UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

BOŠTJAN DELAK

UNIVERZALNO OGRODJE ZA IZVEDBO ZAČETNEGA SKRBNEGA PREGLEDA INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA

LJUBLJANA, 2012

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

BOŠTJAN DELAK

UNIVERZALNO OGRODJE ZA IZVEDBO ZAČETNEGA SKRBNEGA PREGLEDA INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA

Mentor: izredni profesor dr. Marko Bajec

LJUBLJANA, 2012

POVZETEK IN KLJUČNE BESEDE

Informacijski sistem (IS) v podjetju (v nadaljevanju organizaciji) je širši pojem, ki poleg informacijsko komunikacijske tehnologije (IKT), ki jo organizacija uporablja, opredeljuje tudi način uporabe – interakcije uporabnikov s tehnologijo pri izvajanju vsakodnevnih poslovnih in podpornih procesov v organizaciji. Lahko rečemo, da IS zajema IKT, uporabnike, procese, podatke, dogodke in aktivnosti v določeni organizaciji ali okolju.

Dandanes se večina organizacij srečuje z izzivi obvladovanja IS. Za pridobitev trenutnega stanja IS ter posledično tudi stopnje obvladovanja IS v organizaciji izvedemo skrbni pregled. Islovar – terminološki slovar informatike, opredeljuje ta izraz kot analizo stanja organizacije na določenem področju s ciljem, da se poda poslovodstvu oziroma naročniku realno informacijo na segmentu pregleda.

V zadnjih dveh desetletjih so organizacije večale obseg poslovanja na različne načine, med drugim tudi z nakupi in združevanjem (»*mergers & acquisitions*«). Pred samim nakupom oziroma kapitalskim vložkom organizacije se izvede nekaj aktivnosti, od katerih je realizacija izvedbe začetnega skrbnega pregleda (»*initial due diligence*«) ključnega pomena. Pri začetnih skrbnih pregledih je v večini primerov poudarek na likvidnosti, naložbah (kreditne in kapitalske naložbe) in upravljanju tveganj. Z vse večjim vplivom IS na poslovanje družbe je v zadnjem času postal izredno pomemben tudi podroben pregled IS v pregledovani organizaciji, in sicer predvsem zaradi velike odvisnosti organizacij od podpore IS ter velikih vlaganj v kvalitetnejše in sodobnejše podpore, ki zagotavljajo neoporečnost, zaupnost in razpoložljivost informacij.
Začetni skrbni pregled poslovanja organizacije je za področje IS izredno obsežen in zahteven ter sestavljen iz posameznih delov, kamor spadata tudi varnost informacijskega sistema ter ocena operativnih tveganj. Pri izvedbi začetnega skrbnega pregleda je pomembno pregledati in oceniti skladnost delovanja z lokalnimi predpisi, varnostni vidik implementiranega IS ter oceniti in analizirati odstopanje in možnost prilagoditve na korporativen IS v primeru odločitve o kapitalskem vlaganju. Pri tem je potrebno te aktivnosti izvesti v kratkem času.

Med leti 1996 in 2006 sem izvedel več kot 60 skrbnih pregledov v finančnih organizacijah v 15 državah Evrope. Skozi leta izvedbe skrbnih pregledov in analize različnih metod, orodij, standardov, dobrih praks in postopkov (v nadaljevanju pristopov) je nastal Celovit pristop za izvedbo skrbnega pregleda IS. Ta pristop ni nekaj novega, ampak je nekakšen konglomerat različnih pristopov, preverjenih skozi leta pri posameznih pregledih, ter nadgrajen z izkušnjami in novostmi, ki jih analizirani in preverjeni pristopi niso imeli.

S tem pristopom je možno v zelo kratkem času izvesti skrben pregled IS v manjših in večjih organizacijah. V okviru tega celovitega pristopa je vključen tudi odločitveni model, ki omogoča transparenten, enovit in učinkovit sprejem odločitve.

Ta celoviti pristop je bil preverjen s študijo primerov v štirih finančnih organizacijah v letih 2007 in 2008. Poleg tega je bil, v sklopu priprave te naloge, preverjen še v eni nefinančni organizaciji, ki pa ni tipična organizacija, ki bi imela od 2 % do 7 % sodelavcev IT, kakor so jih imele finančne organizacije, kjer smo preverjali ta celoviti pristop. Ta organizacija ima 7 % uporabnikov, ostali so strokovnjaki IT. Pregledana nefinančna organizacija je organizacija, ki razvija rešitve IT za svoje naročnike in tudi izvaja vsakodnevno operativno podporo IS svojim naročnikom. Preverjanje je pokazalo, da se lahko celovit pristop izvedbe skrbnega pregleda IS uporabi tudi pri pregledih tovrstnih organizacij.

Študije primerov potrjujejo, da je s pomočjo tega celovitega pristopa možno izvesti skrbni pregled IS v kratkem času, v pomoč vlagateljem pa je integriran odločitveni model.

Ključne besede: celovit pristop izvedbe skrbnega pregleda IS, skrbni pregled IS, kvaliteta IS, tveganja IS, zadovoljstvo IS, odločitveni model.

ABSTRACT AND KEYWORDS

Information system (IS) in the company (hereinafter referred to as organization) is a broader term, which apart from Information Communication Technology (ICT) defines how users should use technology and how they can interact with technology in delivering day-to-day business activities and support processes within the organization. We can say that IS encompasses ICT, users, processes, data, events and activities in a particular organization or environment.

Nowadays the majority of organizations face the issues of ICT governance. In order to obtain effective information on the status of ICT or IS in general, organizations can perform IS due diligence activities. Islovar - Informatics Terminology Dictionary defines this term as an analysis of a particular area of business in the organization in order to provide the management or client with real information on the reviewed segment.

In the past two decades, organizations used various ways to increase the volume of business, including mergers and acquisitions (M&A). Prior to any acquisition or capital investment, several activities need to be carried out with initial due diligence playing the key role. In most cases the initial DD focuses on reviewing liquidity, investments (credit and equity investments), and risk management. With the ever-growing impact of IS on the organizations' daily business support, reviewing the IS of an organization has become very important, if not vital. This is mainly due to the large dependence of the IS segment on substantial investments in quality and up-to-date support, ensuring the integrity, confidentiality, and availability of information.

IS initial due diligence is very comprehensive and demanding as it covers a range of segments, such as information security and operational risk assessment. Furthermore it should ascertain and assess compliance with the local regulation, security aspects of the implemented information system and establish and analyze any deviations. In addition due diligence of information system should establish the possibility of adjustments to the corporate information system in the event of a positive decision on capital investment. It is necessary that these activities be performed in a short period of time.

Between 1996 and 2006, I conducted over 60 IS due diligences in financial organizations in 15 European countries. Through the implementation of due diligence and analysis of different methods, tools, standards, best practices and procedures (hereinafter approaches) the Universal framework for IS due diligence delivery was formed. The presented framework is not a completely new method to be placed alongside others, but an attempt at creating a comprehensive synthesis method using existing approaches upgraded with innovations that proved useful through extensive personal experience with the use of standard approaches.

With this framework it is possible to perform an IS due diligence in small and large organizations a in a very short period of time. It includes a decision model enabling a transparent, uniform and effective decision-making process.

This universal framework has been tested with a case study of four financial institutions in 2007 and 2008. Moreover, for the purpose of this thesis, it was verified in one non-financial organization. Contrary to typical financial organizations subject to our universal framework, this organization only has 7 % of users and others are ICT experts, whereas the financial institutions have 2 % to 7 % of ICT experts. The non-financial organization develops ICT solutions for their clients and offers daily operational support for their IS. The case study has shown that the universal framework for IS due diligence is also applicable in such organizations.

Case studies confirm that with this universal framework IS due diligence can be conducted in a short period of time and the integrated decision model facilitates decision-making for investors.

Keywords: universal framework for IS due diligence delivery, IS due diligence, IS quality, IS risk, IS satisfaction, decision model.

I Z J A V A O A V T O R S T V U

doktorske disertacije

Spodaj podpisani Boštjan Delak,

sem avtor doktorske disertacije z naslovom

UNIVERZALNO OGRODJE ZA IZVEDBO ZAČETNEGA SKRBNEGA PREGLEDA INFORMACIJSKE TEHNOLOGIJE

S svojim podpisom zagotavljam:

- da sem doktorsko disertacijo izdelal samostojno pod vodstvom mentorja, izrednega profesorja dr. Marka Bajca,
- da so elektronska oblika doktorske disertacije, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko doktorske disertacije,
- da soglašam z javno objavo elektronske oblike doktorske disertacije v zbirki »Dela FRI«.

V Ljubljani, dne 2.7.2012 Podpis avtorja:

ZAHVALA

Posebna zahvala gre izrednemu prof. dr. Marku Bajcu, ki mi je kot mentor nudil strokovno pomoč pri nastajanju naloge in mi je bil pripravljen pomagati ter me bodriti tudi ob najbolj kritičnih trenutkih.

Zahvaljujem se moji ženi Meti, ki mi je ves čas doktorskega študija stala ob strani in mi vlivala optimizem, verjela vame ter me bodrila, ter sinu Tevžu in hčeri Tjaši za njuno podporo. Še enkrat hvala.

Prav tako se zahvaljujem moji mami Nasti, ki me je bodrila po svojih močeh, ter sestri Zvezdi za spodbude.

Zahvaljujem se vsem, ki so sodelovali in me spodbujali pri nastajanju doktorske naloge:

- prijateljem iz »klape«, Andreji P., Andreji S., Andreju, Borutu, Daši, Dušanu, Eni, Franciju, Karmen, Miru, Tomu in Zlatki, ki so me spodbujali in vlivali upanje;
- Mladenu Terčelju, ki je vplival na moje znanje varovanja informacij;
- vodstvu Nove ljubljanske banke d. d., Ljubljana, ki mi je omogočilo izvesti skrbne preglede v finančni dejavnosti v letih 1996–2008;
- kolegom, preizkušenim revizorjem s Slovenskega inštituta za revizijo, ki so mi dajali podporo in nasvete.

Zahvaljujem se tudi sodelavcem v podjetju ITAD, Revizija in svetovanje d. o. o., ki so me spodbujali in podpirali pri pripravi naloge.

Zahvaljujem se tudi lektoricama, gospe Majdi Papež za slovenski tekst, ter gospe Alenki Klarič za angleški tekst. Obe sta pripomogli, da je tekst naloge postal še boljši. Hvala.

Zahvaljujem se tudi podjetju Informatika, informacijski inženiring. d. d., kjer sem lahko v praksi v Sloveniji preveril in potrdil univerzalno ogrodje. Še posebej se zahvaljujem gospodu Pavlu Carju.

Zahvaljujem se tudi vsem, ki so kakorkoli prispevali k nastanku tega dela.

POSVETILO

Moji Meti!

Anyone who stops learning is old, whether at twenty or eighty.

Henry Ford

KAZALO VSEBINE

KAZALO SLIK

KAZALO PREGLEDNIC

1 UVOD

1.1 Opredelitev raziskovalnega problema

Poslovanja organizacije si ne moremo predstavljati brez podpore informacijskih sistemov (IS) v temeljnih, podpornih in ne nazadnje tudi vodstvenih procesih. Informacijska tehnologija (IT) je vključena v večino procesov posameznega podjetja, zato je izredno važno obvladovanje tega pomembnega področja. Danes se večina podjetij srečuje z izzivi obvladovanja IT, pri čemer je potrebno poudariti, da ne gre za osamljeno aktivnost, temveč za del celovitega obvladovanja podjetja, ki je usmerjeno na zaščito lastniške vrednosti in s tem zmanjševanje tveganj. Obvladovanje IT je razdeljeno na pet področij [ISA09]: na strateško uskladitev, ustvarjanje vrednosti, upravljanje tveganja, upravljanje virov ter merjenje izvedbe. Za uspešno pridobljeno informacijo o stanju IT oziroma o stanju celovitega IS nasploh se lahko v podjetju izvedejo aktivnosti skrbnega pregleda IS.

Integracija procesov med podjetji je del običajne strategije rasti v konkurenčnem okolju. Združevanja in prevzemi ustvarijo več izzivov do organizacij in njihovih zainteresiranih strani. Nujno je, da organizacija pred izvedbo strateške naložbe natančno razume potencialna tveganja in priložnosti. Začetni skrbni pregled organizacije je ena izmed najpomembnejših aktivnosti, ki jo je potrebno izvesti pred kakršnimi koli kapitalskimi naložbami. Skrbni pregledi so se tradicionalno osredotočili na vrednotenje finančnih in pravnih zadev, poslovne strategije in upravljanja s tveganji. Zaradi vedno večjih vsakodnevnih vplivov IS na primarne, vodstvene in podporne procese v organizacijah, so le-te postale bolj odvisne od IS, ki jim omogoča rast, omeji/kroji stroške, zagotavlja skladnost, meri uspešnost in nudi podporo odločanju. Kot rezultat aktivnosti pri združevanju in prevzemih je začetni skrbni pregled IS postal bolj kritična, če ne celo nujna aktivnost, ki razkrije in ovrednoti tveganje, stanja, dnevno podporo in varovanje informacij potencialne organizacije.

Več metod, standardov, orodjih in celovitih pristopov (»*framework*«) se lahko uporablja za vodenje, analizo ali postopek izvedbe skrbnih pregledov IS. V analizi obstoječih pristopov nismo mogli najti popolnega pristopa, ki bi zagotovil vse informacije, potrebne za skrbni pregled IS, in hkrati omogočal hitro in natančno oceno obstoječe IS. Veliko obstoječih pristopov je posebej izdelanih in primernih za analizo oziroma obvladovanje posebnih domen IS. Še več - nekateri od teh pristopov so zamudni in zato manj primerni za začetni skrbni pregled IS ali pa nimajo vključenega celovitega modela odločitev, da bi podali natančne in jedrnate informacije, ki bi temeljile na rezultatih skrbnega pregleda IS.

S praktično izvedbo več deset začetnih in splošnih skrbnih pregledov IS sem zato razvil proces – celovit pristop za izvedbo skrbnega pregleda IS, ki omogoča celovito, hitro in učinkovito izvedbo skrbnega pregleda in ima v pristopu integriran odločitveni model, ki omogoča naročniku/lastniku lažje in hitrejše odločanje.

Rezultati, pridobljeni v sklopu celovitega pristopa, zagotavljajo dovolj informacij za zmanjšanje tveganja pred združevanji in prevzemi. Ta celoviti pristop se lahko uporablja za začetni, splošni, izločitveni in tehnološki skrbni pregled IS.

1.2 Opredelitev skrbnega pregleda

Kaj je sploh skrbni pregled oziroma s tujko »*due diligence*«?

Poglejmo si nekaj tolmačenj. Zelo osnovno obrazložitev najdemo na Wikipedii [Wik10]:
"Skrbni pregled je proces, ki omogoča potencialnemu vlagatelju oceniti ciljno podjetje pred kapitalskim vlaganjem".

Malo bolj finančno usmerjena obrazložitev je naslednja [Fit93]:
"Skrbni pregled – v podjetniškem združevanju in pridobivanju je podroben pregled poslovanja s ciljem pregleda premoženja in obvez ciljnega podjetja".

Realizacija začetnega skrbnega pregleda poslovanja finančnih organizacij (»*due diligence*«) je ena izmed ključnih aktivnosti, ki mora biti opravljena pred kapitalskim vlaganjem. Pri začetnih skrbnih pregledih je v večini primerov poudarek na likvidnosti, naložbah (kreditne in kapitalske naložbe) in upravljanju tveganj.

Letno poročilo z revidiranimi računovodskimi izkazi je sicer osnovni vir za finančno analizo poslovanja, a je preozko za podrobne ocene.

V finančni industriji so kot orodje pri vsebinski analizi finančne organizacije primerne različne metode (na primer: CAMELS metoda) [Pod00]. Pri začetnih skrbnih pregledih finančnih organizacij je poudarek na likvidnosti, naložbah (kreditne in kapitalske naložbe) in upravljanju s tveganji. Izvede se tudi ustrezen pravni skrbni pregled [Maz01]. Poleg zgoraj naštetih se v okviru začetnega skrbnega pregleda izvedejo še pregledi drugih poslovnih področij:

- računovodstva z računovodskimi izkazi,
- kreditnega portfelja*,
- upravljanja s tveganji,
- mednarodnega poslovanja,
- zakladništva*,
- plačilnega prometa*,
- kadrov,
- prodaje,
- analize poslovne mreže*.

* velja za finančne družbe

Z vse večjim vplivom informacijskih sistemov na poslovanje družbe je v zadnjem času postal izredno pomemben tudi podroben pregled informacijskega sistema v ciljni organizaciji, in sicer predvsem zaradi velike odvisnosti organizacij od podpore informacijskih sistemov ter velikih vlaganj v kvalitetnejše in sodobnejše podpore, ki zagotavljajo neoporečnost, zaupnost in razpoložljivost informacij.

1.2.1 Skrbni pregled informacijskega sistema

Informacijska tehnologija (IT) je vključena v večino procesov posameznega podjetja, zato je izredno važno obvladovanje tega pomembnega področja. ISACA (*Information System Audit and Control Association*) je pred leti opredelila obvladovanje IT kot:
»*... odgovornost poslovodstva in upravnega odbora. Sestoji od vodenja organizacijskih struktur in vodenja procesov, ki zagotavljajo, da IT podpira strategijo podjetja in zagotavlja realizacijo ciljev podjetja* [ISA03]«.

Pri tem je potrebno poudariti, da obvladovanje IT ni osamljena aktivnost, temveč del celovitega obvladovanja podjetja, ki je usmerjeno na zaščito lastniške vrednosti in s tem zmanjševanje tveganj. Razdeljeno je na pet področij [ISA09]:

- strateško uskladitev,
- ustvarjanje vrednosti,
- upravljanje virov,
- upravljanje tveganja,
- merjenje izvedbe.

Za pridobitev trenutnega stanja IT ter posledično tudi stopnje obvladovanja IT oziroma celotnega IS v podjetju izvedemo skrbni pregled. V nadaljevanju je opisano, kakšne skrbne preglede poznamo in kakšni so cilji posameznih tipov skrbnih pregledov.

1.2.1.1 Tipi skrbnih pregledov

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

Lahko bi ocenili, da je skrbni pregled IS podoben splošnemu revizijskem pregledu delovanja IS 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 oziroma nadzorni svet.
- »***Navadni***« oziroma splošni skrbni pregled je analiza stanja glede na strategijo podjetja in taktične načrte ter se lahko izvede kadarkoli. Takšno odločitev sprejmeta lastnik oziroma 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 poda izvršni direktor informatike ali izvršni direktor tehnologije [And09].
- Skrbni pregled »***ponudnika***« izločanja informatike, ki se izvede pred samo odločitvijo o izločitvi določenih aktivnosti zunanjemu izvajalcu. Pobudo za začetek aktivnosti podata izvršni direktor za operativo ali izvršni direktor za nabave [Bay09].

Vsi načini imajo veliko skupnega, a se razlikujejo predvsem po tem, kdo določene aktivnosti začne oziroma za koga se izvaja pregled ter kakšni so cilji pregleda.

1.2.1.2 Cilji posameznih tipov pregledov

Zgoraj so na kratko navedeni posamezni tipi pregledov, ki se med seboj razlikujejo po vsebini, pobudnikih, namenu in ciljih, ki so naslednji:

- »***Začetni***« skrbni pregled – cilj je podati naročniku pregleda jasno in kratko informacijo o trenutnem stanju IS, trenutnih tveganjih na področju IS, trenutni vrednosti IS ter oceniti, koliko vlaganj (stroškov in investicij) je potrebno za dosego določenega pričakovanega nivoja, ki naj bi ga pregledovana družba dosegla v določenem času. Ti podatki so osnova, da se naročnik odloči, ali naj nadaljuje z aktivnostmi/pogajanji ali pa naj jih zaključi.
- »***Navadni***« skrbni pregled – cilj je podati naročniku pregleda jasno in kratko informacijo o trenutnem stanju IS, trenutnih tveganjih na področju IS, stopnji usklajenosti s strategijo podjetja in usmeritvami, stanjem trenutnih projektov IS itd. Tak pregled se običajno izvede ob menjavi poslovodstva, ali pa na pobudo nadzornikov. V slovenskem prostoru ima trenutno zelo negativen prizvok, saj ga večina vodstev IT razume kot nezaupnico.
- »***Tehnološki***« skrbni pregled ima cilj, da se izvedejo določene aktivnosti pred odločitvijo, ali se določena tehnologija vpelje ali ne. Je mešanica analize možnih odločitev, rešitev za poslovanje družbe kot tudi za integracijo rešitve v obstoječe procese in storitve v IT.
- Skrbni pregled »***ponudnika***« izločanja informatike – cilj je, da se preuči potencialnega ponudnika izločanja storitve ali več storitev ter informatike, pri čemer se spozna njihove procese in način delovanja ter oceni morebitna tveganja. Priporoča se, da se ta aktivnost izvaja periodično tudi po sprejemu odločitve o izločitvi, kar podpirajo tudi nekatere globalne usmeritve (med drugimi: Basel II, Sabena – Oxley).

Podrobnosti o temi tega podpoglavja sem navedel tudi v naslednjih prispevkih:

a) Začetni skrbni pregled za področje informacijskih sistemov v finančnih organizacijah, Zbornik prispevkov: Dnevi slovenske informatike 2008, Portorož ISBN 978-961-6165-26-6

b) 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

c) Celovit pristop izvedbe skrbnega pregleda (soavtor), Zbornik prispevkov: Dnevi slovenske informatike 2010, Portorož ISBN 978-961-6165-32-7

d) Framework for the delivery of Information System Due Diligence, Information System Management, prispevek je bil sprejet 11.3.2012, prispevek bo po navedbah glavnega urednika objavljen v enem letu.

1.3 Namen, cilji in hipoteza doktorske disertacije

1.3.1 Namen doktorske disertacije

Organizacije po svetu in v Sloveniji poskušajo povečati svoje tržne deleže tudi z nakupi drugih organizacij in s kasnejšim združevanjem. V sodobnih organizacijah je informacijska tehnologija (IT) vpeta v večino, če ne v vse procese. Poslovanja organizacije si ne moremo predstavljati brez podpore informacijskih sistemov (IS) v temeljnih, podpornih in ne nazadnje tudi vodstvenih procesih.

Pred vsako odločitvijo o nakupu organizacije oziroma združevanju je smotrno izvesti skrbni pregled in s tem identificirati razlike ter ugotoviti določena tveganja, ki jih lahko z ustreznimi ukrepi ob nadaljnjih aktivnostih tudi ustrezno obvladujemo, če ne celo zmanjšujemo.

Pri skrbnih pregledih je v večini primerov poudarek na likvidnosti, naložbah (kreditne in kapitalske naložbe) in upravljanju tveganj. Z vse večjim vplivom informacijskih sistemov na poslovanje družbe je v zadnjem času postal izredno pomemben tudi pregled informacijskega sistema v ciljni organizaciji. Za pridobitev trenutnega stanja IT ter posledično tudi stopnje obvladovanja IT oziroma celotnega IS v organizaciji izvedemo skrbni pregled.

Področje informatike in sorodna znanstvena področja ne poznajo metode analize IS pri skrbnih pregledih oziroma pripadajočega ogrodja, ki bi temeljilo na znanstvenih dejstvih. Neustrezne in pomanjkljive metode na področju skrbnih pregledov IS imajo lahko pri organizaciji veliko negativnih posledic na virih (času, finančnih, človeških in ostalih virih IS) in tudi mehkih dejavnikih (zadovoljstvu, celostni podobi itd.). Neobstoj učinkovite metode, ki v kratkem času omogoča izvedbo skrbnega pregleda in priprave podatkov/informacij, ki bodo omogočali poslovodstvom oziroma lastnikom enostavne odločitve, predstavlja vrzel na področju analize IS, ki jo nameravam zapolniti z doktorsko disertacijo.

Metodo in pripadajoče ogrodje za skrbne preglede lahko označimo kot artefakt IT.

Iz zgoraj navedenega izhaja raziskovalno vprašanje: » **Ali lahko ta artefakt podpremo z znanstveno metodo, ki temelji na preučevanju študije primerov?**«

1.3.2 Cilji in hipoteze doktorske naloge

Glavni cilji doktorske naloge so:

- analiza obstoječe metodologije in ogrodja za izvedbo skrbnega pregleda informacijske tehnologije,

- predstavitev metodologije in ogrodja za izvedbo skrbnega pregleda informacijske tehnologije,
- predstavitev raziskave, s katero sem iz prakse prišel do ogrodja in jo primerjal z raziskavami v znanstvenih člankih,
- prikaz izvedbe študije primerov izvedenih začetnih in navadnih skrbnih pregledov v finančni industriji (izvedel sem jih v okviru Nove Ljubljanske banke d. d.),
- preučitev zrelosti ogrodja, različnih dejavnikov, ki vplivajo na njegovo kakovost in kakovost njegovih izdelkov, ter preučitev problemov, ki jih lahko imajo z uporabo tega ogrodja. V okviru raziskave bom skušal odgovoriti na naslednja vprašanja:
    a) ali ogrodje omogoča ponovljivost,
    b) ali ogrodje omogoča univerzalnost,
    c) ali ogrodje omogoča globalnost,
    d) kakšna je stopnja predvidljivosti analiz ogrodja,
- predstavitev uporabnosti ogrodja v dveh različnih gospodarskih vejah v prostoru Srednje in Jugovzhodne Evrope ter analiza njegove uporabnosti,
- izdelava prototipa določenih vprašalnikov za nekatera področja, ki bo vsem udeležencem v procesu skrbnega pregleda omogočal enostavno in hitro izvajanje aktivnosti, za katere so odgovorni,
- predlog razvoja informacijske rešitev za hitrejše in učinkovitejše obdelave določenih vprašalnikov za nekatera področja, ki bo izvajalcem v procesu skrbnega pregleda omogočal enostavno, hitro in poenoteno obdelavo (analizo vprašalnikov) in s tem učinkovito pripravo izhodnih podatkov,
- razvoj odločitvenega modela, ki bo poslovodstvu oziroma naročniku pregleda omogočal kvalitetno sprejemanje odločitev,
- priprava načrta vpeljave ogrodja v prakso.

V okviru doktorske disertacije sta zastavljeni dve hipotezi:

> **Hipoteza 1: Predlagana metodologija z ogrodjem omogoča učinkovito izvedbo skrbnega pregleda v zelo kratkem času in pri tem zbere dovolj podatkov/informacij za odločanje.**
>
> **Hipoteza 2: Metodologijo z ogrodjem je možno učinkovito uporabiti tudi v drugih dejavnostih, panogah in industrijah, kot npr. v finančni industriji, v kateri je bila razvita in preverjena.**

1.4 Metode dela

1.4.1 Raziskovalni pristop

Za izvedbo raziskovalnega dela je bil uporabljen pristop zasnovne znanosti (»Design Science«), ki temelji na paradigmi razširiti meje človeške in organizacijske sposobnosti z ustvarjanjem novih in inovativnih artefaktov [Hev04]. Ta paradigma ima osnove v inženiringu in znanosti o umetnem [Sim96]. Tako nastali IT artefakti razširjajo meje človeških reševanj problemov in organizacijske sposobnosti, kar zagotavljajo z intelektualnimi in računalniškimi orodji [Hev04]. IT artefakti so širše opredeljeni kot konstrukti, modeli, metode in naprave.

Preglednica 1: Zasnovno znanstveno raziskovalne smernice

#	smernice	opis
1.	Oblikovanje kot artefakt	Zasnovno znanstveno raziskovanje mora pripraviti uspešne artefakte v obliki konstruktov, modelov, metod ali naprav.
2.	Problem pomembnosti	Cilj raziskav v zasnovni znanosti je razviti tehnologije, rešitve, ki temeljijo na ustreznih in pomembnih poslovnih problemih.
3.	Načrtovanje razvoja	Uporabnost, kakovost in učinkovitost oblikovanja artefakta, je treba strogo dokazati s pomočjo dobro izvedenih metod vrednotenja / dokazovanja.
4.	Raziskovalni prispevek	Učinkovite zasnovne znanstvene raziskave morajo zagotoviti jasne in preverljive prispevke na področju oblikovanja artefakta, oblikovanje fundacije, in/ali oblikovanje metodologije.
5.	Raziskovalna strogost	Zasnovno znanstvena raziskava je odvisna od stroge uporabe metod v gradnji in vrednotenju oblikovanja artefakta.
6.	Načrtovanje kot proces iskanja	Iskanje učinkovitega artefakta zahteva uporabo razpoložljivih sredstev za dosego željenih ciljev in hkrati izpolnjevati zakone v okolju problema.
7.	Komunikacija na področju raziskave	Zasnovno znanstvena raziskava mora biti učinkovito predstavljena tako, da je tehnološko usmerjena, kot tudi upravljalno usmerjena.

vir: [Hev04]

Celovit pristop je nastal kot rezultat spiralnega razvoja [Boe88] izvajanja skrbnih pregledov. Skozi predhodno pridobljene izkušnje sem postopoma dopolnjeval vprašalnike in izpolnjeval metodo izvedbe pregleda do določene stopnje, ko so se izboljšave in dopolnitve umirile.

V tistem trenutku sem s pristopom zasnove znanosti in spodaj navedenimi raziskovalnimi metodami s pomočjo zgoraj navedenih smernic ter hipotez želel dokazati obstoj in veljavnost IT artefakta.

Benbaset in Zmud (1999) v svojem prispevku poudarjata razkorak med znanostjo in prakso, saj menita, da večina IS akademskih raziskav danes nima pomena za prakso. Predlagata taktike, postopke in smernice, ki bi jih lahko IS akademske skupnosti upoštevale v svojih raziskovalnih prizadevanj in pri izdelkih, pomembnih za prakso. Predlagata, da se zmanjša razkorak med znanostjo in vsakodnevno prakso. S tem delom sem želel ta razkorak ustrezno zmanjšati in s pomočjo znanstveno raziskovalnih metod dokazati, da je celovit pristop ustrezen artefakt IT.

1.4.2 Raziskovalne metode

Pri svojem delu sem uporabil kombinacijo raziskovalnih metod:

- pregled literature,
- študijo primera,
- metodo opazovanja,
- intervjuvanje.

1.4.2.1 Metoda pregleda literature

Po Ivanku [Iva07] je zbiranje, proučevanje in urejanje gradiva najtežja, najpomembnejša, najzahtevnejša in najodgovornejša faza tehnologije znanstvenega raziskovanja. Ta faza zajema naslednje aktivnosti: zbiranje literarnega gradiva in informacij, proučevanje literarnega gradiva, izbiranje, analizo in sintezo relevantnih dejstev ter oblikovanje splošnih zaključkov.

Metodo pregleda literature sem uporabil ob pregledovanju znanstvenih in drugih strokovnih prispevkov za različna ciljna področja. Pregled literature za področja naloge lahko razdelimo na naslednja podpodročja:

- Opise terminologije in ciljev skrbnih pregledov ([Alb03], [And07], [And09], [Ang01], [Bau05], [Bay09], [Bha07], [Bin08], [Fit93], [How03], [Maz01], [Meh04], [Meh07], [Pic02], [Pod00], [Sis02a], [Sis02b], [Son09], [Sun06], [Wik10]), kjer sem pridobil ustrezno terminologijo ter cilje skrbnih pregledov IS; pri tem sem tudi sprožil postopek

vpisa dveh terminoloških pojmov v Islovar[1] (slovenski terminološki slovar informatike) in sicer : skrbni pregled, začetni skrbni pregled.

- Opise različnih metod in orodij, ki so v uporabi za analizo IS ([Ako96], [Ala08], [Apa02], [Baj06], [Bau05], [Gre00], [BCI03], [BSI], [Cra07], [Hol05], [ISA08], [ISA09a], [ISA09c], [ISA10a], [ISO08], [ISO10], [ITG07], [ITIL], [Kno08], [McK05], , [PAS03], [Roz05], [Sis02a], [Sis02b], [Sun06], [Šal06], [Šau06]), kjer sem pridobil različne opise metod, standardov, orodij in dobrih praks za analizo IS.
- Opise revizijskih pregledov informacijskih sistemov ([Ana05], [Gol07], [IIA], [IIA05], [ISA04], [ISA08], [ISA10], [ISA10b], [ISACA], [ITG07], [Kar08], [Len04], [Mer08], [Mit10], [Mošo5], [Pod09], [Taj04], [Živ10]), kjer sem pridobil teoretična znanja glede načrtovanja, izvedbe, poročanja in pregledov priporočil revizij IS, kakor tudi praktična znanja revizij, ki sem jih pridobil v letih od 2008 do 2012 (seznam referenc je na spletnih straneh podjetja, kjer sem zaposlen [ITAD]).
- Opise raziskav informacijskih sistemov ([Agr11], [Alt02], [Alt02b], [Alt03], [Alt05], [Alt06], [Avg00], [Baj05], [Bas99], [Ben99], [Boe88], [Cla08], [Den01], [Des06], [Dic99], [Gre06], [Hev04], [Hol03], [Kin05], [Kin07], [Kit04], [Kle99], [Lee01], [Lee03], [Mye99], [Oos06], [Orl01], [Orl01b], [Pal06], [Par04], [Soy97], [Str04], [Str08], [Tem06], [Tru01], [Vai04], [Whe89], [Zmu98]), kjer sem pridobil teoretična znanja o različnih raziskovalnih metodah in pristopih potrjevanja hipotez.
- Opise raziskav tveganj informacijskih sistemov ([Abr09], [Alt04], [Axe09], [Cho07], [Goo07], [Gor04], [Gor05], [Har05], [Hil07], [ISO10], [ISA05], [ITG01], [ITG07], [Jav04], [Kou10], [Loc92], [Ma05], [Pot04], [She04], [Smi01], [Spe10], [Tan04], [Tas07], [War09], [Wes07], [Wil94], [Xu08], [Zaf09]), kjer sem pridobil informacije o strokovnih raziskavah na področju varovanja informacij.
- Opise raziskav uspešnosti informacijskih sistemov ([Alt99], [Can05], [DeL01], [Eve03], [ITG07], [ITG08], [Ive83], [Jia08], [Kre08], [Lei08], [McL08], [Orw07], [Pet08], [Rab09], [Sch11], [Sed04], [Sed05], [Zvi03]), kjer sem pridobil znanja o različnih raziskovalnih metodah in analizah uspešnosti informacijskih sistemov.

1.4.2.2 Metoda študija primera

Metoda študija primera oziroma metoda proučevanja primerov je postopek, s katerim proučujemo posamičen primer z določenega področja [Iva07]. S tem postopkom lahko na podlagi rezultatov opazovanj več primerov izvedemo določene zaključke. Študija primera je raziskovalna metoda, ki raziskuje sodobni fenomen v svojem realnem življenjskem kontekstu [Yin03]. Študije primerov poudarjajo natančno kontekstualno analizo omejenega števila dogodkov ali pogojev in njihovo razmerje [Soy97]. Yin (2003) predlaga šest korakov za izvedbo tega postopka:

- določitev in opredelitev raziskovalnih vprašanj,
- izbiro primerov in določitev zbiranja podatkov in tehnik analize,

[1] http://www.islovar.org

- pripravo na zbiranje podatkov,
- zbiranje podatkov v praksi,
- vrednotenje in analiza podatkov,
- pripravo poročila.

Metoda študija primera v okviru raziskovanj odgovori na enega ali več vprašanj, ki se začenjajo s »kako« in z »zakaj« [Soy97].

1.4.2.3 Metoda opazovanja

Metoda je po mnenju Ivanka (2007) prva in osnovna metoda vsakega raziskovalnega dela. Raziskovalcu omogoča, da se na neposreden način spozna s predmetom, pojavom ali procesom raziskovanja [Iva07]. S pomočjo te metode se zbirajo podatki in informacije o dejstvih, pojavih in procesih ter se spoznavajo odnosi in povezanosti med njimi.

Opazovanje kot raziskovalna metoda mora biti [Iva07]:

- čim bolj objektivno,
- čim bolj vsestransko in popolno,
- čim bolj precizno in čim strožje,
- čim bolj sistematično.

1.4.2.4 Metoda intervjuvanja

Metoda intervjuvanja je postopek, s katerim na podlagi intervjujev raziskujemo in zbiramo podatke, informacije, stališča in mišljenja o predmetu raziskave. Metodo intervjuvanja izvajamo neposredno, to je ustno, v obliki razgovora z intervjuvancem [Iva07]. Za kvalitetno izvedbo intervjuja se predhodno pripravi vprašalnik, ki je lahko odprt ali zaprt in obvezuje izpraševalca, da postavlja vprašanja po vnaprej določenem vrstnem redu. Sodobna metodologija postopka intervjuja predstavlja odprtost vprašalnika, kar pomeni, da le ta ni dokončen in se lahko spremeni [Iva07].

Kakovostna izvedba je zelo pomembna in je odvisna od izpraševalca. V postopku vodenja intervjuva razlikujemo tri glavne faze [Iva07]:

- pripravo intervjuja,
- izvedbo intervjuja,
- analiziranje odgovorov in izdelavo zaključkov.

1.5 Struktura doktorske disertacije

Doktorska disertacija sestoji iz uvoda, sledi poglavje »Uporaba posameznih orodij«, kjer so predstavljene različne metodologije, orodja, standardi in dobre prakse za pregled analize celotnega IS oziroma določenih področij IS. Osrednji del naloge predstavlja poglavje »Celovit pristop izvedbe skrbnega pregleda«, kje je predstavljen celovit pristop. V poglavju »Študija primerov« je prikazan celovit pristop v konkretnih finančnih in nefinančnih organizacijah v praktičnih primerih. Nato sledi »Načrt vpeljave celovitega pristopa skrbnega pregleda IS v prakso«, kjer prikažem, kako nameravam ta pristop predstaviti potencialnim uporabnikom in tudi akademikom na različnih nivojih. V »Zaključku« so povzete ugotovitve doktorske disertacije ter podani predlogi za nadaljnje delo.

V prilogi so prikazani vsi vprašalniki, razen zelo obširnega vprašalnika Status IS, ki ima več kot 70 strani. Ta vprašalnik in tudi vsi elektronski zapisi so v pdf formatu na CD, ki je priloga disertacije. Na CD so tudi vsi ostali vprašalniki ter disertacija.

2 UPORABA POSAMEZNIH METOD IN ORODIJ

Analiza IS se lahko izvede z različnimi metodami, s pomočjo določenih orodij, z usmeritvami nekaterih standardov, z uporabo dobrih praks, s celovitimi pristopi (okviri – »*framework*«) itd. V nadaljevanju bom za vse te možnosti (pristope) uporabljal dva izraza – metode in orodja.
Ker je za skrbni pregled IS določena analiza IS, sem v tem poglavju najprej opisal nekatere metode in orodja, ki sem jih spoznal in analiziral v zadnjih letih. Nato sledi primerjalna analiza teh metod in orodij glede na določena pomembna področja ter tip skrbnega pregleda IS. Na koncu tega poglavja je še navedena obrazložitev, zakaj sem se odločil za nov pristop - Celoviti pristop izvedbe skrbnega pregleda IS – UISDDFW (»*Universal Information System Due Diligence Framework*«), ki je podrobno predstavljen v poglavju 3.

2.1 Opis posameznih metod in orodij

V svetu ni enotne usmeritve za izvajanje aktivnosti skrbnega pregleda IS, vendar obstaja kar nekaj metod in orodij za izvedbo teh nalog. Pred leti so na Univerzi v Austinu (ZDA) razvili tudi okvir – celovit pristop, ki pa se v praksi ni prijel. V nadaljevanju je opisanih 19 možnih načinov uporabe določenih metod in orodij, ki sem jih v teh letih spoznal in analiziral. Ti načini so (razvrščeni po abecedi):

- analiza upravljanja neprekinjenega poslovanja,
- Andriolova predloga za skrbne preglede,
- Bingov seznam za skrbne preglede,
- Howsonov način izvedbe začetnega pregleda,
- INFAUDITOR,
- ISO / IEC 9000,
- ISO / IEC 20000,
- ISO / IEC 27000,
- KnowledgeLeader seznam skrbnih pregledov,
- kontrolni cilji za informacijsko in sorodno tehnologijo,
- Mike Siscov seznam za skrbne preglede,
- ogrodje za ocenjevanje skrbnega pregleda IT,
- ogrodje za upravljanje s tveganji IT,
- ogrodje za zagotavljanje jamstva IT,
- Pickardov seznam za skrbne preglede,
- sistem uravnoteženih kazalnikov,
- Vrednost IT,
- zbirka napotkov za upravljanje in uvajanje storitev IT,
- Zmožnostno zrelostni model.

Pri vsaki metodi in orodju so navedeni: originalni naziv, kratek opis metode in orodja, avtor oz. avtorji, metoda ter opredelitev področja in tudi primernost za določen tip skrbnega pregleda.

2.1.1 Analiza upravljanja neprekinjenega poslovanja

»*Business Continuity Management*« (v nadaljevanju BCM) – upravljanje neprekinjenega poslovanja je eden pomembnejših procesov v sodobni organizaciji, ki je za finančne organizacije opredeljen tudi z obvezujočimi načeli v BASEL II. Samo upravljanje neprekinjenega poslovanja je standardizirano in zajema 10 področij[BCI03]:

- začetek in upravljanje,
- analizo poslovnega vpliva,
- analizo tveganj in vpeljavo kontrol,
- razvoj strategije upravljanja neprekinjenega poslovanja,
- reakcijo na nevarnosti in delovanje,
- razvoj in implementacijo načrta neprekinjenega poslovanja in načrta kriznega upravljanja,
- dvigovanje zavesti in program izobraževanja,
- vzdrževanje in izvajanje načrta neprekinjenega poslovanja in načrta kriznega upravljanja,
- krizno komuniciranje,
- koordinacijo z zunanjim institucijami.

Upravljanje neprekinjenega poslovanja je prevzel BSI (BSI – »*British Standards Institution*«) in ga vključil v standard BS 25999. Prvi del – »*BS 25999-1:2006 BCM Code of Practice*« – opredeljuje splošne smernice in usmeritve za vpeljavo procesov, principov ter terminologije za upravljanje neprekinjenega poslovanja. Sestavlja ga 10 poglavij:

- cilji,
- izrazi in definicije,
- pregled BCM,
- politika BCM,
- program BCM,
- razumevanje organizacije,
- določevanje strategije BCM,
- razvoj (implementiranje) BCM odziva,
- vaja, vzdrževanje in pregledovanje razporeditve,
- vključevanje BCM v kulturo organizacije.

Drugi del – »*BS 25999-2:2007 Specification for BCM*« – določa zahteve za implementacijo, izvajanje in izboljševanje sistema upravljanja neprekinjenega poslovanja ter opisuje zahteve, ki jih lahko objektivno in neodvisno revidiramo.
Sestavlja ga 7 poglavij:

- cilji,
- normativne reference,
- izrazi in definicije,
- načrtovanje sistema BCM,
- vpeljava in izvajanje sistema BCM,
- opazovanje in pregledovanje sistema BCM,
- vzdrževanje in izpopolnjevanje sistema BCM.

BS 23999 je leta 2006 nadomestil dotedanje orodje za upravljanje neprekinjenega poslovanja, ki je vsebovalo orodje za analizo in pomoč pri certificiranju PAS 56 (PAS – »Publicly Available Standards«). Le-ta je sestavljen iz šestih kazalnikov (»scorecard«) in prikazuje življenjski cikel upravljanja neprekinjenega poslovanja. Ti kazalniki so:

- BCM programsko upravljanje,
- razumevanje poslovanja,
- strategija neprekinjenega poslovanja,
- načrtovanje upravljanja neprekinjenega poslovanja,
- izgradnja in vlaganje v BCM kulturo,
- vadba, vzdrževanje in revizija.

V svetu uporabljajo tudi modificirana upravljanja neprekinjenega poslovanja (predvsem v ZDA in Avstraliji).

V sklopu skrbnega pregleda ta standard uporabljamo kot analizo obstoječega stanja pri pregledovanju upravljanja neprekinjenega poslovanja, še posebej v organizacijah, ki imajo sistem upravljanja neprekinjenega poslovanja že vpeljan. Ker tega sistema še nimajo vpeljanega, je ta analiza omejena.

2.1.2 Andriolova predloga za skrbne preglede

Stephen J. Andriole je razvil proces za tehnološke skrbne preglede, ki omogočajo pooblaščencem za IZ pomoč pri odločitvah, katero novo tehnološko rešitev naj nabavijo in implementirajo [And07]. Njegovo stališče je »*čim boje poznamo proces tehnološkega skrbnega pregleda, tem bolje lahko razumemo tehnologijo*«. Tehnološki skrbni pregled pomeni proces, kjer se primerjajo različne tehnologije in tehnološke storitve.

Profesor Andriole je v svoji predlogi opredelil 15 kriterijev, ki lahko vplivajo na odločitve pri tehnološkem skrbnem pregledu. Ti kriteriji so:

- »prava« tehnologija,
- malo ali nič zahtev po infrastrukturi,
- usklajen krog proračuna,
- količinski vpliv,
- spremembe v procesih in kulturi,
- rešitev,
- več možnih poti do rešitve,
- horizontalen in vertikalen vpliv,
- zavedanje industriji,
- partnerji in zavezniki,
- »politično pravilne« rešitve in storitve,
- preusmeritve in zadržanje,
- različnost,
- izkušeno poslovodstvo,
- »paketiranje« in komunikacije.

Pri ocenjevanju – točkovanju kriterijev – Andriole uporablja analitično hierarhičen proces AHP. Možni izhodi po analizi so:

- investirati,
- ne investirati,
- po potrebi pridobiti dodatne informacije.

V svoji knjigi [And09] je podrobno predstavil proces tehnološkega skrbnega pregleda ter tudi potrdil koncept z osmimi podrobno opisanimi primeri.

Andriole je trenutno profesor poslovne tehnologije na univerzi Villanova.

Andriolova predloga za skrbne preglede je namenjena tehnološkim skrbnim pregledom IT. Preizkušena je v praksi, za ostale tipe skrbnih pregledov pa ni primerna.

2.1.3 Bingov seznam za skrbne preglede

Gordon Bing je v svoji knjigi »*Due Diligence: Planning, Questions, Issues*« podrobno opredelil korake skrbnega pregleda. Njegov moto je postavljati prava vprašanja na pravem mestu in s tem zaščititi investitorja in mu pomagati, da ne naredi večjih napak [Bin08]. Bing je že v devetdesetih letih izdal knjigo na temo skrbnih pregledov »*Due Diligence techniques and analysis*« in jo v novejši izdaji ustrezno nadgradil. Za vsako od 46 področij organizacije je opredelil ključne izzive opazovanj ter seznam vprašanj za posamezno področje (skupno več kot 1100 vprašanj). Bing je določil za področje informacijske tehnologije tri ključne izzive

opazovanj s 34 vprašanji ter za internet tri ključne izzive opazovanj z 14 vprašanji za posamezne skrbne preglede

Bingov seznam za skrben preglede IS je dokaj osnoven in ne opredeljuje analize pridobljenih informacij to je prepuščeno vsakemu pregledovalcu.

