševanje storitev
Continuity Management	Upravljanje neprekinjenosti storitve
Critical Success Factors	Kritični dejavniki uspeha
Corporate governance	Korporacijsko upravljanje
Event Management	Upravljanje dogodkov
IEC	Mednarodna elektrotehniška komisija
ISACA	Mednarodno združenje za revizijo in kontrolo informacijskih sistemov
Information Security Management	Upravljanje varovanja informacij
ISO	Mednarodna organizacija za standarde
Information Technology Governance	Upravljanje informatike
ITGI	Inštitut za upravljanje informacijske tehnologije
IT	Informacijska tehnologija
ITIL	Zbirka napotkov za upravljanje in uvajanje storitev informacijske tehnologije
ITSM	Upravljanje storitev informacijske tehnologije
Incident Management	Upravljanje incidentov
ITGI	Inštitut za upravljanje informacijske tehnologije
ISACA	Mednarodno združenje za revizijo in kontrolo informacijskih sistemov
Key Goal Indicators	Ključni kazalniki ciljev
Key Performance Indicators	Ključni kazalniki poslovanja
Knowledge Management	Upravljanje z znanjem
OGC	Urad za trgovino britanske vlade
OECD	Organizacija za gospodarsko sodelovanje in razvoj
OLA	Raven operativne podpore
Problem Management	Upravljanje problemov
Release and Deployment Management	Upravljanje izvedb

se nadaljuje

nadaljevanje

Tuji izraz	**Slovenski prevod**
Request Fulfilment	Upravljanje z zahtevami
Risk Management	Upravljanje tveganj
Service Asset and Configuration Management	Upravljanje konfiguracij in sredstev storitev
Service Catalog Management	Upravljanje kataloga storitev
Service Design	Oblikovanje storitev
Service Level Agreement	Raven nivoja storitev
Service Level Management	Upravljanje ravni storitev
Service Operation	Izvajanje storitev
Service Strategy	Strategija storitev
Service Transition	Prehod storitev
Service Validation and Testing	Kontrola in testiranje storitev
Supplier Management	Upravljanje z dobavitelji
Transition Planing and Support	Planiranje in podpora prehoda storitev