Celoviti pristop izvedbe skrbnega pregleda informacijskega sistema

Boštjan Delak,[1] Marko Bajec[2]
[1] ITAD, revizija in svetovanje, d. o. o., Spodnji Brnik 93, 4207 Cerklje na Gorenjskem, PE Ljubljana – Pot za Brdom 100, 1000 Ljubljana, www.itad.si, bostjan.delak@itad.si
[2] Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Tržaška 25, 1000 Ljubljana, www.fri.uni-lj.si, marko.bajec@fri.uni-lj.si

Izvleček

Dandanes se večina podjetij srečuje z izzivi obvladovanja informacijske tehnologije (IT). Za uspešno pridobljeno informacijo o stanju informacijske tehnologije oz. o stanju celovitega informacijskega sistema (IS) nasploh lahko v podjetju izvedejo aktivnosti skrbnega pregleda informacijskega sistema. Prispevek opisuje definicije različnih tipov skrbnega pregleda informacijskega sistema in predstavi več mogočih načinov – orodij, metod, standardov, ogrodij, okvirov in metodologij – za izvedbo aktivnosti skrbnega pregleda. Na kratko je predstavljen tudi univerzalni celoviti pristop skrbnega pregleda informacijskega sistema, ki je nastal v Sloveniji na podlagi več skrbnih pregledov informacijskih sistemov, ki so se izvajali več desetletij v srednji in vzhodni Evropi. S tem pristopom je mogoče v zelo kratkem času izvesti skrbni pregled informacijskih sistemov v manjših in večjih podjetjih, saj je podana tabela časovnih obsegov izvedbe takih aktivnosti. Na koncu sledi tudi kratka primerjava posameznih načinov izvedbe skrbnih pregledov informacijskih sistemov glede na vsebino in tip.
Ključne besede: skrbni pregled, univerzalni celoviti pristop izvedbe skrbnega pregleda informacijskega sistema, začetni skrbni pregled.

Abstract

UNIVERSAL INFORMATION SYSTEM DUE DILIGENCE FRAMEWORK

Nowadays a majority of organizations face the issues of information technology (IT) governance. In order to obtain effective information on the status of information technology (IT) or information system (IS) in general, organizations may perform IS due diligence activities. The article outlines definitions of various IS due diligence types and presents several approaches to IS due diligence: tools, methods, standards, frameworks and methodologies. It gives a brief overview of universal IS due diligence framework, which was founded in Slovenia and based on more than ten years' experience of conducting several tens of IS due diligence frameworks in Central and Eastern Europe. With this framework IS due diligence may be conducted in a very short time in both, small or large-sized organizations, as shows the time table of activities attached to it. At the end of the article there is a short comparison of different IS due diligence approaches, depending on the content and type of IS due diligence.
Key words: due diligence, initial due diligence, universal information system due diligence framework.

1 UVOD

Informacijska tehnologija (IT) je vključena v večino procesov posameznega podjetja, zato je izredno pomembno obvladovanje tega pomembnega področja. ISACA (Information System Audit and Control Association) je pred leti opredelila obvladovanje informacijske tehnologije kot *»odgovornost poslovodstva in upravnega odbora. Sestoji iz vodenja organizacijskih struktur in vodenja procesov, ki zagotavljajo, da informacijska tehnologija podpira strategijo podjetja in zagotavlja realizacijo ciljev podjetja«* (ISACA, 2003, str. 11).

Pri tem je treba poudariti, da obvladovanje informacijske tehnologije ni osamljena aktivnost, temveč del celovitega obvladovanja podjetja, ki je usmerjeno na zaščito lastniške vrednosti in s tem na zmanjševanje tveganj, medtem ko je obvladovanje informacijske tehnologije razdeljeno na pet področij (ISACA, 2009, str. 10–11): na strateško uskladitev, ustvarjanje vrednosti, upravljanje tveganja, upravljanje virov ter merjenje izvedbe.

Za pridobitev trenutnega stanja informacijske tehnologije ter posledično tudi stopnje obvladovanja informacijske tehnologije oziroma celotnega informacijskega sistema v podjetju izvedemo skrbni pregled. V nadaljevanju je opisano, kaj je skrbni pregled, kakšne skrbne preglede poznamo, kakšni so mogoči načini izvedbe ter predlog univerzalnega celovitega pristopa izvedbe skrbnega pregleda.

Struktura prispevka je takšna:

- opis in definicija skrbnega pregleda,
- opis mogočih načinov pregleda,
- opis univerzalnega celovitega pristopa izvedbe skrbnega pregleda informacijskega sistema,
- kratka primerjava posameznih orodij in njihova mogoča uporaba,
- predstavitev hipoteze o uporabnosti tega okvira v različnih industrijah in usmeritev avtorjevih aktivnosti v prihodnje.

2 SKRBNI PREGLEDI

Kaj je sploh skrbni pregled oz. s tujko »due diligence«? Poglejmo si nekaj tolmačenj. Zelo osnovna je obrazložitev na Wikipedii (Wikipedia, 2010): *»Skrbni pregled je proces, ki omogoča potencialnemu vlagatelju oceniti ciljno podjetje pred kapitalskim vlaganjem.«*

Malo bolj finančno usmerjena obrazložitev je (Fitch, 1993, str. 207): *»Skrbni pregled – v podjetniškem združevanju in pridobivanju je podroben pregled poslovanja s ciljem pregleda premoženja in obvez ciljnega podjetja.«*

Islovar Slovenskega društva Informatika ima za to tujko tole obrazložitev (Islovar, 2010): *»Skrbni pregled je analiza stanja družbe/podjetja na določenem področju s ciljem, da se poda poslovodstvu oziroma naročniku realno informacijo na segmentu pregleda.«*

Za tujko »initial due diligence« pa ima Islovar Slovenskega društva Informatika tole obrazložitev (Islovar, 2010): *»Začetni skrbni pregled se izvede pred kapitalskim vlaganjem, združitvijo ali drugim poslovnim odnosom (npr. izločitvijo) – rezultat pregleda je lahko: se nadaljuje z aktivnostmi, se zaključi z aktivnostmi ali je potrebno pridobiti še dodatne informacije.«*

Glavni cilj skrbnega pregleda informacijskih sistemov je pridobiti čim več informacij o kakovosti in učinkovitosti njihovega delovanja, njihovih virih, dokumentaciji, tveganjih in procesih. Pri tem je treba pridobiti informacije o stanju in učinkovitosti sistema internih kontrol (kakovost kontrolnega okolja delovanja informacijskega sistema) in o tveganjih na področju informacijskega sistema. Za vsa področja skrbnega pregleda je treba oceniti kakovost poročil, ki jih pripravi informacijska tehnologija zaradi ocenitve verodostojnost podatkov in stopnje tveganja zanašanja na informacije iz teh poročil.

Lahko bi ocenili, da je skrbni pregled informacijskega sistema podoben splošnemu revizijskem pregledu delovanja informacijskega sistema v podjetju. Ločimo več načinov skrbnih pregledov:

»Začetni« skrbni pregled, ki se izvede pred kapitalskim vlaganjem in je osnova za poslovne odločitve o tem, ali se nadaljujejo aktivnosti vlaganj ali ne. Pobudo za začetek aktivnosti podata lastnik podjetja oz. nadzorni svet (Delak, 2008).