2.1.4 Howsonov način izvedbe začetnega skrbnega pregleda

Peter Howson v knjigi »*Due Diligence: The Critical Stage in Mergers and Acquisition*« podrobno opisuje proces izvedbe začetnega skrbnega pregleda od začetka, do zaključnega poročila. Podrobno opredeli vlogo pregledovalcev – izvajalcev skrbnega pregleda. Poda prednosti in slabosti zunanjih svetovalcev v procesu. Začetni skrbni pregled, razdeli na posamezna glavna področja:

- finančno,
- pravno in
- komercialno.

Ostala področja začetnega skrbnega pregleda razdeli na:

- kadrovsko področje in kulturo,
- upravljanje,
- načrte upokojevanja,
- davke,
- okolje,
- informacijsko tehnologijo,
- tehnično področje,
- produkcijo,
- intelektualno lastnino,
- lastništvo,
- protimonopolno,
- zavarovanja/tveganja.

Področje za informacijsko tehnologijo razdeli na dva dela:

- informacijsko tehnologijo (IT), informacijski sistem in procese, ki omogočajo izvajanje poslov,
- operativno tehnologijo (PT), to so procesi, oprema in znanja, ki se uporabljajo za izdelavo in dobavo produktov oziroma storitev.

Samo izvedbo skrbnega pregleda pa deli na tri nivoje [How03]:

- revizijski,
- upravljavski,
- strateški.

Howson podrobno opiše posamezna področja pregleda ter poda poglavitne sklope vprašanj, ki so:

- za informacijsko tehnologijo:
  - kadri v IT,
  - poslovni procesi,
  - uporabniška pričakovanja za oddelek IT,
  - prihodnost,
- za tehnični del – operativno tehnologijo:
  - produkti,
  - skupina za razvoj programske opreme,
  - skupina za kakovost in kvaliteto programske opreme,
  - skupina za tehnično podporo,
  - kultura organizacije,
  - zaposleni – kdo je kritičen za uspešno nadaljevanje,
  - izzivi intelektualne lastnine.

Howson podrobno opiše proces začetnega skrbnega pregleda, izvajalce, način komunikacije, način zbiranja informacij ter tudi priporoča obliko poročila.

2.1.5 INFAUDITOR

»INFAUDITOR« je ekspertni sistem za upravljanje revizijskih pregledov informacijskih sistemov in s tem posledično tudi skrbnih pregledov.

INFAUDITOR je nastal v začetku devetdesetih let prejšnjega stoletja in pokriva tako upravljavski kot tudi tehnični vidik informacijskih sistemov. Ta sistem omogoča razdelitev informacijskega sistema na določena področja, ki se nato delijo na določena podpodročja. Ta členitev se lahko ponavlja, dokler ne pridemo do posameznega osnovnega elementa informacijskega sistema. Vsak takšen element se oceni s pomočjo različnih kriterijev. Celoten informacijski sitem se vnese v hierarhično drevo. Po vzpostavitvi tega drevesa se izvede postopek revidiranja s pomočjo ekspertnega sistema [Ako96].

Ta sistem je uporaben, ko imamo podrobno opisano drevo informacijskih sredstev oz. ko revizijske preglede informacijskega sistema v pregledovani organizaciji večkrat ponavljamo. Pri enkratnem (prvem) pregledu je sistem dokaj kompleksen in časovno zamuden.

2.1.6 ISO/IEC 9000

ISO/IEC je družina standardov za kakovostno upravljanje sistemov, izdanih s strani ISO – Mednarodne organizacije za standardizacijo [ISO08]. Z leti so izpopolnjevali sistem, ki je zadnjo nadgradnjo doživel leta 2008 z objavo standarda ISO/IEC 9001:2008 »*Quality Management Systems – Requirements*«, ki vsebuje:

- uvod,
- zahteve:
  - predmet,
  - normativne reference,
  - izrazi in definicije;
- upravljanje:
  - sistem upravljanja kakovosti,
  - odgovornost vodstva,
  - upravljanje virov,
  - realizacija proizvoda,
  - merjenja, analize in izboljševanje.

Ta standard ima še obvezne pripadajoče dokumente:

- nadzor dokumentov,
- nadzor zapisov,
- notranjo revizijo (kontrolo),
- nadzor neprilagojenih izdelkov (storitev),
- korektivne aktivnosti,
- preventivne aktivnosti.

Standard zahteva tudi dva dodatna dokumenta: Politiko kakovosti ter Poslovnik kakovosti.

Skozi leta so v različnih industrijah pripravili različice tega standarda. Za področje IT so nastale »Tick IT« usmeritve, ki so prilagojene procesom IT, še posebej razvoju programske opreme.

V sklopu skrbnega pregleda lahko ta standard uporabljamo kot analizo upravljanja sistema kakovosti, kar velja še posebej v organizacijah, ki imajo sistem upravljanja kakovosti že vpeljan, in lahko pridobimo informacije o notranjih in vodstvenih pregledih. Vendar je to manjši del skrbnega pregleda. V organizacijah, ki tega sistema še nimajo vpeljanega, je ta analiza otežena.

2.1.7 ISO/IEC 20000

ISO/IEC 20000 je prvi mednarodni standard za upravljanje storitev IT. Objavili so ga leta 2005 na osnovi predhodnika BS 15000.

Standard za upravljanje s storitvami je razdeljen na dva dela – na specifikacijo in praktične napotke. Prvi del ISO/IEC 20000 (Part 1) spodbuja vpeljavo integralnega procesa za učinkovito upravljanje storitev, ki uresničujejo poslovne in uporabniške zahteve. Standard je sestavljen iz desetih poglavij:

- predmet,
- izrazi in definicije,
- načrtovanje in uvajanje sistema upravljanja,
- zahteve za sistem upravljanja,
- načrtovanje in uvajanje novih ali spremenjenih storitev,
- proces izdelave storitve,
- proces sodelovanja,
- proces nadzora,
- proces razrešitve,
- proces objave.

Prvi del ISO/IEC 20000 (Part 2) je »*Code of practice*« – Kodeks upravljanja storitev in opisuje najboljše prakse upravljanja storitev IT v skladu z ISO/IEC 20000 (Part 1).

Ta standard povezuje najboljše prakse – ITIL ogrodja, druga ogrodja in metode za upravljanje storitev, kot na primer »*Microsoft Operation Framework*« ter nekatere komponente COBIT-a.

V sklopu skrbnega pregleda lahko ta standard uporabljamo kot analizo upravljanja storitev IT in pripadajoče procese, kar velja še posebej za organizacije, ki imajo sistem upravljanja storitev IT že vpeljan, in lahko pridobimo informacije o notranjih in vodstvenih pregledih. Vendar je to le manjši del skrbnega pregleda. V organizacijah, ki tega sistema še nimajo vpeljanega, je ta analiza otežena.

2.1.8 ISO/IEC 27000

Družina standardov ISO/IEC 27000 se ukvarja z varovanjem informacij. Predhodnik teh standardov je Britanski standard BS 7799 ter BS ISO/IEC 17999:2000. ISO/IEC 27000 sistemsko rešuje področje varovanja informacij, saj ta standard sestavlja družina standardov v zvezi s SUVI - sistemom za upravljanje varovanja informacij. Skupno bo izdanih več kot dvajset standardov, povezanih s tem področjem.

Preglednica 2 prikazuje seznam vseh načrtovanih standardov s področja sistema upravljanja varovanja informacij.

Preglednica 2: Seznam načrtovanih in izdanih standardov družine ISO/IEC 27xxx

Oznaka standarda ISO/IEC	Originalni naslov standarda	Slovenski naslov standarda	Status/izdan ali v pripravi
27000	Information security management systems — Overview and vocabulary	Sistem za upravljanje varovanja informacij - Pregled in slovarček	izdan
27001	Information security management systems — Requirements	Sistem za upravljanje varovanja informacij - Zahteve	izdan
27002	Code of practice for information security management	Kodeks za upravljanje varovanja informacij	izdan
27003	Information security management system implementation guidance	Sistem za upravljanje varovanja informacij - Smernice za implementacijo	izdan
27004	Information security management — Measurement	Sistem za upravljanje varovanja informacij - Meritve	izdan
27005	Information security risk management	Upravljanje tveganj varovanja informacij	izdan
27006	Requirements for bodies providing audit and certification of information security management systems	Zahteve za organe, ki izvajajo preglede in certifikacijo sistema za upravljanje varovanja informacij	izdan
27007	Guidelines for information security management systems auditing	Smernice za pregledovanje sistema za upravljanje varovanja informacij	izdan
27008	Guidance for auditors on ISMS controls	Smernice za pregledovanje SUVI kontrol	v pripravi
27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Smernice za upravljanje varovanja informacij za telekomunikacijske podjetja, ki temeljijo na ISO/IEC 27002	izdan
27013	Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	Smernice za skupno implementacijo ISO/IEC 20000-1 in ISO/IEC 27001	v pripravi
27014	Information security governance framework	Okvir za obvladovanje varovanja informacij	v pripravi
27015	Information security management guidelines for the finance and insurance sectors	Smernice za upravljanje varovanja informacij za finančni in zavarovalniški sektor	v pripravi
27031	Guideline for ICT readiness for business continuity	Smernice za IKT pripravljenost za neprekinjeno poslovanje	v pripravi
27032	Guideline for cybersecurity	Smernice za "spletno" varovanje	v pripravi
27033	IT network security, a multi-part standard based on ISO/IEC 18028:2006	IT varovanje omrežij, večdelni standard, ki je osnovan na ISO/IEC 18028:2006	izdan
27034	Guideline for application security	Smernice za varovanje aplikacij	v pripravi
27035	Security incident management	Upravljanje incidentov varovanja	v pripravi
27036	Guidelines for security of outsourcing	Smernice za varovanje zunanjega izvajanja	v pripravi
27037	Guidelines for identification, collection and/or acquisition and preservation of digital evidence	Smernice za identifikacijo, zbiranje in/ali nabavo in vzdrževanje digitalnih dokazov	v pripravi
27799	Information security management in health using ISO/IEC 27002	Upravljanje varovanja informacij v zdravstvu z uporabo ISO/IEC 27002	izdan

Za analizo IS lahko uporabimo nekatere že izdane standarde. Med njimi sta tudi: ISO/IEC 27001:2005 – specifikacija SUVI, ki je zamenjal predhodni BS 7799 drugi del, in ISO/IEC 27002 – kodeks prakse, ki opisuje 133 sorodnih kontrol, kako preveriti implementacijo SUVI. Preglednica 3 opisuje glavna poglavja standarda ISO/IEC 27002:2005, za vsako poglavje pa je navedeno število podpoglavij ter pripadajoče število kontrol.

Preglednica 3: Poglavja ISO/IEC 27002:2005 in število kontrol

Oznaka poglavja	Opis	Število podpoglavij	Število kontrol
5.	Varnostna politika	1	2
6.	Organizacija varovanja informacij	2	11
7.	Upravljanje sredstev	2	5
8.	Varovanje človeških virov	3	9
9.	Fizična zaščita in zaščita okolja	2	13
10.	Upravljanje s komunikacijami in s produkcijo	10	32
11.	Nadzor dostopa	7	25
12.	Nakup, razvoj in vzdrževanje informacijskih sistemov	6	16
13.	Upravljanje incidentov pri varovanju informacij	2	5
14.	Upravljanje neprekinjenega poslovanja	1	5
15.	Združljivost	3	10

ISO/IEC 27005 je standard, ki opisuje upravljanja s tveganji v SUVI, ISO/IEC 27006 pa je standard, ki opisuje digitalne certifikate in registracijo. ISO/IEC 27007 je standard, ki usmerja revizorje pri izvedbi revizijskih pregledov vpeljanega sistema SUVI.

2.1.9 KnowledgeLeader seznam skrbnih pregledov

KnowledgeLeader so naročniške internetne strani, ki jih nudi podjetje Protiviti. Na teh straneh nudijo programe revizije, kontrolne sezname, orodja, pripomočke in dobre prakse za interne revizorje in vodje upravljanj s tveganji. Nudijo tudi obsežen kontrolni seznam za poslovne skrbne preglede in za skrbne preglede IT [Kno08].

Ta dokumentacija temelji na orodju »*Six Elements of Infrastructure*«, ki se uporablja za kategoriziranje izzivov, razumevanja nastanka problemov in za prikaz zaključkov, ki izhajajo iz priporočil. »*Six Elements*« so skupni za katerikoli proces ali funkcionalnost. Sestavljajo ga:

- poslovne politike,
- poslovni procesi,
- ljudje in organizacija,
- poročila poslovodstvu,
- metodologije,
- sistemi in podatki.

Protiviti uporablja »*Six Elements*« orodje pri vzpostavitvi novih procesov in analizi obstoječih. Svetujejo pa povezavo »*Six Elements*« orodja z zmožnostno zrelostnim modelom (CMM) za določevanje potrebnih nadgradenj v procesu izboljševanja.

Protiviti uporablja za klasifikacijo procesov ali funkcij ogrodje »*Process Classification Scheme*«, ki deli procese v dve skupini:

- produkcijski procesi,
- upravljavski in podporni procesi.

Za področje IT imajo določen proces »Upravljanje IT in virov«, ki vsebuje naslednje procese:

- opredelitev strategije IT in organizacijo,
- upravljanje varnosti in zasebnosti,
- razvijanje in vzdrževanje rešitev,
- upravljanje infrastrukture IT,
- upravljanje s sredstvi IT,
- podpiranje uporabnikov IT,
- zagotovitev neprekinjenosti (kontinuitete).

Za pregledovanje prisotnosti in učinkovitosti internih kontrol Protiviti uporablja COSO model (»*Committee of Sponsoring Organizations of the Treadway Commission*« - COSO), ki temelji na petih komponentah, ki omogočajo doseganje ciljev organizacije ter izvajanje strategije in pripadajočih poslovnih zahtev. Te komponente so:

- kontrolno okolje,
- ocenjevanje tveganj,
- kontrolne aktivnosti,
- informacije in komunikacije,
- nadziranje.

KnowledgeLeader ima poleg večjega števila smernic za preverjanje internih kontrol, izvajanje revizijskih pregledov in pregledovanje neprekinjenega poslovanja tudi področje za izvajanje skrbnih pregledov, ki pokriva celovito izvajanje skrbnega pregleda v organizaciji (vse procese). Za področje IT ima večje število vprašalnikov, od osnovnega vprašalnika za skrbne preglede do podrobnih vprašalnikov za posamezne segmente IT.

Vprašalniki temeljijo tudi na kontrolah informacijske tehnologije, ki jih priporoča GTAG (*Global Technology Audit Guide*) [IIA05].

KnowledgeLeader nudi na področju skrbnih pregledov IT veliko osnovnih in podrobnih vprašalnikov, ne predstavi pa celovitega procesa izvedbe skrbnega pregleda ter usmeritve za analizo zajetih podatkov.

2.1.10 Kontrolni cilji za informacijsko in sorodno tehnologijo

ISACA (*Information System Audit and Control Association*) je pred leti opredelila obvladovanje IT kot:
»*...odgovornost poslovodstva in upravnega odbora. Sestoji od vodenja organizacijskih struktur in vodenja procesov, ki zagotavljajo, da IT podpira strategijo podjetja in zagotavlja realizacijo ciljev podjetja* [ISA03]«.

Pri tem je potrebno poudariti, da obvladovanje IT ni osamljena aktivnost, temveč del celovitega obvladovanja podjetja, ki je usmerjeno na zaščito lastniške vrednosti in s tem zmanjševanje tveganj, medtem ko je obvladovanje IT razdeljeno na pet področij [ISA09]:

- strateško uskladitev,
- ustvarjanje vrednosti,
- upravljanje virov,
- upravljanje tveganja,
- merjenje izvedbe.

Model COBIT (»*Control Objectives for Information and related Technology*«) je orodje za upravljanje IT, ki vsebuje dobro prakso na celotnem področju uporabe informacijske tehnologije. Nastal je sredi 90 let prejšnjega stoletja in se skozi desetletje iz orodja za pomoč reviziji razvil do orodja za pomoč vodenju in obvladovanju IT. Preglednica 4 prikazuje časovni pregled verzij s področjem in namenom delovanja.

Preglednica 4: COBIT skozi čas

Oznaka	Verzija	Leto izdaje	Področje
COBIT	ver.1	1996	revizija ("IT audit")
	ver.2	1998	nadzor ("IT control")
	ver.3	2000	upravljanje ("IT management")
	ver.4	2005	obvladovanje ("IT governance")
	ver.4.1	2007	dopolnitve obvladovanja
	ver.5	2012	obvladovanje organizacije ("enterprise governance")

Model COBIT združuje posamezne procese v štiri domene:

- planiranje in organizacija,
- nabavo in uvedbo,
- dostavo in podporo,
- nadzor in ocenitev.

Vsakemu od COBIT procesov so določeni kontrolni cilji in je prirejen zrelostni model [ITG07]. COBIT temelji na pregledu posameznih kontrol, ki se nahajajo v posameznih področjih informacijske tehnologije.

Preglednica 5 prikazuje osnovne gradnike ogrodja COBIT ver 4.1.

Preglednica 5: COBIT 4.1

POSLOVNE ZAHTEVE	**DOMENE**	Načrtujte in organizirajte	**PROCESI**	PO1 Opredelite strateški načrt za IT	**KONTROLNI CILJI**
				PO2 Opredelite informacijsko arhitekturo	
				PO3 Določite tehnološko usmeritev	
				PO4 Opredelite procese, organizacijo in razmerja IT	
				PO5 Upravljajte investicije v IT	
				PO6 Sporočajte cilje in usmeritev vodstva	
				PO7 Upravljajte človeške vire v sektorju IT	
				PO8 Upravljajte kakovost	
				PO9 Ocenjujte in obvladujte tveganja IT	
				PO10 Upravljajte projekte	
Informacijski kriteriji: uspešnost, učinkovitost, zaupnost, celovitost, razpoložljivost, skladnost in zanesljivost		Nabavite in vpeljite		AI1 Določite avtomatizirane rešitve	**Zrelostni model:** 0-neobstoječe, 1-začetno/ Ad hoc, 2-ponovljivo, vendar intuitivno, 3-opredeljeno, 4-vodeno in merljivo, 5-optimizirano
				AI2 Nabavite in vzdržujte aplikacijske programe	
				AI3 Nabavite in vzdržujte tehnološko infrastrukturo	
				AI4 Omogočite delovanje in uporabo	
				AI5 Zagotovite vire IT	
				AI6 Upravljajte spremembe	
				AI7 Namestite in potrdite rešitve in spremembe	
		Izvajajte in podpirajte		DS1 Opredelite in upravljajte ravni storitve	
				DS2 Upravljajte storitve tretje stranke	
				DS3 Upravljajte delovanje in zmogljivost	
				DS4 Zagotovite neprekinjenost storitev	
				DS5 Zagotovite varnost sistemov	
				DS6 Ugotovite in porazdelite stroške	
				DS7 Izobrazite in usposobite uporabnike	
IT viri: aplikacije, informacije, infrastruktura in ljudje				DS8 Upravljajte službo za pomoč uporabnikom in obvladujte incidente	**SPLOŠNE KONTROLE IT IN APLIKACIJSKE KONTROLE**
				DS9 Upravljajte konfiguracijo	
				DS10 Upravljajte probleme	
				DS11 Upravljajte podatke	
				DS12 Upravljajte fizično okolje	
		Spremljajte in vrednotite		ME1 Spremljajte in vrednotite delovanje IT	
				ME2 Spremljajte in vrednotite notranje kontrole	
				ME3 Zagotovite skladnost z zunanjimi zahtevami	
				ME4 Zagotovite upravljanje IT	

Vsakemu od 34 IT procesov ustreza kontrolni cilj na najvišjem nivoju. Pri doseganju ciljev se upoštevajo poslovne zahteve za naslednje informacijske kriterije:

- učinkovitost,
- uspešnost,
- zaupnost,
- celovitost,
- razpoložljivost,
- skladnost,
- zanesljivost.

Model COBIT je revizorjem informacijskih sistemov dobro znan kot pripomoček za revidiranje informacijskih sistemov. V zadnjem času je postal znan tudi izven revizorskih vrst, saj vse več IT vodstvenih kadrov ugotavlja, da je COBIT možno uporabljati kot mehanizem za obvladovanje IT. S COBIT-om je moč doseči učinkovito in varno uporabo informacijskih sredstev za doseganje poslovnih ciljev družbe[Baj06]. Prav tako lahko COBIT uporabimo kot orodje za oblikovanje procesov IT [Žva10].

Vodstvo IT lahko s COBIT metodologijo poišče odgovore na naslednja vprašanja:

- Kateri so indikatorji dobrega delovanja?
- Kateri so kritični faktorji uspeha?
- Kakšna so tveganja, da ne dosežemo postavljenih ciljev?

S pomočjo COBIT metodologije lahko izvedemo pregled ustreznosti in kakovosti implementacije procesov [Šal06], ki opisujejo sistem ocenjevanja prisotnosti kontrol po sistemu zrelostnega modela.

ISACA je skupaj z IT Governance Institutom sredi aprila 2012 izdala novo verzijo COBIT 5., ki združuje določena ogrodja, metodologije, ki so jih v zadnjih letih objavili v sklopu IT Governance Instituta in ISACA (Vrednost IT, Ogrodje za obvladovanje tveganj IT, Ogrodje za zagotavljanje jamstev IT), in združevanje drugih metodologij, okvirov in dobrih praks (ITIL V3, ISO/IEC 27000, ISO/IEC 9000:2008 in TOGAF V9) [ISA10].

2.1.11 Mike Siscov seznam za skrbne preglede

Mike Sisco je definiral ključne cilje za izvedbo skrbnih pregledov IT [Sis02a]:

- zmanjševanje tveganj,
- doseganje cilje povezovanj (združevanj),
- vpliv na uporabljeno tehnologijo,
- izvedba mirnega prehoda, ki minimizira storitveno problematiko za zaposlene,
- povečanje usmeritev organizacije IT in njeno okrepitev.

Mike Sisco poudarja tudi pomembnost priprave pregledovalca pred odhodom na pregled v organizacijo [Sis02b]. Sisco opredeljuje, da ima vsak IT skrbni pregled naslednje izzive:

- trenutno izvajanje IT,
- tveganja in načrt zmanjševanja le-teh,
- finančni načrt (pričakovani stroški in proračun IT za nadaljevanje izvajanja),
- zahteve za naložbe in investicije,
- priložnosti in priporočen načrt,
- načrt prehoda,
- poročilo o skrbnem pregledu.

Mike Sisco je pripravil tudi vzorčno poročilo skrbnega pregleda IT.

Siscov seznam za skrben pregled IS je bolj procesno (postopkovno) usmerjen, ne spušča pa se v podrobnosti posameznih vprašanj, ki jih mora pregledovalec postavljati, da pridobi želene podatke in s tem informacije o skrbnem pregledu IS.

2.1.12 Ogrodje za ocenjevanje skrbnega pregleda IT

»*Information Technology Assessment Due Diligence Framework*« (v nadaljevanju – ITADD) ogrodje so razvili v letu 2005 kot študentski projekt na Univerzi v Teksasu (Austin, ZDA) v okviru Red McCombs Business School [Bau05]. Mentor projekta je bil prof. Hussein Tandriverdi. Ogrodje temelji na COBIT, ITIL in COSO metodologijah.

Koncept ITADD je hierarhično razdeljeno na:

- podporo strategiji,
- neprekinjenem poslovanju,
- človeškem kapitalu,
- produkciji,
- IT osnovnih sredstvih.

ITADD je sestavljen iz:

- pred nakupnih (nakupnih) predlog,
- vprašalnikov,
- ITADD kontrolne plošče,
- pred nakupnih (nakupnih) predlog za izdelavo poročil.

ITADD ogrodje je namenjeno skrbnim pregledom in začetnim skrbnim pregledom [Sun06], vendar se do sedaj še ni uveljavilo v praksi, kjer bi lahko pridobili povratne praktične izkušnje in informacije o učinkovitosti in uspešnosti tega ogrodja.

2.1.13 Ogrodje za upravljanje s tveganji IT

Upravljanje poslovnih tveganj je eno od osnovnih zadolžitev in odgovornosti poslovodstva vsake organizacije. Skoraj vsaka poslovna odločitev zahteva odločitve najožjega vodstva med možnimi tveganji in potencialnimi prihodki. ISACA je leta 2009 objavila Ogrodje za upravljanje s tveganji IT (»Risk IT«), ki temelji na osnovnih principih tveganja IT [ISA09a]:

- vedno poveži poslovne cilje,
- uskladi upravljanje IT poslovnih tveganj z upravljanjem tveganj organizacije,
- spodbujaj odprto in pošteno komunikacijo o tveganjih IT,
- vzpostavi primerno obveščanje z vrha pri določanju in uveljavljanju osebne odgovornosti za izvajanje s sprejemljivo in primerno določeno stopnjo odstopanja,
- neprestano izvajaj proces kot del dnevnih aktivnosti.

Celovit pristop tveganja IT sestavljajo tri področja:

- obvladovanje tveganj (RG – »Risk Governance«),
- ocenjevanje tveganj (RE – »Risk Evaluation«),
- odziv na tveganje (RR – »Risk Response«).

Ogrodje za upravljanje s tveganji IT dopolnjuje COBIT na področju obvladovanja informacijskega sistema za področje upravljanja s tveganji. Ogrodje za upravljanje s tveganji IT vključuje tudi scenarije tveganj IT [ISA09b]. Nanj, vplivajo naslednje komponente:

- osebe, ki generirajo tveganja (notranji, zunanji),
- tipi tveganj (škodoželjni, slučajen, napake, naravne nesreče, zunanje grožnje),
- dogodki (razkritje, prekinitev, sprememba, kraja, uničenje, neučinkovit načrt, neučinkovita izvedba, nepravilna uporaba, pravila in predpisi),
- viri/sredstva (ljudje in organizacija, procesi, infrastrukturni objekti, podatki in aplikacije),
- čas (trajanje, trenutek dogodka (kritičen/nekritičen), čas odkritja).

Ogrodje za upravljanje s tveganji IT deli tveganja na dva dela – tveganja ob izvajanju IT storitev in pri projektih IT.

Podobno kot za COBIT in vrednost IT ima tudi celovit pristop za upravljanje s tveganji IT zrelostni model za vsak proces.

2.1.14 Ogrodje za zagotavljanje jamstva IT

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 IT [ISA08]. Nastalo je na praktičnih izkušnjah in temelji na dobrih praksah.

Poslovodstva po svetu se srečujejo z vprašanjem o uspešnosti implementiranih internih kontrol. Podobno kot interne kontrole za finančno področje so v zadnjem času postale pomembne tudi interne kontrole v informacijskih sistemih.

To ogrodje se uporablja za učinkovito pregledovanje navedenih kontrol. Sestavljajo ga štirje sklopi:

- uvod v ogrodje,
- standardi jamstva: določitev skupne referenčne točke,
- smernice jamstva: vzpostaviti standarde v praksi,
- orodja in tehnike jamstva.

Smernice jamstva so razdeljene na pet področij s skupno 41 usmeritvami, definicijami, postopki in procesi. Ogrodje za zagotavljanje jamstva v procesu pregledovanja uporablja COBIT metodologijo.

2.1.15 Pickardov seznam za skrbne preglede

Scott S. Pickard je v knjigi »*Due Diligence List*« pripravil več kot 2000 vprašanj v sklopu štirinajstih glavnih funkcionalnih področij organizacije [Pic02]. Ti podatki so dosegljivi tudi na spletnih straneh www.duediligneceliist.com. Področje IT je eno izmed glavnih funkcionalnih področij v organizaciji, za katere Pickard v okviru skrbnega pregleda postavlja 130 vprašanj – nekatera področja jih vsebujejo več, druga manj.

Pickardov seznam za skrben preglede IS je dokaj osnoven. To je bolj kontrolni seznam, ki omogoča pregledovalcu postaviti vsa vnaprej pripravljena vprašanja. Seznam ne opredeljuje analize pridobljenih informacij; to je prepuščeno vsakemu pregledovalcu.

2.1.16 Sistem uravnoteženih kazalnikov

Sistem uravnoteženih kazalnikov v informacijski tehnologiji (nekateri ga prevajajo tudi kot IT sistem uravnoteženih kazalnikov) ali s tujko »*IT Balanced Score Card*« (BSC) sta razvila Robert Kaplan in David Norton v začetku devetdesetih let 20. stoletja. Sistem se je dopolnjeval več let.
Temelji na upravljanju z učinki, ki omogoča podjetjem, da izvajajo strategijo na meritvah in posledično nadaljnjih aktivnostih. Osnovna ideja je, da razvoj podjetja ne temelji samo na tradicionalnem finančnem razvoju, temveč je dopolnjen z meritvami zadovoljstva uporabnikov, internih procesov in z zmožnostjo vpeljave novosti. Ta štiri področja so imenovali perspektive. Metodologija vsebuje tri-nivojsko strukturo za vse štiri predlagane perspektive. Ti nivoji so:

- poslanstvo (»*mission*«),
- cilji (»*objectives*«),
- razmerja (»*measures*«).

Poslovni sistem uravnoteženih kazalnikov [Cra07] je razdeljen na štiri perspektive:

- finančno (»*financial perspective*«), ki predstavlja povečanje dobičkonosnosti,
- uporabniško (»*customer perspective*«), ki predstavlja zmanjševanje uporabniških pritožb,
- interno poslovno procesno (»*internal business process perspective*«), ki predstavlja izboljšano produktivnost izdelave,
- perspektivo izobraževanja in rasti (»*learning and growth perspective*«), ki predstavlja učinek zmanjševanja odpovedi zaposlenih.

Sistem uravnoteženih kazalnikov v informacijski tehnologiji se navezuje na poslovni sistem uravnoteženih kazalnikov [Gre00]. Razdeljen je na štiri perspektive:

- uporabniško usmerjenost (»*user orientation*«), ki predstavlja uporabniško oceno IT – »Kako uporabniki vidijo IT?«,
- operativno-produkcijsko odličnost (»*operational excellence*«), ki predstavlja IT procese za razvoj in implementacijo aplikativne rešitve – »Kako učinkoviti in zmogljivi so IT procesi?«,
- usmerjenost v prihodnost (»*future orientation*«), ki predstavlja tehnološke in kadrovske vire za izvajanje IT storitev – »Kakšna je pozicija IT, da uresniči prihodnje cilje?«,
- poslovno sodelovanje (»*business contribution*«), ki predstavlja učinek poslovnih vrednosti glede na IT investicije – »Kakšen je pogled ravnateljstva – poslovodstva na IT sektor?«.

Vsako od perspektiv je potrebno preoblikovati v ustrezne metrike in izvajati meritve glede na trenutno stanje. To ocenjevanje je potrebno periodično ponavljati in izvajati analize z zastavljenimi cilji in s primerjalnimi informacijami (»*benchmarking*«). V zadnjih letih se je sistem uravnoteženih kazalnikov usmeril na IT. Specializiral se je na individualna upravljanja IT. Razvite so že aplikativne rešitve, ki podpirajo to metodo.

2.1.17 Vrednost IT

Vrednost IT (»Val IT«) je standardno ogrodje za podjetja, ki jim omogoča izbiro in upravljanje IT odvisnih poslovnih investicij in IT osnovnih sredstev. Poudarek je na investicijskih programih, ki omogočajo podjetju optimalno vrednost. Vrednost IT temelji na COBIT-u.

Vrednost IT razširja in dopolnjuje COBIT ter omogoča obsežno kontrolno ogrodje za IT vodenje. Osredotoča se na odločitve o investicijah (ali se izvajajo prave zadeve) ter na realizacijo koristi (ali se pridobivajo koristi), medtem ko se COBIT osredotoča na izvajanje (ali se zadeve izvajajo pravilno in v pravi smeri).

Vrednost IT ima 4 glavna področja:

- strateško (ali izvajamo prave zadeve),
- arhitekturno (ali izvajamo v pravi smeri/konceptu),
- koristno (ali pridobivamo koristi),
- učinkovito (ali izvajamo pravilno).

Okvir Vrednosti IT je komplementaren COBIT-u s poslovne in finančne perspektive in je v pomoč poslovodstvu in strokovnjakom v IT z namenom ustvarjanja vrednosti IT [ITG08]. Vrednost IT definira več procesov, ki so združeni v tri področja:

- procesi obvladovanja vrednosti (»VG - *Value Governance*«, 6 procesov),
- procesi upravljanja portfelja (»PM - *Portfolio Management*«, 6 procesov),
- procesi upravljanja investicij (»IM - *Investment Management*«, 10 procesov).

Podobno kot COBIT ima Vrednost IT za vsakega od treh področji opredeljen zrelostni model, kjer je spekter ocen od 0, ki določa nivo, kjer organizacija še ni prevzela določenega modela, do ocene 5, kjer opredeljuje nivo, da je organizacija v celoti prevzela in vpeljala izkušnje upravljanja merjenja in optimiziranja vrednosti skozi vpeljavo poslovnih sprememb investicij in prav tako prevzela neprestano nadgrajevanje vrednosti tudi v bodoče.

Vrednost IT ima širši pogled kot COBIT. Usmerjena je na obvladovanje informacijske tehnologije v organizaciji, medtem ko je COBIT bolj usmerjen na zgoraj navedene procese na nivoju celotne organizacije.

Kar nekaj je pristopov, kako implementirati Vrednost IT [ISA09c]. ISACA je tudi izdala publikacijo [ISA10a], ki govori o poslovnih študijah za to vrednost, kjer so opisani: doprinos vrednosti IT k poslovnim študijam; poslovne študije, ki jih opredeljuje Vrednost IT; način uporabe zrelostnega modela Vrednosti IT ter poslovna študija za specifične ključne upravljavske primere.

Vrednost IT prav tako kot COBIT tudi opredeljuje zadolžitve posameznikov po profilih v organizaciji za uspešno implementacijo celovitega pristopa.

2.1.18 Zbirka napotkov za upravljanje in uvajanje storitev IT

»*Information Technology Infrastructure Library*« (v nadaljevanju ITIL) je nastal v Evropi kot zbir dobrih praks za razumevanje upravljanja z IT storitvami ter temeljnih IT storitvenih procesov.

ITIL je ogrodje oziroma pristop (»*Framework*«) za uspešno implementacijo IT storitvenih procesov. Zadnja večja sprememba, to je verzija 3, je bila objavljena v maju 2007 in mnogo bolj določa upravljanje s storitvami. Ogrodje je razdeljen na 5 delov, ki tvorijo »življenjski cikel« upravljanja storitev:

- strategija storitev (»*service strategy*«):
  - upravljanje s portfeljem storitev (»*service portfolio management*«),
  - upravljanje z zahtevami (»*demand management*«),
  - finančno upravljanje (»*financial management*«);

- načrtovanje storitev (»*service design*«):
  - upravljanje z nivojem storitev (»*service level management*«),
  - upravljanje kataloga storitev (»*service catalogue management*«),
  - upravljanje z razpoložljivostjo (»*availability management*«),
  - upravljanje z informacijsko varnostjo (»*information security management*«),
  - upravljanje odnosa z dobavitelji (»*supplier management*«),
  - upravljanje s sposobnostmi/zmožnostmi (kapacitetami) (»*capacity management*«),
  - upravljanje z IT neprekinjenimi storitvami (»*IT service continuity management*«);
- prehod storitev (»*service transition*«):
  - upravljanje s spremembami (»*change management*«),
  - aktiva storitev in upravljanje s konfiguracijami (»*service asset and configuration management*«),
  - upravljanje implementacije v produkcijo (»*release and deployment management*«);
- delovanje storitev (»*service operation*«):
  - upravljanje z incidenti (»*incident management*«),
  - upravljanje z dogodki (»*event management*«),
  - izpolnjevanje zahtev (»*request fulfillment*«),
  - upravljanje s problemi (»*problem management*«),
  - upravljanje z dostopi (»*access management*«),
  - pomoč uporabnikom (»*service desk*«),
  - tehnično upravljanje (»*technical mana*gement«),
  - aplikativno upravljanje (»*application management*«),
  - upravljanje z IT delovanjem (»*IT operation management*«);
- nenehno izboljševanje storitev (»*continuous service improvement*«):
  - 7 korakov izboljševanja procesov (»*7 steps process improvement*«).

Osnove ogrodja ITIL so sedaj vključena tudi v standard ISO/IEC 20000 – Standard za upravljanje s storitvami, ki se je razvil iz BS 15000.

ITIL je procesno naravnan in ne predpisuje uporabniku, s katerim delom (storitvijo) naj začne implementacijo. Uporabnik lahko začne z implementacijo kateregakoli procesa. ITIL je eden izmed ogrodij, ki so namenjena usmerjanju IT k produkciji in storitvam [Jia08].

V zadnjem času se veliko govori in piše o storitveno orientirani arhitekturi. Alter poudarja, da sta ITIL in COBIT trenutno orientirana v upravljanje in kontrolo IT storitev, ki jih izvajajo IT skupine za poslovne organizacije [Alt10]. Merhout in Havleka ugotavljata, da lahko COBIT in (ali) ITIL uporabljamo za upravljanje in ocenjevanje IT funkcij v posamezni organizaciji [Mer08].

ITIL ogrodje je možno uporabiti za pristop pri skrbnem pregledu, a se lahko podrobno oceni procese v IT ter z njimi povezane storitve. Celovite slike in analize IT pregledovane organizacije pa ni mogoče pridobiti.

2.1.19 Zmožnostno zrelostni model

CMM (»*Capability Maturity Model*«) je model za izboljšanje in ocenitev učinkovitosti ter kvalitete organizacij, ki razvijajo programsko opremo. Ta model je razvila Univerza Carnegie Mellon University iz ZDA v okviru SEI (»*Software Engineering Institute*«) v osemdesetih letih dvajsetega stoletja- objavili so ga leta 1991. Leta 2002 so objavili CMMI (»*Capability Maturity Model Integration*«) - integralno ogrodje zmožnostno zrelostnega modela [McK05].

Zmožnostni zrelostni model predstavlja priporočila in način izboljšav družbam, ki razvijajo programsko opremo in želijo povečati zmožnost svojih procesov. Uporabljata se dva tipa predstavitvenih modelov: stopenjski in nadaljevalni.

Stopenjski nivoji so (od najnižje razvitega proti najvišjemu):

- začetni (»ad hoc«),
- voden,
- definiran,
- kvalitetno voden,
- optimizacijski.

Zrelostni nivo je stopenjski in zahteva, da organizacija razvije vse svoje procese na določeno zrelostno stopnjo, nato pa nadaljuje z razvojem oziroma nadgradnjo na naslednjo stopnjo.

Nadaljevalni model pa omogoča organizaciji, da bolj razvije posamezno procesno področje. Tu se uporabljajo naslednji zmožnostni nivoji:

- 0 – nepopoln,
- 1 – izvajan,
- 2 – voden,
- 3 – definiran,
- 4 – kvalitetno voden,
- 5 – optimiziran.

Pri nadaljevalnem modelu ni pomembno, da organizacija sočasno razvija posamezne procese na isti nivo, ampak se lahko odloči, kako bo poljubno razvijala določene procese in področja.
SEI je razvil vrsto standardov, ki omogočajo uporabo zmožnostno zrelostnega modela v informacijski tehnologiji, med drugimi tudi SCAMPI (»*Standard CMMI Appraisal Method for Process Improvement*«) in ARC (»*Appraisal Requirements for CMMI*«).

Kot rezultate SCAMPI metode se izdelajo različne ocenitve (določena stopnja zrelosti organizacije ali zmožnosti procesov). Uporablja se za interno ocenitev napredka razvoja procesov. SCAMPI metoda definira fazo priprave in planiranja ocenitve, fazo izvajanja ocenitve in fazo poročanja o ocenitvi, znotraj vsake faze pa so podrobno opisane še posamezne aktivnosti. Vsak proces v SCAMPI metodi je opisan z naslednjimi atributi:

namen, začetni kriteriji, vhodni podatki, aktivnosti, izhodni podatki, rezultati, izhodni kriteriji, ključne točke, orodja in tehnike, metrike, verifikacija in validacija, zapisi, priredbe, povezave z drugimi procesi in seznam aktivnosti [Šau06].

2.1.20 Ostalo

Zgoraj sem naštel nekatere metode, orodja, in celovite pristope (ogrodja) za izvedbo skrbnega pregleda. Zavedam se, da ta seznam ni končen, saj nisem mogel pridobiti podrobnih podatkov ostalih, ki jih lahko delimo v naslednje skupine: veliki 4, svetovalna podjetja, posamezniki in znanstveni pristopi.

Veliki 4
Med velike 4 (s tujko »*Big 4*«) štejemo štiri svetovne revizijske družbe (po abecednem redu): Deloitte, Ernest and Young (E&Y), KPMG in Price Waterhouse Coopers (PWC). Te revizijske hiše svojih metod, ki so jih razvile za izvedbo skrbnega pregleda, ne objavljajo, saj le-te štejejo med svoje konkurenčne prednosti.

Svetovalna podjetja:
V posameznih delih sveta lahko tudi globalno delujejo različna podjetja, ki v svojih storitvah nudijo tudi izvedbe različnih tipov skrbnih pregledov za določena področja pregleda.
Nekatera med njimi so (po abecedi):

- Accenture (New York, ZDA),
- Diomo Coproration (Florida, ZDA),
- Grant Thornton (Illinois, ZDA)
- LCS (Australia),
- One Neck (Arizona, ZDA),
- PSC (Tennessee, ZDA),
- Roach & Stolz Software GmBH (Muenchen, Nemčija),
- Strativa (Kalifornija, ZDA),
- Towers Perrin – sedaj Towers Watson (New York, ZDA),
- in še mnogo drugih.

Tudi ta podjetja, tako kot veliki 4, ne objavljajo podrobnosti o njihovih metodah, orodjih ali celovitih pristopih, ki so jih razvila, prevzela ali dopolnila.

Posamezniki:
Na medmrežju se pojavlja kar nekaj posameznikov, ki ponujajo svetovanja na področju skrbnih pregledov. Zgoraj sem omenil nekatere, med drugimi se pojavlja tudi Curt Sahakian (Illinois, ZDA), ki pa ne ponuja metode, orodja ali celovitega pristopa, temveč nasvete, kako izvesti skrben pregled. Znanih je 12 Sahakianovih nasvetov (zapovedi) za skrbne preglede.

Znanstveni pristopi:
Pri pregledovanju znanstvenih prispevkov nisem zasledil velikega števila objavljenih del na temo skrbnih pregledov. Med redkimi prispevki so objavljene razprave:

- o izzivih tehnološkega skrbnega pregleda [And07],
- o primerih neuspehov sistemov upravljanja varovanja informacij, kje navajajo avtorji tudi potencialni vzrok nekvalitetnega skrbnega pregleda [Cho07],
- o zmanjševanju tveganj pri poslovnem sodelovanju s pomočjo skrbnega pregleda [Goo07],
- o raziskavi procesnega modela izločitve informacijske tehnologije [Lee08],
- o strateškem usklajevanju pri nabavah in združevanju (M&A – »*Merges and Acquisitions*«), kjer je predstavljena pomembnost začetnih skrbnih pregledov [Meh07],
- o učinkovitosti izločanja storitev in učinkovitosti organizacije ter skrbnem pregledu pred samo odločitvijo [Str08].

Z znanstvenega vidika se diskusije o tveganju v IT in informacijskih sistemih vrstijo že več kot trideset let [She04]. Po opažanjih, Shererja in Alterja, IT vodje in tudi raziskave določajo tveganja preko negativnih učinkov. Izbrane delovne skupine so tveganja opisale kot »možnost izgube ali uničenja« in »možnost prenašanja škode ali izgube«. Ker imajo različne dimenzije in nivoje, jih moramo pravilno razumevati in upravljati.
»*Uspešno upravljanje s tveganji v praksi je tisto, ki omogoča, da vsako tveganje neprestano identificiramo in analiziramo njegovo vplivnost. Tveganja se ublažijo, zasledujejo in kontrolirajo z učinkovito uporabo posameznih virov*« [Smi01]. Brez ustreznega upravljanja s tveganji podjetja neprestano »gasijo požare«. Sherer in Alter sta opisala različne primere komponent in faktorjev tveganja v literaturi [She04]. Ugotovila sta 228 faktorjev tveganja v različnih člankih, ki temeljijo na določenem sistemu (»*work system framework*«).

DeLone in McLean opozarjata, da je v raziskavah uspešnosti informacijskih sistemov skoraj toliko načinov merjenja, kot je raziskav [DeL01]. Razvila sta svoj model merjenja uspešnosti informacijskega sistema, ki vsebuje 6 glavnih dimenzij oziroma kategorij uspeha. Alter navaja podobno veliko število merjenj uspešnosti, a se osredotoči na dve dimenziji – tip sistema in interes lastnikov [Alt99].

Veliko znanstvenikov je nadgrajevalo DeLonov in McLeanov model, med njimi tudi Seddon s sodelavci. Razvili so alternativni model, ki temelji na sedmih glavnih vprašanjih in dvodimenzionalni metriki s 30 možnimi meritvami [Sed04].

Različni znanstveniki se odločajo za različne karakteristike merjenja uspešnosti informacijskega sistema. Tako pri raziskavah v laboratorijih kot tudi pri raziskavah v praksi se odločijo za različne metode, ki pa večinoma temeljijo na vprašalnikih.

2.1.21 Izkušnje v Sloveniji

V slovenskem prostoru ni veliko primerov izvedb posebnih IT skrbnih pregledov oz. ni podatkov, da bi bile objavljene za javnost in vsebovale tudi informacije o uporabljenih metodah, orodjih in pristopih.

Po osamosvojitvi 1991 so se nekatera slovenska podjetja začela intenzivno širiti predvsem na jugovzhodne, nekatera pa tudi na druge evropske trge (Gorenje, d. d., Krka, d. d.). Za analizo informacijskih sistemov so v večini primerov uporabljala lastna znanja (Nova Ljubljanska banka, d. d., Nova kreditna banka Maribor, d. d., Telekom Slovenije, d. d., Mobitel, d. d., …).

Glede ostalih tipov skrbnih pregledov je morda še najbolj znan pregled projekta Sigma v eni izmed slovenskih finančnih organizacij, ki ga je opravilo podjetje Accenture v začetku 21 stoletja. Rezultati tega pregleda oziroma zaključno poročilo skrbnega pregleda ni bilo objavljeno za javnost.

2.2 Primerjalna analiza metod in orodij

V začetku tega poglavja sem navedel nekaj orodij, metod, standardov, metodologij in ogrodij za izvedbe skrbnih pregledov IS. Vsak od navedenih načinov je kvaliteten in uporaben za določena področja. Uporaba določenega načina je v največji meri odvisna od predznanja in izkušenj izvajalca skrbnega pregleda IS ter od okolja, ki ga pregledujemo. Priporoča se, da skrbne preglede IS izvaja več strokovnjakov z bogatimi izkušnjami na področju analiz ter revidiranja IS.