»Navadni« skrbni pregled – analiza stanja glede na strategijo podjetja in taktične načrte – se lahko izvede kadar koli. Tako odločitev sprejmeta lastnik oz. nadzorni svet podjetja. Rezultat skrbnega pregleda omogoči lastniku, da sprejme in izvede določene poslovne strateške odločitve.

»Tehnološki« skrbni pregled, ki se izvede pred odločitvijo, ali se določena tehnologija vpelje ali ne. Pobudo za začetek aktivnosti podata izvršni direktor informatike ali izvršni direktor tehnologije (Andriola, 2009, str. ix).

Skrbni pregled »ponudnika izločanja informatike« ali »ponudnika zunanjega izvajanja«, ki se izvede pred samo odločitvijo o izločitvi določenih aktivnosti zunanjemu izvajalcu. Pobudo za začetek aktivnosti poda izvršni direktor za operativo ali izvršni direktor za nabave. Priporoča se, da se ta aktivnost izvaja periodično tudi po sprejemu odločitve o izločitvi (Bayuk, 2009, str. 34–38).

Vsi ti načini imajo veliko skupnega, a se razlikujejo predvsem po tem, kdo je naročnik in kakšni so cilji pregleda.

3 MOGOČI NAČINI IZVEDBE

V svetu ni enotne usmeritve za izvajanje aktivnosti skrbnega pregleda informacijskih sistemov. Obstaja kar nekaj načinov, standardov, metodologij in dobrih praks za izvedbo teh nalog. Pred leti so na univerzi v Austinu (ZDA) razvili tudi okvir – celoviti pristop, ki pa se v praksi ni oprijel. Mogoči načini izvedbe skrbnih pregledov so (razvrščeni po abecedi):

Analiza upravljanja neprekinjenega poslovanja – BCM (Business Continuity Management)/BS25999 BCM standard. Upravljanje neprekinjenega poslovanja je eno najbolj pomembnih procesov v sodobnih podjetjih, ki je tudi določeno z obveznimi principi, izdanimi od različnih globalnih regulatorjev (npr. za finančne ustanove z BASEL II, za zavarovalne ustanove s SOLVENCY II itn.). Business Continuity Institute je izdal deset glavnih domen za to področje (BCI, 2003). Pred nekaj leti je bil Publicly Available Specification 56 (PAS 56) primerno orodje za akreditacijo upravljanja neprekinjenega poslovanja. Britanski in-

štitut za standardizacijo je vključil osnove PAS 56 v standard BS25999 BCM standard.

Andriolova predloga za skrbne preglede. Njegova predloga za skrbne preglede izvajalcev se nanaša na planiranje pregleda, izvedbo in rezultate (Andriole, 2009). Za izvedbo takega skrbnega pregleda je avtor pripravil petnajst različnih kriterijev, po katerih ocenjuje posamezne možnosti uporabe in implementacije nove tehnologije.

Bingov seznam za skrbne preglede. Gordon Bing je določil skupine vprašanj za področje informacijske tehnologije in interneta za skrbne preglede (Bing, 2008, str. 105–110). Njegov seznam za skrbne preglede je splošen in namenjen izključno izvedbi skrbnih pregledov informacijskih sistemov.

INFAUDITOR je ekspertni sistem za revizijo informacijskih sistemov (Akoka in Comyn-Wattiau, 1996, str. 361–375). INFAUDITOR pomaga revizorjem informacijskih sistemov pri vsakem koraku revizijskega procesa.

ISO/IEC 9000 je družina standardov za sistem upravljanja kakovosti, ki ga je izdala mednarodna organizacija za standardizacijo (ISO). Skozi leta je več industrij razvilo več različnih tolmačenj – različic iz osnove 9001. Za informacijsko tehnologijo so tako razvili različico TickIT, ki se prilagaja procesom informacijskih sistemov, še posebno procesom razvoja programske opreme.

ISO/IEC 20000 je družina standardov za upravljanja s storitvami informacijske tehnologije. Sestavljata ga dva dela. Prvi del podpira prisvojitev integriranega procesa približevanja učinkoviti izročitvi upravljanja storitev s ciljem, da se dosežejo zahteve (poslovne ali uporabniške). Drugi del je kodeks prakse in opisuje dobre prakse – izkušnje, kako realizirati prvi del ISO 20000.

ISO/IEC 27000 je družina standardov v zvezi s SUVI – sistemom upravljanja varovanja informacij. Skupno bo izdanih več kot deset standardov, povezanih s tem področjem. Za analizo informacijskih sistemov so že izdali pet standardov, ki so nujno potrebni in pomembni. Med objavljenimi so tudi ISO/IEC 27001 – specifikacija SUVI, ki je zamenjal predhodni BS 7799 drugi del; ISO/IEC kodeks prakse, ki opisuje 133 sorodnih kontrol, in ISO/IEC, ki opredeljuje upravljanje tveganja SUVI.

KnowledgeLeaderjev seznam skrbnih pregledov. KnowledgeLeader so naročniške internetne strani, ki jih ponuja podjetje Protiviti. Na teh straneh ponujajo programe revizij, kontrolne sezname, orodja, pripomočke in dobre prakse za interne revizorje in vodje upravljanj s tveganji ter obsežen kontrolni seznam za poslovne skrbne preglede in tudi za skrbne preglede informacijske tehnologije (KnowledgeLeader, 2010).

Kontrolni cilji za informacijsko in sorodno tehnologijo – COBIT (Control Objective for Information and related Technology – verzija 4.1). Za uspešno obvladovanje informacijske tehnologije je pomembno upoštevati aktivnosti in tveganja v IT, ki jih je treba upravljati. Metodologija COBIT vsebuje štiri domene s 34 IT-procesi in njihovimi pripadajočimi kontrolnimi cilji (ITGI, 2008). Metodologijo COBIT globalno uporabljajo revizorji informacijskih sistemov pri izvajanju aktivnosti revizij informacijske tehnologije. Kontrolni cilji za informacijsko in sorodno tehnologijo so tudi prevedeni v slovenski jezik. Te aktivnosti je izvedel slovenski odsek ISACA (Information System Audit and Control Association) pri Slovenskem inštitutu za revizijo. ISACA z ITGI (IT Governance Institute) sta za prihodnje leto že napovedala izdajo nove verzije COBIT 5.

Metoda ocenjevanja tveganj informacijskih sistemov je ključnega pomena. Obstaja nekaj različnih metod. CRAMM (CCTA Risk Analysis and Management Method) program ponuja nekaj možnosti za analizo kakovosti varnostnih tveganj in upravljanja le-teh.

Siscov seznam za skrbne preglede. Mike Sisco je definiral ključne cilje za izvedbo skrbnih pregledov informacijske tehnologije (Sisco, 2002). Večina njegovih napotkov za to izvedbo je objavljena na straneh TechRepublic (TechRepublic).

Ogrodje za ocenjevanje skrbnega pregleda informacijske tehnologije – ITADD (Information Technology Assessment Due Diligence Framework). Ta okvir omogoča vodjem informacijske tehnologije jasno metodo izvedbe ocenitve skrbnega pregleda za IT funkcionalnosti podjetja, ki so predmet združevanja ali prevzema (Sundberg et al., 2006). ITADD je več kot okvir, sestavljata ga metodologija ITADD in orodjarna ITADD (Baublits et al., 2005). Nastal je v okviru študijskega projekta na poslovni šoli Red Mc Combs v okviru univerze v Austinu, Teksas, ZDA.

Ogrodje za upravljanje s tveganji informacijske tehnologije temelji na nizu smernic za učinkovito obvladovanje in upravljanje tveganj informacijske tehnologije (ITIG, 2009). Ogrodje za upravljanje s tveganji informacijske tehnologije sestavljajo tri po-

dročja oz. procesi: obvladovanje tveganj, ocenjevanje tveganj in odziv na tveganja. Podobno kot za COBIT in vrednost informacijske tehnologije ima tudi ogrodje za upravljanje s tveganji informacijske tehnologije zrelostni model za vsak proces.

Ogrodje za zagotavljanje jamstva informacijske tehnologije – ITAF (Information Technology Assurance Framework) je profesionalno praktično ogrodje za izvajanje revizijskih procesov, ki ga je izdala ISACA v letu 2008 in določa smernice za načrtovanje ciljev, izvedbe in poročanje revizij informacijske tehnologije (ISACA, 2008).

Pickardov seznam za skrbne preglede vsebuje več kot 2000 vprašanj za skrbni pregled, zbranih v 14 funkcionalnih področij poslovanja (Pickard, 2002). Podobno kot Bing je Pickard pripravil vprašanja za različna področja poslovanja in ne samo za informacijsko tehnologijo.

Sistem uravnoteženih kazalnikov – BSC (Balance Score Card) je sistem za vodenje učinkovitosti, ki omogoča podjetjem, da vodijo svojo strategijo na meritvah in spremljavi aktivnosti. Metodologija sistema uravnoteženih kazalnikov temelji na meritvah in sistemu upravljanja, ki je zelo primeren za podporo procesa obvladovanja informatike (Van Grembergen, 2000).

Univerzalni celoviti pristop izvedbe skrbnih pregledov IS – UISDDFW (Universal Information System Due Diligence Framework) je celovit pristop, ki je nastal v Sloveniji in je na kratko opisan v nadaljevanju tega prispevka.

Vrednost informacijske tehnologije – (Val IT) razširja in dopolnjuje COBIT z obsežnim naborom kontrol za ogrodje upravljanja informacijske tehnologije. Osredinja se na odločanje o investicijah in realizacijo koristi (ITGI, 2008). Vrednost informacijske tehnologije je v pomoč poslovodstvu in strokovnjakom pri ustvarjanju vrednosti informacijske tehnologije. Le-to definira več procesov, ki so s posameznimi procesi, skupno jih je 22, združeni v tri področja: obvladovanje vrednosti, upravljanje portfelja in upravljanje investicij. Podobno kot za COBIT in ogrodje za upravljanje s tveganji informacijske tehnologije ima tudi vrednost informacijske tehnologije zrelostni model za vsako področje.

Zbirka napotkov za upravljanje in uvajanje storitev informacijske tehnologije – ITIL (Information Technology Infrastructure Library) je bila ustvarjena v Evropi pred več kot 20 leti kot zbirka dobrih praks za upravljanje storitev informacijske tehnologije. ITIL je ogrodje za uspešno uvajanje informacijske tehnologije storitvenih procesov in jo sestavlja pet domen: strategija storitev, načrtovanje storitev, preoblikovanje storitev, izvajanje storitev in nenehno izboljševanje storitev.

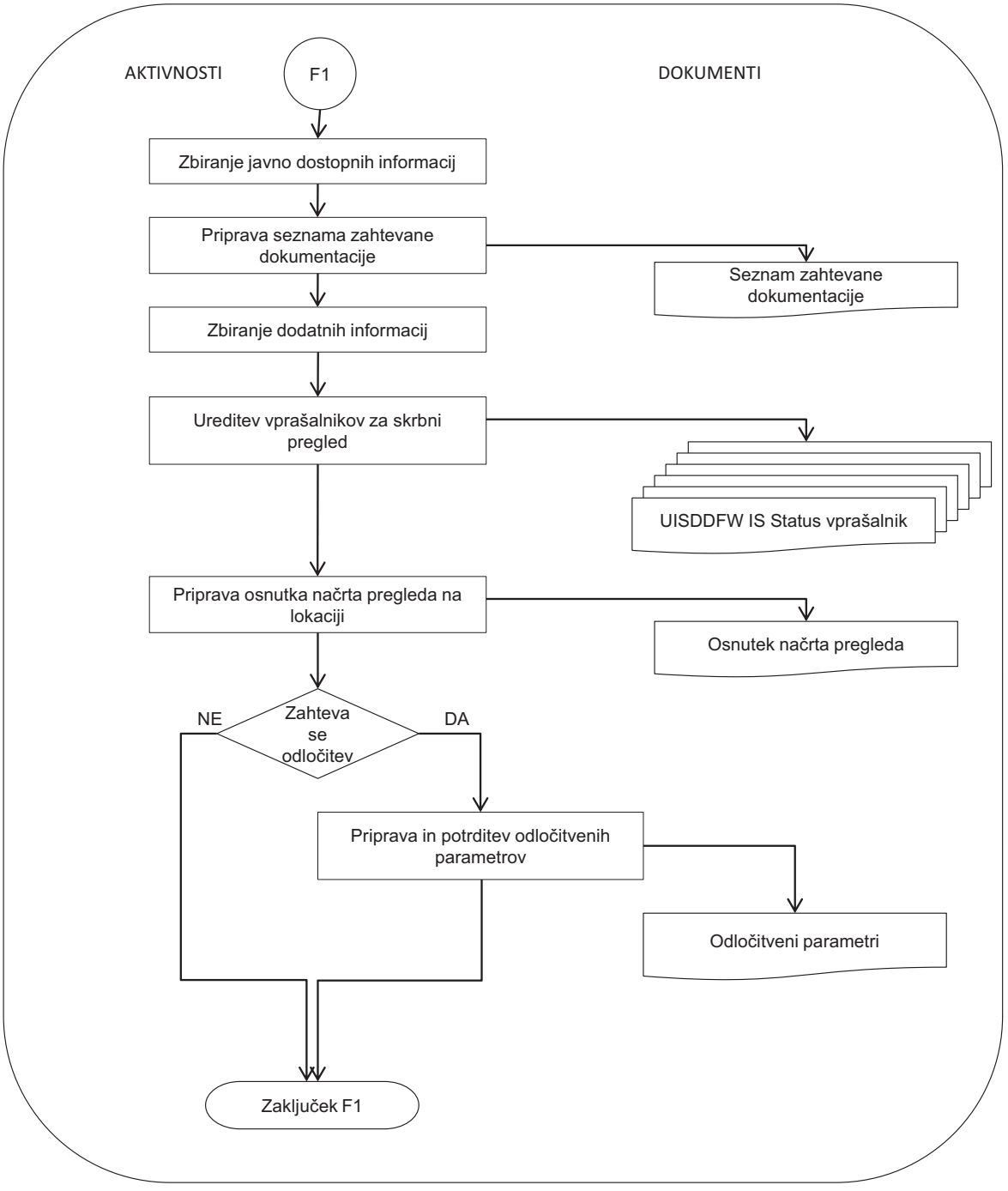
Zmožnostno zrelostni model – CMM (Capability Maturity Model) je največkrat uporabljen za izboljšanje in kakovostno ter učinkovito ocenitev procesa razvoja programske opreme v podjetju. Je zrelostni model oz. celovit pristop, ki pomaga podjetju izboljšati proces življenjskega cikla programske opreme. Zmožnostni model se lahko uporablja za druge procese v drugih modelih in metodologijah (npr. COBIT).