2.2.1 Opis pomembnih podatkov za odločanje pri skrbnih pregledih

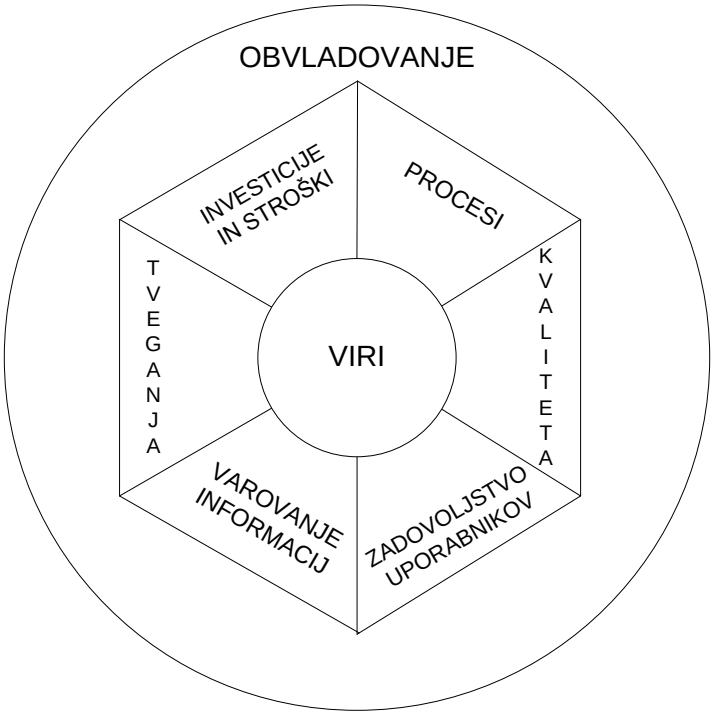
Za primerjalno analizo zgoraj navedenih orodij, metodologij in pristopov je najprej potrebno določiti skupine podatkov, ki tvorijo informacije za določanje in ocenjevanje IS pregledovane organizacije.

Glede na izkušnje, pregledano literaturo in usmeritve sem se odločil za naslednjo delitev (združevanje) skupin primerjalnih parametrov:

- viri IS,
- procesi IS,
- varovanje informacij,
- tveganja IS,
- kvaliteta IS,
- investicije in stroški IS,
- zadovoljstvo uporabnikov IS,
- obvladovanje IS.

Na sliki 1 je grafični prikaz lociranja posameznih skupin primerjalnih parametrov. Osnova, lahko rečem žarišče dogajanja, je skupina Viri, ki se navezuje na vse ostale skupine. Vse skupaj pa obkroža oziroma povezuje parameter obvladovanje. Posamezne skupine primerjalnih parametrov so opisane v nadaljevanju.

Slika 1: Primerjalni parametri



Viri IS:

Med vire informacijskega sistema uvrščam:

- infrastrukturo – v računovodski terminologiji opredmetena osnovna sredstva:
  - strojno opremo,
  - komunikacijsko opremo,
  - ostalo opremo za nemoteno delovanje računalniške opreme (nemotena preskrba elektrike, hlajenje, sistemi za avtomatsko gašenje, ustrezni senzorji, …),
  - prostore (sistemski prostor, rezervna lokacija, lokacija za magnetne medije, pomožni prostori, komunikacijski prostori, pisarne informatikov, …);
- aplikacije - v računovodski terminologiji neopredmetena osnovna sredstva:
  - aplikacijsko programsko opremo,
  - sistemsko programsko opremo,
  - pomožne programe;
- informacije (podatki) v elektronski obliki,
- ljudi:
  - zaposlene v organizaciji v organizacijski enoti, ki podpira IT,
  - zunanje izvajalce,
  - zunanje vzdrževalce,
  - zunanje svetovalce;
- projekte:
  - interne projekte IT,
  - projekte, ki bodo realizirali uporabniške zahteve.

Procesi IS:
Med procese IS uvrščam procese, ki jih izvaja IT za nemoteno delovanje informacijskega sistema v organizaciji, ter procese, ki zagotavljajo izgradnjo novih produktov in storitev oziroma vzdrževanje ali ukinjanje le-teh.

Varovanje informacij:
To področje sicer presega IT v pregledovani organizaciji, a se navezuje tudi na varovanje informacij v elektronski obliki. Med varovanje informacij uvrščam:

- politiko varovanja informacij,
- organiziranost varovanja informacij,
- upravljanje z viri,
- fizično varovanje,
- postopke,
- logično varovanje,
- varovanje informacij v primeru nabave, razvoja in vzdrževanja komponent IT,
- upravljanje z varnostnimi incidenti,
- upravljanje neprekinjenega poslovanja,
- skladnost z zakonodajo.

Tveganja IS:
Med tveganja IS uvrščam aktivnosti na področju načrtovanja pregledovanja tveganj, izvajanja analiz, vrednotenja in zmanjševanja tveganj ter aktivnosti na področju spremljanja in kontrol. Te aktivnosti se nenehno izvajajo in izboljšujejo nivo tveganja IS v pregledovani organizaciji.

Kvaliteta IS:
Med kvaliteto IS uvrščam izvajanje notranjih in vodstvenih presoj ter ukrepov za izboljšanje. Te aktivnosti se podobno kot pri tveganju IS, nenehno izvajajo in izboljšujejo kvaliteto IS.

Investicije in stroški IS:
V to področje uvrščam aktivnosti, ki izvajajo načrtovanje, izvajanje (spremljanje) in kontrolo investicij in stroškov IS, skratka, upravljanje z investicijami in stroški IS v pregledovani organizaciji.

Zadovoljstvo uporabnikov IS:
V to področje uvrščam aktivnosti, ki za notranje uporabnike IS v pregledovani organizaciji, izvajajo: zbiranje, analizo, implementacijo in spremljanje izboljšav, in sicer tako za dnevne operativne aktivnosti IT kot tudi za izvedbo in zaključke uporabniških projektov.

Obvladovanje IS:
V to področje uvrščam naslednje aktivnosti:

- upravljanje IS,
- vodenje IS,
- produkcijo IS,

- prisotnost kontrol IS.

Na kratko sem opisal osem skupin primerjalnih podatkov, ki sem jih izbral za analizo posameznih orodij, metodologij in celovitih pristopov za izvedbo skrbnih pregledov.

2.2.2 Analiza metod in orodij glede na zbrane podatke

Zgoraj navedene metode, orodja in celoviti pristopi ter usmeritve za skrbne preglede so zelo raznolike tako po obsegu in načinu pristopa kot po najpomembnejšem delu skrbnega pregleda – zbranih podatkih, ki nam omogočijo pridobiti določene informacije. Ta del sem razdelil na naslednje dele:

- analizo,
- predpogoje,
- pomanjkljivosti (slabosti).

Analiza:

Za analizo sem uporabil skupine podatkov, ki sem jih opisal v predhodnem poglavju. Preglednica 6 prikazuje analizo glede na zmožnost pridobitve podatkov v določenih sklopih podatkov za določeno metodo, metodologijo, orodje ter celovit pristop. V preglednici so možne naslednje oznake celovitosti pridobitve podatkov: visoka - ***, srednja - **, nizka - * ter prazno, če določena skupina ne omogoča pridobitve podatkov.

Preglednica 6: Analiza glede na skupine podatkov

ogrodja, metode, metodologije, standardi, orodja	obvladovanje: upravljanje, vodenje, produkcija, kontrole.	procesi	viri: aplikacija, informacije, infrastruktura, ljudje, projekti.	investicije in stroški	kvaliteta / kakovost	tveganja	varovanja informacij	zadovoljstvo uporabnikov
Analiza upravljanja neprekinjenega poslovanja (BCM / BS2599 BCM Standard)	**	**	**			**		
Andriolova predloga za skrbne preglede	*	*	**	**	*	*	*	
Bingov seznam za skrbne preglede	**		**		*		*	*
Howsonov način izvedbe začetnega pregleda	*		**		*		*	
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)	*	**	*	*				
Vrednost IT (*Val IT* 2.0)	***	**	**	***	*	**		
Zbirka napotkov za upravljanje in uvajanje storitev IT (ITIL 3.0)	**	***	*		**	**	**	*
Zmožnostno zrelostni model (CMM)	**	**	**		*			

Nekateri načini opisujejo tudi postopek izvedbe posameznih aktivnosti. Razdelil sem jih v tri sklope. Podroben opis postopkov nudi naslednje načine: ogrodje za ocenjevanje skrbnih pregledov (ITADD), KnowledgeLeaderjev seznam skrbnih pregledov in Howsonov način izvedbe začetnega pregleda. Grob opis postopkov nudijo: Mike Siscov, Bingov, in Picardov

seznam za skrbne preglede. Ostali načini ne nudijo opisa postopkov izvedbe aktivnosti skrbnih pregledov IS.

Ta ocena je subjektivna in teoretična, saj v praksi nisem mogel preveriti vseh teh metod, orodij, celovitih pristopov in usmeritev.

Predpogoji:
Določeni načini za svojo učinkovito izvedbo potrebujejo predpogoje, ki omogočajo hitrejše ter kvalitetnejše preglede. Ti načini so:

- INFAUDITOR, ki je učinkovitejši ob drugi ali večkratni ponovitvi analize IS po tej metodi,
- ISO/IEC 9000, ki je učinkovitejši, če ima pregledovana organizacije že implementiran oziroma tudi certificiran sistem upravljanja kakovosti,
- ISO/IEC 20000, ki je učinkovitejši, če ima pregledovana organizacija že implementiran oziroma tudi certificiran sistem upravljanja storitev IT,
- ISO/IEC 27000, ki je učinkovitejši, če ima pregledovana organizacija že implementiran oziroma tudi certificiran sistem upravljanja varovanja informacij,
- kontrolni cilji za informacijsko in sorodno tehnologijo (COBIT 4.1), ki so učinkovitejši, če ima pregledovana organizacija že praktične izkušnje s to metodologijo,
- ogrodje za upravljanje s tveganji IT, ki je učinkovitejši, če ima pregledovana organizacija že praktične izkušnje s tem ogrodjem,
- sistem uravnoteženih kazalnikov (BSC), ki je učinkovitejši, če ima pregledovana organizacija že implementiran tak sistem,
- Vrednost IT (V*al IT 2.0*), ki je učinkovitejša, če ima pregledovana organizacija že praktične izkušnje s to metodo,
- zbirka napotkov za upravljanje in uvajanje storitev IT (ITIL 3.0), ki je učinkovitejša, če ima pregledovana organizacija že praktične izkušnje s to zbirko napotkov,
- zmožnostno zrelostni model (CMM), ki je učinkovitejši ob drugi ali večkratni ponovitvi analize IS po tej metodi.

Ti predpogoji niso obvezni, ampak priporočljivi, če so implementirani, omogočajo učinkovitejšo ter predvsem hitrejšo izvedbo skrbnega pregleda.

Pomanjkljivosti (slabosti):
Načini se med seboj zelo razlikujejo. Nekateri so primernejši za pregled posameznega področja IS, drugi so bolj univerzalni. V nadaljevanju je na kratko podana subjektivna ocena pomanjkljivosti oziroma slabosti posameznega načina:

- Analiza upravljanja neprekinjenega poslovanja je omejena samo na določeno področje, ki je sicer zelo pomembno (upravljanje neprekinjenega poslovanja), a ne omogoča izvedbe pregleda vseh področij (domen) IS. Prav tako ta način nima odločitvenega modela.

- Andriolova predloga za skrbne preglede je razvita za poseben tip skrbnega pregleda – tehnološki skrbni pregled. Ta način je opredeljen do podrobnosti. Za ostale tipe skrbnega pregleda pa opisan način ni primeren.
- Bingov seznam za skrbne preglede vsebuje kontrolni seznam za pregled celotne organizacije in ima dokaj omejen seznam vprašanj za preverjanje IS (46 sklopov s skupaj več kot 1100 vprašanji). Gordon Bing ne opredeljuje analize pridobljenih informacij, kar je prepuščeno vsakemu pregledovalcu. Prav tako ta način nima odločitvenega modela.
- Howsonov način izvedbe začetnega pregleda, opisuje celoten postopek/proces izvedbe začetnega skrbnega pregleda in ima omejen seznam vprašanj za preverjanje IS (11 sklopov s skupaj 93 vprašanji). Peter Howson ne opredeljuje analize pridobljenih informacij, ampak je to prepuščeno vsakemu pregledovalcu. Prav tako ta način nima odločitvenega modela.
- INFAUDITOR je primarno orodje za pomoč revizorjem IS in je uporaben pri večkratni ponovljivosti aktivnosti. Ni primeren za začetne skrbne preglede ali za prvo izvedbo skrbnega pregleda. Omejen je na znane revizorske cilje pregleda in ne prikaže celotne analize IS. Prav tako ta način nima odločitvenega modela.
- ISO/IEC 9000 je primeren za pregled sistema upravljanja kakovosti IS. Ostalih področij (domen) IS ne pokriva. Prav tako ta način nima odločitvenega modela.
- ISO/IEC 20000 je primeren za pregled sistema upravljanja storitev IT. Ostalih področij (domen) IS ne pokriva. Prav tako ta način nima odločitvenega modela.
- ISO/IEC 27000 je primeren za pregled sistema upravljanja varovanja informacij. Ostalih področij (domen) IS ne pokriva. Za nekatera druga področja je možno uporabiti kakšno od 133 kontrol, ki so navedene v kodeksu prakse za preverjanje implementacije SUVI. Prav tako ta način nima odločitvenega modela.
- KnowledgeLeader seznam skrbnih pregledov vsebuje veliko vprašalnikov in seznamov za posamezna področja (domene) IT, vendar pa ne vsebuje odločitvenega modela, nima opisa procesa ter ne opredeljuje analize pridobljenih informacij, ampak je to prepuščeno vsakemu pregledovalcu.
- Kontrolni cilji za informacijsko in sorodno tehnologijo določajo 34 procesov v 4 področjih domen IS. Uporabljajo se za pomoč pri revizijah IT, saj je s skupno 210 kontrolnimi cilji podrobno opisan IS za opredeljene procese. Metodologija je opredeljena kot pomoč pri obvladovanju IS. Pomanjkljivost je v pomanjkanju obzorja za varovanje informacij, drugih procesov v IS ter obvladovanju kakovosti, tveganj in širšemu pogledu IS s stališča celotne organizacije. Teh slabosti se tudi zavedata IT Governance institut in ISACA in sta zato objavila novo verzijo te metodologije [ISA10]. Prav tako ta način nima odločitvenega modela.
- Mike Siscov seznam za skrbne preglede vsebuje vrsto kontrolnih seznamov za začetni skrbni pregled IS. Grobo je opisan tudi proces izvedbe, medtem ko se pa ne spušča v podrobnosti posameznih vprašanj, ki jih mora pregledovalec postavljati, da pridobi željene podatke in s tem informacije o skrbnem pregledu IS. Pomanjkljivosti so v tem, da ni usmeritev za analizo pridobljenih podatkov in v pomanjkanju odločitvenega modela.

- Ogrodje za ocenjevanje skrbnega pregleda IT je med vsemi načini eden izmed najbolj podrobnih, vendar se do sedaj še ni uveljavilo v praksi, kjer bi lahko pridobili povratne praktične izkušnje ter informacije o učinkovitosti in uspešnosti tega ogrodja. Edina pomanjkljivost, poleg povratnih informacij o praktičnih izkušnjah, je, da ta način ne vsebuje odločitvenega modela.
- Ogrodje za upravljanje s tveganji IT je način, ki omogoča podroben pregled tveganj IS, ne pokriva pa ostalih področij IS za celovito analizo IS. Prav tako ta način nima odločitvenega modela.
- Ogrodje za zagotavljanje jamstva IT je način, ki opredeljuje način izvajanja revizije IS. Ne pokriva ostalih področij IS za celovito analizo IS. Prav tako ta način nima odločitvenega modela.
- Pickardov seznam za skrbne preglede vsebuje kontrolni seznam za pregled celotne organizacije in ima dokaj omejen seznam vprašanj za preverjanje IS (14 sklopov s skupaj več kot 2000 vprašanji). Steve S. Pickard ne opredeljuje analize pridobljenih informacij, ampak je to prepuščeno vsakemu pregledovalcu. Prav tako ta način nima odločitvenega modela.
- Sistem uravnoteženih kazalnikov je možno uporabljati za omejeno analizo, torej za tista področja (domene) IS, za katera je ta sistem v pregledovani organizaciji že implementiran in se praktično izvaja, ne more pa se uporabljati za celovito analizo IS.
- Vrednost IT je način, ki omogoča podroben pregled investicij in stroškov IS, ostalih področij pa ne pokriva. Prav tako ta način nima odločitvenega modela.
- Zbirka napotkov za upravljanje in uvajanje storitev IT je način, ki omogoča pregled večine procesov IS, ne opredeljuje pa podrobnosti o investicijah in stroških IS, kontroli v IS in o tveganju ter omejeno pokriva ostale skupine podatkov za primerjavo. Celovite slike in analize IT pregledovane organizacije ni mogoče pridobiti. Prav tako ta način nima odločitvenega modela.
- Zmožnostno zrelostni model je omejen samo na določena področja in procese IS, ne moremo pa ga uporabiti kot edini način za izvedbo skrbnega pregleda. Prav tako ta način nima odločitvenega modela.

2.2.3 Primerjava metod in orodij

Glede na zgoraj navedene analize na skupine podatkov, možne predpogoje ter pomanjkljivosti/slabosti lahko izvedemo primerjavo metod in orodij, ki omogoča celovit pregled le-teh po naslednjih parametrih:

- predpogoji,
- prednosti,
- pomanjkljivosti/slabosti,
- čas, potreben za izvedbo,
- odločitveni model.

Preglednica 7: Primerjava posameznih metod in orodij

Ogrodja, metode, metodologije, standardi, orodja	Predpogoji	Prednosti	Pomanjkljivosti / slabosti	Čas, potreben za izvedbo	Odločitveni model
Analiza upravljanja neprekinjenega poslovanja (BCM / BS2599 BCM Standard)	ni	podrobno opredeli upravljanje neprekinjenega poslovanja	omejen na področje neprekinjenega poslovanja	ni podatka	ne
Andriolova predloga za skrbne preglede	ni	podroben opis procesa, načina pristopa, zbiranja podatkov za tehnološki skrbni pregled	namenjena samo tehnološkem skrbnim pregledom	ni podatka	da - vsebuje
Bingov seznam za skrbne preglede	ni	vprašalnik za IT področje	omejen seznam za IS področje, ne vsebuje smernic za analizo podatkov	ni podatka	ne
Howsonov način izvedbe začetnega pregleda	ni	podroben opis procesa, udeležencev, način pristopa, zbiranja podatkov in poročanja	omejen seznam za IS področje, ne vsebuje smernic za analizo podatkov	od nekaj dni do nekaj tednov	ne
INFAUDITOR	priporočeno	"knowledge base" orodje za revizijo IS	ni primeren za začetni skrbni pregled	ni podatka	ne
ISO/IEC 9001	priporočeno	podrobno opredeli sistem upravljanja kakovosti	omejen na področje upravljanja kakovosti; če organizacija nima vpeljanega tega sistema, je analiza otežena	ni podatka	ne
ISO/IEC 20000	priporočeno	podrobno opredeli sistem upravljanja storitev IT	omejen na področje upravljanja storitev IT; če organizacija nima vpeljanega tega sistema, je analiza otežena	ni podatka	ne
ISO/IEC 27000	priporočeno	podrobno opredeli sistem upravljanja varovanja informacij v organizaciji	omejen na področje upravljanja varovanja informacij; če organizacija nima vpeljanega tega sistema, je analiza otežena	ni podatka (certifikacijski pregled v organizaciji je 2 + 2 dneva za določena področja); v 3 pregledih (letih) se pregleda celota	ne
KnowledgeLeaderjev seznam skrbnih pregledov	ni	podroben opis zbiranja podatkov (veliko število različnih vprašalnikov) za začetni ali splošni skrbni pregled	podroben opis procesa izvedbe, ne vsebuje smernic za analizo podatkov	ni podatka	ne
Kontrolni cilji za informacijsko in sorodno tehnologijo (COBIT 4.1)	priporočeno	podroben način pregledovanja 4 področij s 34 procesi. Vsebuje tudi zmožnostne zrelostne modele za posamezne procese	nima integriranih povezav na storitvene procese IT, analiz tveganja za varovanje informacij na področju organizacije in ne obravnava stroškov in investicij IT	ni podatka	ne
Mike Siscov seznam za skrbne preglede	ni	podroben opis procesa in struktura zaključnega poročila	ni podrobnih vprašalnikov ter ni usmeritev za analizo pridobljenih podatkov	ni podatka	ne
Ogrodje za ocenjevanje skrbnih pregledov (ITADD)	ni	ogrodje temelji na COBIT, ITIL in COSO metodologijah; podroben opis procesa	ni podatkov o praktičnih izkušnjah	od nekaj dni do nekaj tednov	ne
Ogrodje za tveganja IT (Risk IT)	priporočeno	podroben način pregledovanja tveganj IT; vsebuje tudi zmožnostne zrelostne modele za posamezne procese	ne pokriva ostalih področij IS za celovito analizo IS	ni podatka	ne
Ogrodje za zagotavljanje jamstva IT (ITAF)	ni	podrobno opredeljuje način izvajanja IS	ne pokriva ostalih področij IS za celovito analizo IS	ni podatka	ne
Pickardov seznam za skrbne preglede	ni	vprašalnik za IT področje	omejen seznam za IS področje, ne vsebuje smernic za analizo podatkov	ni podatka	ne
Sistem uravnoteženih kazalnikov (BSC)	priporočeno	omogoča spremljavo meritev določenih aktivnosti IS	omejen na domene IS, za katere je sistem že vpeljan; ni primeren za celovito analizo IS	ni podatka	ne
Vrednost IT (V*al IT* 2.0)	priporočeno	omogoča podroben pregled stroškov in investicij IS; vsebuje tudi zmožnostne zrelostne modele za posamezne procese.	ne pokriva ostalih področij IS za celovito analizo IS	ni podatka	ne
Zbirka napotkov za upravljanje in uvajanje storitev IT (ITIL 3.0)	priporočeno	podrobno opredeljuje procese za upravljanje in uvajanje storitev	ne opredeljuje podrobnosti o investicijah in stroških IS, kontrola v IS, tveganja, ter omejeno pokriva ostala skupine podatkov za	ni podatka	ne
Zmožnostno zrelostni model (CMM)	priporočeno	uporablja se za interno ocenitev napredka razvoja procesov; obstajajo tudi nadgradnje SCAMPI in ARC	opredeljen je za določene procese; ne moremo ga uporabiti kot edini način za izvedbo skrbnega pregleda	ni podatka	ne

Preglednica 7 prikazuje primerjavo za zgoraj navedene parametre. Samo en način vsebuje tudi enostaven odločitveni model. Pri dveh načinih je možno grobo oceniti čas, potreben za izvedbo skrbnega pregleda. Pri več kot polovici načinov se priporočajo predpogoji, kar ni odločitvena zahteva, a v primeru predpogojev je prvi pregled s tem načinom dokaj omejen in zahteva več časa za pridobitev ustreznih informacij.

2.2.4 Uporabnost metod in orodij pri različnih tipih skrbnih pregledov

Na začetku so bili pri opisu skrbnih pregledov navedeni različni tipi le-teh. Opisane metode in orodja oz. načini za analizo IS niso enako primerni za različne tipe. Nekateri načini so bolj univerzalni, drugi pa bolj specializirani za posamezen tip skrbnega pregleda.

Preglednica 8: Možnost uporabe določenega načina pri posameznem tipu skrbnega 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	*	*	*	*
Howsonov način izvedbe začetnega pregleda	**	*	*	
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 upravljanje s tveganji IT (Risk IT)	*	*	*	*
Ogrodje za zagotavljanje jamstva IT (ITAF)		**	**	
Pickardov seznam za skrbne preglede	*	*	*	*
Sistem uravnoteženih kazalnikov (BSC)		*	*	
Vrednost IT (Val IT 2.0)	*	*	*	*
Zbirka napotkov za upravljanje in uvajanje storitev IT (ITIL 3.0)	**	**	*	*
Zmožnostno zrelostni model (CMM)		*	*	

Preglednica 8 prikazuje mojo oceno možnosti uporabe določene metode in orodja – načina za posamezen tip skrbnega pregleda. V preglednici so možne naslednje oznake uporabnosti: zelo uporaben, primeren za tak tip skrbnega pregleda - ***, delno uporaben, srednje primeren za izvedbo takega tipa skrbnega pregleda - **, omejeno uporaben, komaj primeren za tak tip skrbnega pregleda - * ter prazno, če določen način ni uporaben oz. ni primeren za izvedbo takega tipa skrbnega pregleda.

S tem sem zaključil primerjalno analizo metod in orodij, ki so bili opisani na začetku tega poglavja.

2.3 Vzroki za odločitev o razvoju novega ogrodja – celovitega pristopa

Zgoraj so opisane metode in orodja (načini) za izvedbe skrbnih pregledov IS. Prav tako so podani analiza glede na različne poglede in predpogoji pri nekaterih načinih ter opisane pomanjkljivosti in slabosti.

Analizo lahko povzamem v naslednjih točkah:

- Nekateri načini za učinkovitejšo izvedbo priporočajo predpogoje. Brez le-teh je možno izvesti analizo določenega področja IS z navedenim načinom, a izvedba zahteva več časa ter aktivnosti pregledovalcev.
- Večina navedenih načinov sama za sebe ne omogoča celovite analize IS. Posamezni načini so osredotočeni na določeno področje (domeno) IS ali na določene aktivnosti. Za izvedbo je potrebno uporabiti kombinacijo različnih načinov, pa še to ne omogoči celovite izvedbe.
- Načini, kot so ogrodje za ocenjevanje skrbnih pregledov (ITADD), KnowledgeLeaderjev seznam skrbnih pregledov in Howsonov način izvedbe začetnega pregleda, omogočajo izvedbo velike večine aktivnosti, vendar nobeden od navedenih ne vsebuje odločitvenega modela. KnowledgeLeaderjev seznam skrbnih pregledov in Howsonov način izvedbe začetnega pregleda tudi nimata navedenih smernic za analizo pridobljenih podatkov, ampak je to prepuščeno posameznemu pregledovalcu. Howsonov način izvedbe začetnega pregleda je, kot že samo ime pove, primarno namenjeno začetnim skrbnim pregledom, a je možno večino navedenih aktivnosti in seznamov uporabiti tudi pri splošnem pregledu.
- Pri večini načinov tudi nista navedena čas pregleda in podatek o obsegu. Pri ogrodju za ocenjevanje skrbnih pregledov (ITADD) ter Howsonovem načinu izvedbe začetnega pregleda je navedeno, da pregled lahko izvedemo med nekaj dnevi in tedni. Za potrebe certifikacije po ISO/IEC standardih je v Sloveniji obseg presoje opredeljen z zahtevami mednarodnega partnerja in odvisen tudi od določenega standarda. Za ISO/IEC 27001:2005 se ob postopku (v letu certifikacije) izvedejo dva dneva predpresoje[2] ter dva dneva presoje[3]. V treh letih se na letnih presojah pregleda celotni sistem v organizaciji. Izračun pokaže, da je za celoto potrebnih 20 ali več človek dni.

Proces izvedbe skrbnega pregleda je pri načinih, ki to opredeljujejo, zelo podoben. Analizirani načini za zbiranje podatkov nudijo veliko vprašalnikov, kontrolnih seznamov ter smernic, kako pridobimo podatke.

[2] dveh ali več presojevalcev, odvisno od velikosti pregledovane organizacije
[3] dveh ali več presojevalcev, odvisno od velikosti pregledovane organizacije

Za kvalitetno izvedbo skrbnega pregleda pa je vendarle potrebno zbrane podatke ustrezno analizirati – pretvoriti v informacije, ki s pomočjo odločitvenega modela naročniku podajo kratko in jasno informacijo glede IS pregledane organizacije. Te aktivnosti je potrebno izvesti v čim krajšem možnem roku, da ne trpi kvaliteta zbranih in analiziranih podatkov.

Zahtev, ki so navedene v okvirju, nisem v celoti zasledil v nobenem od navedenih načinov, zato sem se odločil za razvoj celovitega pristopa (ogrodja), ki bo za vse tipe skrbnih pregledov omogočal celovito analizo vseh področij (domen) IS v pregledovani organizaciji. Celovit pristop naj omogoča:

- podroben opis procesa,
- zahteve za pridobivanje dokumentacije,
- ustrezne vprašalnike,
- smernice za analizo podatkov,
- enostaven odločitven model,
- izvedbo pregleda v kratkem času.

S tem je zaključeno poglavje Uporaba posameznih metod in orodij. Podroben opis celovitega pristopa sledi v naslednjem poglavju.

Podrobnosti o temi tega poglavja sem navedel tudi v naslednjih prispevkih:

a) Začetni skrbni pregled za področje informacijskih sistemov v finančnih organizacijah, Zbornik prispevkov: Dnevi slovenske informatike 2008, Portorož ISBN 978-961-6165-26-6

b) 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

c) Celovit pristop izvedbe skrbnega pregleda, Zbornik prispevkov: Dnevi slovenske informatike 2010, Portorož ISBN 978-961-6165-32-7

d) Celovit pristop izvedbe skrbnega pregleda, Uporabna informatika, 2010, številka 4, stran str. 193-204

e) Analysis of Different Approaches to the Delivery of Information System Due Diligence, Proceedings: 2nd Conference on Information Society and Information Technologies ISIT2010, 2010, Novo mesto, ISBN 978-961-92509-5-2

f) Framework for the delivery of Information System Due Diligence, Information System Management, prispevek je bil sprejet 11.3.2012, prispevek bo po navedbah glavnega urednika objavljen v enem letu

3 CELOVIT PRISTOP IZVEDBE SKRBNEGA PREGLEDA

S skrbnimi pregledi IS se ukvarjam že več kot deset let. Začel sem v letu 1997, ko sem analiziral IS v regijskih bankah bivše Ljubljanske banke, ki so v začetku 90 let prejšnjega stoletja postale samostojne. Te banke so bile v Skupini NLB, a jih je NLB d. d. postopoma ponovno vključila v osnovno banko kot posamezne podružnice.

S širjenjem trgov na Srednjo in Južno Evropo je v prvem desetletju tega tisočletja NLB d. d. izvedla večje število začetnih skrbnih pregledov. Osebno sem se udeležil več kot 80 % teh pregledov, to je več kot 25 začetnih skrbnih pregledov. Poleg tega sem izvedel še več kot 40 splošnih skrbnih pregledov IS.

Skozi večletno prakso so nastajali vprašalniki, vzpostavljala sta se proces in celovit pristop, ki je nastal leta 2007.

3.1 Cilji celovitega pristopa

Osnovni cilj je bil razviti tak celovit pristop, ki bo omogočal hitro in učinkovito izvedbo vseh aktivnosti, da bo mogoče naročniku predstaviti informacije, ki bodo kratko in jedrnato predstavile trenutni status IS, potencialna tveganja na področju IS, trenutno vrednost IS ter pri začetnih skrbnih pregledih IS oceniti vrednost stroškov in investicij za nadaljnjih 5 let v IS pregledovane organizacije. Podroben opis časa, potrebnega za izvedbo začetnega skrbnega pregleda IS, je podan v poglavju 3.2.2.

Skozi razvoj celovitega pristopa sem dodal še razvoj in potrditev enostavnega odločitvenega modela, ki lahko naročniku začetnega skrbnega pregleda IS s pretvorbo analiziranih podatkov v numerične vrednosti omogoča enostavno odločitev: DA – nadaljevanje aktivnosti oziroma NE – zaključek aktivnosti.

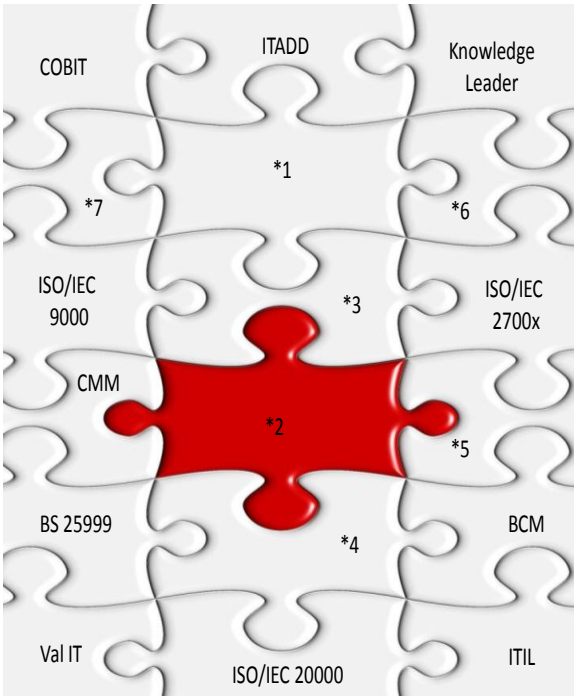
Celovit pristop je nastajal skozi leta in s spoznavanjem različnih drugih metod, standardov, dobrih praks in pristopov. V celovit pristop sem vključeval posamezne aktivnosti, ki sem jih ob naslednjih pregledih testiral in zadržal, nadgradil ali pa opustil.

Grafično lahko celovit pristop prikažemo kot sestavljenko dobrih praks in idej posameznih pristopov, kot sestavljenko – nekakšen »*puzzle*«, ki je predstavljen na sliki 2.

Nekateri v sliki 2 navedeni pristopi so podrobno opisani v poglavju 2. Z znakom * in s številko so označeni deli celovitega pristopa:

1. procesi,
2. odločitveni model,
3. seznami,
4. aktivnosti,
5. vprašalniki,
6. poročila,
7. potrebni časovni okviri.

Slika 2: Grafični prikaz sestavin celovitega pristopa

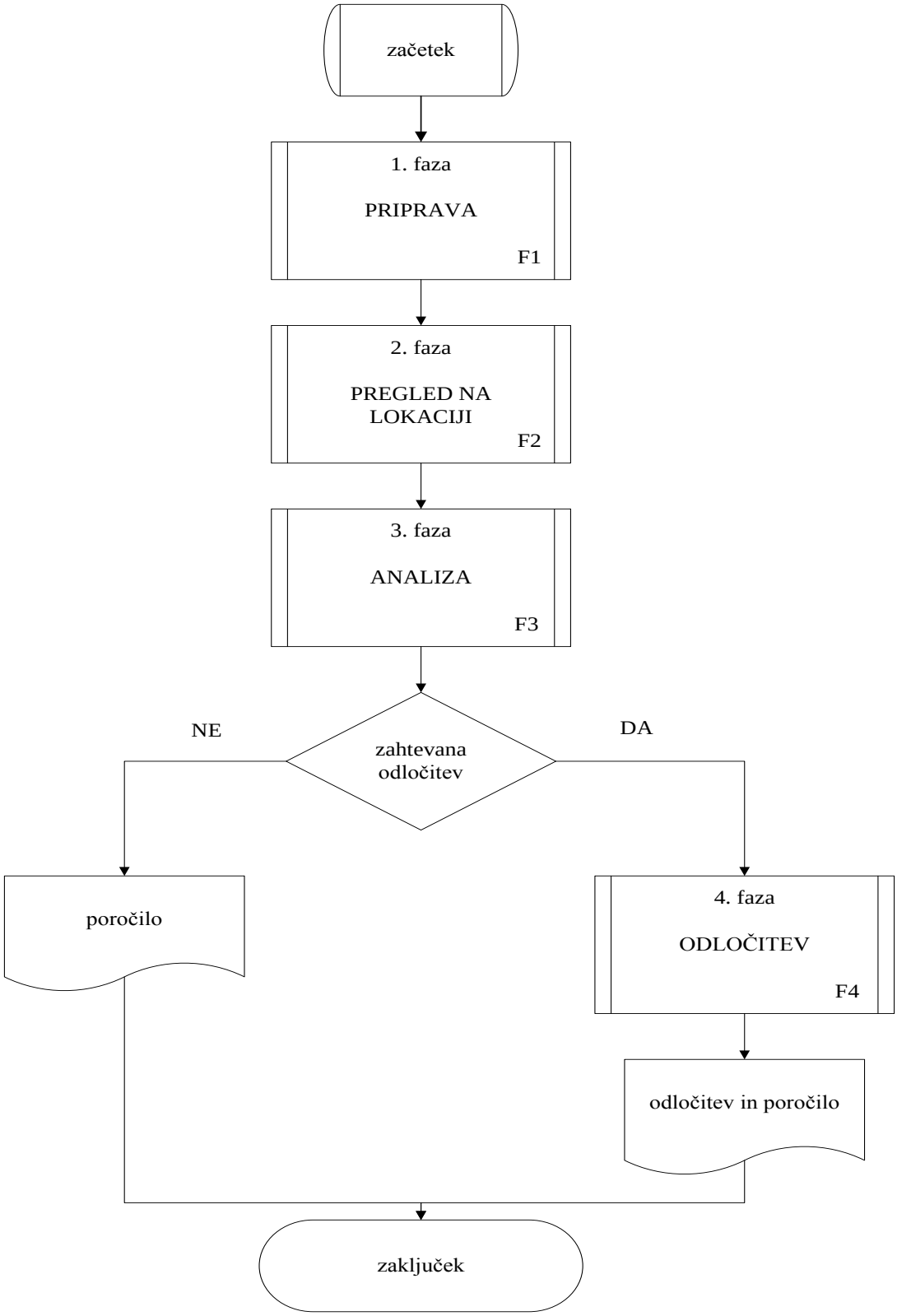


Na področju revizije IS je veliko literature, ki povezuje »*mapping*« - posamezne pristope in s tem uporabniku omogoči uporabo različnih pristopov in dopolnitve z drugimi. ISACA in ITGI sta na tem področju v zadnji 5 letih zelo napredovala in pripravila vrsto dokumentov na področju povezav posameznih metod, standardov in procesov:

- Uvod v poslovni model varovanja informacij [ISA09d],
- PAM (*Process Assessment Model*) z uporabo COBIT [ISA11],
- Povezovanje SEI CMM za programsko opremo z COBIT [ITG06],
- Povezovanje ITIL v3 z COBIT [ITG08a],
- Povezovanje COBIT, ITIL v3 in ISO/IEC 27002:2005 za poslovne koristi [ITG08b],
- Povezovanje ISO/IEC z COBIT [ITG11],
- Pregled mednarodnih smernic IT [ITG11a].

Deli celovitega pristopa so podrobno opisani v nadaljevanju tega poglavja.

Slika 3: Celovit pristop izvedbe skrbnega pregleda



Slike so narejene z MS Visio – uporabljeni so liki za tok poteka (»*Flow chart*«).

3.2 Opis procesa

V okviru Univerzalnega celovitega pristopa izvedbe skrbnega pregleda IS – UISDDFW (»*Universal Information System Due Diligence Framework*«) je opisan proces izvedbe skrbnega pregleda, ki ga sestavljajo štiri faze s pripadajočimi aktivnostmi:

- priprava,
- pregled na lokaciji,
- analiza,
- odločitev.

Grafični prikaz je na sliki 3.

3.2.1 Priprava

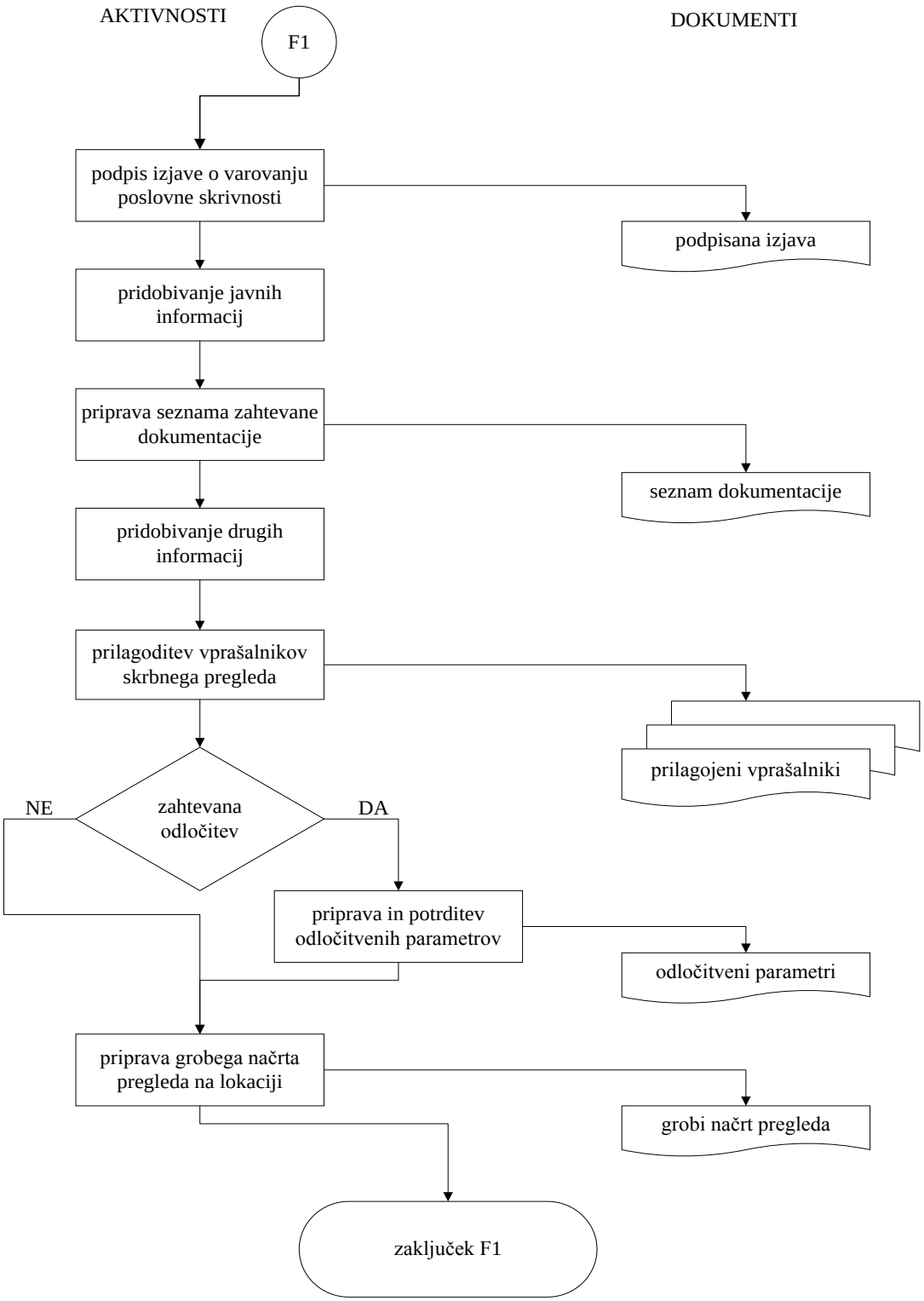
Grafični opis faze je prikazan na sliki 4. V okviru te faze se izvajajo naslednje aktivnosti:

Podpis izjave o varovanju poslovne skrivnosti - pred začetkom aktivnosti pregleda se v skladu z dobro prakso in varovanjem informacij podpiše izjavo – dogovor o varovanju poslovne skrivnosti (»NDA – *nondisclosure agreement*«). Ta dogovor podpišejo organizacija, ki izvaja pregled, pregledovana organizacija in tudi posamezniki, ki izvedejo pregled posameznega področja, med njimi tudi pregled IS. V večini primerov se ta dogovor podpiše v fazi priprave, v redkih primerih se to izvede v sklopu druge faze – pregleda na lokaciji.

Pridobivanje javnih informacij – o pregledovani organizaciji mora ekipa, ki bo v naročnikovem imenu izvedla skrbni pregled IS, pridobiti čim več javnih podatkov. Informacije o letnih poročilih organizacije je danes lahko pridobiti, saj so večinoma objavljene na medmrežnih straneh organizacije. Prav tako je možno preko medmrežja pridobiti tudi druge javne informacije, pripravljene s strani same organizacije in tudi drugih (na primer: bonitetne informacije, statistične podatke, informacije določenih združenj). Ekipa lahko za izvedbo skrbnega pregleda IS pridobi večino informacij, zakonov in drugih aktov, ki jih mora pregledovana organizacija upoštevati oziroma izvajati.

Priprava seznama zahtevane dokumentacije – posreduje se ga vnaprej v pregledovano organizacijo z zahtevo, da se seznam pripravi do samega pregleda na lokaciji, oziroma se določene dokumente posreduje vnaprej pred izvedbo pregleda izvajalcu le-tega. Ta seznam je relativno dolg, saj zahteva okoli 25 tipov različnih dokumentov, ki jih je potrebno pripraviti, kar znese od 50 do 80 ali celo več dokumentov. V prilogi 9.1 je okviren seznam za skrbni pregled IS, ki se posreduje koordinatorju pregleda v pregledovani organizaciji. Ta seznam je nastal iz izkušenj pri izvedbi pregledov. Glede na velikost pregledovane organizacije se lahko seznam ustrezno prilagodi. Seznam ima oznake V - za velike organizacije, S - za srednje velike organizacije in M - za male organizacije.

Slika: 4 Grafični prikaz prve faze



Za razumevanje oznak se v primeru načrtovanja, pregleda velike organizacije zadrži celoten seznam dokumentacije, vse označene dokumente V, S in M. Če se načrtuje pregled srednje

velike organizacije, se posreduje seznam dokumentacije, ki ima oznake S in M. Če se načrtuje pregled majhne organizacije, se posreduje seznam dokumentacije, ki ima oznako M.

Ta seznam je bolj orientacijske narave, saj lahko pregledovalec za področje IS poljubno prilagodi seznam pregledovani organizaciji.

V nekaterih primerih začetnega skrbnega pregleda pripravi ciljna organizacija ustrezno dokumentacijo, ki jo združi v tako imenovano podatkovno sobo oziroma »*data room*«. Člani ekipe pred samim začetnim pregledom pridobijo informacije o dokumentaciji, ki je zbrana v podatkovni sobi – seznam dokumentacije. V takih primerih izvajalec skrbnega pregleda za področje IS pregleda pripravljeni seznam podatkovne sobe in ga primerja s seznamom zahtevane dokumentacije. Odstopanja se identificira in se jih v tem primeru posreduje kot seznam dodatne zahtevane dokumentacije, ki naj se zbere in dopolni v podatkovni sobi.

Pridobivanje drugih informacij se izvede vzporedno s pridobivanjem javnih informacij. Cilj te aktivnosti je zbrati čim več neformalnih informacij o pregledovani organizaciji. V letih 2002, 2003 in 2006 sem se na Gartner simpozijih pogovarjal z njihovimi strokovnjaki o procesih skrbnih pregledov IS. Ti strokovnjaki so na tako imenovanih pogovorih iz oči v oči (»*one to one session*«) svetovali in zagovarjali pridobivanje »mehkih« informacij s pomočjo socialnih omrežij. Zagovarjali so stališča, da so te informacije zelo uporabne, če ne ključne.

Te druge informacije se lahko pridobi od:

- uporabnikov – komitentov pregledovane organizacije,
- zaposlenih v sami organizaciji,
- bivših zaposlenih,
- ponudnikov storitev IS,
- konkurence,
- drugih.

Prilagoditev vprašalnikov skrbnega pregleda – v sklopu pregleda se uporablja nekaj posebnih vprašalnikov, ki so del celovitega pristopa. Vsebina posameznih vprašalnikov bo podrobneje opisana v nadaljevanju. Trenutno so ti vprašalniki v celoti na razpolago v dveh jezikih (slovenščini in angleščini).V tej fazi skrbnega pregleda se odloči o jezikovni varianti ter se te vprašalnike prilagodi pregledovani organizaciji z naslednjimi spremenljivkami:

- naslov pregledovane organizacije,
- kraj pregledovane organizacije,
- koda – kratica pregledovane organizacije,
- mesec in leto pregleda.