V zadnjih sedmih ali osmih letih avtorjema ni uspelo identificirati drugih načinov. Zavedava se, da verjetno obstajajo še druge metode in orodja za učinkovito izvedbo skrbnega pregleda informacijskih sistemov. Nekatera večja globalna podjetja, ki se ukvarjajo z revizijo, ter tudi nekatera globalna svetovalna podjetja so razvila svoje lastne pristope, a jih niso objavila oz. niso omogočila javnega dostopa do njih. Prav tako ni veliko znanstvenih prispevkov na temo skrbnih pregledov informacijskih sistemov.

4 CELOVIT PROCES ZA SKRBNE PREGLEDE

S skrbnimi pregledi informacijskih sistemov se avtor ukvarja že več kot deset let. V tem času je izvedel več kot 40 navadnih in več kot 25 začetnih skrbnih pregledov informacijskih sistemov v 15 državah srednje in vzhodne Evrope. Skozi prakso so nastajali vprašalniki, vzpostavljal se je proces in celovit pristop, ki je nastal pred tremi leti. V okviru univerzalnega celovitega pristopa izvedbe skrbnega pregleda informacijskega sistema – UISDDFW (Universal Information System Due Diligence Framework) je opisan proces izvedbe skrbnega pregleda, ki ga sestavljajo štiri faze (priprava, pregled na lokaciji, analiza in odločitev). V nadaljevanju je na kratko predstavljena vsaka faza.

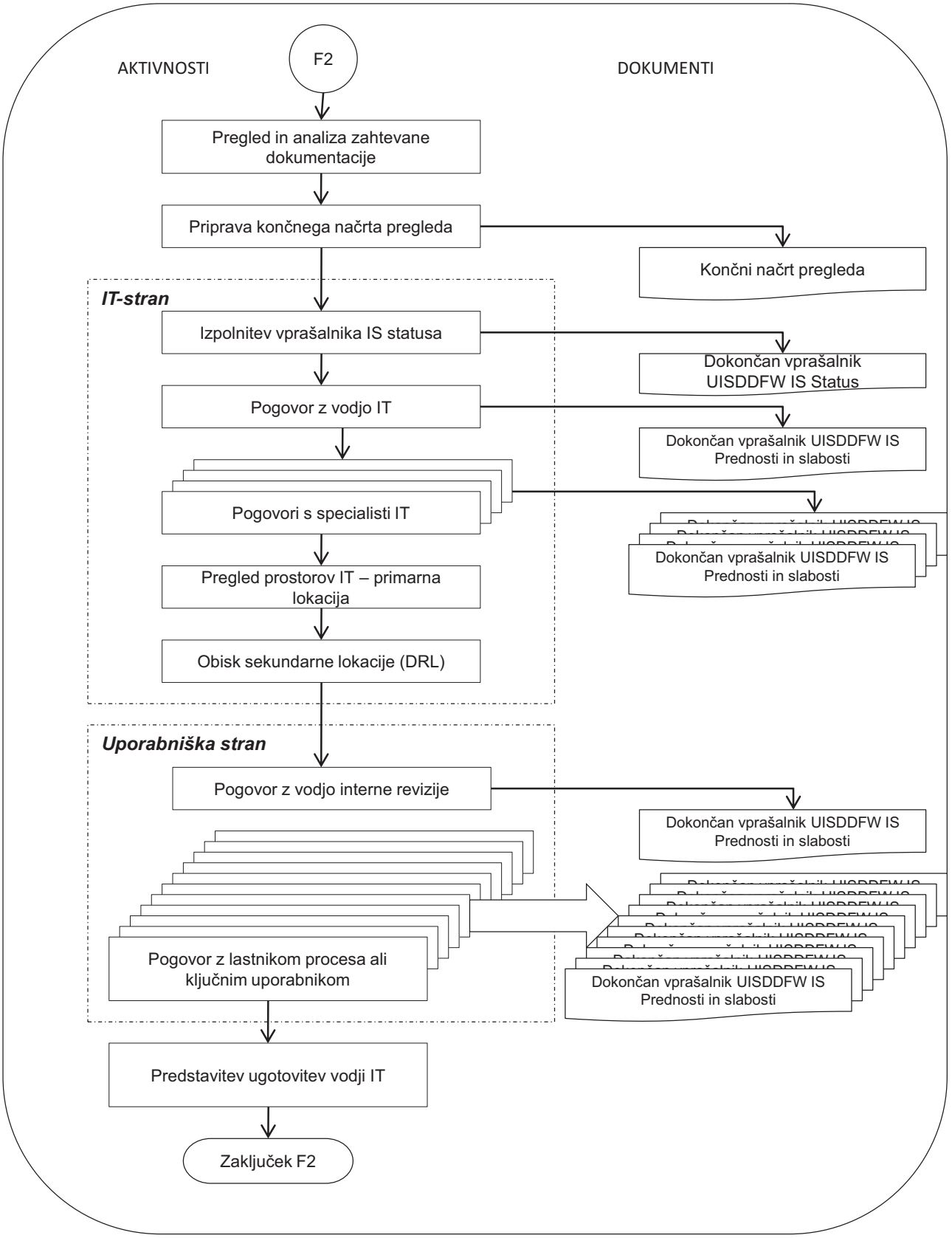
Prvo fazo – pripravo – sestavljajo te aktivnosti: pridobivanje javnih informacij, priprava seznama zahtevane dokumentacije, pridobivanje drugih informacij o podjetju, prilagoditev vprašalnikov skrbnega pregleda, določitev odločitvenih parametrov (v primeru začetnega skrbnega pregleda ali skrbnega pregleda ponudnika izločanja informatike) s strani vodstva ali lastnikov, priprava grobega načrta pregleda na lokaciji ter administrativne zadeve (podpis dogovora o varovanju poslovne skrivnosti) in logistika. Grafični opis te faze je prikazan na sliki 1.