Vnaprej se v pregledovano organizacijo posreduje UISDDFW Status IS z zahtevo, da ga do pregleda vodstvo IT izpolni.

Določitev odločitvenih parametrov – če gre za začetni skrbni pregled, določijo lastniki podjetja oziroma vodstvo podjetja ali investitor, ki naroči skrbni pregled, odločitvene parametre, ki se uporabijo v zadnji – četrti fazi skrbnega pregleda, ko se pripravi odločitev. Potrebno je določiti naslednje parametre ter pripadajoče uteži, ki jih zahteva celovit pristop:

- trenutno vrednost IS,
- investicije v IS v naslednjih petih letih,
- stroške IS v naslednjih petih letih,
- zahtevano število svetovalnih dni investitorja,
- maksimalno odstopanje na področju Prednosti in slabosti IS,
- stopnjo tveganja IS,
- odstopanje produktov in storitev.

Posamezni odločitveni parametri in pripadajoče uteži bodo podrobno opisane v nadaljevanju v okviru odločitvenega modela.

Priprava grobega načrta pregleda na lokaciji – to je zadnja aktivnost, ki se izvede v tej fazi. Odvisna je od naslednjih dejavnikov:

- velikosti organizacije,
- tipa organizacije (centraliziran/decentraliziran),
- industrijsko specifičnih parametrov,
- globalnosti podjetja – razpršenost (enonacionalno, večnacionalno, na enem kontinentu, na več kontinentih, …)
- pripravljene in vnaprej posredovane dokumentacije,
- jezika (dokumentacija, napisana v jeziku, ki je jezik komuniciranja v pregledovani organizaciji). Če izvajalec pregleda ne pozna jezika, v katerem je pripravljena dokumentacija, ter ne more direktno komunicirati z zaposlenimi v organizaciji in je zato potrebno vključiti prevajalce, se čas lahko poveča več kot za enkrat).

V nadaljevanju je v poglavju Čas za izvedbo podrobno opisan čas, potreben za izvedbo skrbnega pregleda.

3.2.2 Pregled na lokaciji

Faza pregleda na lokaciji opisuje vse aktivnosti, ki se morajo izvesti, ko se obišče pregledovano organizacijo. Ta faza je tudi zelo pomembna, če že ne kritična.

Slika 5 grafično prikazuje potek te faze. Izvajalec pregleda mora pridobiti čim več možnih informacij in dokazov. Ta faza je razdeljena na štiri podfaze; vsaka med njimi ima več posameznih aktivnosti.

Posamezne podfaze so:

- priprava,
- pregled IS,
- pogovori z uporabniki IS,
- poročanje.

Celovit pristop izvedbe skrbnega pregleda se razlikuje od drugih pristopov tudi po tem, da je sam pregled na lokaciji razdeljen na dva dela:

- IS del, kjer se pregleda IS in izvede pogovore z IT vodstvom in drugimi strokovnjaki IT;
- uporabniški del, kjer se izvede pogovore z uporabniki, lastniki procesov in lastniki aplikacij v pregledovani organizaciji.

3.2.2.1 Priprava

V tej podfazi izvajalec pregleda izvede dvoje aktivnosti: pregleda pripravljeno dokumentacijo ter pripravi podroben načrt pregleda. Opis posameznih aktivnosti je naslednji:

Pregled pripravljene dokumentacije – izvajalec pregleda skrbno preuči pripravljeno dokumentacijo.

V primeru podatkovne sobe se pregleda pripravljena dokumentacija. Prav tako se pregleda in preuči zahtevana dodatna dokumentacija, za katero smo seznam pripravili v prvi fazi.

Če organizacija nima podatkovne sobe, se pregleda in preuči zahtevana in pripravljena dokumentacija, za katero smo seznam pripravili v prvi fazi.

Prav tako se tudi pregleda, do kolikšne mere je bil izpolnjen vprašalnik – UISDDFW Status IS. Primer tega vprašalnika, ki pa je neizpolnjen, najdemo v prilogi 9.2. Po potrebi se pripravi še dodaten seznam za pripravo dokumentov, podatkov in informacij ter se ga posreduje koordinatorju pregleda v pregledovani organizaciji.

Priprava podrobnega načrta pregleda na lokaciji – po pregledu pripravljene dokumentacije lahko izvajalec pregleda pripravi podroben načrt pregleda. Osnova za določitev sogovornikov je organigram pregledovane organizacije z imeni posameznih vodij, seznam lastnikov aplikacij in lastnikov procesov ter izpolnjen vprašalnik UISDDFW Status IS. V načrt izvajalec pregleda vnese osnutek urnika pregleda s predvidenimi lokacijami in sogovorniki. Izvajalec pregleda posreduje podroben načrt pregleda koordinatorju pregleda v pregledovani organizaciji z namenom, da le-ta obvesti sogovornike o načrtu in terminih za razgovore. Če so določeni sogovorniki v načrtovanih terminih zasedeni, koordinator pregleda v pregledovani organizaciji poskrbi za menjave terminov in potrjen načrt posreduje izvajalcu pregleda.

3.2.2.2 Pregled IS

Celovit pristop izvedbe skrbnega pregleda predvideva, da izvajalec pregleda prvo polovico pregleda na lokaciji »preživi« v okolju IT pregledovane organizacije. Izvedejo se naslednje aktivnosti:

Popolnitev vprašalnika UISDDFW Status IS – ta vprašalnik se posreduje vnaprej z zahtevo, da ga vodstvo IT pregledovane organizacije skupaj z določenimi strokovnjaki IT izpolni do določene mere. Preostala vprašanja, ki niso bila izpolnjena oz. odgovorjena, se pridobi na skupnem sestanku, kjer izvajalec pregleda neodgovorjena vprašanja, jih razloži in obširneje opiše, kaj se od določenega vprašanja pričakuje.

Vprašalnik UISDDFW Status IS je zelo podroben vprašalnik, ki vsebuje celovit popis IS. Podroben opis je v nadaljevanju naloge – v poglavju Opis vprašalnikov. Z odgovori si lahko izvajalec pregleda pridobi teoretično sliko IS pregledovane organizacije. Informacije iz tega vprašalnika so osnova za nadaljnji pregled IS.

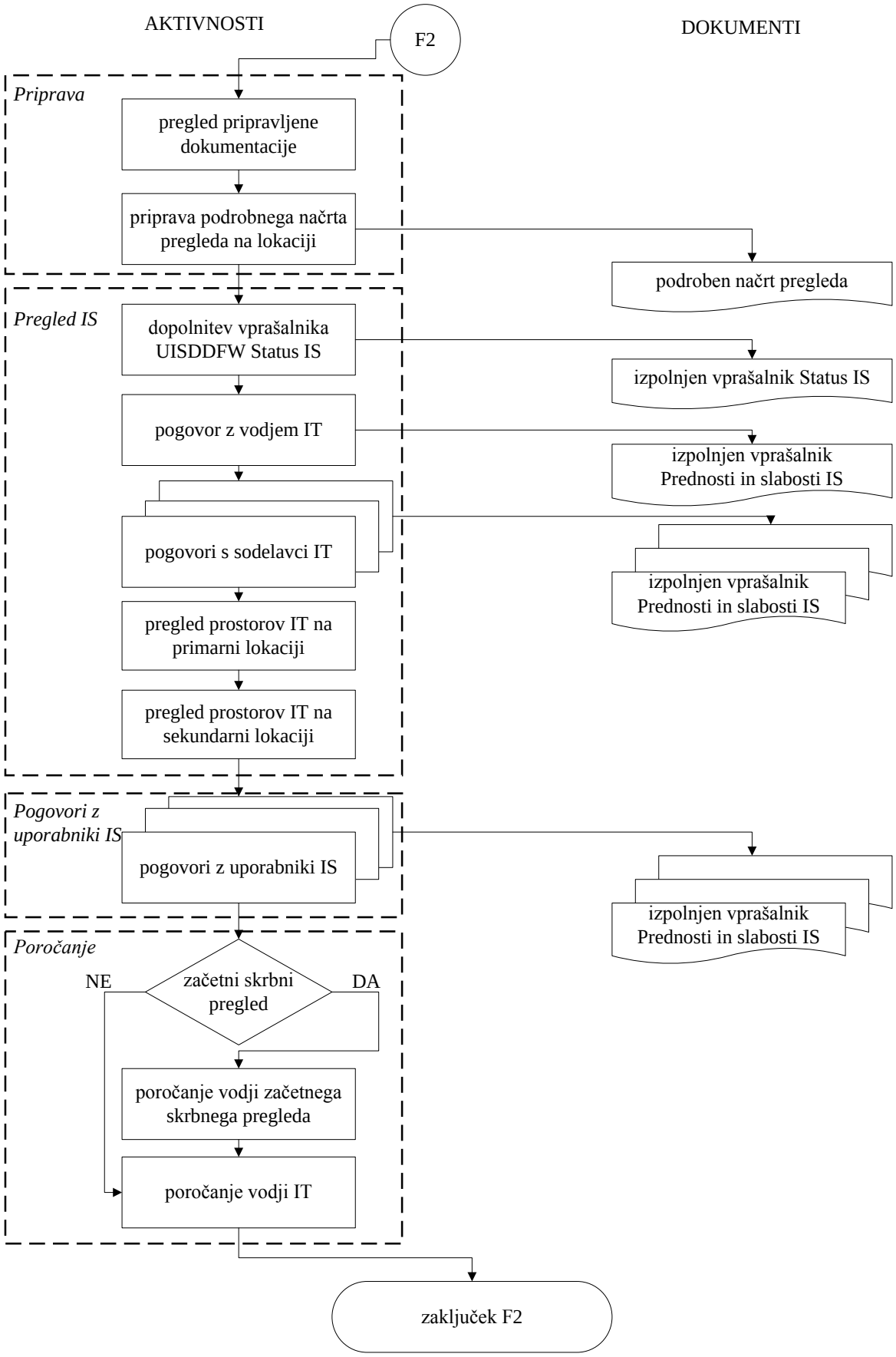
Pogovor z vodjem IT – izvajalec pregleda nadaljuje pregled s pogovorom z osebo, odgovorno za vodenje IT (glede na velikost in organiziranost pregledovanega podjetja so to lahko: vodja skupine, vodja službe, vodja oddelka, direktor sektorja, direktor divizije, direktor podjetja, …).

Na kratko se s sogovornikom pregleda cilje pregleda, usklajen načrt pregleda na lokaciji ter pridobi odgovore na dodatna vprašanja, vezana na posredovane odgovore v okviru vprašalnika UISDDFW Status IS. Ob koncu pogovora se predstavi še vprašalnik UISDDFW Prednosti in slabosti IS, ki je podrobno opisan v poglavju Opis vprašalnikov. Prazen (neizpolnjen) vprašalnik je tudi v prilogi 9.2. Izvajalec pregleda s pomočjo intervjuja izpolni ta vprašalnik skladno z odgovori, ki jih posreduje vodja IT.

Pogovor s strokovnjakom IT – izvajalec pregleda nadaljuje pregled s pogovori z vrsto strokovnjakov IT. Število pogovorov je odvisno predvsem od velikosti IT v pregledovani organizaciji (od največ 50 % do najmanj 10 % zaposlenih). Pogovori vključujejo ključne strokovnjake IT.

Izvajalec pregleda v razgovoru s sogovornikom pridobi odgovore na dodatna vprašanja, vezana na posredovane odgovore v okviru vprašalnika UISDDFW Status IS, katere sogovornik strokovno pokriva. Ob koncu pogovora se predstavi še vprašalnik UISDDFW Prednosti in slabosti IS. Izvajalec pregleda s pomočjo intervjuja izpolni ta vprašalnik skladno z odgovori, ki jih posreduje sogovornik.

Slika 5: Grafični prikaz druge faze



Ogled prostorov IT na primarni lokaciji – izvajalec pregleda v spremstvu vodje IT in po potrebi še kakšnih strokovnjakov IT izvede pregled prostorov. Ta pregled vsebuje oglede:

- sistemskega prostora,
- pomožnih prostorov za sistemski prostor:
  - hlajenje,
  - rezervno napajanje,
  - sistem gašenja,
  - drugi pomožni prostori;
- komunikacijskega prostora,
- lokalnih vozlišč,
- hrambe dokumentacije in medijev,
- pisarniških prostorov,
- prostora za testiranje,
- prostora za uporabniško spremno testiranje,
- drugo.

Ogled prostorov IT na sekundarni lokaciji – če ima pregledovana organizacija sekundarno IT lokacijo, izvajalec pregleda v spremstvu skrbnika lokacije ter vodje IT opravi ogled teh prostorov. Ta pregled vsebuje oglede:

- sekundarnega sistemskega prostora,
- pomožnih prostorov za sekundarni sistemski prostor:
  - hlajenje,
  - rezervno napajanje,
  - sistem gašenja,
  - drugi pomožni prostori;
- prostora za hrambo dokumentacije in medijev,
- pisarniških prostorov IT,
- pisarniških prostorov uporabnikov.

3.2.2.3 Pogovori z uporabniki IS

V drugi polovici pregleda na lokaciji izvajalec pregleda pogovore z nekaterimi ključnimi uporabniki, lastniki aplikacij in lastniki procesov. Število sogovornikov je odvisno od velikosti pregledovane organizacije. Vsak posamezen pogovor traja od 45 do 60 minut, če je možna direktna komunikacija, če pa je potreben prevajalec, pa se čas pogovora podvoji.

Seznam sogovornikov je tudi odvisen od dejavnosti pregledovane organizacije. Poleg lastnikov primarnih procesov in lastnikov primarnih aplikacij IS, ki podpirajo primarne procese, se izvede pogovore še z naslednjimi strokovnjaki (če jih pregledovana organizacija ima), zadolženimi za naslednja področja:

- z vodjo notranje revizije,
- z vodjo finančnega področja (»CFO« ali »CAO«)

- z vodjo kadrovskega področja (»CHRO«),
- z vodjo za upravljanje s tveganji (»CRO«),
- s pooblaščencem za varovanje informacije (»CISO«),
- z vodjo področja skladnosti poslovanja (»CCO«),
- s članom poslovodstva, zadolženim za IT (»CIO«);

Pri zelo veliki organizaciji se izvajalec pregleda pogovori tudi z drugimi »C« pooblaščenci, kot so:

- vodja nabave (»CPO«),
- vodja analitike (»CAO«),
- vodja pravnega področja (»CLO«),
- pooblaščenec za strategijo (»CSO«),
- drugi.

Pogovor z uporabnikom IT – izvajalec pregleda z vsemi zgoraj naštetimi opravi enak način pogovora, ki je sestavljen iz treh delov. To so:

- dnevna uporaba IS,
- opis procesa, posredovanje zahteve na IT (zase ali za svoje podrejene),
- izpolnitev vprašalnika UISDDFW Prednosti in slabosti IS. Izvajalec pregleda predstavi vprašalnik ter s pomočjo intervjuja izpolni ta vprašalnik, skladno z odgovori, ki jih posreduje sogovornik.

Pri teh pogovorih je priporočljivo, da niso prisotni sodelavci IT, saj praktične izkušnje dokazujejo, da so pogovori veliko bolj realni in učinkoviti; če predstavnikov IT ni na teh pogovorih.

Ob pogovorih se lahko tudi pregleda lokacije IT na dislociranih lokacijah. To se izvede v sodelovanju s skrbniki posameznih prostorov.

3.2.2.4 Poročanje

Izvajalec pregleda ob zaključku te faze vodji začetnega skrbnega pregleda ter vodji IT pripravi še kratki poročanji.

Poročanje vodji začetnega skrbnega pregleda – izvajalec pregleda na kratko ustno poroča vodji pregleda o prvih ugotovitvah, kritičnih opažanjih in morebitnih tveganjih.

Poročanje vodji IT – izvajalec pregleda ob zaključku aktivnosti na lokaciji pregledovane organizacije vodji IT ustno poroča o ugotovitvah v zahvalo za sodelovanje in trud, ki ga je IT vložil v pripravo dokumentacije, podatkov ter informacij.

To poročanje zajema celotni IS in je razdeljeno na naslednja poglavja:

- Splošni vtis,
- Revizija IS,
- Organiziranost IS,
- Sredstva IS,
- Varovanje informacij,
- Sekundarna lokacija in upravljanje neprekinjenega poslovanja,
- Razvoj in vzdrževanje,
- Procesi v IS,
- Upravljanje s tveganji,
- Dokumentacija,
- Priporočila,
- Opis naslednjih aktivnosti,
- Zahvala.

Podrobno je to poročilo opisano v poglavju Opisi poročil.

S to aktivnostjo se tudi zaključi ta faza Celovitega pristopa izvedbe skrbnega pregleda.

3.2.3 Analiza

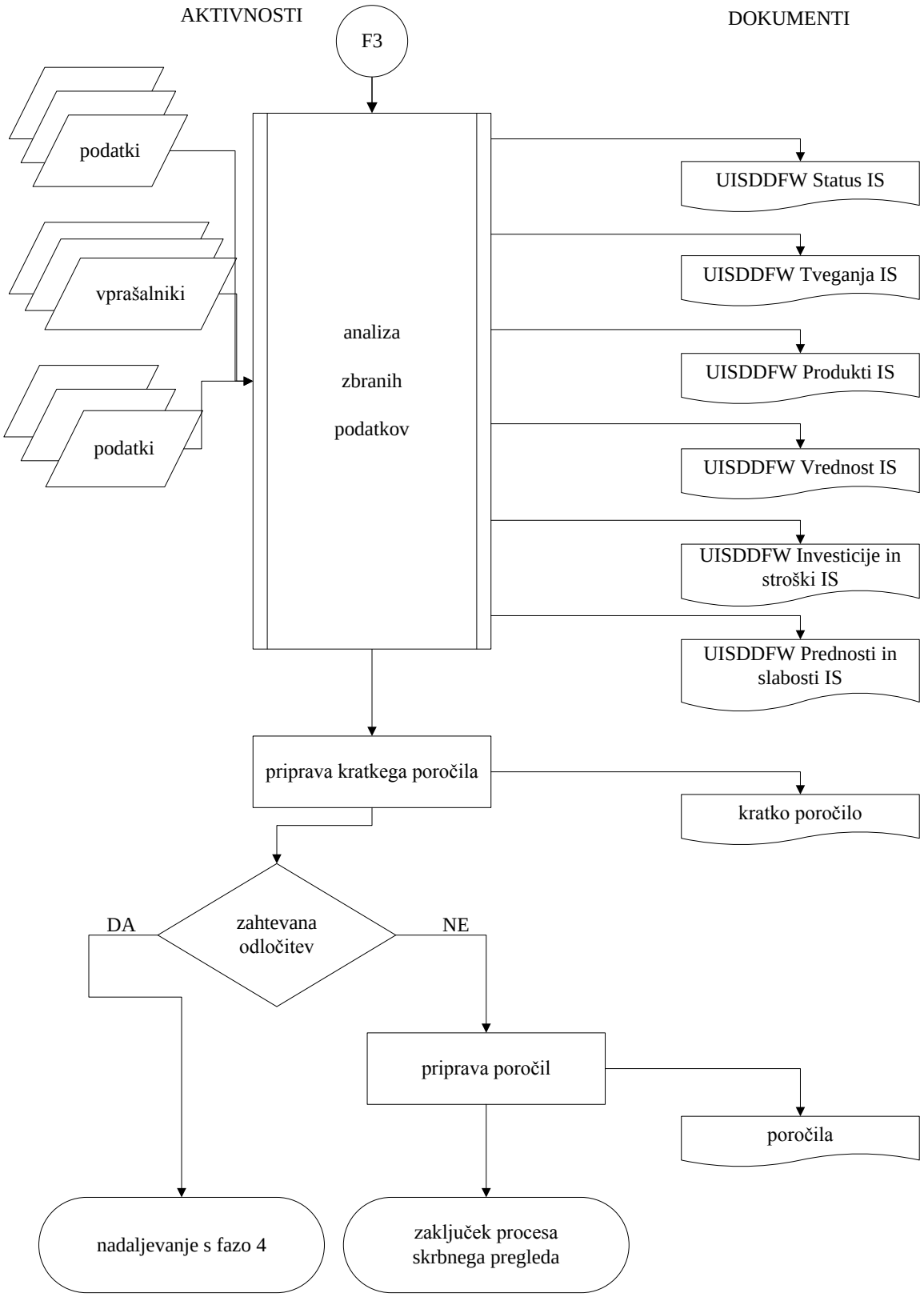
V fazi analize izvajalec pregleda ustrezno obdela pridobljene podatke in prejete informacije. Slika 6 grafično prikazuje potek te faze. Za analizo se uporabijo:

- podatki iz posredovane dokumentacije,
- pridobljene informacije v sklopu pogovorov,
- pridobljene informacije ob pregledu prostorov IT,
- odgovori na vprašalnik Status IS,
- odgovori na vprašalnike Prednosti in slabosti IS,
- odgovori na vprašalnik Vrednost IS,
- informacije in podatki, pridobljeni iz aktivnosti pridobivanja drugih podatkov.

Izvajalec pregleda po vrnitvi iz pregleda na lokaciji po posameznih sklopih analizira podatke in jih uredi v naslednje dokumente:

- Tveganja IS – kjer glede na vnesene odgovore vprašalnika Status IS ter druge pridobljene informacije izvajalec pregleda oceni tveganje s pomočjo modificirane preglednice kontrol ISO 27001. Izvajalec glede na videno oceni vsako opredeljeno kontrolo s tremi možnostmi (0 – v celoti implementirano, 1 – delno implementirano ter 2 – ni implementirano), kar se pomnoži z utežjo tveganja. To je zmnožek stopnje verjetnosti in stopnje posledic, ki so jo ocenili nekateri slovenski eksperti za to področje, ki imajo bogate izkušnje iz IS ter varovanja informacij. Podrobno bo ta dokument, kot vsi ostali, našteti v nadaljevanju, predstavljen v poglavju Opisi vprašalnikov.

Slika 6: Grafični prikaz tretje faze



- Produkti IS - kjer izvajalec pregleda vnese seznam produktov/storitev IS, ki jih nudi IS v pregledovani organizaciji.
- Vrednost IS – kjer izvajalec pregleda vnese podatke o knjigovodski vrednosti IS (za opredmetena in neopredmetena osnovna sredstva), zneske vzdrževalnih pogodb, ocenjene zneske projektov, ki so v delu, zneske izvajalcev storitev ter na koncu še lokalno ceno nekaterih novih osnovnih sredstev IS.
- Prednosti in slabosti IS – kjer izvajalec pregleda ločeno vnese v skupno preglednico odgovore sogovornikov iz IT ter ločeno odgovore sogovornikov – končnih uporabnikov. Nevtralne odgovore ustrezno izloči.
- Investicije in stroški IS – to je zadnja analiza, ki jo izvede izvajalec pregleda. V njej po svojih izkušnjah, podatkih in usmeritvah podjetja, ki je naročilo pregled, ustrezno oceni stroške in investicije pregledovane organizacije za naslednjih 5 let. Dolžina obdobja 5 let sem izbral zato, ker ima večina podjetij amortizacijsko dobo za opremo IT, določeno za to obdobje. Prav tako se oceni potrebni obseg svetovalnih dni za področje IS za obdobje naslednjih 4 let. To obdobje je izbrano glede na izkušnje pri implementaciji večjih projektov IT, ki zahtevajo določen čas za spoznavanje, pripravljalne analize, izvedbo projekta ter za izvedbo analize po uvedbi (po izvedbena analiza) izvedene med 6 do 18 mesecev po zaključku projekta. Nekateri imenujejo to analizo tudi »*postmortem analysis*«.

S tem izvajalec pregleda zaključi analizo podatkov. Pripravi tudi kratko poročilo, ki je podrobno opisano v poglavju Opisi poročil. Če se izvaja začetni skrbni pregled ali skrbni pregled izvajalca, se nadaljuje z naslednjo fazo to je odločitev, ki je opisana v naslednjem poglavju. Drugače izvajalec pripravi ustrezno poročilo, ki je podrobno opisano v poglavju Opisi poročil, po potrebi pa izvede še poročanje naročniku pregleda in zaključi aktivnosti skrbnega pregleda.

3.2.4 Odločitev

Ta faza je zadnja pri izvajanju začetnega skrbnega pregleda ali skrbnega pregleda izvajalca. V tej fazi je tudi vključen enostaven odločitveni model, ki naročniku pregleda omogoča enostaven numeričen odgovor: 0 pomeni NE, 1 pomeni DA.

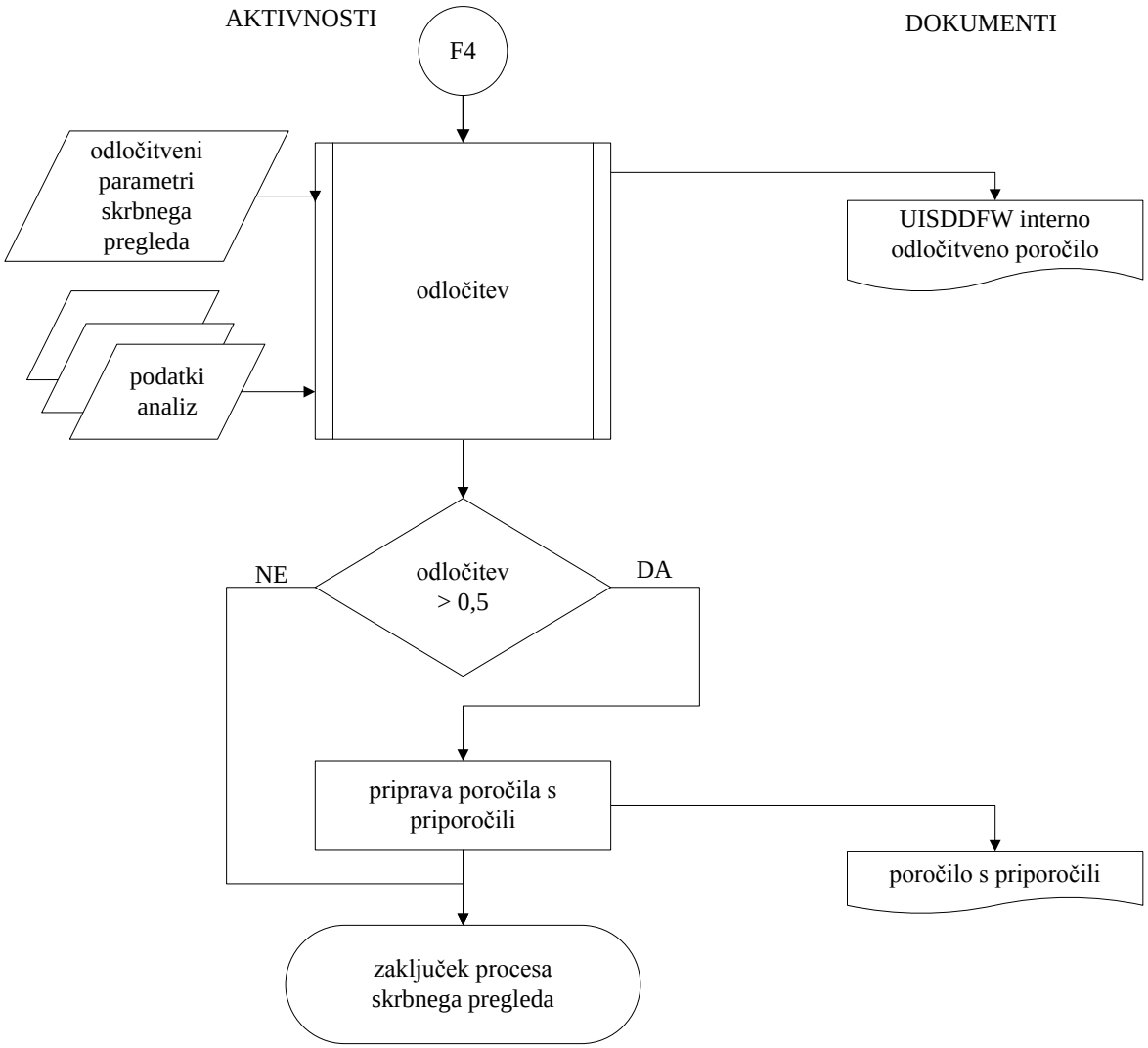
NE pomeni priporočilo, da se aktivnosti ne nadaljujejo, da se ne investira oziroma da se aktivnosti zaključijo.

DA pomeni priporočilo, da se aktivnosti nadaljujejo oziroma da se investira.

Grafični opis faze je prikazan na sliki 7. Podroben opis odločitvenega modela je opisan v poglavju Opis odločitvenega modela. V tej fazi se v odločitveno preglednico vnesejo predhodno določeni odločitveni parametri s posameznimi utežmi, ki so opisani na začetku tega poglavja v sklopu opisa prve faze. Poleg tega se v odločitveni model vnesejo naslednji

rezultati analiz, ki jih izvajalec pregleda pridobi v tretji fazi celovitega pristopa izvedbe skrbnega pregleda.

Slika 7: Grafični prikaz četrte faze



Rezultati (podatki analiz) so naslednji:

- Trenutna vrednost IS je ocenjena knjigovodska vrednost IS iz analize Vrednost IS. Numerična vrednost je od nekaj tisoč denarnih enot (v Evropi – EUR) do nekaj milijonov - odvisno od velikosti pregledovane organizacije.
- Vložek investicij v IS za naslednjih petih letih je ocenjena vrednost vseh investicij v IS pregledovane organizacije za obdobje naslednjih petih let. Ta podatek se dobi iz analize Investicije in stroški IS. Numerična vrednost je od nekaj deset tisoč do nekaj sto milijonov denarnih enot ali celo še več, odvisno od velikosti pregledovane organizacije.

- Vložek stroškov v IS za naslednjih pet let je ocenjena vrednost vseh stroškov v IS pregledovane organizacije za obdobje naslednjih petih let. Ta podatek se dobi iz analize Investicije in stroški IS. Numerična vrednost ocenjenih stroškov v IS je od nekaj deset tisoč do nekaj sto milijonov denarnih enot ali celo še več, odvisno od velikosti pregledovane organizacije.
- Zahtevano število svetovalnih dni investitorja je ocenjeno število svetovalnih dni strokovnjakov – svetovalcev, izraženo v človek dnevih (FTE), ki jih bo moral napotiti investitor v pregledovano organizacijo v naslednjih štirih letih, da bo lahko dvignil nivo IS na določeno dogovorjeno raven. Ti podatki se pridobijo tudi iz analize Investicije in stroški IS. Ocenjeno število svetovalnih človek dni (FTE) sodelavcev investitorjeve organizacije ali zunanjih strokovnjakov je od nekaj svetovalnih dni do nekaj sto oz. nekaj tisoč svetovalnih dni, odvisno od velikosti pregledovane organizacije.
- Maksimalno odstopanje na področju Prednosti in slabosti IS je izračunana vrednost, ki je rezultat analize Prednosti in slabosti IS. Ta podatek se lahko giblje od 0 do 10 in je neodvisen od velikosti pregledovane organizacije.
- Stopnja tveganja IS je izračunana vrednost stopnje tveganja IS pregledovane organizacije, ki je rezultat analize Tveganja IS. Ta podatek se lahko giblje od 1 do 10 in je neodvisen od velikosti pregledovane organizacije.
- Odstopanje produktov in storitev IS je izračunana vrednost Produktov in storitev IS, ki je rezultat analize Produkti IS. Ta podatek se lahko giblje od 10 % do 100 % in je neodvisen od velikosti pregledovane organizacije.

Ko izvajalec pregleda vnese vse podatke v preglednico, se pridobi tudi odločitev, ki je numerična. Ta rezultat se ustrezno dokumentira v UISDDFW interno odločitveno poročilo. Če je rezultat večji ali enak 0,5 oziroma zaokrožen na 1, je odločitev pritrdilna oziroma pozitivna. Če je rezultat manjši od 0,5 oziroma zaokrožen na 0, je odločitev odklonilna oziroma negativna.

V primeru pozitivnega rezultata se pripravi še podrobno končno poročilo s priporočili. Podrobno je poročilo predstavljeno v poglavju Opis poročil. Izvajalec pregleda lahko po potrebi naročniku predstavi tudi končno poročilo s priporočili v obliki predstavitve.

S tem so vse aktivnosti v procesu Celovitega pristopa izvedbe skrbnega pregleda zaključene.

V nadaljevanju so v okviru tega poglavja podrobno opisani: čas za izvedbo, posamezni vprašalniki, posamezna poročila ter odločitveni model.

3.3 Čas za izvedbo skrbnega pregleda

V okviru Celovitega pristopa izvedbe skrbnega pregleda IS – UISDDFW je čas za izvedbo skrbnega pregleda opredeljen od dveh primarnih ključnih parametrov velikosti organizacije ter jezika dokumentacije in komunikacije. Ostali sekundarni parametri so: tip organizacije, specifičnosti veje industrije pregledovanje organizacije, pripravljenost organizacije, vključenost tretjih oseb – zunanjih svetovalcev pri skrbnem pregledu in ne nazadnje še stopnja globalnosti pregledovane organizacije.

V poglavju je predstavljena tudi podrobna preglednica potrebnega časa glede na primarna parametra obseg in jezik.

3.3.1 Časovni parametri

Zgoraj omenjeni parametri vplivajo na čas izvedbe skrbnega pregleda. Primarna parametra sta ključnega pomena.

- Velikost pregledovane organizacije je osnovni parameter, a ni vezana na finančne pokazatelje (na primer: bilančna vsota ter kapital), ki so ključnega pomena pri drugih področjih skrbnega pregleda, temveč na fizično velikost organizacije, število zaposlenih in število lokacij.
- Jezik dokumentacije in komunikacije je drug osnovni parameter, ki lahko bistveno vpliva na čas izvedbe. Če je dokumentacija pripravljena v jeziku, ki je materni jezik izvajalca pregleda, ali v takem jeziku, ki ga izvajalec suvereno obvlada ter lahko v tem jeziku tudi neodvisno in suvereno komunicira, je čas pregleda občutno krajši. Če je potrebno vključiti prevajalce za prevajanje dokumentacije ter pisno in ustno komuniciranje, se čas občutno poveča. Glede na velikost pregledovane organizacije pa čas, ko so vključeni prevajalci, nelinearno narašča.

Sekundarni parametri niso tako pomembni, a tudi niso zanemarljivi:

- Tip organizacije pomeni način organiziranosti pregledovane organizacije. Tu so možnosti naslednje: centralizirani način organiziranosti, decentralizirani način organiziranosti ter mešanica prvega in drugega načina.
- Specifičnosti veje industrije pregledovane organizacije veljajo predvsem za izkušnje izvajalca pregleda. Če izvajalec nima dovolj izkušenj z določeno vejo industrije, se čas priprave pregleda ustrezno poveča, da izvajalec pridobi informacije in ustrezno pripravi vprašalnike, ki so industrijsko specifični.
- Pripravljenost organizacije na aktivnosti skrbnega pregleda. Tu sta dva faktorja, ki lahko vplivata na čas izvajanja. Prvi faktor se nanaša na stopnjo ažurnosti in dokumentiranosti IS, drugi pa na pripravljenost sogovornikov na skrbni pregled.

- Vključenost tretjih oseb – zunanjih izvajalcev v sam skrbni pregled. Zgodi se, da pregledovana organizacija najame tretjo osebo, da pripravi in koordinira aktivnosti skrbnega pregleda. V tem primeru so prisotne prednosti in slabosti. Prednosti so v tem, da pred samim skrbnim pregledom na zahtevo tretjih oseb ter njihovo metodologijo pregledovana organizacija pripravi podatkovno sobo (»*Data room*«). Dokumentacija je pripravljena in morda tudi prevedena v jezik, ki je sprejemljiv za izvajalce pregleda. Slabost podatkovne sobe je ta, da je dokaj težko pridobiti dodatno dokumentacijo. Še večja slabost pri vključenosti tretjih oseb je ta, da te osebe koordinirajo aktivnosti in zelo nerade odobrijo prosto gibanje po pregledovani organizaciji ter direktno komuniciranje s sogovorniki, ki jih opredeljuje proces Celovitega pristopa izvedbe skrbnega pregleda. To je razumljivo saj je želja tretjih oseb, da se ne vidi celovita slika pregledovane organizacije ter da se čim bolje skrije slabe informacije, ki lahko vplivajo na končno odločitev.
- Stopnja globalnosti – razpršenosti pregledovane organizacije je zadnji parameter, ki vpliva na čas organizacije. Tu so lahko tri možnosti: Prva je ta, da je pregledovana organizacija globalna in razpršena po večji površini (po možnosti po več kontinentih). Druga možnost pa je, da je pregledovana organizacija koncentrirana v ožji ali malo širši regiji in deluje lokalno. Zadnja možnost je kombinacija obeh predhodno navedenih – globalnosti in lokalnosti.

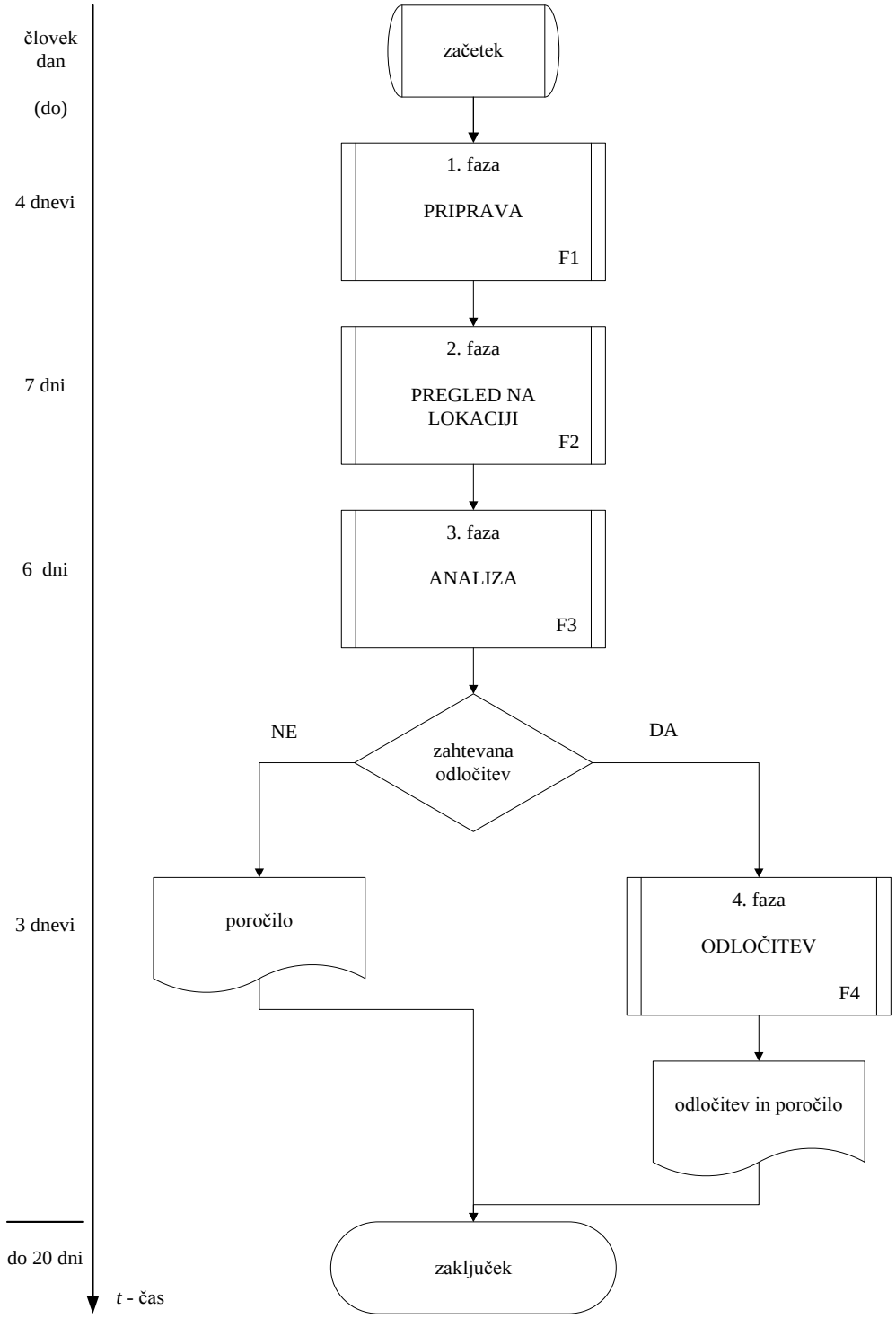
Vsi navedeni sekundarni parametri posamezno ne vplivajo veliko na čas izvedbe pregleda, pri odvisnosti posameznih ali vseh sekundarnih parametrov pa je lahko njihov vpliv velik. Izvajalec pregleda lahko oceni faktor vpliva sekundarnih parametrov. Na skupen čas izvedbe vpliva le na osnovi večletnih izkušenj.

3.3.2 Potreben čas

Za izvedbo skrbnega pregleda je potrebno pripraviti podroben načrt pregleda, ki zajema vse faze opisanega procesa Celovitega pristopa.

Slika 8 predstavlja primer časa, potrebnega za izvedbo skrbnega pregleda s Celovitim pristopom za izvedbo začetnega skrbnega pregleda IS v podjetju tipa B. V tem primeru v pregledovani organizaciji ni težav z jezikom za komuniciranje, prav tako ne s pregledovanjem dokumentacije in tudi ni vpliva sekundarnih parametrov. Velikost podjetja je opredeljena glede na število zaposlenih in število lokacij.

Slika 8: Primer načrta pregleda za podjetje tipa B



.

Preglednica 9: Čas, potreben za začetni skrbni pregled

		Osnova			Faktor jezika			Sekundarni parameti			Skupaj		
tip	Agenda - velikost pregledovanega podjetja	min dni	max dni	dnevi na lokac.	min dni	max dni	dnevi na lokac.	min dni	max dni	dnevi na lokac.	min dni	max dni	dnevi na lokac.
A	do 150 zaposlenih, ena glavna lokacija in do 3 druge lokacije	13	17	5	21	27	9	25	33	11	13	33	5 - 11
B	od 150 do 350 zaposlenih, ena glavna lokacija in do 5 drugih lokacij	18	22	7	29	35	13	35	42	15	18	42	7 - 15
C	od 350 do 750 zaposlenih, dve do štiri večje lokacije in med 5 do 15 drugih lokacij	25	29	9	40	46	16	48	56	19	25	56	9 - 19
D	od 750 do 2000 zaposlenih, tri do pet večjih lokacij in med 15 in 30 drugih lokacij	30	35	11	48	56	20	58	67	24	30	67	11 - 24
E	od 2000 do 3500 zaposlenih, pet do sedem večjih lokacij in med 30 in 50 drugih lokacij	36	44	15	58	70	27	69	84	32	36	84	15 - 32
F	od 3500 do 6000 zaposelnih, sedem do deset večjih lokacij in med 50 in 75 drugih lokacij	49	61	21	78	98	38	94	117	45	49	117	21 - 45
G	od 6000 do 10000 zaposlenih, deset do petnajst večjih lokacij in med 75 do 100 drugih lokacij	69	85	29	110	136	52	132	163	63	69	163	29 - 52
H	več kot 10000 zaposlenih, več kot petnajs večjih lokacij in več kot 100 drugih lokacij	88	112	36	141	179	65	169	215	78	88	215	36 - 65

Preglednica 9 prikazuje preglednico osmih tipov podjetij (po številu zaposlenih in številu lokacij). Numerične vrednosti predvidevajo enote v človek dnevih (FTE). V stolpcih, ki opredeljujejo osnovo, so navedeni: minimalno število dni za izvedbo pregleda, maksimalno število dni za izvedbo pregleda ter predviden čas pregleda na lokaciji (za izvedbo faze 2). Osnova je takrat, ko jezik za sporazumevanje in pregled dokumentacije nista ovira ter tudi ni drugih vplivov sekundarnih parametrov, navedenih na začetku poglavja.

Navedene enote v človek dnevih temeljijo na izkušnjah. Za organizacije tipa A in tipa B so določeni časovni podatki preizkušeni in potrjeni v študiji primerov opisanih v nadaljevanju.

V stolpcih, ki opredeljujejo faktor jezika, so navedeni predvideni dnevi za izvedbo skrbnega pregleda, ko je pri določenih aktivnostih potrebno vključiti prevajalce.

V stolpcih, ki jih opredeljujejo sekundarni parametri, so navedeni predvideni dnevi za izvedbo skrbnega pregleda, ko je potrebno upoštevati določene vplive nekaterih ali vseh sekundarnih parametrov.

V stolpcih, ki opredeljuje naslov skupaj, pa so navedeni najmanjše število dni za izvedbo začetnega skrbnega pregleda, maksimalno število dni za izvedbo začetnega skrbnega pregleda ter v zadnjem stolpcu še razpon dni, ki jih potrebuje izvajalec pregleda na lokaciji.

Če začetni skrbni pregled izvaja več izvajalcev, ki so uigrani, se čas ustrezno zmanjša.

Za ostale tipe skrbnih pregledov je preglednica identična.

3.4 Opisi vprašalnikov

V sklopu Celovitega pristopa za izvedbo začetnega ali drugega skrbnega pregleda IS se uporablja vrsta dokumentov – vprašalnikov. V večini primerov podatke v te dokumente vnašajo sogovorniki v procesu Celovitega pristopa izvedbe skrbnega pregleda. V nadaljevanju so podrobno opisani vsi vprašalniki - kdo jih izpolnjuje, v kateri fazi se uporabljajo in kaj je njihov cilj. Preglednica 10 prikazuje zbir vseh dokumentov.

Preglednica 10: Pregled vseh vprašalnikov celovitega pristopa

Oznaka	Opis	Cilj	Izpolnjevalec	Faza pregleda
UISDDFW Status IS	Celovit opis IS	Celovit prikaz IS pregledovane organizacije (vseh virov, procesov, organizacije , dokumentacije, …)	vodja IT in izvajalec pregleda	pregled na lokaciji
UISDDFW Tveganja IS	Ocena tveganj IS	Oceniti vsa identificirana tveganja IS v času pregleda	izvajalec pregleda	analiza
UISDDFW Produkti IS	Seznam produktov / storitev IS	Predstaviti seznam vseh trenutnih produktov in storitev IS	izvajalec pregleda	analiza
UISDDFW Vrednost IS	Trenutna vrednost in stroški IS	Predstaviti trenutno vrednost IS (OS, obsotječe pogodbe, projekte v delu, stroške dobaviteljev)	vodja IT in izvajalec pregleda	pregled na lokaciji / analiza
UISDDFW Investicije in stroški IS	Ocena investicij in stroškov ter potrebe po stokovnjakih	Predstaviti oceno investicij IS in stroškov IS po določenih področij za obdobje naslednjih 5 let	izvajalec pregleda	analiza
UISDDFW Prednosti in slabosti IS	Numerični pregled Prednosti in slabosti IS	Predstaviti odgovore sogovornikov z ocenami prednosti ali slabosti za določene sklope vprašanj	sogovorniki in izvajalec pregleda	pregled na lokaciji / analiza

V nadaljevanju so opisani posamezni vprašalniki, ki so trenutno v celoti na voljo v dveh jezikih: slovenskem in angleškem. Nekateri med njimi so na voljo tudi v drugih jezikih (hrvaškem, nemškem, srbskem). V celoti bodo na voljo ob poslovnih zahtevah za izvedbo Celovitega pristopa v določenem jeziku. Vsi navedeni vprašalniki v slovenščini so tudi navedeni v prilogi 7 ter priloženi na mediju v elektronski obliki.