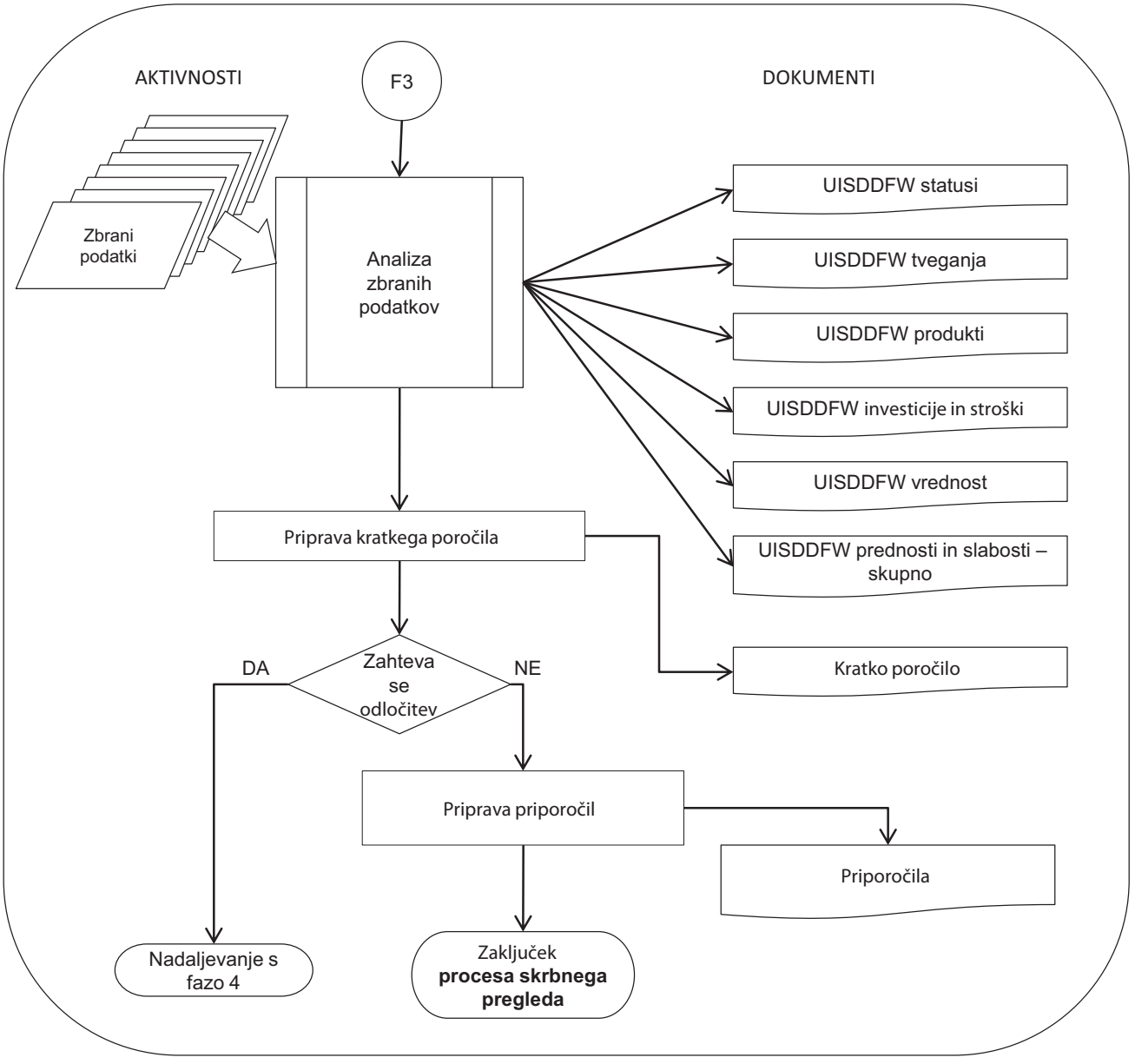
Slika 1: **Grafični prikaz prve faze**

Druga faza – pregled na lokaciji – vključuje te aktivnosti: pregled posredovane dokumentacije, priprava podrobnega načrta pregleda, pregled in pogovori s predstavniki informacijske tehnologije, pregled in pogovori s predstavniki uporabnikov (lastniki procesov in aplikacij) ter kratko poročilo lokalnemu vodji informacijske tehnologije. Grafični opis te faze je prikazan na sliki 2.

Tretja faza – analiza – vključuje dve aktivnosti, to sta analiza pridobljenih podatkov in priprava kratkega poročila. Grafični opis te faze je prikazan na sliki 3.



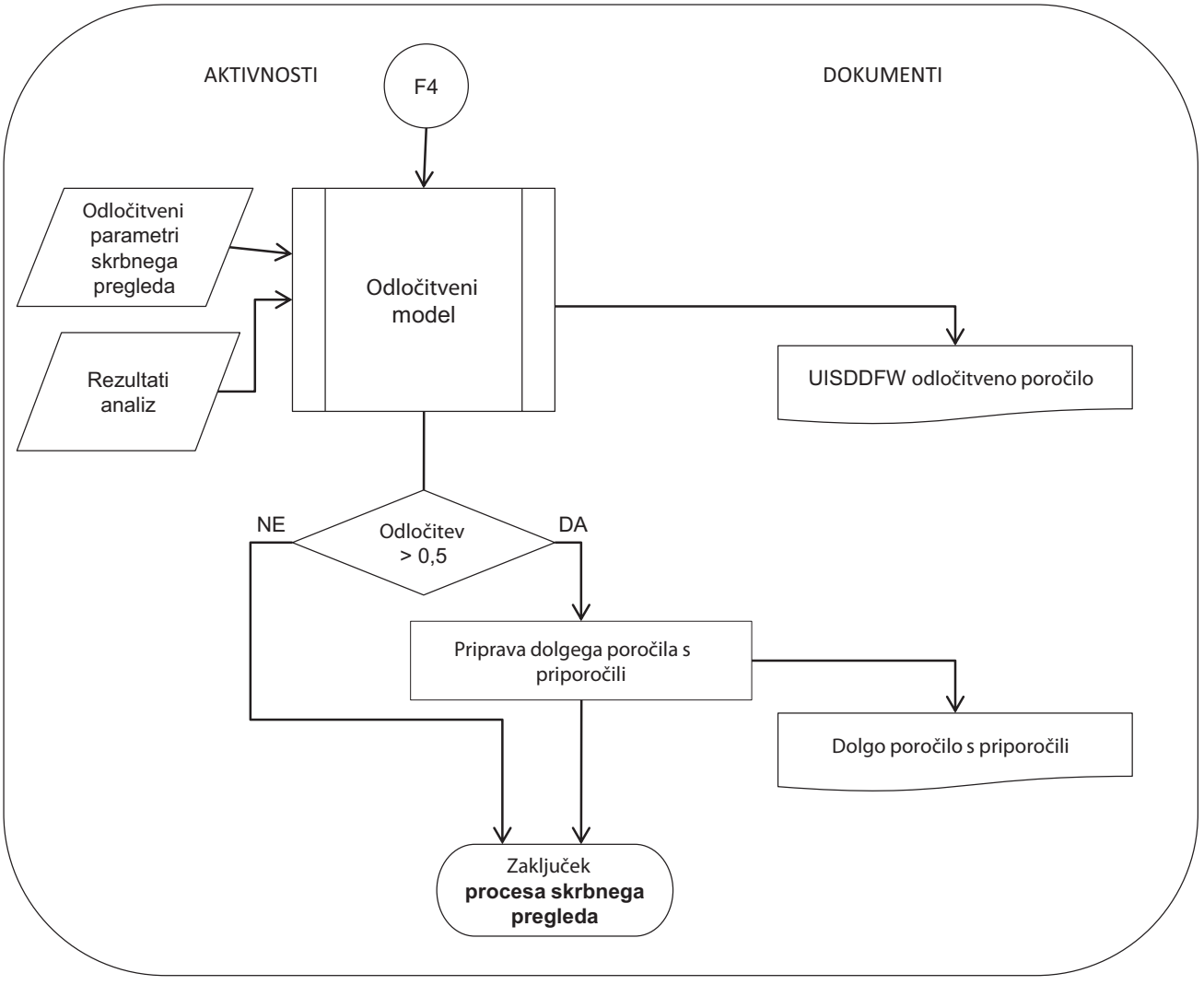
Slika 2: **Grafični prikaz druge faze**



Slika 3: **Grafični prikaz tretje faze**

Zadnja, četrta faza – odločitev – ima dve aktivnosti: vnos analiziranih podatkov v odločitveni model ter pripravo daljšega poročila (v primeru pozitivnega odgovora odločitvenega modela). Grafični opis te faze je prikazan na sliki 4.

Te štiri faze se uporabljajo pri začetnih skrbnih pregledih informacijskih sistemov ter skrbnih pregledih ponudnikov informacijskih sistemov. Pri splošnih skrbnih pregledih informacijskih sistemov ter tehnoloških skrbnih pregledih informacijskih sistemov se uporabljajo samo prve tri faze. V sklopu celovitega pristopa je pripravljeno večje število vprašalnikov, med katerimi so najbolj pomembni: UISDDFW IS statusni vprašalnik, UISDDFW IS vrednotenje, investicije in stroški, UISDDFW produkti podjetja ter USIDDFW prednosti in slabosti informacijskega sistema. Trenutno so ti dokumenti pripravljeni za slovenski in angleški jezik.



Slika 4: **Grafični prikaz četrte faze**

Prav tako so v sklopu celovitega pristopa izvedbe skrbnega pregleda pripravljeni tudi vzorci različnih poročil ter enostaven odločitveni model. Vhodni parametri odločitvenega modela so: a) predhodno določeni odločitveni parametri, ki jih potrdi vodstvo oz. naročnik skrbnega pregleda pred samo izvedbo pregleda, ter b) z analizo pridobljeni podatki. Izhodni parameter odločitvenega modela je numerična vrednost 0 ali 1. Če je rezultat 1, za začetni skrbni pregled informacijskega sistema ali za skrbni pregled ponudnika izločanja informacijskega sistema predlagamo nadaljevanje aktivnosti, to pomeni nadaljevanje pogajanj. V nasprotnem primeru pa se aktivnosti končajo, to pomeni, da se opustijo pogovori s tem podjetjem.

Ta univerzalni celoviti pristop je bil tudi testiran v praksi v treh finančnih organizacijah v srednji in vzhodni Evropi za začetne in splošne skrbne preglede informacijskih sistemov.

V primerjavi z drugimi načini ta univerzalni celoviti pristop omogoča v kratkem času pridobiti informacijo, ki jo zahteva nalogodajalec. V tabeli 1 je opisan čas, potreben za izvedbo skrbnega pregleda informacijskega sistema. Ti podatki veljajo za preglede, pri katerih komunikacija med izvajalci skrbnega pregleda in predstavniki pregledovanega podjetja ni ovira. Če je treba vključiti prevajalce, se čas ustrezno podaljša.

Pri tem je treba upoštevati, da mora imeti izvajalec skrbnega pregleda praktične izkušnje z analizami informacijskih sistemov. Priporočamo, da je to revizor informacijskih sistemov ali preizkušen revizor informacijskih sistemov z večletno prakso.

Tabela 1: **Čas izvedbe skrbnega pregleda informacijskega sistema po UISSDDFW**

Tip	Velikost pregledovanega podjetja	Minimalno število dni	Maksimalno število dni	Število dni na lokaciji
A	Do 150 zaposlenih, ena glavna lokacija in do 3 druge lokacije	13	17	5
B	Od 150 do 350 zaposlenih, ena glavna lokacija in do 5 drugih lokacij	18	22	7
C	Od 350 do 750 zaposlenih, 2 do 4 večje lokacije in od 5 do 15 drugih lokacij	25	29	9
D	Od 750 do 2000 zaposlenih, 3 do 5 večjih lokacij in od 15 do 30 drugih lokacij	30	35	11
E	Od 2000 do 3500 zaposlenih, 5 do 7 večjih lokacij in od 30 do 50 drugih lokacij	36	44	15
F	Od 3500 do 6000 zaposlenih, 7 do 10 večjih lokacij in od 50 do 75 drugih lokacij	49	61	21
G	Od 6000 do 10000 zaposlenih, 10 do 15 večjih lokacij in od 75 do 100 drugih lokacij	69	85	29
H	Več kot 10000 zaposlenih, več kot 15 večjih lokacij in več kot 100 drugih lokacij	88	112	36

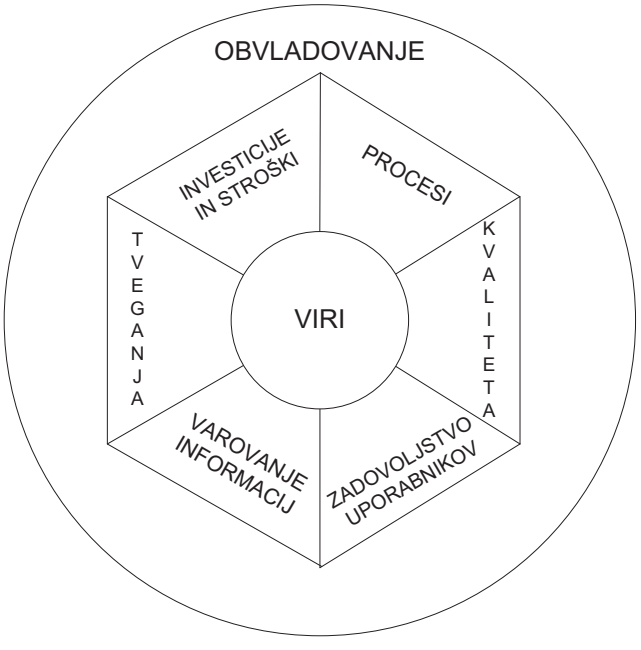
Predvideno število dni za skrbni pregled je odvisno od velikosti podjetja. Glede na izkušnje pri do sedaj izvedenih skrbnih pregledih v srednji in vzhodni Evropi se čas za izvedbo enako velikega podjetja lahko razlikuje v obsegu dni zaradi kakovosti in obsega dokumentacije informacijskega sistema ter glede na stopnjo pripravljenosti odgovarjanja sogovornikov (minimalno/maksimalno število dni). Podatki v tabeli 1 so nastali na podlagi izkušenj dosedanjih izvedenih skrbnih pregledov.

5 PRIMERJAVA

V tretjem razdelku tega prispevka navajamo nekaj orodij, metod, standardov, metodologij in ogrodij za izvedbe skrbnih pregledov informacijskih sistemov. Vsak od navedenih načinov je kakovosten in uporaben za določena področja. Uporaba določenega načina je v največji meri odvisna od predznanja in izkušenj izvajalca skrbnega pregleda informacijskega sistema. Priporočamo, da skrbne preglede informacijskih sistemov izvaja več strokovnjakov z bogatimi izkušnjami pri analizah informacijskih sistemov ter revidiranju informacijskih sistemov.