3.4.1 UISDDFW Status IS

Ta vprašalnik je najobsežnejši med vsemi. Izvajalec pregleda ga posreduje v fazi Priprave vnaprej v pregledovano organizacijo skupaj s seznamom zahtevane dokumentacije. Zahteva se, da vodja IT skupaj s svojimi sodelavci vnaprej izpolni ta vprašalnik, kolikor se da. Preostali deli, ki jih ne izpolnijo, se izpolnijo skupaj z izvajalcem pregleda, saj le-ta dodatno obrazloži vprašanja, na katere niso odgovorili.

Velikost – obsežnost vprašalnika je odvisna od velikosti pregledovane organizacije ter razvejanosti IS. Neizpolnjen vprašalnik ima več kot petdeset, izpolnjen pa od osemdeset do nekaj sto strani.

Vprašalnik je v obliki datoteke z več preglednicami in ima 11 poglavij, skupno v 13 zavihkih, saj ima poglavje IV – tri zavihke. Izkušnje predhodnih skrbnih pregledov so narekovale razbitje enega dokumenta v 11 posameznih celot. Zaradi učinkovitosti in vzporednega

delovanja – izpolnjevanja posameznih zavihkov sem ta vprašalnik iz prvotne tekstne datoteke (MS Word) preoblikoval v datoteko, ki vsebuje preglednice (MS Excel).
Ta poglavja so:

- I: Osnovni podatki – kjer je na eni strani povzetek vseh bistvenih podatkov IS:
  - lokacija,
  - zaposleni v pregledovani organizaciji,
  - osnovni podatki o strojni opremi in sistemski programski opremi,
  - aplikativna programska oprema;
- II: Revizija IS – kjer so navedeni osnovni podatki o notranji in zunanji reviziji v povezavi z IS:
  - notranja revizija,
  - zunanja revizija,
  - zunanja revizija regulatorja;
- III: Upravljanje načrtovanja in organizacija IS - kjer so navedeni podatki o strateških usmeritvah, organizaciji in upravljanju IS v okviru naslednjih točk:
  - strategija,
  - taktični načrti,
  - katalog storitev IS,
  - politike in postopki IS,
  - izvajanje upravljanja IS,
  - struktura organizacije in odgovornosti v IS,
  - Dnevna dejavnost IS, ki se deli na naslednje sklope:
    - pregled standardov in procedur v IT,
    - analiza procesov v IT,
    - stabilnost IS,
    - delitev razvoja, testa in produkcije,
    - podpora uporabnikom,
    - časovni pregled izvajanja operacij v IT;
- IV: Viri IT - strojna oprema IS – kjer so navedeni podatki o strojni opremi v okviru naslednjih točk:
  - tehnična infrastruktura,
  - Strojna oprema, ki se deli na naslednje sklope:
    - centralni sistem,
    - frontalni sistemi,
    - strežniki na primarni lokaciji,
    - strežniki na sekundarni lokaciji,
    - virtualni strežniki na primarni lokaciji,
    - virtualni strežniki na sekundarni lokaciji,
    - osebni računalniki,
    - prenosni računalniki (prenosniki, dlančniki, …),
    - tiskalniki,
    - ostala oprema.

  - Komunikacijska oprema, ki se deli na naslednje sklope:
    - oprema prostranega omrežja (WAN),
    - oprema lokalnega omrežja (LAN),
    - oprema brezžičnega lokalnega omrežja (WLAN),
    - naročniška telefonska centrala (PBX);
  - Vzorci topologij;
- IV: Viri IT - programska oprema IS – kjer so navedeni podatki o sistemski programski opremi v naslednjih točkah:
  - sistemska programska oprema,
  - seznam licenc,
  - podatkovne baze in sistemi za upravljanje podatkovnih baz,
  - struktura podatkov in podatkovnih datotek,
  - sistem elektronske pošte,
  - ponudnik internetnih storitev,
  - oprema v postopku nabave,
  - moderni poslovni kanali,
  - distribucijski kanali (za finančno industrijo) oziroma posebne aplikacije glede na dejavnost organizacije,
  - sredstva aplikativne programske opreme IS – kjer so navedeni podatki o aplikativni programski opremi v naslednjih točkah:
    - pregled glavnih sklopov aplikativne programske opreme za podporo osnovne dejavnosti pregledovane organizacije,
    - pregled sklopov aplikativne programske opreme za ostala področja,
    - pregled sklopov aplikativne programske opreme za podporne procese,
    - pregled izločenih storitev in izločene aplikativne programske opreme,
    - pregled projektov v delu,
    - pregled načrtovanih projektov v tem letu;
- IV: Viri IT – kadri in prostori – kjer so navedeni podatki o kadrih v IT v naslednjih točkah:
  - pregled izobrazbe / številčno glede na profil delovnega mesta,
  - seznam zaposlenih v IT,
  - seznam ljudi, ki so v zadnjih treh letih zapustili pregledovano organizacijo,
  - načrt izobraževanja zaposlenih v IT za tekoče leto,
  - seznam izobraževanj zaposlenih v IT za zadnje tri leta,
  - program IT izobraževanj za ostale zaposlene v pregledovani organizaciji,
  - prostori IT;
- V: Varovanje informacij – kjer so navedeni podatki o varovanju informacij in informacijskih sredstev v naslednjih točkah:
  - splošno,
  - odgovornost za informacijske vire,

- dostop do sistemov, ki se deli na naslednje sklope:
  - fizična zaščita in kontrole,
  - logična zaščita in kontrole,
  - izzivi zasebnosti podatkov,
  - identifikacija in avtorizacija,
  - upravljanje identifikacije in avtorizacije,
  - šifriranje,
  - spremembe produkcijskih podatkov,
  - zaščita pred zunanjim okoljem;
- upravljanje produkcije, ki se deli na naslednje sklope:
  - postopki,
  - dnevniški zapisi,
  - upravljanje pripomočkov;
- rokovanje z mediji, ki se deli na naslednje sklope:
  - delovni postopki,
  - varnostno kopiranje in postopki restavriranja,
  - upravljanje oddaljene hrambe,
  - odlaganje / odstranjevanje in uničevanje medijev;
- revizijska sled;

- VI: Upravljanje neprekinjenega poslovanja (BCM) in upravljanje okrevanja po katastrofi (DRM) – kjer so navedeni podatki vezani na upravljanje neprekinjenega poslovanja v naslednjih točkah:
  - splošno,
  - neprekinjeno poslovanje in načrti okrevanja po katastrofi, ki se deli na naslednja sklopa:
    - analiza poslovnih učinkov (BIA),
    - klasifikacija operacij in analiza kritičnosti;
  - upravljanje neprekinjenega poslovanja in upravljanje okrevanja po katastrofi, ki se deli na naslednja sklopa:
    - upravljanje neprekinjenega poslovanja,
    - upravljanje okrevanja po katastrofi;
- VII: Razvoj, nabava, implementacija in vzdrževanje aplikacij – kjer so navedeni podatki vezani na navedena področja v naslednjih točkah:
  - razvoj aplikacij, ki se deli na naslednje sklope:
    - metodologija,
    - vloge in odgovornosti,
    - ocenjevanje tveganj pri razvoju;
  - nabava rešitev,
  - vzdrževanje aplikacij, ki se deli na naslednja sklopa:
    - proces,
    - vzdrževalne pogodbe;

    - vodenje projektov, ki se deli na naslednje sklope:
        - splošno,
        - načrtovanje,
        - upravljanje,
        - zaključevanje,
        - analiza po uvedbi;
- VIII: Ocenjevanje poslovnih procesov in upravljanje s tveganji – kjer so navedeni podatki, vezani na navedeni področji v naslednjih točkah:
    - preoblikovanje poslovnih procesov in projekti spremembe procesov,
    - upravljanje s tveganji,
    - obvladovanje IT;
- IX: Ostalo – kjer so navedeni preostali podatki v naslednjih točkah:
    - svetovalne pogodbe,
    - primerjalna preglednica procesov z ITIL procesi,
    - primerjalna preglednica s COBIT 4.1 procesi,
    - primerjalna preglednica z ISO/IEC 27001:2005;
- X: Problemi in pričakovanja – kjer so navedeni podatki vezani na naslovna področja v naslednjih točkah:
    - pregled problemov na IS,
    - pričakovanja vodstva IT za:
        - naslednjih 3 – 6 mesecev,
        - v naslednjem letu,
        - v naslednjih treh letih;
- XI: Pogoji uporabe vprašalnika:
    - zahvala za izpolnjevanje,
    - izvaja o zaupnosti dokumenta in pogoji uporabe;

Cilji tega temeljitega vprašalnika so, da izvajalec pregleda pridobi celovito sliko o organizaciji, sredstvih, procesih, upravljanju in problemih v pregledovani organizaciji. Dokument se lahko po skrbnem pregledu uporablja tudi kot osnovna dokumentacija IT, če se ustrezno obnavlja in osvežuje ob spremembah.

3.4.2 UISDDFW Tveganja IS

Zelo težko je pričakovati, da bi imela pregledovana organizacija uveden sistem upravljanja varovanja informacij – SUVI (s tujko ISMS). Da izvajalec pregleda ne bi obremenjeval vodstvo IT še z dodatnim vprašalnikom za področje SUVI, ima Celoviti pristop za izvedbo začetnega skrbnega pregleda IT v sklopu dokumentacije ta modificiran vprašalnik – Tveganja IS, ki je nekakšna podmnožica vprašalnika Status IS. Izpolni ga izvajalec pregleda v fazi analize.

Ta vprašalnik je modificirana preglednice kontrol ISO 27001, vezana na osnovni vprašalnik Status IS. Razdeljen je na posamezne poglavja, kot jih opredeljuje standard ISO/IEC 27001:2005 in kontrolni seznam ISO/IEC 27002:2005. Razdeljen je na naslednja področja:

- varnostna politika,
- organizacija varovanja informacij,
- upravljanje sredstev,
- varovanje človeških virov,
- fizična zaščita in zaščita okolja,
- upravljanje s komunikacijami in produkcijo,
- nadzor dostopa,
- nakup, razvoj in vzdrževanje informacijskih sistemov,
- upravljanje incidentov pri varovanju informacij,
- upravljanje neprekinjenega poslovanja,
- združljivost (z zakonskimi zahtevami);

Vprašalnik ni toliko obsežen kot osnovni vprašalnik Status IS. Preglednica je v enem zavihku in vsebuje malo manj kot 200 vrstic.

Ta vprašalnik je nekakšna povezava med kontrolnim seznamom ISO/IEC 27002:2005 in Vprašalnikom Status IS. Izvajalcu pregleda omogoča, da lahko iz odgovorov vprašalnika Status IS pridobi informacijo o tveganjih na IS skozi oči standarda ISO/IEC, pri tem pa ne zahteva od pregledovane organizacije direktnih odgovorov na vprašanja kontrolnega seznama.

Ta vprašalnik temelji na pred definiranih uteži tveganj IS za vsako področje, ki je tudi opredeljeno v osnovnem vprašalniku Status IS. Opredeljene uteži niso subjektivne ocene izvajalca pregleda temveč rezultat ocen ekspertov tega področja iz Slovenije. Ti eksperti imajo bogata in večletne (v povprečju več kot petindvajset let) izkušnje iz IS ter praktične izkušnje iz varovanja informacij.

Izvajalec pregleda v času analize poda objektivno oceno glede na videno oziroma dokumentirano v okviru vprašalnika Status IS. Izvajalec oceni vsako opredeljeno kontrolo s tremi možnostmi (0 – v celoti implementirano, 1 – delno implementirano ter 2 – ni implementirano), ki se pomnoži z utežjo tveganja. Posamezne kontrole se združijo na osnovi posameznih poglavij, kjer se pridobi ocena tveganja za vsako poglavje ter končno skupen numerični rezultat, ki je med 0 in 10.

Cilj tega vprašalnika je pridobiti neodvisno oceno Tveganja IS v pregledovani organizaciji. To numerično vrednost izvajalec pregleda uporabi kot izhodni podatek analize Tveganja in vhodni podatek za odločitveni model.

Preglednica 11 opredeljuje relacijo med numerično oceno ter opisno oceno Tveganja IS v pregledovani organizaciji.

Preglednica 11: Ocena tveganja IS

Numerična vrednost	Ocena tveganja IS
0 - 1,9	sprejemljivo
2,0 - 3,9	nizko
4,0 - 7,9	srednje
8,0 - 10	visoko

3.4.3 UISDDFW Produkti IS

Vprašalnik Produkti IS lahko imenujemo tudi Katalog storitve IS. Opredeljuje, katere storitve izvaja IT v pregledovani organizaciji za potrebe naročnika – to je različnih organizacijskih enot pregledovane organizacije. Izpolni ga izvajalec pregleda v času analize. Glede na posredovano dokumentacijo, izpolnjen osnovni vprašalnik Status IS, videno ob pregledu in obiskih v IT ter poslovnih področjih / končnih uporabnikov IS pregledovane organizacije, izvajalec pregleda subjektivno opredeli prisotnost in stopnjo razvitosti storitev glede na seznam oziroma katalog IS storitev naročnika pregleda.

Ta vprašalnik je najmanjši med vsemi – sestavlja ga ena preglednica v enem zavihku.

Cilji tega vprašalnika so, da se pridobi celovit seznam produktov IS pregledovane organizacije in primerjava z naročnikovim seznamom. Numeričen izhod v okviru analize produktov IS je procent odstopanja od naročnikovega seznama.

3.4.4 UISDDFW Vrednosti IS

Ta vprašalnik je z vidika financ najpomembnejši. Opredeljuje trenutno vrednost IS v pregledovani organizaciji. Izpolni ga izvajalec pregleda glede na posredovane dokumente ter izpolnjen osnovni vprašalnik Status IS. Izvajalec pregleda ga izpolni v fazi analize.

Vprašalnik sestavlja datoteka z več preglednicami, vsaka v svojem zavihku. Te preglednice so:

- Vrednost osnovnih sredstev (v dveh stolpcih – nabavna vrednost in trenutna vrednost), ki se deli na:
    - opredmetena osnovna sredstva:
        - strojna oprema,
        - sistemska programska oprema;
    - neopredmetena osnovna sredstva;

- Letni stroški vzdrževanja (v dveh stolpcih – za preteklo in predpreteklo koledarsko leto), ki se delijo na:
  - vzdrževanje strojne opreme,
  - stroške licenc in morebitnega vzdrževanja sistemske programske opreme,
  - vzdrževanje aplikacijske programske opreme;
- Stroški projektov v delu (za vsak posamezen projekt s podatki o datumu implementacije in datumih finančnih vplivov):
  - projekti IT (infrastrukturni projekti),
  - poslovni projekti s komponento IT;
- Stroški dobaviteljev (v dveh stolpcih – za preteklo in predpreteklo koledarsko leto), ki se deli na:
  - stroške izločitev (»*outsourcing*«),
  - stroške drugih dobaviteljev (na primer: energija, komunikacije, hlajenja, ..);
- Cenik produktov in storitev za posamezne komponente IS v določeni državi – ki se deli na:
  - strojno opremo,
  - sistemsko programsko opremo,
  - komunikacijsko opremo,
  - ostalo industrijsko specifično opremo,
  - človeške vire
  - ostalo.

Število zavihkov dokumenta je nastalo na podlagi izkušenj pri izvedbi vrste skrbnih pregledov.

Obseg vprašalnika je dinamičen in odvisen od velikosti pregledovane organizacije, razvejanosti IS ter števila projektov. Obsega od deset do nekaj deset strani.

Cilji vprašalnika so, da se pridobi trenutna vrednost IS s trenutnimi stroški. Ti podatki so osnova za naslednji vprašalnik, kjer se načrtuje obseg investicij in stroškov pregledovane organizacije za naslednjih pet let.

3.4.4 UISDDFW Investicije in stroški IS

Ta vprašalnik izpolni izvajalec pregleda v fazi analize. Vhodni podatki so podatki, pridobljeni iz posredovane dokumentacije, podatki iz izpolnjenega osnovnega vprašalnika Status IS, informacij in vtisov z ogledov prostorov IT in uporabniških prostorov, informacije, pridobljene s pogovori s strokovnjaki iz IT in končnimi uporabniki storitev IT pregledovane organizacije ter z izkušnjami izvajalca pregleda. Ta vprašalnik je najbolj subjektiven med vsemi in izpolnjevanje le-tega je najbolj zahtevno in najbolj dolgotrajno med vsemi.

Po obsegu ni obsežen, saj datoteka vsebuje dve preglednici v dveh zavihkih, ki jih je moč stiskati na dveh straneh.

Ta vprašalnik ima v prvem zavihku obsežno preglednico, kamor se vnese obseg posameznih komponent IS, ki jih bo potrebno implementirati po posameznih letih v pregledovano organizacijo. Obdobje je za naslednjih 5 let. V začetku tega poglavja sem obrazložil, zakaj načrtujem potrebe za 5 let, saj je to v veliki večini amortizacijska stopnja posameznih komponent IS.

Posamezni sklopi načrtovanih investicij in stroškov po področjih so:

- Strojna oprema, ki se deli na:
  - centralni sistem,
  - strežnike,
  - delovne postaje / osebne računalnike,
  - prenosnike in PDA,
  - komunikacijsko opremo prostranega omrežja,
  - komunikacijsko opremo lokalnega omrežja,
  - naročniško telefonsko centralo,
  - opremo za neprekinjeno napajanje,
  - tiskalnike,
  - več funkcijskih naprav,
  - ostalo;
- Licence in sistemska programska oprema, ki se deli na:
  - sistemsko programsko opremo za centralni sistem,
  - opremo za centralno podatkovno bazo,
  - sistemsko programsko opremo za strežnike,
  - sistemsko programsko opremo za osebne računalnike,
  - programske pripomočke,
  - protivirusno zaščito,
  - komunikacijsko sistemsko programska opremo;
- Industrijsko specifična strojna oprema (na primer za finančno industrijo: bančni avtomati, druga posebna strojna oprema za finančno industrijo, ki je vključena v celovit IS pregledovane organizacije; za trgovinsko industrijo: POS blagajne, POS sistemi, sistemi za nadzor in vodenje skladišč (visoko regalnih, navadnih, …) ter druge);
- Aplikativna programska oprema in podpora, ki se deli na:
  - ERP sistem (ERP),
  - ključno aplikativno programsko opremo,
  - podporno aplikativno programsko opremo,
  - ostalo aplikativno programsko opremo;

- Stroški vzdrževanj, ki se delijo na:
  - vzdrževanje strojne opreme,
  - vzdrževanje in licence za sistemsko programsko opremo,
  - vzdrževanje in licence za aplikativno programsko opremo;
- Stroški dobaviteljev, ki se delijo na:
  - stroške izvajanja (»*outsourcing*«),
  - stroške drugih dobaviteljev;
- Stroški projektov, ki se delijo na:
  - infrastrukturne projekte IT,
  - poslovne projekte s komponento IT;
- Stroški človeških virov, ki se delijo na:
  - bruto osebne dohodke zaposlenih v IT,
  - stroške izobraževanj zaposlenih v IT,
  - stroške literature v IT,
  - ostale stroške;
- Ostalo.

V pripravi skupnega podatka se upošteva še letna stopnja inflacije ter korekcijski faktor.

Vprašalnik Investicije in stroški IS ima v drugem zavihku enostavno preglednico potreb po dodatnih zunanjih svetovalcih in izvajalcih, ki so lahko sodelavci naročnika skrbnega pregleda ali njegovi zunanji izvajalci. V tej preglednici se za določena področja in procese v IT opredeli, koliko svetovalnih človek dni (FTE) za določeno leto je potrebno, da se skozi svetovanje in upravljanje ustrezno nadgradi IS v pregledovani organizaciji. Ta preglednica predvideva načrtovanje svetovalcev za naslednja štiri leta.

Cilji vprašalnika so, da se pridobi neodvisna analiza načrtovanih vrednost investicij in stroškov v IS za naslednjih pet let ter ocena potreb po svetovalcih za nadgradnjo IS ter procesov v pregledovani organizaciji.

3.4.4 UISDDFW Prednosti in slabosti IS

Ta vprašalnik je najbolj nenavaden izmed vseh, ki se uporabljajo pri Celovitem pristopu izvedbe skrbnega pregleda. Izpolnjuje ga izvajalec skrbnih pregledov v sklopu pogovorov s strokovnjaki IT ter v sklopu pogovorov s končnimi uporabniki IS pregledovane organizacije v fazi pregleda na lokaciji.

Vsak od sogovornikov ob pogovoru sicer dobi vprašalnik, a ga ne izpolnjuje, temveč samo odgovarja. Na vsako postavljeno vprašanje oziroma postavko najprej odgovori, ali je to prednost in slabost.

Nato pa poda še numerično oceno, ki je od – 5 do 5:

- V primeru slabosti je -1 majhna slabost ter -5 največja možna slabost.
- V primeru prednosti je +1majhna prednost ter +5 največja možna prednost.
- Če oseba, ki odgovarja, nima izkušenj ali ne pozna določene postavke, odgovori z 0.

Tako se odgovarja na vsa vprašanja razen enega, kjer se sprašuje po usmeritvi IT, kjer so možni samo naslednji odgovori:

- +10 – IT je zelo aplikativno usmerjen,
- + 5 – IT je aplikativno usmerjen,
- 0 – IT je v ravnotežju med aplikativno in sistemsko usmeritvijo,
- - 5 – IT je sistemsko usmerjen,
- -10 – IT je zelo sistemsko usmerjen.

Pri dveh vprašanjih pa se odgovori z DA ali NE. Ti vprašanji sta v sklopu varovanju informacij in sicer: Ali ima organizacija rezervno (sekundarno) lokacijo? ter Ali obstaja upravljanje neprekinjenega poslovanja za področje, ki ga izvajajo?

Vprašalnik ima skupaj 53 vprašanj, ki so združeni v naslednje sklope:

- Produktivnost IT centra,
- Sistemski razvoj,
- Sodelavci v IT,
- Kvaliteta obstoječega aplikacijskega sistema,
- Učinkovita uporaba tehnologij,
- Uporaba naprednih in modernih tehnologij,
- Sodelovanje med uporabniki in IT,
- Varovanje informacij (Zaupnost, celovitost, razpoložljivost informacij).

Ti sklopi in posamezna vprašanja so nastali na podlagi dolgoletnih izkušenj, pri izvajanju intervjujev tako z zaposlenimi v okoljih IT, kot tudi njihovih internih uporabnikih.

Cilji vprašalnika so, da se pridobi neodvisna informacija o delovanju IS, sodelovanju in razumevanju IS v pregledovani organizaciji.

Izvajalec pregleda v fazi analize vnese vse odgovore v skupno preglednico UISDDFW Prednosti in slabosti IS. Združi odgovore iz IT v en del ter odgovore končnih uporabnikov v drug del preglednice. Izračunajo se povprečne vrednosti, kjer se odgovori – ocene 0 ne upoštevajo.

Pridobi se skupna ocena IT in končnih uporabnikov. Razlike med temi ocenami lahko projiciramo kot zrelostni model IS v pregledovani organizaciji. Čim bolj so odgovori ocen enotni, tem bolj je zrel IS v pregledovani družbi. Po drugi strani, pa če odgovori čim bolj

odstopajo, tem bolj je IS v pregledovani družbi na začetnih stopnjah zrelosti (oziroma je nezrel).

3.5 Opisi poročil

V sklopu Celovitega pristopa izvedbo začetnega ali drugega skrbnega pregleda IS se uporablja vrsta vnaprej pripravljenih vzorcev poročil, ki jih izvajalec pregleda izpolni v okviru Celovitega pristopa. Nekatera poročila se izpolni in preda naročniku, druga se uporabljajo v posamezni fazi skrbnega pregleda za ustno poročanje. V sklopu Celovitega pristopa je trenutno šest poročil z naslovi:

- Odločitveni parametri,
- Prvi vtisi,
- Stanje IS,
- Kratko poročilo,
- Odločitev,
- Dolgo poročilo.

Glede na tip skrbnega pregleda se tudi uporabljajo določena poročila. Preglednica 12 prikazuje celovit pregled glavnih značilnosti posameznih priporočil. Vzorci poročil se nahajajo tudi v prilogi.

Preglednica 12: Pregled poročil

Oznaka	Opis	Tipi skrbnih pregledov	Pripravljalec	Prejemnik	Oblika	Faza pregleda
odločitveni parametri	priprava odločitvenih parametrov pred pregledom	"začetni" in "ponudnika"	naročnik	izvajalec pregelda	pisno	priprava
prvi vtisi	poročanje vodji pregleda, če se pregled izvaja v sklopu več pregledov	za vse	izvajalec pregleda	vodji pregleda	ustno	pregled na lokaciji
stanje IS	poročanje vodji IT ob zaključku faze Pregled na lokaciji	za vse	izvajalec pregleda	vodja IT	ustno	pregled na lokaciji
kratko poročilo	poročilo, opravljeno po analizi podatkov	za vse	izvajalec pregleda	del sokumentacije UISDDFW	pisno	analiza
odločitev	kratko poročilo odločitve po vnosu podatkov v odločitveni model	"začetni" in "ponudnika"	izvajalec pregleda	del dokumentacije UISDDFW	pisno	odločitev
dolgo poročilo	daljše poročilo	za vse*	izvajalec pregleda	naročnik	pisno	zaključek

* odvisno od rezultata

V nadaljevanju tega poglavja so na kratko predstavljena vsa poročila: kdo jih pripravi in kdo je prejemnik, način poročanja (pisno ali ustno), faza poročanja, za katere tipe skrbnih pregledov se uporablja ter cilji posameznega poročila.

3.5.1 Odločitveni parametri

To poročilo je kratko in dokumentira odločitev naročnika, ki opredeli ustrezne uteži in mejne vrednosti odločitvenih parametrov. Podatke pripravi naročnik oziroma delovna skupina po pooblastilu naročnika. Prejemnik je izvajalec pregleda skrbnega pregleda IS. Poročilo se izvede v fazi Priprava in se uporablja pri začetnih skrbnih pregledih IS ter pri skrbnih pregledih ponudnika IS. Ti podatki se zapišejo, da kasneje lahko ob potencialnih revizijah dokazujemo ustreznost dokazil in sledi.

Cilji tega poročila so, kot že njegov naslov pove, ustrezno dokumentirati odločitvene parametre pred pridobivanjem večine informacij v fazi pregled na lokaciji. Vzorec poročila je v prilogi (Priloga 9.10)

3.5.2 Prvi vtisi

Poročilo se pripravi ob zaključku faze pregled na lokaciji. Poročilo pripravi izvajalec pregleda IS. Poročanje je ustno, izvajalec pregleda posreduje svoje vtise vodji ekipe izvajalcev skrbnega pregleda v primeru, da se vzporedno izvaja več skrbnih pregledov različnih področij v eni pregledovani organizaciji.

Cilj tega poročila je, da vodja vseh pregledovalcev ob zaključku faze pregleda na lokaciji pridobi prvo informacijo o stanju IS v pregledovani organizaciji. Vzorec točk poročanja je v prilogi (Priloga 9.11)

3.5.3 Stanje IS

Poročilo se pripravi ob zaključku faze pregled na lokaciji. Poročilo pripravi izvajalec pregleda IS. Poročanje je ustno, izvajalec pregleda posreduje svoje vtise vodji IT pregledovane organizacije. Morda pri tem poročanju sodelujejo tudi drugi strokovnjaki IT, a se o tem odloči vodja IT pregledovane organizacije.

Cilj tega poročila je, da izvajalec pregleda neodvisno od rezultata skrbnega pregleda poroča o svojih neodvisnih vtisih o stanju IS vodji IT pregledovane organizacije in morda tudi njegovim sodelavcem. S tem se izkaže zahvala za pomoč pri izvedbi te faze in pripravi vseh podatkov, informacij, dokumentov in vprašalnikov. Vzorec točk poročanja je v prilogi (Priloga 9.12)

3.5.4 Kratko poročilo

Poročilo se pripravi ob zaključku faze analiza. Poročilo pripravi izvajalec pregleda IS. Poročanje je pisno in je del dokončne dokumentacije skrbnega pregleda IS.

Cilj tega poročila je, da se ne glede na odločitev pripravi informacija po opravljeni analizi. Po vsebini je podobno dolgemu poročilu, ne vsebuje opise podrobnosti ter nima poročila za vodstvo in priporočil. Vzorec poročila je v prilogi (Priloga 9.13)

3.5.5 Odločitev

Poročilo se pripravi ob zaključku faze odločitev. Ta faza se uporablja pri začetnih skrbnih pregledih in skrbnih pregledih ponudnika, pri ostalih pa se ta faza preskoči. Poročilo je zajem vodnih podatkov v proces odločitve in zajem izhodnih podatkov – numerične odločitve. Poročanje je pisno in je del končne dokumentacije skrbnega pregleda IS.

Cilj tega poročila je, da se dokumentira odločitev. Vzorec poročila je v prilogi (Priloga 9.14).

3.5.6 Dolgo poročilo

Poročilo z drugim naslovom Končno poročilo se pripravi ob zaključku faze Analiza, v primeru splošnega skrbnega pregleda in v primeru tehnološkega skrbnega pregleda ali ob zaključku faze odločitev v primeru začetnega skrbnega pregleda ali skrbnega pregleda ponudnika. Poročilo pripravi izvajalec pregleda IS. Poročanje je pisno in je del končne dokumentacije skrbnega pregleda IS. Prejemnik poročila je naročnik pregleda. Iz tega poročila se lahko pripravi predstavitev zaključkov skrbnega pregleda naročniku.

Cilj tega poročila je priprava končnega zaključnega poročila s priporočili. Vzorec poročila je v prilogi (Priloga 9.15)

3.6 Odločitveni model

V okviru Celovitega pristopa izvedbe skrbnega pregleda IS – UISDDFW je tudi enostaven odločitveni model, ki se uporablja v fazi odločitve pri začetnih skrbnih pregledih in skrbnih pregledih ponudnika. Preglednica 13 prikazuje odločitveno preglednico. Podatki v preglednici se delijo na tri dele: predhodno določeni DD parametri, pridobljeni podatki iz analiz ter izračun z odločitvijo.

Preglednica 13: UISDDFW Odločitvena preglednica

			Predhodo določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**faktor A**	**max A**	rezultat analize A	izračun A
2	Investicije v IS v naslednjih petih letih	B	**faktor B**	**max B**	rezultat analize B	izračun B
3	Stroški IS v naslednjih petih letih	C	**faktor C**	**max C**	rezultat analize C	izračun C
4	Zahtevano število svetovalnih dni investitorja	D	**faktor D**	**max D**	rezultat analize D	izračun D
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**faktor E**	**max E**	rezultat analize E	izračun E
6	Stopnja tveganja IS	F	**faktor F**	**max F**	rezultat analize F	izračun F
7	Odstopanje produktov in storitev	G	**faktor G**	**max G**	rezultat analize G	izračun G
	SKUPAJ		100			skupni izračun
		Fmax	**maks. faktor**			
		finančni	razmerje fin.		ODLOČITEV	**"GO / NO GO"**
		nefinančni	razmerje nef.			

3.6.1 Določitev parametrov

V prvi fazi Celovitega pristopa skrbnega pregleda IS naročnik oziroma njegovi predstavniki določijo »predhodno določene DD parametre« in sicer uteži za posamezne postavke (Preglednica 13 – stolpec uteži) ter maksimalne vrednosti za posamezne postavke (Preglednica 13 – stolpec maksimalna vrednost).

Vsota vseh uteži mora biti 100 enot. Prve štiri postavke so finančne in se uteži seštejejo v polju finančno razmerje (razmerje fin.). Postavke od vključno 5 do 7 so nefinančne in se njihove uteži seštejejo v polju nefinančno razmerje (razmerje ne f.). F_{max} opredeljuje največjo utež, ki se uporablja pri tej odločitvi.

Naročnik oziroma njegovi predstavniki opredelijo tudi maksimalne vrednosti:

- Trenutna vrednost IS (vpiše se predhodno določena vrednost IS med nekaj 10.000 DE[4] do nekaj mio. DE),
- Investicije v IS v naslednjih petih letih (vpiše se predhodno določena vrednost investicij v IS med nekaj 100.000 DE do nekaj mio DE),

[4] DE – denarnih enot (v Evropi najpogosteje € (EUR), lahko tudi $ (USD), Ł (GBP) ali CHF oziroma druge valute)

- Stroški IS v naslednjih petih letih (vpiše se predhodno določena vrednost stroškov IS med nekaj 100.000 DE do nekaj mio DE),
- Zahtevano število svetovalnih dni investitorja (vpiše se predhodno določeno število Človek dni (FTE) svetovalcev za naslednje štiri leta),
- Maksimalno odstopanje na področju Prednosti in slabosti IS (vpiše se predhodno določena vrednost odstopanja Prednosti in slabosti IS. Ta vrednost je lahko med 1 in 5),
- Stopnja tveganja IS (vpiše se predhodno določena stopnje tveganja, ki je lahko med 1 in 10),
- Odstopanje produktov in storitev (vpiše se predhodno določena vrednost % odstopanja produktov in storitev pregledovane organizacije od kataloga produktov in storitev organizacije investitorja. Ta vrednost je lahko med 0 % do 100 %).

S tem so opredeljeni vsi podatki, ki se določijo v prvi fazi priprava.

3.6.2 Vhodni podatki iz analiz

V fazi analiza se po obdelavi vseh podatkov in popolnitvijo vseh dokumentov, ki so določeni v okviru Celovitega pristopa za izvedbo začetnega pregleda IS, pridobi tudi izračunane vrednosti, ki so vhodni podatki za odločitveni model in se jih vnese v stolpec rezultati analiz in rezultati vprašalnikov.

V poglavju 3.2.3 in 3.2.4 je podrobno opisano, kako s pomočjo analizi pridobimo te podatke, ki so:

- trenutna vrednost IS (vnese se izračunana trenutna vrednost IS, ki je od nekaj 10.000 DE do nekaj mio. DE),
- investicije v IS v naslednjih petih letih (vnese se izračunana vrednost investicij v IS od nekaj 100.000 DE do nekaj mio DE),
- stroški IS v naslednjih petih letih (vnese se izračunana vrednost stroškov IS med nekaj 100.000 DE do nekaj mio DE),
- zahtevano število svetovalnih dni investitorja (vnese se izračunana vrednost Človek dni (FTE) svetovalcev za naslednje štiri leta),
- maksimalno odstopanje na področju Prednosti in slabosti IS (vnese se izračunana vrednost odstopanja Prednosti in slabosti IS od 1 do 5),
- stopnja tveganja IS (vnese se izračunana vrednost stopnje tveganja od 0 do 10),
- odstopanje produktov in storitev (vnese se izračunana vrednost % odstopanja produktov in storitev od 0 % do 100 %).

S tem so določeni vsi vhodni podatki odločitvenega modela, ki smo jih pridobili v fazi analize.

3.6.3 Izhodni podatki / odločitev

V odločitveni preglednici je v vsaki vrstici enaka formula, ki preračunajo vnesene podatke.

$Izracun_x$ = 1 če je ($maks_x - rezultat\_analize_x \geq 0$) drugače

$$(\frac{maks_x - rezultat\_analize_x}{maks_x}) \times (1 - \frac{F_{max} - faktor_x}{F_{max}})$$

Kjer so posamezni elementi:
$izracun_x$ – izračun posamezne postavke
$faktor_x$ – pred definirani DD parameter posamezne postavke
$maks_x$ – maksimalna določena vrednost posamezne postavke
F_{max} – skupni maksimalni faktor izmed vseh pred definiranih DD parametrov
$rezultat\_analize_x$ – rezultat analize in vprašalnikov posamezne postavke

Kjer je: x = { A..G }

Ti izračuni se prikažejo v stolpcu izračuni.

Skupni izračun je povprečna vrednost vseh izračunov posameznih postavk.

$$Skupni\ izračun = (\frac{\sum Izracun_x}{7})$$

Če je rezultat enak 0,5 ali večji od 0,5 je odločitev zaokrožena na 1, oziroma je akcija »GO« / »INVESTIRAJ« - se nadaljuje z aktivnostmi.

Če je rezultat manjši od 0,5 je odločitev zaokrožena na 0, oziroma je akcija »NO GO« / »NE INVESTIRAJ« - se NE nadaljuje z aktivnostmi.

S tem je zaključeno poglavje Celovit pristop izvedbe skrbnega pregleda.

Podrobnosti o temi tega poglavja sem navedel tudi v naslednjih prispevkih:

a) Začetni skrbni pregled za področje informacijskih sistemov v finančnih organizacijah, Zbornik prispevkov: Dnevi slovenske informatike 2008, Portorož ISBN 978-961-6165-26-6

b) 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

c) Celovit pristop izvedbe skrbnega pregleda (soavtor), Zbornik prispevkov: Dnevi slovenske informatike 2010, Portorož ISBN 978-961-6165-32-7

d)Postopek pregleda in analize stroškov in investicij IS v podjetju, Zbornik prispevkov: 18. Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, Slovenski inštitut za revizijo, 2010, Ljubljana, ISBN 978-961-6495-49-3.

e) Framework for the delivery of Information System Due Diligence, Information System Management, prispevek je bil sprejet 11.3.2012, prispevek bo po navedbah glavnega urednika objavljen v enem letu

4 ŠTUDIJA PRIMEROV

Namen študije primerov je, da se celovit pristop skrbnega pregleda IS formalno potrdi kot pristop in se predstavijo rezultati. Yin [Yin03] predpostavlja, da je lahko študija primerov z več kot dvema primeroma močan argument. V nadaljevanju bom navedel več študij – primerov iz prakse, ki so bili uporabljeni v realnih izvedbah posameznih skrbnih pregledov v različnih organizacijah s področja finančne industrije v različnih državah Južne in Vzhodne Evrope. Univerzalnost pristopa sem potrdil s skrbnim pregledom in študijo primera v Sloveniji v organizaciji Informatika, informacijske storitve in inženiring d. d., Maribor.

4.1 Predpostavke

Osnovni cilj je bil razviti tak celovit pristop, ki bo omogočal hitro in učinkovito izvedbo vseh aktivnosti skrbnega pregleda, da bo mogoče naročniku predstaviti informacije, ki bodo na kratek in jedrnat način prikazale trenuten status IS, potencialna tveganja na področju IS in trenutno vrednost IS ter pri začetnih skrbnih pregledih IS oceniti vrednost stroškov in investicij za nadaljnjih 5 let v IS pregledovane organizacije. Podroben opis časa, potrebnega za izvedbo začetnega skrbnega pregleda IS, je podan v poglavju 3.2.2.

Razvoju celovitega pristopa sem dodal še razvoj in potrditev enostavnega odločitvenega modela, ki lahko naročniku začetnega skrbnega pregleda IS s pretvorbo analiziranih podatkov v numerične vrednosti omogoča enostavno odločitev: DA – nadaljevanje aktivnosti, NE – zaključek aktivnosti.

Predpostavka pri pripravi študije primerov je, da skozi terenske študije praktičnih primerov formalno dokažem zmožnosti celovitega pristopa, s katerim lahko hitro in učinkovito izvedemo skrbni pregled IS in potrditev kvalitetnih izhodnih informacij odločitvenega modela.

Za potrditev celovitega pristopa v okviru študije primerov sem pripravil naslednje predpostavke:

Predpostavka 1:
Končni rezultat začetnega skrbnega pregleda IS zagotavlja dovolj podatkov za nadaljnja pogajanja.

Predpostavka 2:
Vprašalnik o prednostih in slabostih IS, ki je del celovitega pristopa IS, ter analiza pridobljenih podatkov omogočata dovolj informacij, da se oceni stopnjo zrelosti IS v pregledovani organizaciji.

Predpostavka 3:
Predlagana priporočila so v pomoč vodjem IT in lastnikom organizacije, da izboljšajo stanje IS v pregledovani organizaciji.

Predpostavka 4:
Proces izvedbe skrbnega pregleda, ki ga nudi celovit pristop, ne vpliva veliko na izvajanje dnevnih operativnih procesov IS v pregledovani organizaciji. S tem opredelimo, da niso moteni dnevni procesi IS pregledovane organizacije.

Predpostavka 5:
Predlagan celovit pristop pomaga poslovodstvu/naročniku zmanjšati tveganja pri prevzemih in združitvah (»*Merger and Acquisition*« – v nadaljevanju: M&A).

V okviru terenske študije primerov bom skušal potrditi oziroma ovreči navedene postavke.

4.2 Primeri iz finančnih organizacij

Celovit pristop skrbnega pregleda IS je nastal po več kot desetih let praktičnih izkušenj pri pregledovanju IS v finančnih organizacijah Srednje in Južne Evrope. Razvoj je potekal, podobno kot pri procesu razvoja programske opreme, z metodo spiralnega modela razvoja [Boe88]. Proces, vprašalniki in celovit pristop so se razvili skozi več iteracij, kar je bilo praktično preizkušeno v okviru splošnih in začetnih skrbnih pregledih IS med leti 1997 in 2006 v finančnih organizacijah v 15 državah Srednje in Južne Evrope. V tem obdobju sem bil zaposlen v Novi Ljubljanski banki, d. d., Ljubljana, na različnih delovnih mestih v IT.

Za uvedbo tega celovitega pristopa sem se odločil po več kot 60 opravljenih skrbnih pregledih.

4.2.1 Načrtovanje študije primerov v finančnih organizacijah

V letih 2007 in 2008 sem v sklopu rednih delovnih nalog sodeloval pri začetnih in splošnih skrbnih pregledih IS, ki sem jih izvedel kot koordinator IT za Skupino NLB.

Začetne skrbne preglede je v banki načrtovala in izvajala organizacijska enota - Center za upravljanje Skupine NLB v skladu s poslovnimi zahtevami in sklepi nadzornega organa. V tem primeru sem sodeloval za področje IT kot eden izmed stalnih članov skupine za skrbne preglede. Glede na velikost in lokalne posebnosti pregledovane organizacije je sodelovalo od 6 do 10 poslovnih področij. IT je bil stalni član začetnih skrbnih pregledov predvsem zaradi ocenjevanja tveganj in finančnih posledic (potencialne investicije in stroški) ter zaradi vse večje informacijske podpore poslovnim procesom.

Načrtovanje splošnih skrbnih pregledov IS sem izvajal v skladu s strategijo IT in z letnim načrtom analiz IS pri članicah Skupine NLB. Te aktivnosti sem načrtoval in izvajal v dogovoru z vodstvom IT v banki.

V navedenem obdobju sem začetne skrbne preglede IS izvajal v skladu s celovitim pristopom in v okviru štirih faz pregleda, ki so opisani v poglavju 3. Splošne skrbne preglede IS sem v letih 2007 in 2008 izvajal v okviru prvih treh faz celovitega pristopa skrbnega pregleda IS.

4.2.2 Izvedba študije primerov v finančnih organizacijah

Študijske primere sem izvedel v štirih bankah v štirih različnih državah Vzhodne in Južne Evrope. Preglednica 14 prikazuje seznam študije primerov, lokacije organizacij, kjer so bili primeri izvedeni, in tip skrbnega pregleda, ki se je izvedel v posamezni organizaciji.

Preglednica 14: Študija primerov v finančnih organizacijah

Oznaka organizacije	Država	Tip skrbnega pregleda
banka A	Kosovo	začetni
banka B	Ruska federacija	začetni
banka C	Bolgarija	splošni
banka D	Bosna in Hercegovina	začetni

Banka A se nahaja na Kosovu. Prevzem in združitev (»M&A«) sta bila cilj za ta skrbni pregled IS. Banka A je univerzalna banka, ki je bolj usmerjena na poslovanje s fizičnimi osebami. Po velikosti je manjša banka s 257 zaposlenimi, 23 lokacijami (s centralo in poslovalnicami), njen kapital pa je ob pregledu znašal 18.000.000,00 €.

Začetni skrbni pregled banke je bil izveden v januarju in februarju 2007. Aktivnosti skrbnega pregleda za področje IS so bile izvedene v štirih fazah, kot jih predvideva celovit pristop. Za pregled področja IS na lokacijah sem porabil 5 dni. V ekipi za skrbni pregled banke A je sodelovalo 14 strokovnjakov, od tega en strokovnjak za področje IT, preostali pa so pokrivali ostalih 8 področij skrbnega pregleda.

Skupen čas za izvedbo začetnega pregleda IS z vsemi aktivnostmi, ki jih predvideva celovit pristop, je bil 12 delovnih dni (od tega en dan za potovanje). Naročnik izvedbe skrbnega pregleda, je pred odhodom ekipe na lokacijo določil odločitvene parametre in pripadajoče uteži za odločitveni model skrbnega pregleda IS. Osnove teh odločitvenih parametrov sem predstavil in opisal v preglednici 13 v poglavju 3.6 .

Preglednica 15: Odločitveni parametri in uteži za banko A

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**10,0**	**500.000**		
2	Investicije v IS v naslednjih petih letih	B	**17,5**	**4.000.000**		
3	Stroški IS v naslednjih petih letih	C	**17,5**	**1.500.000**		
4	Zahtevano število svetovalnih dni investitorja	D	**12,5**	**700**		
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**3**		
6	Stopnja tveganja IS	F	**15,0**	**4**		
7	Odstopanje produktov in storitev	G	**12,5**	**20**		
	SKUPAJ		100			
		Fmax	**17,5**			
		finančni	57,5		ODLOČITEV	
		ne finančni	42,5			

Preglednica 15 prikazuje predhodno določene parametre s pripadajočimi utežmi. Naročnik se je v tem primeru odločil, da z najvišjimi utežmi (17,5) obteži investicije in stroške IS v naslednjih petih letih. Z drugo najtežjo utežjo (15,0) je naročnik obtežil stopnjo tveganja IS ter maksimalno odstopanje na področju Prednosti in slabosti IS.

V drugi skupini odločitvenih parametrov je naročnik določil posamezne mejne vrednosti za posamezne parametre in sicer so mejne vrednosti za:

- trenutno vrednost IS: 500.000,00 €
- investicije v IS: 4.000.000,00 €
- stroške v IS: 900.000,00 €
- maksimalno število človek dni za sinhronizacijo: 700
- maksimalno odstopanje na področju Prednosti in slabosti IS: 3
- ocenjeno stopnjo tveganja: 4
- odstopanje produktov in storitev: 20

Razmerje finančnih parametrov proti nefinančnim je 57,5 : 42,5, kar kaže na to, da je naročnika skrbnega pregleda v sklopu tega pregleda zanimala predvsem finančna stran pregleda.

Po opravljenem pregledu na lokaciji, kjer so bile izvedene aktivnosti, ki so opisane v drugi fazi celovitega pristopa skrbnega pregleda IS, sem pridobil dovolj dokumentacije in informacij o IT v delu pregleda IT in pogovorih s končnimi uporabniki. Ob zaključku pregleda na lokaciji sem pripravil dve poročili: kratko poročilo o prednostih in slabostih ter možnih tveganjih za vodjo skrbnega pregleda ter ustno poročilo za direktorico IT, kateri sem prenesel ugotovitve o stanju IS:

- splošni vtis,
- revizija IT,

- organizacija in načrtovanje IS,
- sredstva IS,
- varovanje informacij,
- neprekinjeno poslovanje,
- razvoj in vzdrževanje IS,
- procesi in obvladovanje tveganj,
- dokumentacija,
- namesto zaključka,
- povezave,
- odprta vprašanja.

V tretji fazi začetnega skrbnega pregleda banke A sem izvedel analizo pridobljenih podatkov. Za posamezna področja odločitvenega modela sem pridobil numerične vrednosti ter jih vnesel v preglednico 16.

Trenutno vrednost IS, ki je znašala 279.302,00 €, sem pridobil iz finančnih podatkov za opredmetena osnovna sredstva.

Investicije v IS v naslednjih petih letih zahtevajo več podatkov ter pomožnih obdelav v različnih preglednicah – skupni izračunan znesek teh investicij za banko A je bil 3.263.000,00 €.

Preglednica 16: Rezultati analize za banko A

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**10,0**	**500.000**	**279.302**	
2	Investicije v IS v naslednjih petih letih	B	**17,5**	**4.000.000**	**3.263.000**	
3	Stroški IS v naslednjih petih letih	C	**17,5**	**1.500.000**	**900.000**	
4	Zahtevano število svetovalnih dni investitorja	D	**12,5**	**700**	**800**	
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**3**	**2,67**	
6	Stopnja tveganja IS	F	**15,0**	**4**	**4,5**	
7	Odstopanje produktov in storitev	G	**12,5**	**20**	**15**	
	SKUPAJ		100			
		Fmax	**17,5**			
		finančni	57,5		ODLOČITEV	
		ne finančni	42,5			

Stroški IS v naslednjih petih letih zahtevajo prav tako nekaj pomožnih obdelav v različnih pripravljenih preglednicah. Skupni izračunan znesek stroškov IS v naslednjih petih letih je znašal 900.000,00 €.

Med vsemi analizami je najbolj subjektivna ocena svetovalnih dni investitorja. V preglednico je bilo potrebno za različne profile vnesti število svetovalnih dni posameznih strokovnjakov

kot pomoč/svetovanje potencialni novi organizaciji za naslednja štiri leta. Pregledovalec to oceni po svojih izkušnjah. Za banko A je ta ocena znašala 800 človek dni.

Maksimalno odstopanje na področju Prednosti in slabosti IS se izračuna na osnovi analize odgovorov na vprašalnik Prednosti in slabosti IS. V okviru začetnega skrbnega pregleda IS v banki A sem pridobil 11 odgovorov (4 od informatikov in 7 od končnih uporabnikov), kar je 4,28 % vseh zaposlenih. Analiza vseh vprašalnikov ni pokazala bistvenih odstopanj. Povprečna vrednost odstopanj je bila 2,33, kar prinese v zmožnostno zrelostnem modelu (CMM) oceno 2,67. Glede na pridobljeno oceno je zrelostni model med 2 – ponovljivo, vendar intuitivno, ter 3 – opredeljeno.

S pomočjo izpolnjenega vprašalnika Status IS se lahko s podatki, pridobljenimi ob obisku posameznih lokacij, in pogovori s predstavniki IT, analizira stopnjo tveganja IS. S pomočjo preglednice, ki preslika pridobljene podatke iz statusa IS, se v fazi analize pridobi numerično stopnjo tveganja IS. Za banko A je ta stopnja znašala 4,5.

Zadnje področje, ki ga je potrebno vnesti v odločitveni model, je odstopanje produktov in storitev. Glede na pridobljene podatke se vnese v preglednico, ki kot rezultat poda odstopanje produktov in storitev od predhodno pripravljene preglednice. V banki A je bil izračun odstopanja 15.

Preglednica 17 prikazuje podatke po vnosu vseh podatkov analize v odločitveni model in končno numerično odločitev, ki je v banki A znašala 0,562. To je pomenilo, da odločitveni model predlaga odločitev nadaljevanja pogajanj za nakup organizacije in kasnejšo združitev.

Seveda pridobljeni podatek ni edini, ki ga izvajalec skrbnega pregleda posreduje naročniku začetnega skrbnega pregleda. Pregledovalec pripravi za področje IS še podrobno zajetno poročilo, kjer so opisani vsi pridobljeni rezultati in ocene.

Preglednica 17: Končna odločitev za banko A

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**10,0**	**500.000**	**279.302**	**0,571**
2	Investicije v IS v naslednjih petih letih	B	**17,5**	**4.000.000**	**3.263.000**	**1,000**
3	Stroški IS v naslednjih petih letih	C	**17,5**	**1.500.000**	**900.000**	**1,000**
4	Zahtevano število svetovalnih dni investitorja	D	**12,5**	**700**	**800**	**-0,102**
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**3**	**2,67**	**0,857**
6	Stopnja tveganja IS	F	**15,0**	**4**	**4,5**	**-0,107**
7	Odstopanje produktov in storitev	G	**12,5**	**20**	**15**	**0,714**
	SKUPAJ		100			**0,562**
		Fmax	**17,5**			
		finančni	57,5		ODLOČITEV	**GO**
		ne finančni	42,5			

V banki A je tudi vseh preostalih 14 pregledovalcev za 8 pregledanih področij podalo pozitivno oceno začetnega skrbnega pregleda celotne organizacije.

Naročnik je preučil skupno poročilo začetnega skrbnega pregleda banke A. Rezultati so bili predstavljeni tudi nadzornemu odboru, ki je potrdil investicijo. Nakup se je realiziral v drugi polovici leta 2007. Investitor je v tej državi že imel banko v svoji lasti in strategiji za povečanje tržnega deleža je sledila združitev, ki se je zaključila v letu 2008. S 1. 1. 2009 je začela delovati nova združena banka. Finančni rezultati iz letnega poročila za leto 2009, objavljenega v sredini 2010, potrjujejo, da so bili informacije začetnega skrbnega pregleda prave in potrjujejo sprejeto pravilno odločitev.

Banka B se nahaja v Ruski federaciji. Prevzem (»*Acquisition*«) je bil cilj za ta skrbni pregled IS. Banka B je univerzalna banka, ki je bolj usmerjena na poslovanje s fizičnimi osebami. Po velikosti je zelo majhna in ima 60 zaposlenih, 2 lokaciji (centralo in poslovalnico), njen kapital pa je ob pregledu znašal 15.000.000,00 €.

Začetni skrbni pregled banke je bil izveden v februarju in marcu 2007. Aktivnosti skrbnega pregleda za področje IS so bile prav tako izvedene v štirih fazah, kot jih predvideva celovit pristop. Za pregled področja IS na lokacijah sem porabil 4 dni. Glede na velikost banke bi za pregled na lokaciji potreboval manj časa, če ne bi bilo jezikovnih ovir. Vsa dokumentacija je bila v lokalnem jeziku in večina sogovornikov je razumela in govorila samo ruščino. Pri pregledu je zato sodelovala tudi prevajalka, ki ji je pomagal tudi eden izmed ostalih članov ekipe za skrbne preglede, ki je tekoče obvladal ruski jezik. V ekipi za skrbni pregled banke B je sodelovalo 12 strokovnjakov, od tega en strokovnjak za področje IT, preostali so pokrivali ostalih 8 področij.

Preglednica 18: Odločitveni parametri in uteži za banko B

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**5,0**	**500.000**		
2	Investicije v IS v naslednjih petih letih	B	**15,0**	**2.000.000**		
3	Stroški IS v naslednjih petih letih	C	**15,0**	**1.000.000**		
4	Zahtevano število svetovalnih dni investitorja	D	**20,0**	**700**		
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**4**		
6	Stopnja tveganja IS	F	**20,0**	**5**		
7	Odstopanje produktov in storitev	G	**10,0**	**10**		
	SKUPAJ		100			
		Fmax	**20,0**			
		finančni	55,0		ODLOČITEV	
		ne finančni	45,0			

Skupen čas za izvedbo začetnega pregleda IS z vsemi aktivnostmi, ki jih predvideva celovit pristop, je bil 10 delovnih dni (od tega en dan za potovanje). Naročnik izvedbe skrbnega pregleda je pred odhodom ekipe na lokacijo določil odločitvene parametre in pripadajoče uteži za odločitveni model skrbnega pregleda IS. Osnove teh odločitvenih parametrov sem predstavil in opisal v preglednici 13 v poglavju 3.6 .

Odločitveni parametri in uteži za banko B prikazujejo predhodno določene parametre s pripadajočimi utežmi (preglednica 18). Naročnik se je v tem primeru odločil, da z najvišjo utežjo (20,0) obteži zahtevano število svetovalnih dni investitorja. Z drugo najtežjo utežjo (15,0) je naročnik obtežil investicije in stroške IS v naslednjih petih letih ter maksimalno odstopanje na področju Prednosti in slabosti IS.

V drugi skupini odločitvenih parametrov je naročnik določil mejne vrednosti za posamezne parametre:

- trenutno vrednost IS: 500.000,00 €
- investicije v IS: 2.000.000,00 €
- stroške v IS: 1.000.000,00 €
- maksimalno število človek dni za sinhronizacijo: 700
- maksimalno odstopanje na področju Prednosti in slabosti IS: 4
- ocenjeno stopnjo tveganja: 5
- odstopanje produktov in storitev: 10

Razmerje finančnih parametrov proti nefinančnim je 55,0 : 45,0, kar kaže na to, da je naročnika skrbnega pregleda v sklopu tega pregleda zanimala predvsem finančna stran.

Po opravljenem pregledu na lokaciji, kjer so bile izvedene aktivnosti, ki so opisane v drugi fazi celovitega pristopa skrbnega pregleda IS, sem pridobil dovolj dokumentacije in informacij o IT v delu pregleda IT in pogovorih s končnimi uporabniki. Ob zaključku pregleda na lokaciji sem pripravil dve poročili: kratko poročilo o prednostih in slabostih ter možnih tveganjih za vodjo skrbnega pregleda ter ustno poročilo za direktorja IT, kateremu sem prenesel ugotovitve o stanju IS kot zahvalo za pomoč in sodelovanje pri začetnem skrbnem pregledu IS v organizaciji (banki B).

Po vrnitvi s pregleda na lokaciji sem v tretji fazi začetnega skrbnega pregleda banke B izvedel analizo pridobljenih podatkov. Za posamezna področja odločitvenega modela sem pridobil numerične vrednosti ter jih vnesel v preglednico 19.

Trenutno vrednost IS, ki je znašala 15.000,00 €, sem pridobil iz finančnih podatkov za opredmetena osnovna sredstva.

Preglednica 19: Rezultati analize za banko B

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**5,0**	**500.000**	**15.000**	
2	Investicije v IS v naslednjih petih letih	B	**15,0**	**2.000.000**	**1.300.000**	
3	Stroški IS v naslednjih petih letih	C	**15,0**	**1.000.000**	**1.676.000**	
4	Zahtevano število svetovalnih dni investitorja	D	**20,0**	**700**	**800**	
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**4**	**1,4**	
6	Stopnja tveganja IS	F	**20,0**	**5**	**6**	
7	Odstopanje produktov in storitev	G	**10,0**	**10**	**10**	
	SKUPAJ		100			
		Fmax	**20,0**			
		finančni	55,0		ODLOČITEV	
		ne finančni	45,0			

Investicije v IS v naslednjih petih letih zahtevajo več podatkov ter pomožnih obdelav v različnih preglednicah – skupni izračunan znesek teh investicij za banko B je bil 1.300.000,00 €.

Stroški IS v naslednjih petih letih zahtevajo prav tako nekaj pomožnih obdelav v različnih pripravljenih preglednicah. Skupni izračunan znesek stroškov IS v naslednjih petih letih je znašal 1.676.000,00 €.

Število svetovalnih dni posameznih strokovnjakov kot pomoč/svetovanje potencialni novi organizaciji za naslednja štiri leta je za banko B znašalo 800 človek dni.

Maksimalno odstopanje na področju Prednosti in slabosti IS: v okviru začetnega skrbnega pregleda IS v banki B sem pridobil 8 odgovorov (1 od informatika in 7 od končnih uporabnikov), kar je 13,3 % vseh zaposlenih. Analiza vseh vprašalnikov ni pokazala bistvenih odstopanj. Povprečna vrednost odstopanj je bila 4,56, kar prenese v zmožnostno zrelostnem modelu (CMM) oceno 1,44. Glede na pridobljeno oceno je zrelostni model med 1 – začetno/ad hoc ter 2 – ponovljivo, vendar intuitivno.

S pomočjo izpolnjenega vprašalnika Status IS, sem lahko s podatki, pridobljenimi ob obisku posameznih lokacij, in pogovori s predstavnikom IT analiziral stopnjo tveganja IS. Numerična stopnja tveganja IS za banko B je znašala 6.

Odstopanje produktov in storitev je v primeru banke B znašalo 10.

Preglednica 20: Končna odločitev za banko B

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**5,0**	**500.000**	**15.000**	**0,250**
2	Investicije v IS v naslednjih petih letih	B	**15,0**	**2.000.000**	**1.300.000**	**0,750**
3	Stroški IS v naslednjih petih letih	C	**15,0**	**1.000.000**	**1.676.000**	**-0,507**
4	Zahtevano število svetovalnih dni investitorja	D	**20,0**	**700**	**800**	**-0,143**
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**4**	**1,4**	**0,750**
6	Stopnja tveganja IS	F	**20,0**	**5**	**6**	**-0,200**
7	Odstopanje produktov in storitev	G	**10,0**	**10**	**10**	**0,500**
	SKUPAJ		100			**0,200**
		Fmax	**20,0**			
		finančni	55,0		ODLOČITEV	**NO GO**
		ne finančni	45,0			

Preglednica 20 prikazuje podatke po vnosu vseh podatkov analize v odločitveni model in končno numerično odločitev, ki je v banki B znašala 0,200. To je pomenilo, da odločitveni model predlaga predčasen zaključek aktivnosti nakupa organizacije, tako da ne pride do realizacije investicije.

Seveda pridobljeni podatek ni edini, ki ga izvajalec skrbnega pregleda IS posreduje naročniku začetnega skrbnega pregleda. Pregledovalec za področje IS pripravi še podrobno zajetno poročilo, kjer so opisani vsi pridobljeni rezultati in ocene.

V banki B je tudi večina preostalih 11 pregledovalcev za 7 pregledanih področij podalo negativno oceno začetnega skrbnega pregleda celotne organizacije.

Naročnik je preučil skupno poročilo začetnega skrbnega pregleda banke B. Odločil se je upoštevali mnenje skupine za začetni skrbni pregled organizacije. Informacija je bila predstavljena tudi nadzornemu odboru.

Finančni rezultati iz letnega poročila za leto 2008, objavljenega v sredini 2009, in finančni rezultati iz letnega poročila za leto 2009, objavljenega v sredini 2010, potrjujejo, da so bile informacije začetnega skrbnega pregleda prave in da je bila sprejeta negativna odločitev prava odločitev.

Banka C se nahaja v Bolgariji. Za razliko od ostalih študij primerov, je bil v tem primeru izveden splošni skrbni pregled IS. Banka je univerzalna banka, ki je bolj usmerjana na poslovanje z manjšimi pravnimi in s fizičnimi osebami. Banka C je izredno majhna, ima 30 zaposlenih in 2 lokaciji (centralno in sekundarno nadomestno lokacijo). Kapital banke C je ob pregledu znašal 12.000.000,00 €.

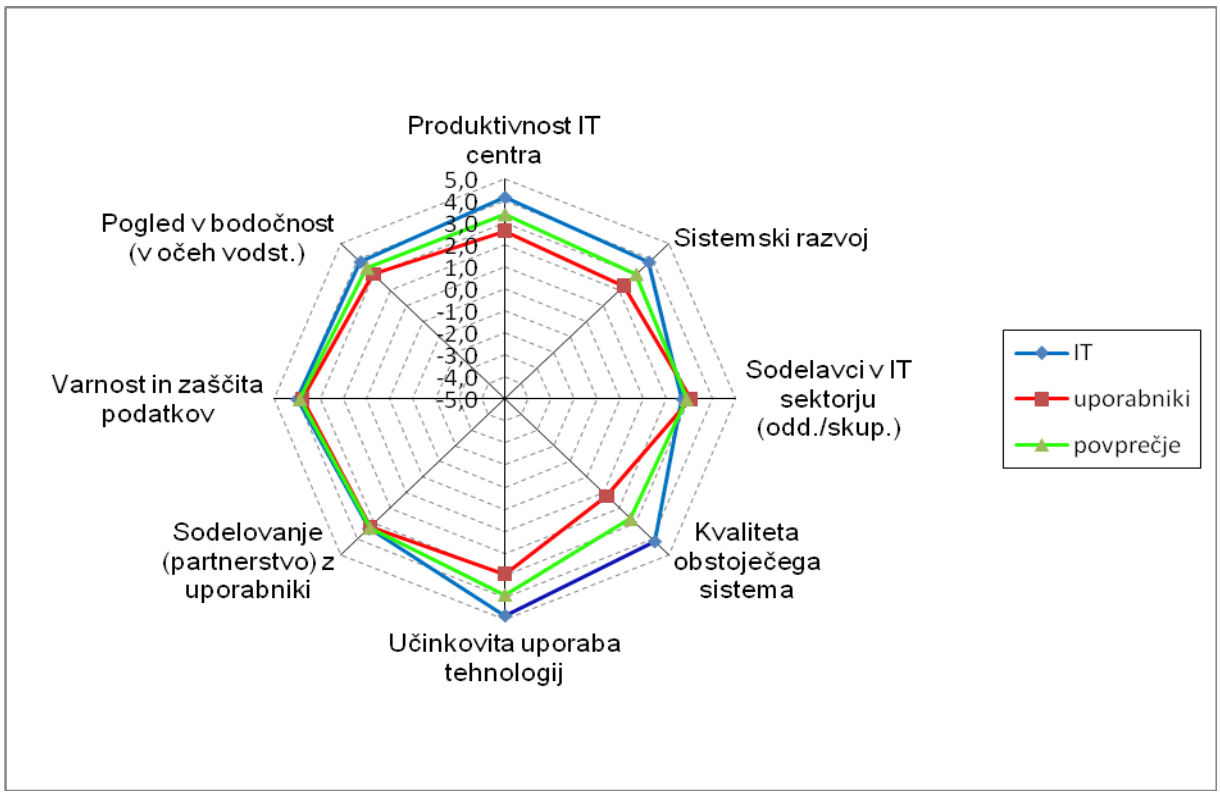
Splošni skrbni pregled IS banke sem izvedel v maju 2008. Aktivnosti skrbnega pregleda za področje IS so bile zaradi splošnega tipa skrbnega pregleda izvedene v treh fazah, kot jih predvideva celovit pristop. Za pregled področja IS na lokacijah sem porabil 3 dni. Skupen čas za izvedbo splošnega skrbnega pregleda IS z vsemi aktivnostmi, ki jih predvideva celovit pristop, je bil 7 delovnih dni (od tega en dan za potovanje).

V primeru izvedbe splošnega skrbnega pregleda IS so samo 3 faze in ni vključenih aktivnosti odločitvenega modela, zato naročniku izvedbe tega pregleda ni bilo potrebno določiti odločitvenih parametrov in pripadajočih uteži za odločitveni model skrbnega pregleda IS.

Po opravljenem pregledu na lokaciji, kjer so bile izvedene aktivnosti, ki so opisane v drugi fazi celovitega pristopa skrbnega pregleda IS, sem pridobil dovolj dokumentacije in informacij o IT v delu pregleda IT in pogovorih s končnimi uporabniki. Ob zaključku pregleda na lokaciji sem pripravil dve poročili: kratko poročilo o prednostih in slabostih ter možnih tveganjih za upravo banke ter ustno poročilo za direktorja IT, kateremu sem prenesel ugotovitve o stanju IS kot zahvalo za pomoč in sodelovanje pri splošnem skrbnem pregledu IS v organizaciji (banki C).

Po vrnitvi s pregleda na lokaciji sem v tretji fazi splošnega skrbnega pregleda banke C izvedel analizo pridobljenih podatkov.

Slika 9: Prednosti in slabosti IS v banki C



Maksimalno odstopanje na področju Prednosti in slabosti IS se izračuna na osnovi analize

odgovorov na vprašalnik Prednosti in slabosti IS. V okviru splošnega skrbnega pregleda IS sem v banki A pridobil 11 odgovorov (3 od informatikov in 8 od končnih uporabnikov), kar je 30,56 % vseh zaposlenih. Analiza vseh vprašalnikov ni pokazala bistvenih odstopanj. Povprečna vrednost odstopanj je bila 2,66, kar prenese v zmožnostno zrelostnem modelu (CMM) oceno 2,34. Glede na pridobljeno oceno je zrelostni model med 2 – ponovljivo, vendar intuitivno, ter 3 – opredeljeno.

Analiza podatkov izpolnjenih vprašalnikov Prednosti in slabosti IS je prikazala različen pogled uporabnikov in sodelavcev IT – podrobnosti so na sliki 9.

S pomočjo izpolnjenega vprašalnika Status IS, podatkov, pridobljenih ob obisku posameznih lokacij, in pogovorov s predstavniki IT se lahko analizira stopnjo tveganja IS. S pomočjo preglednice, ki preslika pridobljene podatke iz statusa IS, se v fazi analize pridobi numerično stopnjo tveganja IS. Za banko C je ta stopnja znašala 2,5.
Pripravil sem širše poročilo skrbnega pregleda, ki je vsebovalo več kot 20 ugotovitev in priporočil.

Naročnik je preučil ugotovitve in priporočila. Sprejel je poročilo in pripravil taktičen načrt za realizacijo priporočil in večino le-teh realiziral do konca leta 2008.

Banka D se nahaja v Bosni in Hercegovini. Cilj za ta skrbni pregled IS je bil prevzem in združitev (»M&A«). Banka D je univerzalna banka, ki je bolj usmerjena na poslovanje s fizičnimi osebami. Po velikosti je manjša banka s 179 zaposlenimi, 14 lokacijami (centralo in poslovalnicami), njen kapital pa je ob pregledu znašal 22.000.000,00 €.
Začetni skrbni pregled banke je bil izveden v septembru in oktobru 2007. Aktivnosti skrbnega pregleda za področje IS, so bile izvedene v štirih fazah, kot jih predvideva celovit pristop. Za pregled področja IS na lokacijah sem porabil 5 dni. V ekipi za skrbni pregled banke D je sodelovalo 14 strokovnjakov, od tega en strokovnjak za področje IT, preostali pa so pokrivali ostalih 9 področij skrbnega pregleda.

Skupen čas za izvedbo začetnega pregleda IS z vsemi aktivnostmi, ki jih predvideva celovit pristop, je bil 12 delovnih dni (od tega en dan za potovanje). Naročnik izvedbe skrbnega pregleda je pred odhodom ekipe na lokacijo določil odločitvene parametre in pripadajoče uteži za odločitveni model skrbnega pregleda IS. Osnove teh odločitvenih parametrov sem predstavil in opisal v preglednici 13 v poglavju 3.6 .

Preglednica 21: Odločitveni parametri in uteži za banko D

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**5,0**	**300.000**		
2	Investicije v IS v naslednjih petih letih	B	**20,0**	**3.200.000**		
3	Stroški IS v naslednjih petih letih	C	**20,0**	**1.200.000**		
4	Zahtevano število svetovalnih dni investitorja	D	**15,0**	**500**		
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**3**		
6	Stopnja tveganja IS	F	**15,0**	**5**		
7	Odstopanje produktov in storitev	G	**10,0**	**10**		
	SKUPAJ		100			
		Fmax	**20,0**			
		finančni	60,0		ODLOČITEV	
		ne finančni	40,0			

Preglednica 21 prikazuje predhodno določene parametre s pripadajočimi utežmi. Naročnik se je v tem primeru odločil, da z najvišjo utežjo (20,0) obteži investicije in stroške IS v naslednjih petih letih. Z drugo najtežjo utežjo (15,0) je naročnik obtežil zahtevano število svetovalnih dni investitorja, maksimalno odstopanje na področju Prednosti in slabosti IS ter stopnjo tveganja IS.

V drugi skupini odločitvenih parametrov je naročnik določil posamezne mejne vrednosti za posamezne parametre:

- trenutno vrednost IS: 300.000,00 €
- investicije v IS: 3.200.000,00 €
- stroške v IS: 1.200.000,00 €
- maksimalno število človek dni za sinhronizacijo: 500
- maksimalno odstopanje na področju Prednosti in slabosti IS: 3
- ocenjeno stopnjo tveganja: 5
- odstopanje produktov in storitev: 10

Razmerje finančnih in nefinančnih parametrov je 60,0 : 40,0, kar kaže na to, da je naročnika skrbnega pregleda v sklopu tega pregleda zanimala predvsem finančna stran pregleda.

Po opravljenem pregledu na lokaciji, kjer so bile izvedene aktivnosti, ki so opisane v drugi fazi celovitega pristopa skrbnega pregleda IS, sem pridobil dovolj dokumentacije in informacij o IT v delu pregleda IT in pogovorih s končnimi uporabniki. Ob zaključku pregleda na lokaciji sem pripravil dve poročili: za vodjo skrbnega pregleda kratko poročilo o prednostih in slabostih ter možnih tveganjih in ustno poročilo za direktorico IT, kateri sem prenesel ugotovitve o stanju IS kot zahvalo za pomoč in sodelovanje pri začetnem skrbnem pregledu IS v organizaciji (banki D).

Po vrnitvi s pregleda na lokaciji sem v tretji fazi začetnega skrbnega pregleda banke D izvedel analizo pridobljenih podatkov. Za posamezna področja odločitvenega modela sem pridobil numerične vrednosti ter jih vnesel v preglednico 22.

Preglednica 22: Rezultati analize za banko D

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**5,0**	**300.000**	**242.646,00**	
2	Investicije v IS v naslednjih petih letih	B	**20,0**	**3.200.000**	**3.810.000,00**	
3	Stroški IS v naslednjih petih letih	C	**20,0**	**1.200.000**	**1.120.000,00**	
4	Zahtevano število svetovalnih dni investitorja	D	**15,0**	**500**	**640**	
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**3**	**2,80**	
6	Stopnja tveganja IS	F	**15,0**	**5**	**5**	
7	Odstopanje produktov in storitev	G	**10,0**	**10**	**8**	
	SKUPAJ		100			
		Fmax	**20,0**			
		finančni	60,0		ODLOČITEV	
		ne finančni	40,0			

Trenutno vrednost IS, ki je znašala 242.646,00 €, sem pridobil iz finančnih podatkov za opredmetena osnovna sredstva.

Investicije v IS v naslednjih petih letih zahtevajo več podatkov ter pomožnih obdelav v različnih preglednicah – skupni izračunan znesek teh investicij za banko D je bil 3.810.000,00 €.

Stroški IS v naslednjih petih letih zahtevajo prav tako nekaj pomožnih obdelav v različnih pripravljenih preglednicah. Skupni izračunani znesek stroškov IS v naslednjih petih letih je znašal 1.120.000,00 €.

Število svetovalnih dni posameznih strokovnjakov kot pomoč/svetovanje potencialni novi organizaciji za naslednja štiri leta je za banko D znašalo 640 človek dni.

Maksimalno odstopanje na področju Prednosti in slabosti IS: v okviru začetnega skrbnega pregleda IS v banki B sem pridobil 11 odgovorov (4 od informatika in 7 od končnih uporabnikov), kar je 6,15 % vseh zaposlenih. Analiza vseh vprašalnikov ni pokazala bistvenih odstopanj. Povprečna vrednost odstopanj je bila 3,2, kar prenese v zmožnostno zrelostnem modelu (CMM) oceno 2,8. Glede na pridobljeno oceno je zrelostni model med 2 – ponovljivo, vendar intuitivno, ter 3 – opredeljeno.

S pomočjo izpolnjenega vprašalnika Status IS, podatkov, pridobljenih ob obisku posameznih lokacij, in pogovorov s predstavnikom IT sem lahko analiziral stopnjo tveganja IS: Numerična stopnja tveganja IS za banko D je znašala 5.

Odstopanje produktov in storitev je v primeru banke D znašalo 8.

Preglednica 23: Končna odločitev za banko D

			Predhodno določeni DD parametri		Rezultati analiz in rezultati vprašalnikov	
#	**Opis**	oznaka	utež	maksimalna vrednost		izračuni
1	Trenutna vrednost IS	A	**5,0**	**300.000**	**242.646,00**	**0,250**
2	Investicije v IS v naslednjih petih letih	B	**20,0**	**3.200.000**	**3.810.000,00**	**-0,191**
3	Stroški IS v naslednjih petih letih	C	**20,0**	**1.200.000**	**1.120.000,00**	**1,000**
4	Zahtevano število svetovalnih dni investitorja	D	**15,0**	**500**	**640**	**-0,210**
5	Maksimalno odstopanje na področju Prednosti in slabosti IS	E	**15,0**	**3**	**2,80**	**0,750**
6	Stopnja tveganja IS	F	**15,0**	**5**	**5**	**0,750**
7	Odstopanje produktov in storitev	G	**10,0**	**10**	**8**	**0,500**
	SKUPAJ		100			**0,407**
		Fmax	**20,0**			
		finančni	60,0		ODLOČITEV	**NO GO**
		ne finančni	40,0			

Preglednica 23 prikazuje podatke po vnosu vseh podatkov analize v odločitveni model in končno numerično odločitev, ki je v banki D znašala 0,407. To je pomenilo, da odločitveni model predlaga predčasen zaključek aktivnosti nakupa organizacije tako, da ne pride do realizacije investicije.

Seveda pridobljeni podatek ni edini, ki ga izvajalec skrbnega pregleda IS posreduje naročniku začetnega skrbnega pregleda. Pregledovalec za področje IS pripravi še podrobno zajetno poročilo, kjer so opisani vsi pridobljeni rezultati in ocene.

V banki D je bila tudi polovica pregledovalcev za nadaljevanje aktivnosti, polovica pa je temu nasprotovala, med njimi tudi pregledovalec za IT. Od skupaj 9 področij jih je bilo 5 proti nadaljevanju aktivnosti in za pogajanje, 4 področja pa so bila za nadaljevanje aktivnosti. Vsa področja so pripravila podrobna poročila. Vodja pregleda se je po pogovorih odločil, da je skupno poročilo negativno.

Naročnik je preučil skupno poročilo začetnega skrbnega pregleda banke D. Odločil se je upoštevali mnenje skupine za začetni skrbni pregled organizacije (banke D). Informacija je bila predstavljena tudi nadzornemu odboru. Finančni rezultati iz letnih poročil za leto 2008 (objavljeni v sredini 2009) in za leto 2009 (objavljeni v sredini 2010) za banko D potrjujejo, da so bili informacije začetnega skrbnega pregleda prave in da je bila sprejeta negativna odločitev prava odločitev.

S tem sem zaključil kratko predstavitev študije primerov.

4.2.3 Analiza študije primerov v finančnih organizacijah

Analiza študije primerov finančnih organizacij podrobno predstavi posamezni primer v konceptu potrditve ali zavrnitve posameznih predpostavk, ki so opisana v poglavju 4.1. Na kratko so predstavljene v preglednici 24. Povratne informacije o posamezni predpostavki za posamezen primer sta posredovala naročnik (predpostavke: 1,2 in 5) ali direktor IT pregledovane organizacije (predpostavki: 3 in 4). Naročnik je v našem primeru eden izmed odločevalcev, ki so naročili skrbni pregled določene organizacije.

Predpostavke so bile ocenjene za vsak primer posebej. Odgovori so bili posredovani na podlagi pogovorov z naročnikom oziroma pridobljeni po opravljenem pregledu preko elektronske pošte z vprašanjem, naslovljenim na direktorja IT. Glede na pozicijo oseb, preko katerih smo pridobili povratne informacije o predpostavkah celovitega pristopa, njihove izobrazbe ter izkušenj, lahko njihova mnenja upoštevamo kot ekspertna.

Preglednica 24: Kratek opis predpostavk za ocenjevanje študije primerov

#	Opis predpostavke	Ocenjevalec
1	Končni rezultat začetnega skrbnega pregleda IS zagotavlja dovolj podatkov za nadaljnja pogajanja.	naročnik
2	Analiza pridobljenih podatkov iz izpolnjenih vprašalnikov Prednosti in slabosti IS omogoča dovolj informacij, da se oceni stopnjo zrelosti IS v pregledovani organizaciji	naročnik
3	Predlagana priporočila so v pomoč vodjem IT in lastnikom organizacije, da izboljšajo stanje IS v pregledani organizaciji	pregledanec / naročnik
4	Proces izvedbe skrbnega pregleda, ki ga nudi celoviti pristop, ne vpliva veliko na izvajanje dnevnih operativnih procesov IS v pregledovani organizaciji - ne moti dnevnih procesov IS pregledovane organizacije.	pregledanec
5	Predlagani celoviti pristop pomaga poslovodstvu naročniku zmanjšati tveganja pri prevzemih in združitvah.	naročnik

Banka A:

Predstavnik naročnika je ocenil, da rezultat s končnim zaključnim poročilom zagotavlja dovolj informacij – predvsem finančnih - ter opisov tveganj IS za dobro osnovo pri nadaljevanje aktivnosti in pogajanj. Iz samega poročila IS je moč razbrati stopnjo zrelosti IS.

S pomočjo finančnih ocen, ki jih je naročnik pridobil iz zaključnega poročila, ocen potreb kadrovskih virov ter opisa tveganj na področju IS, so se zmanjšala tveganja pri prevzemih in združitvah, saj je prevzem v banki A potekal nemoteno. Po združitvi so nekatera priporočila odpravili. Sledila je tudi uspešna združitev dveh organizacij, ki jih je imel investitor v državi. Pri pripravah na združitev je bila pridobljena dokumentacija s poročili, kar je dobra osnova za projektno skupino pri pripravi načrtov združevanja obeh organizacij oziroma njihovih IS.

Ob zaključku pregleda na lokaciji so bile direktorici IT posredovane ugotovitve z nekaterimi priporočili, kar je bilo zanjo veliko presenečenje.

V fazi analize celovitega pristopa je sledila še komunikacija med pregledovalcem in direktorjem IT pregledovane organizacije. V korespondenci je bilo posredovano tudi vprašanje, do kakšne mere je skrbni pregled IS motil dnevni proces IS v pregledovani organizaciji. Prejel sem odgovor, da le-ta operativnih procesov ni motil.

Banka B:

Predstavnik naročnika je ocenil, da rezultat s končnim zaključnim poročilom IS zagotavlja dovolj informacij za odločitev. V tem primeru je bila soglasna odločitev vseh področij, da se ne priporoča investiranje.

Predstavnik naročnika je zatrdil, da je iz poročila moč razbrati stopnjo zrelosti IS v pregledovani organizaciji. Prav tako sem pridobil potrditev, da je bilo iz zaključnega poročila, kjer je bilo dokumentiranih veliko ugotovitev s priporočili, možno oceniti obseg aktivnosti za izvedbo predlaganih priporočil.

Naročnik v tem primeru ni mogel oceniti pomoči pri prevzemih in združitvah, saj je bil predlog negativen; a tudi negativna informacija lahko vpliva na zmanjšanje tveganj.

Ob zaključku pregleda na lokaciji sem direktorju IT posredoval kratko informacijo o ugotovitvah IS ter nekatera priporočila kot zahvalo za pomoč pri izvedbi pregleda IS na lokaciji. Direktor je potrdil večino ugotovitev.

V fazi analize sem imel še e-komunikacijo z direktorjem IT. Posredoval sem mu vprašanje, če lahko oceni, kako je pregled IS motil dneve procese IS v banki B. Posredoval je povratno informacijo, da osnovni procesi niso bili moteni, le sam obisk večjega števila tujcev je vlival

na redne aktivnosti vodij in vodstva banke, ki se je večino časa ukvarjala s pregledovalci na različnih področjih pregleda.

Banka C:

V banki B je bil izveden splošni skrbni pregled. Naročnik, v tem primeru sta to dva predstavnika - član uprave banke C, zadolžen za IS, ter član vodstvo koordinacije Skupine NLB.
V tem študijskem primeru ni bilo ocenjene predpostavke 1, ker ni bil izveden začetni skrbni pregled IS. Vse ostale predpostavke pa so bile ocenjene. Zaključno poročilo je opisalo stopnjo zrelosti IS in je bilo pridobljeno z analizo izpolnjenih 11 vprašalnikov Prednosti in slabosti IS. To sta potrdila tako predstavnik banke B kot tudi član vodstva koordinacije Skupine.

Oba naročnika sta tudi potrdila, da so ugotovitve s priporočili kvalitetna informacija za načrtovanje nadaljnjih aktivnosti pri vodenju IS organizacije – banke B. To je potrdil tudi direktor IT pregledovane organizacije, ki je tudi izjavil, da splošni pregled IS ni motil dnevne produkcije IS. Med pregledom so le zamrznili razvojno vzdrževalne aktivnosti.

Član uprave, zadolžen za IS, in član vodstva koordinacije skupine sta potrdila, da so ugotovitve identificirale nekatera tveganja, ki pa so jih uspešno zmanjšali z implementacijo priporočil. Ti podatki so bili pridobljeni leto po opravljenem splošnem pregledu IS.

Banka D:

Predstavnik naročnika je ocenil, da rezultat s končnim zaključnim poročilom IS zagotavlja dovolj informacij za odločitev, da se ne nadaljuje z aktivnostmi nakupa organizacije. V tem primeru je bila pomembna odločitev vodje začetnega skrbnega pregleda, saj so pregledovalci za različna področja imeli različna mnenja in ni bilo enotne odločitve. Predlog pregledovalca za področje IS je bilo negativno. Predstavnik naročnika je potrdil, da je za področje IS posredovana numerična vrednost, končno poročilo pa je bilo zadostna informacija o stanju IS pregledovane organizacije.

Predstavnik naročnika je tudi potrdil, da je bilo iz končnega poročila moč razbrati stopnjo zrelosti IS v pregledovani banki D. Pridobil sem tudi potrditev, da je bilo iz zaključnega poročila, kjer je bilo dokumentiranih večje število ugotovitev s priporočili, možno oceniti obseg aktivnosti za izvedbo predlaganih priporočil.

Naročnik v tem primeru in primeru banke B ni mogel oceniti pomoči celovitega pristopa pri prevzemih in združitvah. Predlog je bil sicer negativen, vendar tudi negativna informacija, ki ustavi nadaljnje aktivnosti prevzema, zelo vpliva na zmanjšanje tveganj. Če namreč ne nadaljuješ z aktivnostmi, tudi ni tveganj. Če pa nisi prisoten, se pojavijo druga tveganja

poslovne narave in izguba potencialnega prihodka, kar je čisto druga zgodba in nima direktnega vpliva na tveganja pri prevzemih in združitvah.

Ob zaključku pregleda na lokaciji sem direktorici IT posredoval kratko informacijo o ugotovitvah IS ter nekatera priporočila kot zahvalo za pomoč pri izvedbi pregleda IS na lokaciji. Direktorica ni pričakovala, da bo prejela te informacije in je bila prijetno presenečena. Potrdila je večino ugotovitev in si zabeležila priporočila.

V fazi analize sem imel še e-komunikacijo z direktorico IT. Vprašal sem jo, če lahko oceni, kako je pregled IS motil dneve procese IS v banki D. Posredovala je povratno informacijo, da dnevni procesi v IS niso bili moteni.

Glede na posamezne odgovore naročnikov in pregledovalcev je v preglednici 25 skupen pregled vseh študijskih primerov.

Preglednica 25: Povzetek predpostavk

#	Opis predpostavke	Ocenjevalec	Banka A Začetni skrbni pregled IS	Banka B Začetni skrbni pregled IS	Banka C Splošni skrbni pregled IS	Banka D Začetni skrbni pregled IS	SKUPNO
1	Končni rezultat začetnega skrbnega pregleda IS zagotavlja dovolj podatkov za nadaljnja pogajanja.	naročnik	DA - dovolj informacij	DA - dovolj informacij za odločitev	ni vpliva	DA - dovolj informacij za odločitev	3 x DA; 1 x ni vpliva
2	Analiza pridobljenih podatkov iz izpolnjenih vprašalnikov Prednosti in slabosti IS omogoča dovolj informacij, da se oceni stopnjo zrelosti IS v pregledovani organizaciji.	naročnik	DA - iz poročila je moč razbrati stopnjo zrelosti IS	DA - naročnik je zatrdil, da je moč razbrati stopnjo zrelosti	DA - poročilo opisuje stopnjo zrelosti	DA - iz poročila je moč razbrati stopnjo zrelosti IS	4 x DA
3	Predlagana priporočila so v pomoč vodjem IT in lastnikom organizacije, da izboljšajo stanje IS v pregledovani organizaciji.	pregledanec/ naročnik	DA - pokazalo pri kasnejši združitvi	ni podatka	DA- usmeritve za izboljšanje IS	DA - potrditev ugotovitev s strani vodstva IT	3 x DA; 1 x ni podatka
4	Proces izvedbe skrbnega pregleda, ki ga nudi celoviti pristop, ne vpliva veliko na izvajanje dnevnih operativnih procesov IS v pregledovani organizaciji - ne moti dnevnih procesov IS pregledovane organizacije.	pregledanec	DA - ni motil dnevih operativnih procesov	DA - osnovni procesi niso bili moteni	DA - pregled ni motil dnevne produkcije IS	DA - dnevni procesi v IT niso bili moteni	4 x DA
5	Predlagani celoviti pristop pomaga poslovodstvu/naročniku zmanjšati tveganja pri prevzemih in združitvah.	naročnik	DA - nakup in kasnejša združitev	DA - tudi negativna informacija je pomoč pri zmanjševanju tveganj	ni direktnega vpliva- z implementacijo priporočil so zmanjšali določena identificirana tveganja	DA - tudi priporočilo, da se ne izvede nakupa vpliva na zmanjšanje tveganja	3 x DA; 1 x ni vpliva; a je mogoče z implementacijo priporočil zmanjšati tveganja

4.3 Univerzalnost pristopa

Celovit pristop izvedbe skrbnega pregleda IS je možno uporabljati tudi pri pregledu IS v organizacijah izven finančne industrije. V nadaljevanju bo predstavljen postopek, kako se obstoječ pristop razširi z ustreznimi prilagoditvami na posamezne industrije, panoge in dejavnosti. S tem želim v teoriji predstaviti univerzalnost tega celovitega pristopa.

Faze in način dela so nespremenjeni, in sicer ne glede na industrijo, iz katere je organizacija, ki jo nameravamo pregledati (kot začetni skrbni pregled, kot splošni skrbni pregled, kot pregled tehnologije ali kot pregled pred izločanjem).

Prilagoditev na posamezno industrijo, panogo ali dejavnost organizacije je potrebno izvesti le pri nekaterih vprašalnikih, ki jih potrebujemo pri pridobivanju podatkov v okviru faze pregleda na lokaciji ali pri pomožnih vprašalnikih, ki jih uporabljamo v fazi analize.

Preglednica 26 prikazuje seznam vprašalnikov ter njihovo univerzalnost (ali so statični in se ne spreminjajo/prilagajajo organizaciji, ali so dinamični in se spreminjajo/prilagajajo organizaciji).

Preglednica 26: Univerzalnosti - prilagodljivost vprašalnikov

#	Oznaka vprašalnika	Opis vprašalnika	Tip pregleda	Tip
1	UISDDFW Status IS	Celovit opis IS organizacije	vsi	statičen
2	UISDDFW Tveganja IS	Ocena tveganj IS v organizaciji	vsi	statičen
3	UISDDFW Produkti IS	Seznam produktov in storitev IS organizacije	vsi	dinamičen
4	UISDDFW Vrednost IS	Trenutna vrednost in stroški IS organizacije	začetni & izločitev	statičen
5	UISDDFW Investicije in stroški IS	Ocena investicij in stroškov IS po področjih ter ocena potrebnih svetovalnih dni	začetni & izločitev	dinamičen
6	UISDDFW Prednosti in slabosti IS	Numerični pregled prednosti in slabosti IS v organizaciji	vsi	statičen

Podroben opis teh vprašalnikov je v poglavju 3.4 Opisi vprašalnikov. Preglednica 26 prikazuje, ali je potrebno določen vprašalnik pred pregledom prilagoditi organizaciji, ki prihaja iz drugega okolja (industrije/panoge/dejavnosti).

4.3.1 Predpriprave

V okviru predpriprav na pregled je potrebno pred samim začetkom vse dokumente, ki jih uporabljamo v sklopu celovitega pregleda IS, ustrezno prilagoditi.

Najprej je potrebno izbrati jezik, ki ga bomo uporabljali kot jezikovno različico izhodnih dokumentov pregleda (trenutno so vsi vprašalniki v dveh jezikovnih različicah: slovenščini in v angleščini; nekateri posamezni dokumenti so tudi v nemškem, srbskem in hrvaškem jeziku).

O jezikovni različici odloča naročnik. Če zahteva jezikovno različico, ki še ni prilagojena izbranemu jeziku, je potrebno vse vzorce dokumentov prevesti.

Po izbiri jezika je potrebno vse dokumente (med njimi tudi vse statične/univerzalne vprašalnike), ki so v MS Wordu ali MS Excelu, ustrezno minimalno prilagoditi glede na pregledovano organizacijo: ime organizacije, naslov, kraj, država, mesec pregleda ter oznake pregledovalca oziroma pregledovalcev.

Večje prilagoditve je potrebno izvesti pri dveh vprašalnikih v primeru, da organizacija ne izhaja iz finančne industrije/bančne panoge:

- UISDDFW Produkti IS – vprašalnik opisuje seznam produktov in storitev IS pregledovane organizacije. Tu je potrebno seznam prilagoditi organizaciji, njenim procesom in velikosti – kadrovski zasedbi enote, ki izvaja podporo IT. Pri tem vprašalniku ni večjih sprememb, saj so si produkti in storitve IS v organizacijah ne glede na dejavnost, panogo in industrijo podobni.
- UISDDFW Investicije in stroški IS – vprašalnik opisuje oceno investicij in stroškov IS po področjih ter oceno svetovalnih dni. V tem primeru se vprašalniki razlikujejo na dveh delih. Prvi del se nanaša na zavihek Investicije in stroški, kjer je potrebno v rubriki Industrijsko specifična sredstva opredeliti vsa posamezna specifična sredstva, ki jih organizacija lahko uporablja. Drugi del se nanaša na zavihek Investitorjevi človeški viri, kjer je potrebno ustrezno prilagoditi drugi del preglednice, ki zahteva poslovno tehnološke profile. V prvem delu te preglednice, ki ostaja nespremenjen, so opredeljeni profili IT strokovnjakov, ki se pojavljajo v vsaki sredini, ki izvaja podporo IT. Pri tem vprašalniku lahko pride do večjih sprememb in je za njegovo prilagoditev potrebno več priprav. Spoznati se moramo z vsemi komponentami IT – industrijsko specifičnimi sredstvi IT, ki jih taka organizacija dnevno uporablja. Še posebej je potrebno pridobiti znanja, podatke in informacije o industrijsko specifičnih komponentah IT (na primer o tehtnicah in delilnikih pri poštnih organizacijah, različnih računalniško vodenih zdravstvenih aparatih v medicini, posebnih računalniških blagajnah v trgovinah, napravah za nadzor visoko regalnih skladišč in podobno).

Ta dva vprašalnika se uporabljata pri dveh tipih skrbnih pregledov: pri začetnem skrbnem pregledu in skrbnem pregledu zunanjega izvajanja (izločitve – »*outsourcing*«).