Slika 5 prikazuje parametre, ki so podlaga za primerjavo posameznih načinov. V skupino obvladovanje uvrščamo upravljanje informacijskega sistema, vodenje informacijskega sistema, produkcijo informacijskega sistema in kontrole v informacijskem sistemu. Procesi so povezani z informacijskim sistemom. Med vire uvrščava aplikacije (aplikacijsko programsko opremo), informacije iz informacijskega sistema, infrastrukturo informacijskega sistema, ljudi v informatiki in projekte, povezane z informacijskim sistemom. Sledijo investicije in stroški, povezani z informacijskim sistemom. Kakovost informacijskega sistema je vezana na posamezne parametre primerjave. Naslednji parameter so tveganja, povezana z informacijskim sistemom. Sledi področje varovanja informacij in na koncu še zadovoljstvo uporabnikov informacijskega sistema.

V tabeli 2 je primerjava posameznih načinov glede na vsebino pridobljenih podatkov.



Slika 5: **Parametri za primerjavo med posameznih načinov**

Tabela 2: **Primerjava posameznih načinov glede na vsebino pridobljenih podatkov**

Ogrodja, metode, metodologije, standardi, orodja	Obvladovanje: upravljanje, vodenje, produkcija, kontrole	Procesi	Viri: aplikacija, informacije, infrastruktura, ljudje, projekti	Investicije in stroški	Kakovost	Tveganja	Varovanja informacij	Zadovoljstvo uporabnikov
Analiza upravljanja neprekinjenega poslovanja (BCM / BS2599 BCM Standard)	**	**	**			**		
Andriolova predloga za skrbne preglede	*	*	**	**	*	*	*	
Bingov seznam za skrbne preglede	**		**		*		*	*
INFAUDITOR	*	**	**		*	*	*	*
ISO/IEC 9001	**	**	*		***			**
ISO/IEC 20000	**	***	*		*			*
ISO/IEC 27000	***	*	***			***	***	
KnowledgeLeaderjev seznam skrbnih pregledov	**	**	***	***	*	***	***	**
Kontrolni cilji za informacijsko in sorodno tehnologijo (COBIT 4.1)	***	**	*	*	**	**	**	
Mike Siscov seznam za skrbne preglede	*	*	**	*		*		
Ogrodje za ocenjevanje skrbnih pregledov (ITADD)	**	*	***	**	*	**	**	*
Ogrodje za tveganja IT (Risk IT)	***	**	*	*		***	*	
Ogrodje za zagotavljanje jamstva IT (ITAF)	***	**	*	*		***	*	
Pickardov seznam za skrbne preglede	**	*	**		*	**	*	
Sistem uravnoteženih kazalnikov (BSC)	*	**	*	*				
Univerzalni celoviti pristop izvedbe skrbnih pregledov IS (UISDDFW)	***	**	***	***	**	**	***	***
Vrednost IT (*Val IT* 2.0)	***	**	**	***	*	**		
Zbirka napotkov za upravljanje in uvajanje storitev IT (ITIL 3.0)	**	***	*		**	**	**	*
Zmožnostno zrelostni model (CMM)	**	**	**		*			

V tabeli so mogoče te oznake primernosti: visoka – ***, srednja – **, nizka – * ter prazno, če določeni parameter ni primeren oz. ni uporaben za določen način.

Nekateri načini opisujejo tudi postopek izvedbe aktivnosti. Avtorja sta razdelila načine v tri sklope. Podroben opis postopkov omogočajo tele metode: ogrodje za ocenjevanje skrbnih pregledov (ITADD), KnowledgeLeaderjev seznam skrbnih pregledov in univerzalni celoviti pristop izvedbe skrbnih pregledov informacijskih sistemov (UISDDFW). Grobi opis postopkov nudijo Mike Siscov, Bingov in Picardov seznam za skrbne preglede. Drugi načini ne dajejo opisa postopkov izvedbe aktivnosti skrbnih pregledov informacijskih sistemov.

Nekatere načine je mogoče učinkoviteje uporabiti pri različnih tipih skrbnih pregledov informacijskih sistemov. V tabeli 3 je primerjava posameznih načinov glede na štiri mogoče načine: začetni skrbni pregled, splošni skrbni pregled, skrbni pregled ponudnika izločanja informatike oz. zunanje izvajanje informatike in tehnološki skrbni pregled.

Tabela 3: **Možnost uporabe določenega načina za določen tip pregleda**

Ogrodja, metode, orodja, metodologije, standardi	**Začetni skrbni pregled**	**Splošni skrbni pregled**	**Skrbni pregled ponudnika zunanjega izvajalca**	**Tehnološki skrbni pregled**
Analiza upravljanja neprekinjenega poslovanja (BCM / BS2599 BCM Standard)	*	*	*	
Andriolova predloga za skrbne preglede	*	*	**	***
Bingov seznam za skrbne preglede	*	*	*	*
INFAUDITOR		*	*	
ISO/IEC 9001	*	*	*	
ISO/IEC 20000	**	**	*	
ISO/IEC 27000	**	**	**	*
KnowledgeLeaderjev seznam skrbnih pregledov	***	*	*	
Kontrolni cilji za informacijsko in sorodno tehnologijo (COBIT 4.1)	*	*	*	
Mike Siscov seznam za skrbne preglede	*	*	*	
Ogrodje za ocenjevanje skrbnih pregledov (ITADD)	***	***	*	
Ogrodje za tveganja IT (Risk IT)	*	*	*	*
Ogrodje za zagotavljanje jamstva IT (ITAF)		**	**	
Pickardov seznam za skrbne preglede	*	*	*	*
Sistem uravnoteženih kazalnikov (BSC)		*	*	
Univerzalni celovit pristop izvedbe skrbnih pregledov IS (UISDDFW)	***	***	**	*
Vrednost IT (*Val IT* 2.0)	*	*	*	*
Zbirka napotkov za upravljanje in uvajanje storitev IT (ITIL 3.0)	**	**	*	*
Zmožnostno zrelostni model (CMM)		*	*	

Na kratko sva opisala grobe primerjave posameznih načinov, bralec pa si lahko ustvari svoj pogled, saj ima lahko drugačno mnenje glede na svoje morebitne bogate izkušnje, ki jih ima s kakšnim od navedenih načinov.

6 SKLEP

Skrbni pregled informacijskega sistema je analiza informacijskega sistema s cilji pridobitve informacij o trenutnem stanju informacijskega sistema, sredstvih, skladnosti delovanja in dokumentacije, upravljanju s tveganji in zadovoljstvu uporabnikov. Skrbni pregled informacijskega sistema je podoben splošnemu revizijskemu pregledu le-tega. V primerjavi z revidiranjem informacijskega sistema so cilji pri skrbnem pregledu mnogo širši.

Naključni bralec bo morda sklepal, da je skrbni pregled informacijskega sistema preprosto opravilo, vendar praktične izkušnje kažejo, da je to zelo zahtevna in kompleksna naloga. Z uporabo univerzalnega celovitega pristopa skrbnega pregleda informacijskega sistema, opisanega v tem prispevku, je izvedba bolj preprosta, saj celoviti pristop daje »kuharski recept« za izvedbo teh aktivnosti.