Razlika se pojavi, kadar ne pregledujemo/analiziramo IS znotraj organizacije, temveč pregledujemo IS v organizaciji, ki nudi izločanje storitev IS (»IS *outsourcing*«). Tudi v tem primeru moramo nekatere vprašalnike ustrezno prilagoditi obsegu in tipu storitev, ki jih ta organizacija nudi svojim naročnikom.

Prav tako je potrebno glede na velikost pregledovane organizacije izbrati ustrezen seznam zahtevane dokumentacije za skrbni pregled IS (priloga), ki se posreduje v prvi fazi priprave na

pregled, da pregledovana organizacija pripravi potrebno dokumentacijo, ki je osnova za pripravo in pregled na lokaciji.

Trenutno so v celovitem pristopu izvedbe skrbnega pregleda trije možni obsegi seznama potrebne dokumentacije. Seznam se izbere glede na velikost pregledovanih organizacij, ki so lahko: male (do 150 zaposlenih), srednje (do 500 zaposlenih) in velike (več od 500 zaposlenih).

Za velika podjetja se posreduje vseh 25 zahtev (vse točke, ki imajo oznako V in S in M). Za srednja podjetja se posreduje 23 zahtev (vse točke, ki imajo oznako S ali M). Za mala podjetja se posreduje seznam 19 zahtev (vse točke, ki imajo oznako M); pri tem je 7 zahtev pogojnih.

Pri tem je potrebno tudi upoštevati tip pregleda, saj pri splošnih skrbnih pregledih ni potrebno pridobiti finančne vrednosti IS ter podrobnosti o stroških in investicijah, prav tako pa tudi ni potrebno izvesti vpogleda v vse nabavne pogodbe. Od pregledovane organizacije se zahteva samo prikaz indeksa stroškov in investicij za zadnje štiri leta.
V prilogi je ob seznamu tudi opredeljeno, katere dokumente je potrebno v primeru začetnega skrbnega pregleda podrobno preučiti (označeno s kratico ZSP – začetni skrbni pregled). Pri splošnem primeru je pregled te dokumentacije manj temeljit, saj je potrebno pregledati le register pogodb z opisom namena in roki.

Organizacija, ki pripravi/zbere dokumentacijo, v odgovoru tudi sporoči, če kakšne zahteve nimajo. Pred samim pregledom je nesmiselno na hitro kreirati dokumentacijo, saj se s pregledom hitro odkrije, da je bila le-ta pripravljena zaradi skrbnega pregleda.

Za ustrezno dopolnitev vprašalnika UISDDFW Investicije in stroški IS, kakor tudi vprašalnika UISDDFW Status IS, se pridobi manjkajoče podatke na različne načine.

Pomemben način je brskanje po medmrežju, kjer se da pridobiti podatke, kakšno specifično opremo IT nudijo ponudniki take opreme po svetu in pri nas. Te aktivnosti raziskovanja in analiziranja pridobljenih podatkov so pogosto časovno zamudne.

Drug način je spoznavanje procesov in ustrezna podpora IT skozi znanstveno in strokovno literaturo s pomočjo elektronskih knjižnic. Pri tem lahko pridobimo podatke iz različnih zapisov srečanj, zbornikov konferenc, strokovnih razprav in objavljenih prispevkov. Tudi te aktivnosti so časovno zamudne in zahtevajo analitski pristop.

Tretji način je spoznavanje organizacij s pomočjo pridobivanja podatkov od zaposlenih v podobnih organizacijah v Sloveniji. Ta način zahteva aktivno sodelovanje v različnih socialnih omrežjih in veliko število poznanstev in pripravljenost le-teh na prenos znanja in informacij.

4.3.2 Izvedba študije primera

V predhodnem poglavju je bil opisan teoretičen pristop priprave in modifikacije vprašalnikov za skrbni pregled IS v dejavnosti/panogi oziroma industriji, za katero še ni praktičnih izkušenj s pomočjo celovitega pristopa izvedbe skrbnih pregledov.

S pomočjo prijateljev, kolegov in znancev sem našel organizacijo, ki je želel izvesti skrbni pregled IS v svojem okolju.

Za izvedbo tega pregleda so bili uporabljeni vsi vprašalniki, razen Vrednosti IS in Investicije in stroški IS.

Izbrana organizacija je bila iz Slovenije in uporabili smo slovenske predpripravljene vprašalnike. V okviru predpriprav na pregled je bilo potrebno pred samim začetkom vse dokumente, ki so v MS Wordu ali MS Excelu, in ki jih uporabljamo v sklopu celovitega pregleda IS, ustrezno prilagoditi. Dopolnili smo jih z naslednjimi podatki: ime organizacije, naslov, kraj, mesec pregleda ter oznake pregledovalca oziroma pregledovalcev.
Izbrana organizacija se razlikuje od zgoraj naštetih finančnih organizacij. Nudi namreč izločanje storitev IS (»IS outsourcing«) tako pri razvoju in vzdrževanju aplikativne programske opreme kot tudi pri dnevnemu upravljanju produkcije IS za svoje naročnike. Za razliko od dosedanjih pregledovanih organizacij je bilo razmerje notranjih uporabnikov ter sodelavcev IT v pregledovani organizaciji v obratnem razmerju.

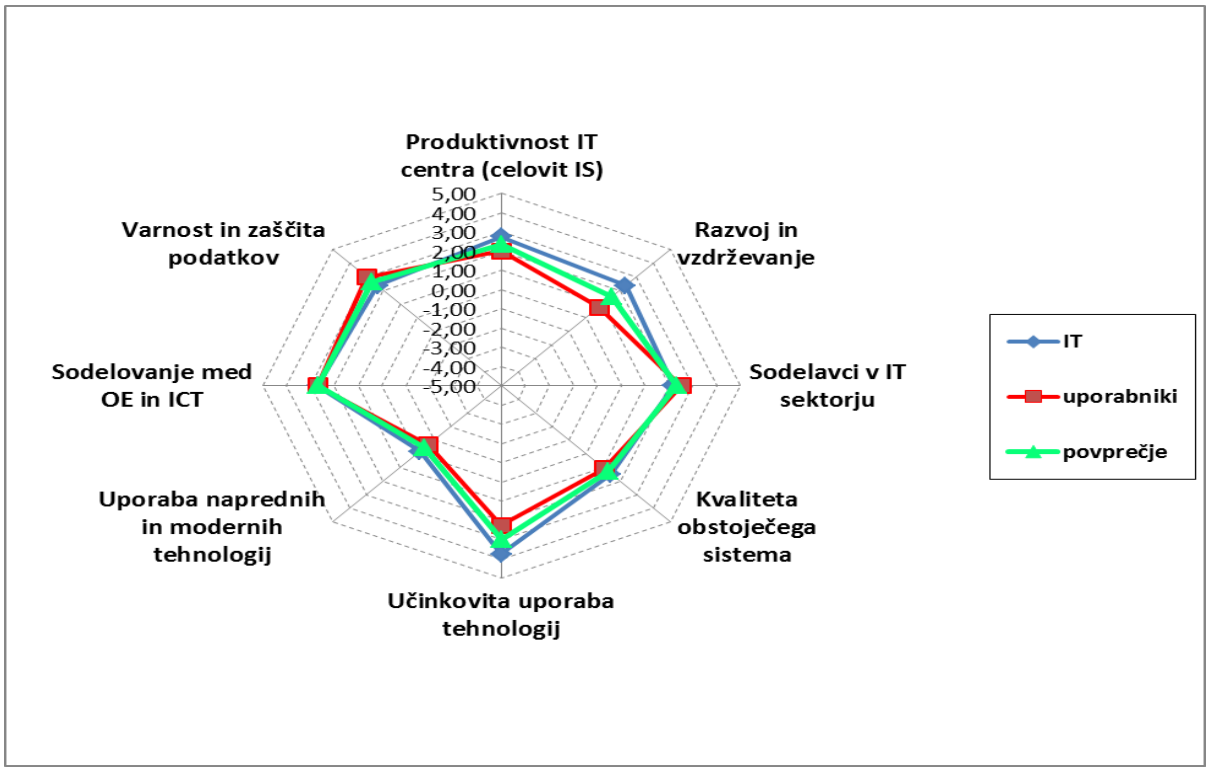
Izbrani organizaciji smo na uvodnem sestanku predstavili metodo in način dela. Koordinatorju pregleda smo predali seznam zahtevane dokumentacije, ki jo želimo pregledati, in tudi vprašalnik Status IS. Predstavili smo jim predlog časovnega načrta pregleda, ki smo ga na njihovo zahtevo ter zaradi zasedenosti njihovih strokovnjakov ustrezno prilagodili.

V dogovorjenem času so nam pripravili in izročili zahtevano dokumentacijo (skupno več kot 30 dokumentov z okoli 500 stranmi) in tudi delno izpolnjen vprašalnik Status IS (okrog 35 % - 40 % celotnega vprašalnika).

S poslovodstvom smo se dogovorili za seznam razgovorov in pregledov njihovih IS prostorov. Po načrtu smo pregledali njihove IS prostore (primarno in sekundarno lokacijo ter ostale prostore z IS opremo in viri). Prav tako smo izvedli 15 razgovorov s strokovnjaki IT ter 9 razgovorov z uporabniki njihovih storitev. Razgovori so trajali od 45 do 120 minut. Z osebama, zadolženima za razvoj in sistemske operacije ter za ta razvoj aplikativne programske opreme, sta bila pogovora daljša. S strokovnjaki IS smo tudi izpolnili manjkajoča poglavja vprašalnika Status IS. V povprečju je trajal en razgovor malo manj kot 90 minut. Vsakdo izmed sogovornikov je na koncu razgovora izpolnil tudi vprašalnik Prednosti in slabosti IS.

Z opazovanjem, s predhodnimi pregledi dokumentacije in z razgovori smo pridobili dovolj informacij za analizo podatkov.

Slika 10: Prednosti in slabosti IS v nefinančni organizaciji



Analiza podatkov v okviru splošnega skrbnega pregleda je bila krajša, saj ni bilo potrebno izpolnjevati vprašalnika Vrednost IS ter Investicije in stroški IS. Potrebno pa je bilo izpolniti vprašalnik Tveganja IS ter obdelati vse vprašalnike Prednosti in slabosti IS. Rezultat analize podatkov s pomočjo Tveganja IS je dal oceno 6,1 (na lestvici od 1 do 10).
Analiza vprašalnika Prednosti in slabosti IS je potrdila že s strani poslovodstva znana dejstva o stanji in klimi v organizaciji, podrobnosti so na sliki 10.

Ocene uporabnikov sodelavcev IS so bile zelo podobne in so kazale določeno stopnjo stabilnosti in zrelosti ter razumevanja IS organizacije.

Ob zaključku faze analize smo pripravili dve poročili. Krajše poročilo za poslovodstvo naročnika obsega povzetek vseh ugotovitev in na kratko podana priporočila v naslednjih sklopih: povzetek ugotovitev s priporočili, stališče, analiza prednosti, slabosti, priložnosti in nevarnosti (»SWOT« analiza) in zaključek. Krajše poročilo je imelo 7 strani.

Daljše poročilo je bilo obsežnejše in namenjeno operativnemu izvajanju priporočil, če se bo tako odločil naročnik.

Za pregledovano organizacijo smo pripravili poročilo z naslednjimi poglavji:

- povzetek za poslovodstvo,
- povzetek ugotovitev s priporočili,
- osnova za pregled,
  - ugotovljene podrobnosti v naslednjih podpoglavjih:
  - splošno,
  - revizije IS,
  - organizacija IT in načrtovanja,
  - sredstva IS (stojna oprema, programska oprema, kadri v IT, prostori),
  - varovanje informacij,
  - upravljanje neprekinjenega poslovanja in upravljanje okrevanja po katastrofi,
  - razvoj, nabava, vzdrževanje in implementacija aplikacij
  - upravljanje procesov in upravljanje tveganja IS,
  - dokumentacija;
- analiza prednosti, slabosti, priložnosti in nevarnosti (»SWOT« analiza),
- analiza razgovorov,
- analiza tveganj,
- stališče,
- priporočila in
- zaključek.

Daljše poročilo je imelo več kot 40 strani.

Na zaključnem sestanku so bile naročniku in nekaterim sogovornikom predstavljene ugotovitve s priporočili. Posredovan je bil tudi dopolnjen vprašalnik Status IS.

4.3.3 Analiza študije primera

IS v organizaciji je zelo kompleksen. Organizacija ima dolgoletno tradicijo razvoja in produkcije IT za svoje naročnike. V organizaciji imajo veliko znanj in izkušenj na področju, ki ga nudijo svojim naročnikom.
Priporočila sem razdelil v 4 kategorije: zelo pomembna, srednje pomembna, pomembna in manj pomembna. Skupno sem oblikoval 52 ugotovitev s pripadajočimi priporočili od tega 14 - zelo pomembnih, 22 - srednje pomembnih, 13 – pomembnih in 3 - manj pomembna.
Predlagal sem, da organizacija realizira kategorije priporočil v naslednjih časovnih obdobjih:

- zelo pomembna: v 3 do 9 mesecih,
- srednje pomembna: v 6 do 12 mesecih,
- pomembna: v 9 do 18 mesecih,
- manj pomembna: v 12 do 30 mesecih.

Splošni skrbni pregled IS v izbrani organizaciji smo izvedli v skladu z metodologijo – predhodno opisanim celovitim pristopom izvedbe skrbnega pregleda. Preglednica 27 prikazuje čas, porabljen za izvedbo skrbnega pregleda IS po posameznih fazah. Izbrana organizacija po svoji usmeritvi ni tipična organizacija, kjer je v povprečju od 3 % do 8 % zaposlenih strokovnjakov za IT, ostalo pa so uporabniki, temveč je bilo razmerje v izbrani organizaciji ravno nasprotno, saj je v organizaciji 9 % zaposlenih notranjih uporabnikov, 91 % zaposlenih je strokovnjakov za IT (od tega 63,3 % razvijalcev).

Preglednica 27: Čas, porabljen po fazah

#	faza	opis vprašalnika	število ur	število človek dni
1	Priprava	Pridobivanje javnih podatkov	3,5	3,20
		Priprava vprašalnikov in prilagoditev na ne finančno organizacijo	4,5	
		Priprava na uvodni sestanek in uvodni sestanek	3	
		Pregled dokumentacije	10,5	
		Priprava načrta pregleda in usklajevanje z naročnikom	2,5	
2	Pregled na lokaciji	Razgovori s strokovnjaki IT	29	5,40
		Razgovori z uporabniki	9	
		Pregled prostorov	2,5	
3	Analiza	Dopolnitev vprašalnika in izpolnitev delovnih vprašalnikov	8	4,13
		Analiza tveganj in analiza prednosti in slabosti	5	
		Priprava daljšega poročila	15,5	
		Priprava krajšega poročila	2,5	
4	Predstavitev	Priprava na zaključni sestanek in zaključni sestanek	4	0,53
	SKUPAJ		**99,5**	**13,27**

Razmerje razgovorov smo zato pri tem pregledu ustrezno spremenili in opravili 62,5 % razgovorov s strokovnjaki IT in preostalo z uporabniki, ki pa niso bili samo notranji uporabniki, temveč tudi nekateri zunanji uporabniki storitev te organizacije.

Druga posebnost tega primera je bila odprtost sogovornikov. V dosedanji praksi pregledov še nismo srečali tako odprtih sogovornikov, ki so želeli predstaviti čim več informacij pregledovalcem.

4.3.4 Kontrolni seznam za adaptacijo celovitega pristopa na novo področje

Glede na izkušnje celovitega pristopa skrbnega pregleda IS izven finančne industrije in potrditve izvedbe vseh aktivnosti v fazi predpriprav lahko strnem proces adaptacije pristopa v enostaven kontrolni seznam, ki je predstavljen v preglednici 28.

Kontrolni seznam vsebuje posamezno aktivnost, opis le-te, način izvedbe ter okviren obseg dela. Največja neznanka pri tem je obseg spremembe, kjer je oznaka ali »večja« ali »odvisno od jezika«. Predvsem sta tu pomembni dve aktivnosti: spoznavanje ter prevod vprašalnikov in seznama dokumentacije, ki jo mora pregledovana organizacija pripraviti pred samo fazo pregleda na lokaciji.

Kot je teoretično opisano v poglavju 4.3.1., je potrebno na začetku izbrati jezik. Ker gre za slovensko organizacijo, ki je v 100 % slovenski lasti, ni bilo dileme glede izbire jezika – slovenščina.

Vse uporabljene vprašalnike je bilo potrebno dopolniti z naslovom organizacije in datumi pregleda. Ker tip pregleda ni bil začetni skrbni pregled, ni bilo nobenih prilagoditev pri vprašalniku UISDDFW Investicije in stroški IS ter UISDDFW Produkti IS.

Preglednica 28: Kontrolni seznam za izvedbo priprav na skrbni pregled v novi dejavnosti

#	Aktivnost	Opis	Način	Obseg spremembe
1	Dogovor o jezikovni različici za pisno in ustno komunikacijo	uskladitev z naročnikom	usklajevanje	
2	Spoznavanje	pridobiti informacije o virih IS, ki se uporabljajo v tej dejavnosti	pregled literature, opazovanje, pogovori	odvisno od značilnosti dejavnosti
3	Dopolnitev vprašalnika - UISDDFW Status IS	prilagoditev vprašalnika na organizacijo/spremembe glave in noge	urejanje	majhna
4	Dopolnitev vprašalnika - UISDDFW Tveganje IS	prilagoditev vprašalnika na organizacijo/spremembe glave in noge	urejanje	majhna
5	Dopolnitev vprašalnika - UISDDFW Produkti IS	prilagoditev vprašalnika na organizacijo/spremembe glave in noge ter produktov	urejanje	večja
6	Dopolnitev vprašalnika - UISDDFW Vrednost IS	prilagoditev vprašalnika na organizacijo/spremembe glave in noge	urejanje	majhna
7	Dopolnitev vprašalnika - UISDDFW Investicije in stroški IS	prilagoditev vprašalnika na organizacijo/sprememba glave in noge ter postavk	urejanje	večja
8	Dopolnitev vprašalnika - UISDDFW Prednosti in slabosti IS	prilagoditev vprašalnika na organizacijo/spremembe glave in noge	urejanje	majhna
9	Izbira seznama dokumentacije	odvisno od velikosti organizacije	urejanje	majhna
10	Pismo o nameri	prilagoditev pisma glede na organizacijo	urejanje	majhna
11	Dogovor o varovanju poslovne skrivnosti	prilagoditev dogovora na organizacijo	urejanje	majhna
12	Prevod vprašalnikov in seznama	po potrebi, če vprašalniki še niso bili prilagojeni na organizacijo	urejanje	odvisno od jezika
13	Dogovor o logistiki in terminu začetka pregleda	uskladitev z naročnikom	usklajevanje	
14	Določitev parametrov in uteži odločitvenega modela pri začetnem skrbnem pregledu	pridobitev podatkov od naročnika	usklajevanje in urejanje	majhna
15	Začetek pregleda	uskladitev z naročnikom	usklajevanje	

Podrobno je bilo potrebno pregledati tudi najpomembnejši vprašalnik – UISDDFW Status IT.

Preglednica 29 opisuje poglavja vprašalnika, kjer sem izvedel modifikacijo.

Preglednica 29: Spremembe v vprašalniku Status IS

#	Zavihek	Področje/vprašanje	Opis spremembe	Obseg spremembe
1	Osnovni podatki	število lokacij strojna in programska oprema aplikacijski sistemi	finančna industrija ima drugačno poimenovane lokacije in hierarhijo le-tej; finančna industirja ima posebne naprave - bančni avtomati; finančna industrija ima drugačne sklope/aplikacijske sisteme za podporo primarnih procesov	majhna majhna majhna
2	Revizija IS			brez sprememb
3	Upravljanje IS, načrtovanja in organizacija			brez sprememb
4	Viri IT - HW (strojna oprema)	diski strežniki/povezave virtualizacija ostala oprema pri končnih uporabnikih naprava za brezprekinitveno napajanje električni generator/agregat WAN - storitve Telekoma WAN - druga omrežja LAN - brezžični telefonska centrala	posodobitev: souporaba podatkovne hrambe; posodobitev: način povezovanja stežnikov; posodobitev: virtualizacija strežnikov; finančna industrija - bančni avtomati; posodobitev: čas neodvisnosti; posodobitev: čas preklopa; posodobitev: ADSL, VDSL; finančna industrija - SWIFT, Reuters posodobitev: uporabljeni standardi višji od 802.11 n posodobitev: UMTS	večja majhna večja majhna majhna majhna majhna majhna majhna majhna
5	Viri IT - SW (programska oprema)	posebne aplikacije glede na dejavnost	prilagoditev glede na dejavnost organizacije	večja
6	Viri IT - ljudje in prostori	izobraževanje uporabnikov	posodobitev: izvajalec	majhna
7	Zavarovanje virov IT	zaščita pred zunanjim svetom - IDS nadzor nad okoljsko izpostavljenostjo	posodobitev (združitev vrstic); posodobitev (senzorji gibanja, senzorji vrtanja/vibracij)	majhna majhna
8	Upravljanje neprekinjenega poslovanja in upravljanje okrevanja	upravljanje okrevanja - metode verifikacije načrta	posodobitev: uporabljen standard ISO/IEC 25999	majhna
9	Aplikacije: razvoj, nabava, implementacija in vzdrževanje	razvoj aplikacij - metodologija	posodobitev: prenehanje delovanja aplikacije	majhna
10	Ocenjevanje poslovnega procesa in upravljanje s tveganji	prenova poslovnih procesov	posodobitev: delo na projektih (izkušnje, dokumentiranje, odobritve sponzorja)	majhna
11	Ostalo			brez sprememb
12	Problemi in pričakovanja			brez sprememb
13	Splošni pogoji			brez sprememb

Pri tem je potrebno poudariti, da sem v vprašalniku izvedel dva tipa sprememb:

- Spremembe zaradi posodobitve vprašalnika (novosti, ki so nastale v zadnjih 3-4 letih na področju IT). Teh sprememb je bilo največ.
- Spremembe zaradi prilagoditve vprašalnika Status IS za finančno dejavnost na vprašalnik za drugo dejavnost. Te spremembe so bile v naslednjih zavihkih:
    - Osnovni podatki (manjše spremembe zaradi prehoda na drugo dejavnost),
    - Viri IT – strojna oprema (manjši spremembi – pri opremi in omrežjih),
    - Viri IT – programska oprema (večja sprememba – zaradi prilagoditve na drugo dejavnost).

Na uvodnem sestanku smo tudi opredelili, ali organizacija uporablja posebne računalniške naprave, ki so vezane na podporo izvajanja njihove dejavnosti. V Informatiki d. d. so sogovorniki obrazložili, da v svojem poslovanju ne uporabljajo nobenih posebnih naprav, ki bi vsebovale računalniške gradnike, kot so na primer pametni električni števci, ki jih v Sloveniji za enkrat še ne uporabljamo).

4.4 Potrditev predpostavk

Vse aktivnosti smo izvedli v skladu s celovitim pristopom izvedbe skrbnega pregleda IS. V preglednici 30 so prikazane vse predpostavke za vseh pet študij primerov. Porabljen čas za velikost organizacije je bil v okviru načrtovanih dni (Preglednica 9).

Preglednica 30: Povzetek predpostavk za vse študije primerov

#	Opis predpostavke	Ocenjevalec	Banka A Začetni skrbni pregled IS	Banka B Začetni skrbni pregled IS	Banka C Splošni skrbni pregled IS	Banka D Začetni skrbni pregled IS	Družba E Splošni skrbni pregled IS	SKUPNO
1	Končni rezultat začetnega skrbnega pregleda IS zagotavlja dovolj podatkov za nadaljnja pogajanja.	naročnik	DA - dovolj informacij	DA - dovolj informacij za odločitev	ni vpliva	DA - dovolj informacij za odločitev	ni vpliva	3 x DA; 2 x ni vpliva
2	Analiza pridobljenih podatkov iz izpolnjenih vprašalnikov Prednosti in slabosti IS omogoča dovolj informacij, da se oceni stopnjo zrelosti IS v pregledovani organizaciji.	naročnik	DA - iz poročila je moč razbrati stopnjo zrelosti IS	DA - naročnik je zatrdil, da je moč razbrati stopnjo zrelosti	DA - poročilo opisuje stopnjo zrelosti	DA - iz poročila je moč razbrati stopnjo zrelosti IS	DA - poročilo opisuje stopnjo zrelosti	5 x DA
3	Predlagana priporočila so v pomoč vodjem IT in lastnikom organizacije, da izboljšajo stanje IS v pregledovani organizaciji.	pregledanec/ naročnik	DA - pokazalo pri kasnejši združitvi	ni podatka	DA- usmeritve za izboljšanje IS	DA - potrditev ugotovitev s strani vodstva IT	DA- usmeritve za izboljšanje IS	4 x DA; 1 x ni podatka
4	Proces izvedbe skrbnega pregleda, ki ga nudi celoviti pristop, ne vpliva veliko na izvajanje dnevnih operativnih procesov IS v pregledovani organizaciji - ne moti dnevnih procesov IS pregledovane organizacije.	pregledanec	DA - ni motil dnevih operativnih procesov	DA - osnovni procesi niso bili moteni	DA - pregled ni motil dnevne produkcije IS	DA - dnevni procesi v IT niso bili moteni	DA - pregled ni motil dnevne produkcije IS	5 x DA
5	Predlagani celoviti pristop pomaga poslovodstvu/naročniku zmanjšati tveganja pri prevzemih in združitvah.	naročnik	DA - nakup in kasnejša združitev	DA - tudi negativna informacija je pomoč pri zmanjševanju tveganj	ni direktnega vpliva- z implementacijo priporočil so zmanjšali določena identificirana tveganja	DA - tudi priporočilo, da se ne izvede nakupa vpliva na zmanjšanje tveganja	ni direktnega vpliva- z implementacijo priporočil so zmanjšali določena identificirana tveganja	3 x DA; 2 x ni vpliva; a je mogoče z implementacijo priporočil zmanjšati tveganja

Študija primera je potrdila hipotezo, da je celovit pristop izvedbe skrbnega pregleda IS primeren tudi za nefinančne organizacije in ga je moč izvesti učinkovito in v zelo kratkem času.

4.5 Razprava

V tem poglavju sem prikazal uporabo celovitega pristopa za izvedbo skrbnega pregleda IS v petih primerih. V prvem delu so opisani 4 primeri v finančnih organizacijah Vzhodne in Jugovzhodne Evrope. V treh primerih sem izvedel začetne skrbne preglede in uporabil vse 4 faze celovitega pristopa. V enem primeru je šlo za splošni skrbni pregled.

V nadaljevanju sledi prikaz pristopa v nefinančni organizaciji v Sloveniji. Pri tem je opisano, katere vprašalnike je bilo potrebno spremeniti, da so se lahko uporabili pri pregledu organizacije, ki ne izhaja iz finančne dejavnosti.

Izbrana organizacija je bila nekaj posebnega, saj je bil delež uporabnikov v izbrani organizaciji v obratne razmerju, kot pri pregledih v finančnih organizacijah. Izbrana organizacija je bila namreč izvajalka razvoja in vzdrževanja aplikativne programske opreme za svoje naročnike, poleg tega pa je za svoje naročnike izvajala tudi dnevno operativno produkcijo IS.

Pregled je pokazal, da celovit pristop izvedbe skrbnega pregleda IS omogoča izvedbo splošnega skrbnega pregleda tudi v taki organizaciji v časovnih okvirih, ki so predvideni za finančne organizacije.

Ekonomska situacija v Sloveniji mi ni omogočila, da bi v letu 2011 in 2012 izvedel še kakšen začetni ali splošni pregled, saj se v slovenskih podjetjih pozna zmanjševanje stroškov na področju IS.

Imel sem resne pogovore z dvema organizacijama, ki sta po številu strokovnjakov IT in uporabnikov bolj podobni pregledanim finančnim organizacijam, a so imeli zamrznjene račune za investicije in stroške IT.

Morda se bodo časi v prihodnje izboljšali in bodo poslovodstva organizacij ter njihovi lastniki želeli pridobiti neodvisno mnenje o stanju IS v njihovih sredinah.

Študije primerov so pokazale, da je skrbni pregled IS možno izvesti v predvidenih kratkih časovnih obdobjih tako v finančnih kot tudi nefinančnih organizacijah.

S tem je zaključeno poglavje Študija primerov.

Podrobnosti o temi tega poglavja sem navedel tudi v naslednjih prispevkih:

a) *Odločitveni model pri skrbnem pregledu informacijskih sistemov, Zbornik prispevkov: Dnevi slovenske informatike 2011, Portorož ISBN 978-961-6165-34-1*

b) *Celovit pristop izvedbe skrbnega pregleda informacijskega sistema, Uporabna Informatika, 2010, št. 4, str. 193-204*

c) *Prilagoditev celovitega pristopa za izvedbo skrbnega pregleda informacijskega sistema v nefinančni organizaciji – študija primera, Zbornik prispevkov: Dnevi slovenske informatike 2012, Portorož ISBN 978-961-6165-37-2*

d) *Framework for the delivery of Information System Due Diligence, Information System Management, prispevek je bil sprejet 11.3.2012, prispevek bo po navedbah glavnega urednika objavljen v enem letu.*

5 NAČRT VPELJAVE CELOVITEGA PRISTOPA SKRBNEGA PREGLEDA IS V PRAKSO

Namen tega poglavja je predstaviti načrt predstavitve in vpeljave celovitega pristopa skrbnega pregleda IS v prakso.

V sklopu priprave teze sem tudi navedel, da bom v sklopu doktorske disertacije pripravil tudi okviren načrt vpeljave celovitega pristopa v prakso. To metodo bom ustrezno predstavil na različnih nivojih (v praksi in na akademskem nivoju) in s tem povečal zanimanje za uporabo v slovenskem prostoru in širši regiji Alpe Jadran.

Informacijo o tej rešitvi mislim predstaviti na različnih področjih in nivojih:

- v izobraževalnih ustanovah,
- na strokovnih srečanjih,
- potencialnim uporabnikom,
- v strokovni literaturi.

5.1 Izobraževalne ustanove

S pomočjo poznanstev in zanimive teme nameravam to metodo predstaviti na diplomskem in morda tudi magistrskem študiju informatike in poslovne informatike na naslednjih inštitucijah:

- na Univerzi v Ljubljani – Fakulteti za informatiko in računalništvo,
- na Univerzi v Ljubljani – Ekonomski fakulteti,
- na Univerzi v Ljubljani – Fakulteti za družbene vede,
- na Univerzi v Mariboru – Fakulteti za elektrotehniko, računalništvo in informatiko,
- na Univerzi v Mariboru – Fakulteti za organizacijske vede,
- na Univerzi v Mariboru – Fakulteti za logistiko,
- na Univerzi v Mariboru – Fakulteta za varnostne vede,
- na Univerza na Primorskem – Fakulteti za matematiko, naravoslovje in informacijsko tehnologijo,
- na Univerzi na Primorskem – Fakulteti za management,
- na Univerzi v Novi gorici – Poslovno-tehniški fakulteti,
- na Fakulteti za informacijske študije, Novo mesto,
- na IEDC – Poslovni šoli Bled,
- na drugih inštitucijah.

To metodo nameravam predstaviti tudi na strokovnih mednarodnih srečanjih, ki jih organizirajo univerze in fakultete v Sloveniji in bližnji okolici, in sicer v obliki predavanj, predstavitev študije primerov in nadgradenj te metode v prihodnosti.

5.2 Strokovna srečanja

To metodo nameravam ustrezno predstaviti na različnih strokovnih srečanjih informatikov in revizorjev.

Na področju informatike načrtujem to metodo predstaviti:

- na Dnevih slovenske informatike,
- na srečanjih – Informatika v javni upravi,
- na drugih strokovnih srečanjih.

Na področju revizije nameravam to metodo predstaviti na srečanjih, ki jih organizira Slovenski inštitut za revizijo:

- na Mednarodni konferenci o revidiranju in kontroli informacijskih sistemov – v sklopu posebne delavnice,
- na letni konferenci za revizorje,
- na letni konferenci za notranje revizorje,
- na srečanjih sekcije ocenjevalcev vrednosti,
- na drugih dogodkih v okviru inštituta.

5.3 Potencialni uporabniki

Na področju managementa, poslovodij in lastnikov podjetij nameravam to metodo predstaviti na različnih srečanjih in dogodkih združenja Manager ter v sklopu ZITex sekcije pri Gospodarski zbornici Slovenije (GZS) in tudi v sklopu sekcije upravljanja varovanja informacij (SUVI) pri Območni zvezi Ljubljana GZS.

Prav tako bom predstavil metodo v okviru Tehnološkega parka Ljubljana, saj je podjetje, v katerem sem zaposlen, član tega parka.

5.4 Strokovna literatura

Nekatere slovenske publikacije so že objavile večje ali manjše dele Celovitega pristopa. To nameravam še nadaljevati z nadaljnjim razvijanjem metode ter s praktičnimi primeri.

V nadaljevanju so našteti nekateri prispevki na to temo, objavljeni med 2008 in 2012:

a) *Začetni skrbni pregled za področje informacijskih sistemov v finančnih organizacijah, Zbornik prispevkov: Dnevi slovenske informatike 2008, Portorož ISBN 978-961-6165-26-6*

b) *Odločitveni model pri skrbnem pregledu informacijskih sistemov, Zbornik prispevkov: Dnevi slovenske informatike 2011, Portorož ISBN 978-961-6165-34-1*

c) *Celovit pristop izvedbe skrbnega pregleda informacijskega sistema, Uporabna Informatika, 2010, št. 4, str. 193-204*

d) *Postopek pregleda in analize stroškov in investicij IS v podjetju, Zbornik prispevkov: 18. Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, Slovenski inštitut za revizijo, 2010, Ljubljana, ISBN 978-961-6495-49-3.*

e) *Initial Due Diligence of Information Technology as Risk Identification before Capital Investment in Finance Industry, Zbornik referatov: Doctoral Consortium, 20th international Conference on Advanced Information System Engineering, 2008, Montpellier*

f) *Analysis of Different Approaches to the Delivery of Information System Due Diligence, Proceedings: 2nd Conference on Information Society and Information Technologies ISIT2010, 2010, Novo mesto, ISBN 978-961-92509-5-2*

g) *Prilagoditev celovitega pristopa za izvedbo skrbnega pregleda informacijskega sistema v nefinančni organizaciji – študija primera, Zbornik prispevkov: Dnevi slovenske informatike 2012, Portorož ISBN 978-961-6165-37-2*

h) *Framework for the delivery of Information System Due Diligence, Information System Management, prispevek je bil sprejet 11.3.2012, prispevek bo po navedbah glavnega urednika objavljen v enem letu*

5.5 Obdobje predstavitev

Aktivnosti, ki sem jih navedel zgoraj, nameravam izvesti v obdobju 2012–2014. Glede na nadaljnje praktične izkušnje nameravam metodo celovitega pristopa še nadgrajevati in predstavljati nadgradnje ter praktične primere v okviru različnih prispevkov.

6 ZAKLJUČEK

V zadnjem času so zaradi gospodarskega stanja investicije v IS pod drobnogledom in pritiski, da upravičijo svojo vrednost in prispevek k dvigu produktivnosti, h kvaliteti in konkurenčnosti organizacije [Sed05]. Po drugi strani pa kljub ekonomski recesiji nekatere organizacije nadaljujejo s povečanjem stroškov in investicij v IS [Kan08]. V prvem in drugem primeru morajo poslovodstva in lastniki dobro poznati svoje IS. Ena izmed možnih metod analize stanja IS je tudi skrbni pregled IS, ki sem ga podrobno opisal v predhodnih poglavjih.

Celovit pristop izvedbe skrbnega pregleda IS, ki je opisan v tej nalogi, je metoda, postopek, način, ki omogoča hitro in učinkovito izvedbo skrbnega pregleda IS. Če gre pri tipu pregleda za začetni skrbni pregled IS ali pregled izvajanja IS, ta pristop omogoča tudi numerično odločitev o nadaljevanju aktivnosti v smislu kapitalskega vložka, nakupa določene organizacije ali o sklenitvi pogodbe za zunanje izvajanje IS oziroma o prenehanju aktivnosti in nedokončanju načrtovanega posla.

6.1 Povzetek

Izvedba skrbnega pregleda IS je zelo podobna reviziji IS, vendar se ne opredeljuje na ozko domeno IS, posamezno področje, proces, implementacijo sistemske ali programske rešitve oziroma na razvoj aplikativne rešitve. Pri skrbnem pregledu IS je predmet pregleda mnogo širši in se ne poglablja v prisotnost kontrol in skladnost z zahtevami kot pri reviziji IS. Poleg tega skrbni pregled IS pokrije tudi druge poglede, ki jih pri reviziji IS načeloma ne ugotavljamo, kot na primer: investicije in stroške, analizo kadrov v IT, zadovoljstvo uporabnikov in informatikov ter drugo.

Naloga je predstavila način, kako je nastal celovit pristop izvedbe skrbnega pregleda IS, in temelji na dolgoletnih izkušnjah izvedbe skrbnih pregledov v finančnih organizacijah v Evropi, preučevanju oz. analizi alternativnih možnosti, drugih načinov, postopkov, standardov in dobrih praks, katerih določene ideje oziroma načini so bili preizkušeni v naslednjih skrbnih pregledih, ki sem jih izvedel, in v primeru pozitivnih učinkov tudi vključeni v nadaljnje postopke skrbnega pregleda IS.

Celovit pristop izvedbe skrbnega pregleda ni popolnoma nov način, temveč nekakšen konglomerat različnih metod, standardov, postopkov izvedb skrbnega pregleda IS. Ta pristop se je izkazal za časovno učinkovitega, saj omogoča hitro izvedbo pregleda IS, tako da lahko naročniku podamo podrobne informacije o vseh domenah IS.

V kratkem času se pregleda stanje IS, njihove vire, procese, tveganja in varovanje informacij, dokumentacijo, stroške in investicije in se pridobi informacije o zadovoljstvu uporabnikov z IS.

6.2 Končne ugotovitve

Celovit pristop je bil preverjen skozi študije primerov v štirih finančnih organizacijah. V obdobju 2007 – 2008 so bili izvedeni trije začetni skrbni pregledi IS ter en splošen skrbni pregled IS v štirih različnih državah Evrope: v Bolgariji, Bosni in Hercegovini, na Kosovem in v Rusiji. Konec leta 2011 in v začetku 2012 je bil celovit pristop izvedbe skrbnega pregleda IS preverjen tudi v eni nefinančni organizaciji, in sicer kot splošni pregled IS. Ta pregled je bil izveden v Sloveniji.

S študijami primerov sem pridobil odgovore na vse predpostavke.

Predpostavka 1:
Končni rezultat začetnega skrbnega pregleda IS zagotavlja dovolj podatkov za nadaljnja pogajanja.

Predpostavka 2:
Vprašalnik o prednostih in slabostih IS, ki je del celovitega pristopa IS, ter analiza pridobljenih podatkov omogočajo dovolj informacij, da se oceni stopnjo zrelosti IS v pregledovani organizaciji.

Predpostavka 3:
Predlagana priporočila so v pomoč vodjem IT in lastnikom organizacije, da izboljšajo stanje IS v pregledovani organizaciji.

Predpostavka 4:
Proces izvedbe skrbnega pregleda, ki ga nudi celovit pristop, ne vpliva veliko na izvajanje dnevnih operativnih procesov IS v pregledovani organizaciji. S tem opredelimo, da niso moteni dnevni procesi IS pregledovane organizacije.

Predpostavka 5:
Predlagan celovit pristop pomaga poslovodstvu/naročniku zmanjšati tveganja pri prevzemih in združitvah (»*Merger and Acquisition*« – v nadaljevanju: M&A).

Vseh pet predpostavk velja pri začetnih skrbnih pregledih IS ter pri skrbnih pregledih izvajanja IS. Predpostavke od 2 do 4 pa so veljavne pri splošnih skrbnih pregledih IS.

Poleg tega so roki izvedb skrbnih pregledov IS v navedenih organizacijah potrdili, da je s pomočjo celovitega pristopa izvedbe skrbnega pregleda IS možno v kratkem času pridobiti dovolj informacij za odločitve oziroma ugotovitve s priporočili.

Integriran odločitveni primer je v primeru začetnih skrbnih pregledov IS podal numerične rezultate o nadaljevanju ali zaključku aktivnosti o pogajanjih za kapitalske vložke oziroma združitve in prevzeme (M&A).

Celovit pristop, predstavljen v tej nalogi, omogoča podroben opis procesov, ki jasno opredeljujejo posamezne postopke za vsako fazo pregleda, posameznih orodij (vprašalnikov) in predlog za pripravo raznih poročil.

S pomočjo tega pristopa je izvedba skrbnega pregleda IS lažja in izvedena na bolj strukturiran način. Celovit pristop izvedbe skrbnega pregleda IS zagotavlja »recept« za izvedbo skrbnega pregleda IS.

6.3 Prispevek znanosti

Kot so ugotovili že Bhatia (2007), Sundberg et al.(2006) in Bablits et al. (2005), so področje skrbnega pregleda IS, ter tudi uporabljene metode in pristopi med znanstvenimi prispevki dokaj nepokriti.

Nekateri prispevki omenjajo skrbni pregled IS kot pomemben dejavnik v okviru aktivnosti združitev in prevzemov [Ang01], [Apa02], [Gat07], [Meh04], [Meh07] in poudarjajo pomanjkanje poudarka na analizah IS.

Zmud (1998) poudarja pomembnost sodelovanja teorije in prakse oziroma pomen raziskave v praksi, saj bi se s tem zmanjšala vrzel med znanstvenimi deli in praktičnimi primeri.

V nalogi sem dokazal, da je celovit pristop skrbnega pregleda IS artefakt IT. S pomočjo študije primerov kot načina znanstvenega dokazovanja sem dokazal oziroma odgovoril na zastavljena vprašanja:

a) ali ogrodje omogoča ponovljivost,
b) ali ogrodje omogoča univerzalnost,
c) ali ogrodje omogoča globalnost,
d) kakšna je stopnja predvidljivosti analiz ogrodja.

V okviru naloge sem tudi odgovoril na zastavljeni hipotezi:

Hipoteza 1: Predlagana metodologija z ogrodjem omogoča učinkovito izvedbo skrbnega pregleda v zelo kratkem času in pri tem zbere dovolj podatkov/informacij za odločanje.

Hipoteza 2: Metodologijo z ogrodjem je možno učinkovito uporabiti tudi v drugih dejavnostih, panogah in industrijah, kot npr. v finančni industriji, v kateri je bila razvita in preverjena.

6.4 Možnosti za nadaljnje delo

Celovit pristop izvedbe skrbnega pregleda IS ni zaključena celota. Je živ sistem, ki se bo v naslednjih letih lahko ustrezno nadgrajeval.

Ena od možnosti nadgradnje je realizacija večjega števila skrbnih pregledov zunanjega izvajanja ter ustrezna nadgradnja.

Druga možnost razširitve in nadaljnjega dela ter raziskovanja je podrobnejša vključitev analize zadovoljstva IS in primerjava z različnimi modeli IS na tem področju.

Tretja možnost za nadaljnje delo je primerjalna analiza ocenjevanja tveganj IS v okviru celovitega pristopa z drugimi metodami in orodji za analizo tveganj IS.

Celovit pristop bo dan na uporabo različnim strokovnjakom na področju IS. V petem poglavju sem navedel, kako nameravam ta pristop promovirati med izobraževalno znanstvenimi inštitucijami, konferencami IS in revizorji. Pri tem pričakujem, da bom lahko tudi z njihovimi povratnimi informacijami in predlogi za izboljšanje ustrezno nadgradil ta pristop, da bo še bolj učinkovit in uspešen.