Različni načini – nekateri so omenjeni tudi v tem prispevku – omogočajo ožjo ali širšo analizo informacijskega sistema pregledovanega podjetja, univerzalni celoviti pristop pa omogoča globalno izvedbo aktivnosti. V prihodnje nameravata avtorja prispevka preizkusiti in potrditi univerzalnost celovitega pristopa v različnih industrijah in izvesti skrbni pregled po predlaganem načinu morda tudi zunaj meja srednje in vzhodne Evrope.

V Sloveniji smo tak pregled že ponudili več podjetjem. Na začetku je precej zanimanja, ko pa interesente obvestimo, katere dokumente in podatke želimo pridobiti in analizirati, se zanimanje hitro zmanjša. Ocenjujeva, da v Sloveniji v tem trenutku ni po-

sebno velikega zanimanja za tako podrobno analizo informacijskega sistema, a verjameva, da bo prišel tudi čas, ko bodo lastniki in potencialni vlagatelji želeli pridobiti informacije o stanju informacijskega sistema v organizaciji.

8 VIRI IN LITERATURA

[1] AKOKA Jacky, COMYN-WATTIAU, Isabelle: A Knowledge--Based System for Auditing Computer and Management Information Systems, Expert Systems With Applications, 1996, št. 3, str. 261–375.

[2] ANDRIOLE, J. Stephen: Technology Due Diligence, Best Practices for Chief Information Officers, Venture Capitalists, and Technology Vendors; Information Science Reference, 2009, ISBN 987-1-60566-018-9.

[3] BAUBLITS, Trey, LEE, Hae Joon, STANIS, Grant, SUNDBERG, Barrett., TAN, Zheng-Da: Development of an IT Assessment Program for Acquisition. Final Report of the student project in the IT Audit and Security Course at the Red McCombs Business School of the University of Texas at Austin (USA), 2005.

[4] BAYUK, Jennifer: Vendor Due Diligence, ISACA Journal, 2009, št.3, str. 34–38.

[5] BCI: The ten certification standard for Business Continuity Practitioners, Business Continuity Institute, 2003.

[6] BING Gordon: Due Diligence Planning Questions, Issues; Praeger Publishers, 2008, ISBN 978-0-313-34540-1, str. 105–110.

[7] DELAK, Boštjan: Initial Due Diligence of Information Technology as Risk Identification before Capital Investment in Finance Industry, Zbornik referatov: Doctoral Consortium, 20. konferenca: Advanced Information System Engineering, 2008, Montpellier.

[8] FITCH, P. Thomas: Dictionary of Banking Terms 2nd edition, Barron's Educational Series, 1993 – ISBN 0-8120-1530-4, str. 207.

[9] GATTIKER, E. Urs: Merger and Acquisition – Effective Information Security Depends on Security Metrics, Information System Control Journal, 2007, št. 5, str. 51–56.

[10] ISACA: ITAF – A Professional Practices Framework for IT Assurance, ISACA, 2008, ISBN 978-1-60420-036-2.

[11] ISACA, Board Briefing on IT Governance, 2nd Edition, USA, 2003, ISBN 1-893209-64-4.

[12] ISACA, Implementing and Continually Improving IT Governance, USA, 2009, ISBN 978-1-60420-119-2.

[13] Islovar: http://www.islovar.org/izpisclanka.asp?id=9302 geslo = due diligence (na dan 15. 8. 2010).

[14] Islovar: http://www.islovar.org/izpisclanka.asp?id=9303 geslo = initial due diligence (na dan 15. 8. 2010).

[15] ITGI: COBIT 4.1: Control Objectives for Information and Related Technology, IT Governance Institute, 2008; prevod Slovenski odsek ISACA pri Slovenskem inštitutu za revizijo leta 2009 (www.si-revizija/isaca (na dan 15. 8. 2010)).

[16] ITIG: Enterprise Value: Governance of IT Investments – The Val IT Framework 2.0, IT Governance Institute, 2008.

[17] ITIG: Enterprise Risk: Identify, Govern and Manage IT Risk, The IT Risk Framework, exposure draft, IT Governance Institute, 2009.

[18] KnowledgeLeader: http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/CLITDueDiligence!OpenDocument (na dan 15. 8. 2010).

[18] PICKARD, Scott. S.: Due Diligence List, Writers Club Press, 2002, ISBN 0-595-26130-2.

[19] SISCO Mike: The art of technology due diligence, TechRepublic, 2002, http://articles.techrepublic.com.com/5100-10878_11-1038683.html (na dan 15. 8. 2010).

[20] SUNDBERG, Barrett, TAN, Zheng-Da, BAUBLITS, Trey, STANIS, Grant, TANRIVERDI, Huseyin: A Framework for Conducting IT Due Diligence in Mergers and Acquisitions. ISACA Information System Control Journal, 2006, št. Online 6.

[21] TechRepublic: http://techrepublic.com.com/5100-10878_11-1040541.html?tag=content;leftCol (na dan 15. 8. 2010).

[22] VAN GREMBERGEN, Wim.: The Balanced Scorecard and IT Governance, ISACA Information System Control Journal, 2000, št. 2.

[23] Wikipedia: http://en.wikipedia.org/wiki/Due_diligence (na dan 15. 8. 2010).

▪

Boštjan Delak je na Fakulteti za elektrotehniko Univerze v Ljubljani diplomiral leta 1982 in magistriral leta 1985. Ima več kot sedemindvajset let izkušenj na različnih področjih informatike. Zaposlen je bil v Iskri Avtomatiki, Intertradu, IBM Slovenija, Novi Ljubljanski banki. Deloval je na različnih področjih in vodil različne oddelke in projekte informacijskih sistemov. Od leta 2008 je zaposlen v podjetju ITAD, revizija in svetovanje, d. o. o., kjer je samostojni svetovalec in revizor informacijskih sistemov (CISA ter preizkušen revizor IS). Od 1998 do 2008 je izvedel več kot 65 skrbnih pregledov informacijskih sistemov v petnajstih državah srednje in vzhodne Evrope. Razvil je univerzalni celoviti pristop skrbnega pregleda informacijskega sistema in to področje je tudi tema njegove teze na Fakulteti za računalništvo in informatiko Univerze v Ljubljani.

▪

Marko Bajec je na Fakulteti za računalništvo in informatiko diplomiral, magistriral in doktoriral v letih 1996, 1998 in 2001. Od takrat dela na katedri za informatiko in izvaja dodiplomske in podiplomske programe za informacijske sisteme in podatkovne baze. Leta 2009 je postal izredni profesor. Njegovo glavno področje raziskovanja so metodologije razvoja programske opreme (posebno Situational Method Engineering, obvladovanje informacijske tehnologije – IT Governance) in kakovost programske opreme. Svoje raziskovalne ugotovitve je objavil na domačih in mednarodnih konferencah in v znanstvenih revijah. Ustanovil je laboratorij za podatkovne tehnologije, ki ga tudi vodi. Kot vodja ali koordinator je vključen v različne industrijske in razvojne projekte.