7. SEZNAM KRATIC

kratica	angleški izraz / slovenski izraz
AHP	Analytical Hierarchy Process / analitično hierarhičen proces
BCM	Business Continuity Management / upravljanje neprekinjenega poslovanja
BIA	Business Impact Analysis / analiza poslovnih učinkov
BSC	Balanced Score Card / sistem uravnoteženih kazalnikov
CAO	Chief Accounting Officer / vodja računovodstva *ALI*
CAO	Chief Analytics Officer / vodja analitike
CCO	Chief Compliance Officer / vodjo področja skladnosti poslovanja
CD	Compact Disk / zgoščenka oziroma CD-plošča
CFO	Chief Financial Officer / vodja finančnega področja
CHRO	Chief Human Resources Officer / vodjo kadrovskega področja
CIO	Chief Information Officer / član poslovodstva zadolžen za informatiko
CISO	Chief Information Security Officer / pooblaščenec za varovanje informacij
CLO	Chief Legal Officer / vodja pravnega področja
CMM	Capability Maturity Model / zmožnostno zrelostni model
CMMI	Capability Maturity Model Integration / integracijsko ogrodje za zmožnostno zrelostni model
COBIT	Control Objectives for Information and related Technology / kontrolni cilji za informacijsko in sorodno tehnologijo

COSO	Committee of Sponsoring Organizations of the Treadway Commission / COSO - odbor sponzorskih organizacij v komisiji Treadway (nacionalna komisija za goljufivo računovodsko poročanje)
CPO	Chief Procurement Officer / vodjo nabave
CRO	Chief Risk Officer / vodja za upravljanje s tveganji
CSO	Chief Strategy Officer / pooblaščenec za strategijo
DD	Due Diligence / skrbni pregled
DRM	Disaster Recovery Management / upravljanje okrevanja po katastrofi
ERP	Enterprise Resource Planning / celovita programska rešitev
FTE	Full Time Equivalent / človek dni
GDD	General Due Diligence (glej kratico SSP)
GTAG	Global Technology Audit Guide / usmeritve za globalno tehnološko revizijo
ICT	Information Communication Technology (glej kratico IKT)
IDD	Initial Due Diligence (glej kratico ZSP)
IEC	International Electro technical Commission / mednarodna komisija za področje elektrotehnike
IIA	Institute of Internal Auditors / inštitut notranjih revizorjev
IKT	informacijsko komunikacijska tehnologija (glej kratico ICT)
IOS	Integrated Operation System / integriran operacijski sistem
IS	Information System / informacijski sistem
ISACA	Information System Audit and Control Association / združenje za kontrolo in revizijo informacijskih sistemov
ISMS	Information Security Management System (glej kratico SUVI)
ISO	International Organization for Standardization / mednarodna organizacija za

	standardizacijo
IT	Information Technology / informacijska tehnologija
ITADD	Information Technology Assessment Due Diligence Framework / ogrodje za ocenjevanje skrbnega pregleda informacijske tehnologije
ITAF	Information Technology Assurance Framework / ogrodje za zagotavljanje jamstva informacijske tehnologije
ITIL	Information Technology Infrastructure Library / zbirka napotkov za upravljanje in uvajanje storitev informacijske tehnologije
LAN	Local Area Network / lokalno omrežje
M & A	Mergers & Acquisitions / združitve in prevzemi
MS	Microsoft (www.microsoft.com)
NDA	Nondisclosure Agreement / dogovor o varovanju poslovne skrivnosti
PAM	Process Assessment Model / model ocenjevanja procesa
PBX	Private Branch Exchange / naročniška telefonska centrala
PDA	Personal Digital Assistant / dlančnik
POS	Point of Sale Terminal / prodajni terminal
PSPN	analiza prednosti, slabosti, priložnosti in nevarnosti (glej kratico SWOT)
PT	Production Technology / operativna tehnologija
ROI	Return on Investment / povrnitev investicije
SEI	Software Engineering Institute / inštitut za programsko inženirstvo
SSP	splošni skrbni pregled (glej kratico GDD)
SUVI	sistem za upravljanje varovanja informacij (glej kratico ISMS)
SWOT	Strengths, Weaknesses, Opportunities, and Threats / analiza prednosti, slabosti, priložnosti in nevarnosti (glej kratico PSPN)

UISDDFW	Universal Information System Due Diligence Framework / Celovit pristop za izvedbo skrbnega pregleda informacijskega sistema
UPS	Uninterruptable Power Supply / brezprekinitveno napajanje
WAN	Wide Area Network / prostrano omrežje
WLAN	Wireless Local Area Network / brezžično lokalno omrežje
ZSP	začetni skrbni pregled (glej kratico IDD)

8. SEZNAM VIROV

[Abr09] Abram, T. *The Hidden Values of IT Risk Management,* ISACA Journal, 2009, Volume 2, str. 52-56

[Agr11] Agresti, W.W. *Toward an IT Agenda,* Communication of the Association for Information Systems, 2011, Volume 28, Article 17 http://aisel.aisnet.org/cais/vol28/iss1/17

[Ako96] Akoka, J., Comyn_Wattiau, I. *A Knowledge-Based System for Auditing Computer and Management Information Systems;* Expert Systems with Applications, 1996, vol.11, št.3, str. 361-375

[Ala08] Alaranta, M., & Henningsson, S. *An approach to analyzing and planning postmerger IS integration: Insights from two field studies,* Information Systems Frontiers, 2008, Volume 10, Number 3, str. 307-319

[Alb03] Alborz, S., Seddon, P., & Scheepers, R. *A Model for Studying IT Outsourcing Relationship,* PACIS 2003 Proceedings, 2003, prispevek 90

[Alt99] Alter, S. *Dimension of Information System Success: Letter to the Editor: The Siamese Twin Problem: A Central Issue Igonred by "Dimension on Information System Effectiveness",* Communication of the Association for Information Systems, 1999, Article 20

[Alt02] Alter, S. *The Work System Method for Understanding Information System and Information System Research,* Communication of the Association for Information Systems, 2002, Volume 9, Article 6

[Alt02b] Alter, S., & Dennis, A. *Selecting Research Topics: Personal Experience and Speculations for the Future,* Communication of the Association for Information Systems, 2002, Volume 8, str. 314-329

[Alt03] Alter, S. *18 Reasons Why IT-Reliant Work Systems Should Replace "The IT Artifact" as a Core Subject Metter of the IS Field,* Communication of the Association for Information Systems, 2003, Volume 12, Article 23, str. 366-395

[Alt04] Alter, S., & Sherer, S. *A General but Readily Adaptable Model for Information System Risk ,* Communication of the Association for Information Systems, 2004, Volume 14, Article 1

[Alt05] Alter, S., & Browne, G. *A Broad View of System Analysis and Design: Implication for Research,* Communication of the Association for Information Systems, 2005, Volume 16, Article 50

[Alt06] Alter, S. *Work Systems and IT Artifacts - Does the Definition Matter?*, Communication of the Association for Information Systems, 2006, Volume 17, Article 14

[Alt10] Alter, S. *Viewing System as Service: A Fresh Approach in the IS Field*; Communication of the Association for Information Systems, 2010, vol. 26, art. 11, str. 195-224

[Ana05] Anantha Sayana, S. *Auditing Realization of Benefits from IT,* Information System Control Journal, 2005, Volume 3, str. 11-13

[And07] Andriole, J. S. *Mining for Digital Gold: Technology Due Diligence for CIOs,* Communication of the Association for Information Systems, 2007, Volume 20, Article 24, str. 371-381

[And09] Andriole, J. S. *Technology Due Diligence, Best Practices for Chief Information Officers, Venture Capitalists, and Technology Vendors,* Information Science Reference, 2009, ISBN 987-1-60566-018-9

[Ang01] Angwin, D. *Mergers and Acquisitions across European Borders; National Perspectives on Preacquisitions Due Diligence and the Use of Professional Advisers,* Journal of World Business, 2001, Volume 36, Number 1, str. 32-57

[Apa02] Aponovich, D. *IS Integration Seen as Key to Merger Success,* CIO Update, 27.3.2002, http://www.cioupdate.com/reports/article.php/11050_999541 (na dan 16.3.2011)

[Avg00] Avgerou, C. *Information Systems: what sort of science is it?*, Omega, 2000, Volume 28, str. 567-579

[Axe09] Axelrod, C. W., Bayuk, J. L. & Schutzer, D. *Enterprise Information Security and Privacy*, Artech House, INC, 2009, ISBN 13:978-1-59693-190-9

[Baj05] Bajec, M., & Krisper, M. *Issues and Challenges in Business Rule Based Information System Development*, ECIS (European Conference on Information Systems) 2005 Proceedings, 2005, http://aisel.aisnet.org/ecis2005/100

[Baj06] Bajec, M. *Uporaba modela COBIT za celovit pregled IT postopkov v okviru strateškega načrtovanja informatike*, Zbornik referatov: 15. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2006, ISBN 961-6495-24-0, str. 223-236

[Bas99] Baskerville, R. L. *Investigating Information System with Action Research,* Communication of the Association for Information Systems, 1999, Volume 2, Article 19

[Bau05] Baublits, T., Lee, H-J., Stanis, G., Sundberg, B., Tan, *Z-D. 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

[Bay09] Bayuk, J. *Vendor Due Diligence,* ISACA Journal, 2009, št.3, str. 34-38

[BCI03] The Business Continuity Institute. *The ten certification standard for Business Continuity Practitioners* – 2003

[Ben99] Benbaset, I., & Zmud, W. *Empirical Research in Information Systems: The Practice of Relevance,* MIS Quarterly, 1999,Number 1, str. 3-16

[Bin08] Bing, G. *Due Diligence Planning, Questions, Issues,* Praeger Publishers, 2008, str. 105-110, ISBN 978-0-313-34540-1

[Bha07] Bhatia, M. *IT Merger Due Diligence - A Blueprint,* Information System Control Journal, 2007, Volume 1, str. 46-49i

[Boe88] Boehm, B.W. *Spiral Model of Software Development and Enhancement*, IEEE Computer, 1988, Volume 21, Article 5, str. 61-72

[Can05] Cangemi, P. *Issues and Comments,* Information System Control Journal, 2005, Volume 5, str. 5-7.

[Cho07] Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees J. *Management of Information Security: Challenges and Research Directions,* Communications of the Association for Information Systems, 2007, Volume 20, str. 958-971

[Cla08] Clarke, R. *Man Exploratory Study of Information Systems Research Impact,* Communications of the Association for Information Systems, 2007, Volume 22, Article 1, str. 1-32

[Cra07] Cram, A. *The IT Balanced Scorecard Revisited,* Information System Control Journal, 2007, ISACA, Vol. 5, str. 33-36.

[DeL01] DeLone, W., & McLean, E. *Information System Success: The Quest for the Dependent Variable,* Information System Research, 2001, 1, str. 60-95.

[DeL03] DeLone, W., & McLean, E. *TheDeLone and Mcleanmodel of Information System Success: a Ten-year Update,* Journal of Management Information System, 2003, Volume 19, Number 4, str. 9-30.

[Den01] Dennis, A., & Valacich, J. *Conducting Research in Information Systems,* Communication of the Association for Information Systems, 2011, Volume 7, Article 5

[Des06] Desouza, K.C., El Sawy, O.A, Galliers, R.D., Loebbecke, C., & Watson, R.T. *Beyond Rigor and Relevance Towards Responsibility and Reverberation: Information System Research That Really Matters,* Communications of the Association for Information Systems, 2006, Volume 17, str. 341-353

[Dic99] Dick, B. *Qualitative action research: improving the rigor and economy* [On line], 1999, available at http://www.scu.edu.au/schools/gcm/ar/arp/rigour2.html

[Eve03] Evens, E. G., & Costa, B. A. *Outcome Based Systems Evaluation to Access Information Technology Using Arima Methods,* Communications of the Association for Information Systems, 2003, Volume 11, Article 34, str. 660-677

[Fit93] Fitch, P.T. *Dictionary of Banking Terms 2nd edition*, Barron's Educational Series, 1993 – ISBN 0-8120-1530-4, str. 207

[Gat07] Gattiker, U. *Merger and Acquisition - Effective Information Security Depends on Security Metrics,* Information System Control Journal, 2007, Vol. *5*, str. 51-56.

[Gol07] Golob, P., & Hmelak Ajdič, M. *Dobre prakse revidiranja informacijskih sistemov,* Zbornik referatov - 15. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2007, Ljubljana: Slovenski inštitut za revizijo, str. 205-221

[Goo07] Goodman, S.E, & Ramer, R. *Global Sourcing of IT Services and Information Security: Prudence before Playing*, Communications of the Association for Information Systems, 2007, Volume 20, str. 812-823

[Gor04] Gornik, R. *Upravljanje operativnih tveganj v informatiziranih bankah*, Maribor, 2004

[Gor05] Gornik, R. *Upravljanje operativnih tveganj v bankah po novem kapitalskem sporazumu BASEL II*, Zbornik referatov - 13. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2005, Ljubljana: Slovenski inštitut za revizijo, str. 125-148

[Gre06] Gregor, S. *The Nature of Theory on Information Systems* , MIS Quarterly, 2006, Number 2, str. 611-642

[Gre00] van Grembergen, W. *The Balanced Scorecard and IT Governance,* ISACA, Information System Control Journal, 2000, Volume 2

[Har05] Hardy, G. *Information Risks: Whose business are they?* IT Governance institute

[Hev04] Hevnver, A., March, S.T., Park, J., & Ram, S. *Design Science in Information System Research*, 2004, MIS Quarterly, str. 75-105

[Hil07] Hiles, A. *The Definitive Handbook of Business Continuity Management*, 2nd Edition, 2007, Wiley, ISBN 978-0-470-51638-6

[Hol03] Holland, Ch.P. *The IS Core – X: Information Systems Research and Practice: IT Artifact or a Multidisciplinary Subject?*, Communications of the Association for Information Systems, 2003, Volume 12, Article 40, str. 599-606

[Hol05] Holm-Larsen, M. *ICT Integration in an M&A Process*, PACIS 2005 Proceedings, 2005, prispevek 95

[How03] Howson, P. *Due Diligence: The Critical Stage in Mergers and Acquisitions,* Gower Publishing Limited, 2003, ISBN 978-0-566-08524-6

[IIA05] IIA, *Global Technology Audit Guide: Information Technology Controls*, 2005

[ISA03] ISACA *Board Briefing on IT Governance*, 2nd Edition, USA, 2003, ISBN 1-893209-64-4.

[ISA04] ISACA CISA Review Manual 2005, USA, 2004, ISBN 1-893209-80-6.

[ISA05] ISACA *Information Security Harmonization- Classification of Global Guidance*, ISACA, 2005

[ISA08] ISACA *ITAF - A Professional Practices Framework for IT Assurance*, USA, 2008, ISBN 978-1-60420-036-2.

[ISA09] ISACA *Implementing and Continually Improving IT Governance*, USA, 2009, ISBN 978-1-60420-119-2

[ISA09a] ISACA *The Risk IT Framework*, USA, 2009, ISBN 978-1-60420-111-6

[ISA09b] ISACA *The Risk IT Practitioner Guide*, USA, 2009, ISBN 978-1-60420-116-1

[ISA09c] ISACA *IT Value; IT Value Special Compilation*, 2009, ISACA Journal

[ISA09d] ISACA *An Introduction to the Business Model of Information Security*, 2009

[ISA10] ISACA *COBIT 5 Design Paper Exposure Draft*, 2010

[ISA10a] ISACA *The Business Case Guide: Using VAL IT 2.0*, 2010, ISBN 978-1-60420-105-5

[ISA10b] ISACA Certified Information System Auditor – CISA Review Manual 2011, USA, 2010, ISBN 978-1-60420-127-7

[ISA11] ISACA *COBIT Process Assessment Model (PAM): Using COBIT 4.1*, 2011, ISBN 978-1-60420-188-8

[ISO08] Slovenski standard SIST EN ISO 9001:2008, 2008, http://www.sist.si/slo/z1/z162.htm#slo (na dan: 12. julij 2010)

[ISO10] Slovenski standard SIST EN ISO 27001:2010, 2010, http://www.sist.si/ecommerce/catalog/project.aspx?id=aefeae39-95a7-4cfb-940d-ca8d9e427b81 (na dan: 15. avgust 2011)

[ITG01] IT Governance Institute *Information Security Governance: Guidance for Board of Directors and Executive Managers,* 2001

[ITG06] IT Governance Institute. *COBIT Mapping: Mapping of SEI CMM for Software With COBIT 4.0* , 2006, ISBN 1-933284-49-8

[ITG07] IT Governance Institute. *COBIT 4.1 – Frameworks, Control Objectives, Management Guidelines, Maturity Models,* 2007, ISBN 1-933284-72-2

[ITG08] IT Governance Institute. *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, 2008, ISBN 978-1-60420-066-9
[ITG08a] IT Governance Institute. *COBIT Mapping: Mapping of ITIL v3 With COBIT 4.1*, 2008, ISBN 978-1-60420-035-5

[ITG08b] IT Governance Institute, Office of Government Commerce. *Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002:2005 for Business Benefit,* 2008

[ITG09] IT Governance Institute. *Enterprise Risk: Identify, Govern and Manage IT Risk, The IT Risk Framework,* exposure draft, IT Governance Institute, 2009

[ITG09a] IT Governance Institute. *EITGI Enables ISO/IEC 38500:2008 Adoption Framework,* 2009

[ITG11] IT Governance Institute. *COBIT Mapping: Mapping of ISO/IEC 20000 with COBIT 4.1*, 2011, ISBN 1-978-1-60420-171-0

[ITG11a] IT Governance Institute. *COBIT Mapping: Overview of International IT Guidance, 3rd Edition*, 2011

[Iva07] Ivanko, Š. *Raziskovanje in pisanje del: Metodologija in tehnologija raziskovanja ter pisanja strokovnih in znanstvenih del,* 2007, Kamnik, Cubus image d.o.o.

[Ive83] Ives, B., Olson, M.H.,& Baroudi, J.J. *The Measurement of User Information Satisfaction,* Communication of the ACM Volume 26, 1983, Number 10, str. 785-793

[Jav04] Javornik, M. *Obvladovanje varnostnih incidentov*, Zbornik referatov - 12. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2004, Ljubljana: Slovenski inštitut za revizijo, str. 45-60

[Jia08] Jia, R., Reich, B.H., Pearson, J.M. *IT Service Climate: An Extension to IT Service Quality Research*, Journal of the Association for Information Systems, 2008, Volume 8, Article 5, str. 294-320

[Kan08] Kanaracus, C. *Global IT spending growth stable*, 2008, Gartner, InfoWorld, April 3

[Kar08] Karnet, I. *Zbiranje in ustreznost revizijskih dokazov*, Zbornik referatov - 16. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2008, Ljubljana: Slovenski inštitut za revizijo, str. 207-227

[Kin05] King, R. W., & He, J. *External Validity in IS Survey Research*, Communications of the Association for Information Systems, 2005, Volume 16, Article 45, str. 880-894

[Kin07] King, R. W., & Liu, Ch. Z. *Methods Effects in IS Survey Research: An Assessment and Recommendations*, Communications of the Association for Information Systems, 2007, Volume 20, Article 30, str. 457-482

[Kit04] Kitchenham, B. *Procedures for Performing Systematic Reviews*, Keele University, 2004

[Kle99] Klein, H., & Myers, M. *A Set of Principles for Conducting and Evaluating Interpretative Filed Studies in Information Systems*, MIS Quarterly, 1999, Number 1, str. 67-94

[Kno08] KnowledgeLeader *IT Due Diligence Checklist*, 2008 http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/CLITDueDiligence!OpenDocument (na dan: 11. julij 2010)

[Kou10] Kouns, J., & Minoli, D. *Information Technology Risk Management in Enterprise Environments,* Wiley, 2010, ISBN 978-0-471-76254-6

[Kre08] Kress, B. *Running IT as a Business: IT Metrics Propel Transformation,* Information System Control Journal, 2008, *Volume 5*, str. 5-6.

[Lee01] Lee, S. *Editorial,* MIS Quarterly, 2001, Number 1, str. ii-vii

[Lee03] Lee, S., & Baskerville, R. *Generalizing Generalizability in Information System Research,* Information System Research, 2003, Number 3, str. 221-243

[Lee08] Lee, J.-N. *Exploring the Vendor's Process Model in Information Technology Outsourcing,* Communications of the Association for Information Systems, 2008, Volume 22, str. 569-588

[Lei08] Leimeister, S., Leimeister, J. M., Faehling, J., & Krcmar, H. *Exploring Success Factors for IT Carve Out Projects,* ECIS Proceedings, 2008, prispevek 178

[Len04] Lenarčič, A., & Moškon, S. *Ocena učinkovitosti notranjih kontrol*, Zbornik referatov - 12. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2004, Ljubljana: Slovenski inštitut za revizijo, str. 211-228

[Loc92] Loch, K.D., Carr, H.H., & Warkentin, M.E. *Threats to Information Systems: Today's Reality, Yesterday's Understanding,* 1992, MIS Quarterly, volume 16, number 2, str. 173-186

[Ma05] Ma, Q., & Pearson, J. M. *ISO 1799: "Best Practices" in Information Security Management?,* Communications of the Association for Information Systems, 2005, Volume 15, Article 32, str. 577-591

[Maz01] Mazovec, F. *Pravni Due Diligence*, Pripravniška naloga NLB d.d., Ljubljana, 2001

[McK05] McKinney, C. *Capability Maturity Models and Outsourcing: A Case for Sourcing Risk Management,* Information System Control Journal, 2005, ISACA, Volume 5, str. 28-34

[McL08] McLeod, Jr., A. J, Carpenter, D. R., & Clark, J. G. *Measuring Success in Interorganizational Information Systems: A Case Study*, Communications of the Association for Information Systems, 2008, Volume 22, Article 34, str. 617-637

[Meh04] Mehta, M., & Hirschheim, R. *A Framework for Assessing IT Integration Decision Making in Mergers and Acquisition,* Proceedings of the 37th Hawaii International Conference on System Science, 2004

[Meh07] Mehta, M., & Hirschheim, R. *Strategic Alignment In Mergers And Acquisitions: Theorizing IS Integration Decision making.* Journal of Association for Information System, 2007, Volume 8, Number 3, str. 143-174

[Mer08] Merhout, J. W., & Havelka, D. *Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit,* Communications of the Association for Information Systems, 2008, Volume 23, Article 26, str. 463-482

[Mye99] Myers, D. M. *Investigating Information Systems with Ethnographic Research,* Communications of the Association for Information Systems, 1999, Volume 2, Article 23

[Mit10] Mitrovič, A, *Primer praktičnega pristopa notranje revizije k revidiranju zunanjega izvajanja storitev IT,* Zbornik referatov - 18. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2010, Ljubljana: Slovenski inštitut za revizijo, str. 245-262

[Mošo5] Moškon, S. *Revizija informacijskega sistema v manjših in srednje velikih podjetjih*, Zbornik referatov - 13. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2005, Ljubljana: Slovenski inštitut za revizijo, str. 199-212.

[Oos06] van Oosterhout, M., Waarts, E., van Hillegersberg, J. *Change Factors Requiring Agility and Implications for IT,* European Journal of Information Systems, 2006, Volume 15, number 3, str. 132-145

[Orl01] Orlikowski, J., & Iacono, C. *Research Commentary: Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact,* Information System Research, 2001, Volume 3, str. 121-134

[Orl01b] Orlikowski, W., & Barley, S. *Technology and Institution; What Can Research on IT and Research on Organization Learn From Each Other,* MIS Quarterly, 2001, Number 2, str. 145-165

[Orw07] Orwing, R., & Dean, D. L. *A Method for Building a Referent Business Activity Model for Evaluating Information Systems: Results from a Case Study,* Communications of the Association for Information Systems, 2007, Volume 20, Article 53, str. 872-891

[Pal06] Palvia, P., Midha, V., & Pinjani, P. *Research Models in Information Systems,* Communications of the Association for Information Systems, 2006, Volume 17, Article 47, str. 1042-1063

[Par04] Pare, G. *Investigating Information Systems with Positivist Case Research,* Communications of the Association for Information Systems, 2004, Volume 13, Article 18, str. 233-264

[Pet08] Petter, S., DeLone, W., & McLean, E. *Measuring Information System Success: Models, Dimensions, Measures and Interrelationships,* European Journal of Information System, 2008, Volume 18, str. 236-263

[Pic02] Pickard, S.S. *Due Diligence List*, Writers Club Press, 2002, str. 88-105, ISBN 0-595-26130-2

[Pod09] Podgoršek, U., Grasselli, P., & Dolinar, D. *Revidiranje IS od načrta do izvedbe,* Zbornik referatov - 17. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2009, Ljubljana: Slovenski inštitut za revizijo, str. 191-217

[Pod00] Podlesnik B. *Vsebinska analiza poslovne banke*, Zbornik referatov, 2000, 6. strokovno posvetovanje o bančništvu – Analiza bančnih tveganj, Portorož

[Pot04] Potočnik, M. *Analiza tveganosti za odločanje o ravni varovanja informacij*. Zbornik referatov - 12. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2004, Ljubljana: Slovenski inštitut za revizijo, str. 111-120

[Rab09] Rabaa'i, A.A. *Assessing Information System Success Models: Empirical Comparison (Research in Progress),* 2009, ACIS 2009 Proceedings, prispevek 61, http://aisel.aisnet.org/acis2009/61 (na dan 1. april 2012)

[Roz05] Roztocki, N., & Weistroffer, H.R. *Evaluating Information Technology Investments: A Fuzzy Activity-Based Costing Approach*, Journal of Information Science and Technology, 2005, Volume 2, Article 5, str. 30-43

[Sch11] Schmidt, Ch., & Buxmann, P. *Outcomes and success factors of enterprise IT architecture management: empirical insight from the international financial services industry*, European Journal of Information Systems, 2011, Volume 20, number 2, str. 168-185

[Sed04] Seddon, P., Staples, S., Pantanaykuni, R. in Bowtell, M. *Dimension of Information System Success,* Communication of the Association for Information Systems, 2004, Volume 14, Article 2.

[Sed05] Sedera, D. & Tan, F. *User Satisfaction: An Overarching Measure of Enterprise System Success,* PACIS 2005 Proceedings, 2005, prispevek 80, http://aisel.aisnet.org/pacis2005/80 (na dan 1. april 2012)

[She04] Sherer, A., & Alter, S. *Information System Risks and Risk AFactors; Are they mostly about Information Systems?,* Communication of the Association fro Information Systems, 2004, Volume 14, Article 2

[Sim96] Simon, H. A. *IThe Sciences of the Artificial",* 3rd edition, MIT Press, Cambridge, 1996

[Sis02a] Sisco, M. *The Art of Technology Due Diligence*, TechRepublic, 2002, http://articles.techrepublic.com.com/5100-10878_11-1038683.html (na dan: 5. junij 2010)

[Sis02b] Sisco, M. *IT Due Diligence: The on-site discovery visit,* TechRepublic, 2002, http://articles.techrepublic.com.com/5100-10878_11-1038685.html (na dan: 10. julij 2010)

[Smi01] Smith, A., McKeen, J., & Staples, D. *Risk Management in Information Systems Problems or Potential,* Communication of the Association for Information Systems, 2001, Volume 7, Article13

[Son09] Sondag, M. *The Value of IT Due Diligence*, The Journal, West Monroe Partners, 2009, http://www.westmonroepartners.com/~/media/Files/Published%20Articles/The%20Value%20of%20IT%20Due%20Diligence.ashx (na dan 3. april 2011)

[Soy97] Soy, S.K. *The case study as a research model,* Unpublished paper, University of Texas at Austin, 1997

[Spe10] Spears, J.L., & Barki, H: *User Participation in Information Systems Security Risk Management,* MIS Quarterly, 2010, Volume 34, No. 3, str.503-522

[Str04] Straub, D., Boudreau, M-C., & Gefen D. *Validation Guidelines for IS Positivist Research,* Communication of the Association for Information Systems, 2004, Volume 13, Article 24, str-380-427

[Str08] Straub, W.D., & Ang, S. *Editor's Comments- Readability and the Relevance Versus Rigor Debate,* MIS Quarterly, 2008, Vol.32, No.4, str. iii-xiii

[Sun06] Sundberg, B., Tan, Z-D., Baublits, T., B., Lee, H-J., Stanis, G., Tandriverdi, H. *A Framework for Conducting IT Due Diligence in Mergers and Acquisitions,* ISACA Information System Control Journal Online, 6, 2006 http://www.isaca.org/Journal/Past-Issues/2006/Volume-6/Pages/JOnline-A-Framework-for Conducting-IT-Due-Diligence-in-Mergers-and-Acquisitions1.aspx (na dan: 5. junij 2010)

[Šal06] Šalej, A. *Pregled IT procesov po COBIT metodologiji*, Zbornik referatov: 15. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2006, ISBN 961-6495-24-0, str. 237-245

[Šau06] Šauperl, B., Vajde Horvat, R. *Uporaba SCAMPI ocenitvene metode pri skrbnem pregledu procesov v IT*, 2006, Zbornik referatov: Dnevi slovenske informatike 2006, str. 151

[Taj04] Tajnik, F. *Revizijsko poročanje in uporaba COBIT metodologije.* Zbornik referatov - 12. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2004, Ljubljana: Slovenski inštitut za revizijo, str. 241-252

[Tan04] Tanriverdi, H., & Ruefli. T. W. *The Role of Information Technology in Risk/Return Relations of Firms,* Journal of the Association for Information Systems, 2004, Volume 5, Number 11-12, str. 421-447

[Tas07] Tashi, I., & Ghernaouti-Helie, S. *ISO Security Standards as a leverage on IT Security Management,* Proceedings AMCIS 2007, 2007, prispevek 63 http://aisel.aisnet.org/amcis2007/63 (na dan 5.april 2011)

[Tem06] Templeton, G.F., Lee, CH-P., & Snyder, Ch. *Validation of a Content Analysis System Using an Iterative Prototyping Approach in Action Research,* Communication of the Association fro Information Systems, 2006, Volume 17, Article 24, str. 539-561

[Tru01] Truex, D. P. *Three Issues Concerning Relevance in IS Research: Epistimology, Audience and Method,* Communication of the Association for Information Systems, 2001, Volume 6, Article 24, str. 94-98

[Vai04] Vaishnavi, V., & Kuechler, W. *Design research,* IS World, 2004

[War09] Warkentin, M.,& Willison, R. *Behavioral an Policy Issues in Information System Security: the Insider threat,* European Journal of Information Systems, 2009, Volume 18, str. 101-105

[Wes07] Westerman, G. & Hunter, R. *IT Risk Turning Business Threats into Competitive Advantage,* Harvard Business School Press, 2007, ISBN-13: 978-1-4221-0666-2

[Whe89] Whetten, D.A. *What Constitutes a Theoretical Contribution?*, Academy of Management Review, 1989, Volume 14, Number 4, str. 490-495

[Wik10] Wikipedia http://en.wikipedia.org/wiki/Due_diligence (na dan: 9. januar 2010)

[Wil94] Willcocks, L., & Margetts, H. *Risk Assessment and Information Systems,* European Journal of Information Systems, 1994, Volume 3, Number 2, str. 127-138

[Xu08] Xu, W., Grant, G., Nguyen, H., & Dai, X. *Security Breach: The Case of TJX Companies, Inc.,* Communication of the Association fro Information Systems, 2008, Volume 23, Article 31, str. 575-590

[Yin03] Yin, R.K. *Case Study Research: Design and Methods*, Sage, 2003, Thousand Oaks

[Zab05] Zabel, J. *Writing for Computer Science, 2nd edition,* CSpringer Science+Business Media , LCC, 2005, ISBN: 978-1-85233-802-2

[Zaf09] Zafar, H., & Clark, J. G. *Current State of Information Security Research in IS,* Communication of the Association fro Information Systems, 2009, Volume 24, Article 34, str. 557-596

[Zmu98] Zmud, R. *Conducting and Publishing Practice-Driven Research,* IFIP Working groups 8.2 and 8.6 joint Working Conference on Information Systems: Current Issues and Future Change, Helsinki, 1998

[Zvi03] Zviran, M, & Erlich, Z. *Measuring IS User Satisfaction: Review and Implications,* Communications of the Association for Information Systems, 2003, Volume 12, Article 5, str. 81-103

[Živ10] Živkovič, A, & Heričko, M. *Dobre prakse pri pripravi strategije IT in vloga strategije pri reviziji IS,* Zbornik referatov - 18. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, 2010, Ljubljana: Slovenski inštitut za revizijo, str. 29-39

[Žva10] Žvanut, B. & Bajec, M. *A tool for IT process construction,* Information and Software Technology, 2010, vol. 52, str. 397-410

8.1 OSTALI VIRI

[BSI] British Standards Institution, BS 25999 Business continuity http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/ (na dan: 15. avgust 2011)

[Del13] Delak, B. & Bajec, M. *Framework for the Delivery of Information System Due Diligence,* 11. marca 2012, je bil prispevek sprejet za objavo v reviji Information System Management, in bo objavljen najkasneje v enem letu

[Del12] Delak, B. & Bajec, M. *Prilagoditev celovitega pristopa za izvedbo skrbnega pregleda informacijskega sistema v nefinančni organizaciji – študija primera*, 2012, zbornik referatov 19. Dnevi slovenske informatike, ISBN 978-961-6165-37-2

[Del11] Delak, B. & Bajec, M. *Odločitveni model pri skrbnem pregledu informacijskih sistemov*, 2011, zbornik referatov 18. Dnevi slovenske informatike, ISBN 978-961-6165-34-1

[Del10d] Delak, B. & Bajec, M. *Analysis of Different Approaches to the Delivery of Information System Due Diligence*, 2010, Proceedings: 2nd International Conference on Information Society and Information Technologies ISIT 2010, ISBN 978-961-92509-5-2

[Del10c] Delak, B. & Bajec, M. *Celovit pristop izvedbe skrbnega pregleda informacijskega sistema*, 2010, Uporabna informatika, št. 4, letnik XVIII, str 193 – 204, ISSN 1318-1882

[Del10b] Delak, B. *Postopek pregleda in analiza stroškov ter investicij informacijskega sistema v podjetju*, 2010, zbornik referatov 18. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, str: 9 – 28, ISBN 978-961-6495-49-3

[Del10a] Delak, B. & Bajec, M. *Celovit pristop izvedbe skrbnega pregleda,* 2010, zbornik referatov 17. Dnevi slovenske informatike, ISBN 978-961-6165-32-7

[Del08c] Delak, B. *Začetni skrbni pregledi za področje informacijskih sistemov v finančnih organizacijah*, 2008, Uporabna Informatika, Slovensko društvo Informatika, št. 2, letnik /2008, str. 116 – 122, ISSN 1318-1882

[Del08b] Delak, B. *Initial Due Diligence of Information Technology as Risk Identification before Capital Investment in Finance Industry*, 2008, proceedings: 20th conference CAISE Doctoral Consortium Workshop

[Del08a] Delak, B. *Začetni skrbni pregledi za področje informacijskih sistemov v finančnih organizacijah*, 2008, zbornik 15. Dnevi slovenske informatike, ISBN 978-961-6165-26-6

[IIA] Institute of Internal Auditors – Global Technology Audit Guide http://www.theiia.org/guidance/technology/ (na dan: 15. avgust 2011)

[ISACA] Information System Audit and Control Association – uradna stran http://www.isaca.org/about-isaca/Pages/default.aspx (na dan: 15. avgust 2011)

[Islovar] terminološki slovar informatike – uradna stran
http://www.islovar.org/slovar_oslovarju.asp (na dan: 12. april 2012)

[ISM] Information System Management – uradna stran
http://www.tandf.co.uk/10580530 (na dan: 12. april 2012)

[ITAD] ITAD, Revizija in svetovanje, d.o.o. http://www.itad.si/ (na dan: 15. avgust 2011)

[ITIL] ITIL uradna stran http://www.itil-officialsite.com/ (na dan: 15. avgust 2011)

[MSPP] Microsoft Power Point – predloge za »puzzle« http://office.microsoft.com/en-us/templates/results.aspx?ck=1&ex=2&qu=puzzle&av=zpp140 (na dan 22. januar 2012)

[PAS03] Publicly Available Specification - 2003 http://www.pas56.com/ (na dan: 15. avgust 2011)

9 PRILOGE

9.1 Seznam zahtevane dokumentacije za skrbni pregled IS

V- velika organizacija,
S- srednja organizacija,
M – mala organizacija.

1. Zadnje letno poročilo družbe (**V**)

2. Vsa interna IT dokumentacija (**S**)
    - politike,
    - standardi,
    - navodila,
    - obrazci.

3. Vse stroške IT (za 2008, 2009, 2010, in prvo četrtletje / ali prvo polletje 2011) (**M**)
    - investicije,
    - vzdrževanje:
        - strojna oprema,
        - programska oprema,
        - podporna oprema (klimatske naprave, UPS, agregati, sistem gašenja, sistem javljalcev, sistem za fizično zaščito, …) (V in S),
    - komunikacije,
    - izobraževanje,
    - zunanje izvajanje (V in S),
    - stroški IT osebja.

4. Vse vzdrževalne pogodbe: za IT opremo, komunikacijo, … (**M**) (ZSP)

5. Vse pogodbe o dogovoru o nivoju storitev (SLA) (**S**) (ZSP)

6. Poročila zunanje revizije IT od leta 2008 do danes (**V**)

7. Poročila notranje revizije IT od leta 2004 do danes (**S**)

8. Vse pogodbe, ki se nanašajo na nakup aplikativne programske opreme (**M**) (ZSP)

9. Vse pogodbe, ki se nanašajo na izvajanje IT storitev (**M**) (ZSP)

10. Vse svetovalne pogodbe (**M** če jih imajo; **S**) (ZSP)

11. Seznam vseh licenc skupaj z številom licenc (**M**)

12. Seznam vse IT opreme instalirane na dan 31 december 2010 (**M**)

13. Knjigovodska vrednost IT opreme na dan 31 december 2010, 31 december 2009 in 31 december 2008 (**M**)

14. Seznam vse IT opreme na novo instalirane od 1 januarja 2011 do danes (**M**)

15. Seznam vse IT opreme izločene od 1 januarja 2009 do danes (**M**)

16. Načrtovane investicije IT in vsi načrtovani stroški za leta 2011 ter načrt nabave IT za 2011 (**M,** če jih imajo; **S**)

17. Načrt izobraževanja IT za leta 2010, 2011 in 2012 če že obstaja (**M,** če jih imajo; **S**)

18. Strategija IT za obdobje (in načrti za posamezna obdobja) (**M,** če jih imajo; **S**)

19. Slika IT arhitekture (**M**)

20. Slika komunikacijske topologije (brez IP naslovov) (**M**)

21. Upravljanje / načrt obnovitve po nesreči (BCP/BCM) (**M,** če jih imajo; **S**)

22. Okrevalni načrt / upravljanje z okrevanjem za IT (DRP / DRM) (**M,** če jih imajo; **S**)

23. Opis IT tveganj (**M,** če jih imajo; **S**)

24. Organizacijski načrt družbe (**M**)

25. Podroben organizacijski načrt IT (s priimki vodij oddelkov in sektorjev) (**M** če jih imajo; **S**)

9.2 Vprašalnik - UISDDFW Status IS – za nefinančne organizacije

Vprašalnik je preglednica s 13 zavihki.

Prva stran prvega zavihka je:

Ime organizacije

Ime in priimek osebe, ki odgovarja na ta dokument / list:

Datum: **(kraj) , dan, mesec 201x**

I. OSNOVNI PODATKI O ORGANIZACIJI

I.1 Lokacija	
Naslov centrale organizacije:	
www naslov:	
Telefonska številka centrale:	
Število lokacij na dan: Skupaj Število lokacij centrale Število drugih enot	

I.2 Število zaposlenih
Skupno število
Število v prodaji
Število v podpori
Zaposleni v IT

I.3 Osnovni podatki o strojni in programski opremi (povzetek)
Centralni sistem
Število vseh strežnikov
Število vseh osebnih računalnikov
Posebnost - število procesnih naprav (glede na dejavnost)
Centralni operacijski sistem
Operacijski sistemi na strežnikih
Operacijski sistemi na osebnih računalnikih
Sistem za upravljanje podatkovnih baz (SUPB) (*"DBMS"*)
Anti virusi sistemi

Celoten vprašalnik v slovenskem jeziku in v elektronski obliki se nahaja na priloženem mediju.

9.3 Vprašalnik - UISDDFW Status IS – za finančne organizacije

Vprašalnik je preglednica s 13 zavihki.

Prva stran drugega zavihka je:

Name of the Institution's

Name and Family name of the person who are answering to this document:

Date: (town) , month , day th 200x

II. INFORMATION SYSTEM AUDIT

II.1 Internal Audit	**(YES, NO)**	**(If NO, skip to the next question)**
Presence of the Organization Unit / Reporting to		
Last Activities		
Last Remarks		
Last Recommendation		
Plans for the IT Audit Activities by the End of this Year		

II.2 External Audit	**(YES, NO)**	**(If NO, skip to the next question)**
Chosen Audit Company		
Last Activities		
Last Remarks		
Last Recommendation		

II.2 External Audit	**(Continues)**	**(If NO, skip to the next question)**
Regulatory Audit		
Last Activities		
Last Remarks		
Last Recommendation		

Celoten vprašalnik v angleškem jeziku in v elektronski obliki se nahaja na priloženem mediju.

9.4 Vprašalnik - UISDDFW Tveganja IS

Celoten vprašalnik v elektronski obliki se nahaja na priloženem mediju.

9.5 Vprašalnik - UISDDFW Produkti IS

Celoten vprašalnik v elektronski obliki se nahaja na priloženem mediju.

9.6 Vprašalnik - UISDDFW Vrednost IS

Celoten vprašalnik v elektronski obliki se nahaja na priloženem mediju.

9.7 Vprašalnik - UISDDFW Investicije in stroški IS

Celoten vprašalnik v elektronski obliki (v angleškem jeziku) se nahaja na priloženem mediju.

9.8 Vprašalnik – UISDDFW Prednosti in slabosti IS

ime organizacije/podjetja/družbe	
Zaporedna številka osebe, ki odgovarja na ta vprašalnik:	
Datum: kraj, dd.mm.llll	

I. Produktivnost IT Centra (Celovit IS)	***Ocena****
I.1 - Sposobnost doseganja dogovorjenih ciljev	
I.2 - Dogovor o nivoju opravljanja storitev ("SLA = service level agreement")	
I.3 - Učinkovitost dnevne produkcije	

II. Sistemski razvoj	***Ocena****
II.1 - Hitrost in učinkovitost razvoja in implementacije novih rešitev	
II.2 - Tehnična pristojnost - zmožnost	
II.3 - Zaupanje uporabnikov v nov sistem	
II.4 - Projektno vodenje	
II.5 - Hitrost in učinkovitost nadgradenj obstoječih sistemov (zahteve za spremembe)	
II.6 - Dokumentacija, Izobraževanje - uvajanje	
II.7 - Nivo sodelovanja končnih uporabnikov pri uporabniško sprejemnem testiranju ("UAT - User Acceptance Testing")	

III. Sodelavci v IT	***Ocena****
III.1 - Dovolj tehničnega znanja? (Dovolj izšolani?)	
III.2 - Dobro motivirani?	
III.3 - Dovolj izkušenj?	
III.4 - Dovolj kadrovskih virov? (Dovolj kadra?)	
III.5 - Sposobnost in pripravljenost komuniciranja z uporabniki?	

IV. Kvaliteta obstoječega aplikacijskega sistema	***Ocena****
IV.1 - Dobro strukturiran? Enostaven za uporabo/za vzdrževanje?	
IV.2 - Sistem zadovoljuje uporabniške zahteve?	
IV.3 - Sistem je dovolj integriran? (ni večkratnega vnosa istih podatkov)	
IV.4 - Stopnja kvalitete Upravljavskega IS ("MIS = Management Information System")?	
IV.5 - Stopnja integriranosti Uporabniškega IS ("CIS = Customer Information System") / ("CRM-Customer Relationship Management")?	
IV.6 - Zadovoljivi odzivni časi in zadovoljiva razpoložljivost sistema?	
IV.7 - Sistem omogoča pripravo/izpis vseh eksternih in internih poročil? (ni dodatnega ročnega dela)	
IV.8 - Učinkovit direktorski IS ("EIS - Executive Information System")?	
IV.9 - Integriran plačilni promet ("B2B - Business to Business", "B2C-Business to Customer")?	
IV.10 - Skrbništvo (IT in uporabniško) je opredeljeno, ažurno ter objavljeno?	

V. Učinkovita uporaba tehnologij	***Ocena****
V.1 - Dovolj osebnih računalnikov ("PC = Personal Computer")?/Zadovoljiva stopnja avtomatizacije pisarne ("Office Automation")?	
V.2 - Nivo komunikacije - lokalna omrežja ("LAN = Local Area Network") in prostrana omrežja ("WAN = Wide Area Network")?	
V.3 - Relacijske baze podatkov	
V.4 - Podpora in raznolikost različnih distribucijskih kanalov?	

** Ocena - > Prednosti so od 10 (maksimalna) do 1 (minimalna), Slabosti so od -1 (minimalna) do -10 (maksimalna). 0 je nevtralna oziroma oseba, ki odgovarja na vprašalnik, nima dovolj izkušenj in znanja, da bi ocenjevala (ta ocena se ob analiz ne upošteva).*

1 od 2

VI. Uporaba naprednih in modernih tehnologij	*Ocena**
VI.1 - Ekspertni sistemi	
VI.2 - Uporaba pametnih kartic	
VI.3 - Elektronsko podpisovanje	
VI.4 - Modern pristop k arhitekturi in programiranju ("EA = Enterprise Arhitecture", "Clouds", "SOA = Service Oriented Architecture")?	
VI.5 - Integracija modernih naprav - na primer dlančniki ("PDA = Personal Digital Assistant")?	

VII. Sodelovanje (partnerstvo) med uporabniki in IT	*Ocena**
VII.1 - Dnevno sodelovanje?	
VII.2 - Pomoč pri načrtovanju procedur in procesov (projekti, zahteve)?	
VII.3 - Pripravljenost za prenos znanja (izobraževanja, šolanja, uvajanja, delavnice, "hej Joe princip")?	
VII.4 - Pripravljenost za pomoč pri implementaciji rešitev?	
VII.5 - Prenos/distribucija informacij na poslovne enote?	
VII.6 - Pomoč pri doseganju zastavljenih ciljev enote?	
VII.7 - Razpoložljivost (IT sodelavci so razpoložljivi, ko jih potrebujejo - zahtevajo uporabniki / in obratno)	
VII.8 - Kvaliteta, učinkovitost, uporabnost in frekvenca formalnih srečanj	
VII.9 - Sodelovanje pri posebnih srečanjih (na primer: načrtovanje ali strateški razvoj)	
VII.10 - IT je aplikacijsko orientiran / IT je v ravnotežju / IT je sistemsko orientiran (*možni odgovori: 10,5,0,-5,-10)*	

VIII. Varovanje informacij (Zaupnost, celovitost, razpoložljivost informacij)	*Ocena**
VIII.1 - Logična zaščita dostopa do podatkov – sistem pooblastil (delitev pooblastil je opredeljena in delujoča)	
VIII.2 - Prisotnost politike varovanja informacij	
VIII.3 - Zaščita osebnih podatkov	
VIII.4 - Fizična zaščita dostopov do sistemov in prostorov	
VIII.5 - Obstaja proces javljanja in upravljanja z incidenti? Oziroma obvladujoč življenjski cikl incidentov.	
VIII.6 - Zaščita pred zunanjim svetom ("FW = Fire Wall")	
VIII.7 - Zaščita pred zlonamerno in prenosno kodo	
VIII.8 - Sekundarna lokacija ("DRL = Disaster Recover Location") obstaja ? (*možen odgovor DA ali NE*)	
VIII.9 - Upravljanje neprekinjenega poslovanja za področje se izvaja ("BCM = Business Continuity Management")	

** Ocena - > Prednosti so od 10 (maksimalna) do 1 (minimalna), Slabosti so od -1 (minimalna) do -10 (maksimalna). 0 je nevtralna oziroma oseba, ki odgovarja na vprašalnik, nima dovolj izkušenj in znanja, da bi ocenjevala (ta ocena se ob analiz ne upošteva).*

9.9 Analiza - UISDDFW Prednosti in slabosti IS

Celotna preglednica za analizo je v elektronski obliki in se nahaja na priloženem mediju.

9.10 Poročilo –Odločitveni parametri

UISDDFW - Poročilo o odločitvenih parametrih

strogo zaupno

Naslov pregledovane organizacije:

Predlagatelji:

-
-
-
-
-

Uteži (vsota vseh uteži je 100):

- Trenutna vrednost IS,
- Investicije v IS v naslednjih petih letih,
- Stroški IS v naslednjih petih letih,
- Zahtevano število svetovalnih dni investitorja,
- Maksimalno odstopanje na področju Prednosti in slabosti IS,
- Stopnja tveganja IS,
- Odstopanje produktov in storitev.

Maksimalne vrednosti:

- Trenutna vrednost IS (se izpiše pred definirana vrednost IS od nekaj 10.000 DE[5] do nekaj mio. DE),
- Investicije v IS v naslednjih petih letih (se izpiše pred definirana vrednost investicij v IS od nekaj 100.000 DE do nekaj mio DE),
- Stroški IS v naslednjih petih letih (se izpiše pred definirana vrednost stroškov IS od nekaj 100.000 DE do nekaj mio DE),
- Zahtevano število svetovalnih dni investitorja (se izpiše pred definirana vrednost človek dni (FTE) svetovalcev za naslednje štiri leta),
- Maksimalno odstopanje na področju Prednosti in slabosti IS (se izpiše pred definirana vrednost odstopanja Prednosti in slabosti IS od 1 do 5),
- Stopnja tveganja IS (se izpiše pred definirana vrednost stopnje tveganja od 0 in 10),
- Odstopanje produktov in storitev (se izpiše pred definirana vrednost % odstopanja produktov in storitev od 0 % do 100 %).

Kraj in datum:

[5] DE – denarnih enot (v Evropi najpogosteje € (EUR))

9.11 Poročilo – Prvi vtisi

UISDDFW - Poročilo o prvih vtisih o IS
(ob zaključku pregleda na lokaciji)

zaupno

Naslov pregledovane organizacije:

Poročevalec:

Stanje IS:

Osnovna sredstva:
- Strojna oprema:
- Sistemska programska oprema:
- Aplikativna programska oprema:

Organizacija IS:

Dokumentacija IS.

Podprti procesi v IS:

Kadri v IT:

Odnosi:

Varovanje informacij:

Tveganja IS:

Analiza prednosti, slabosti, priložnosti in nevarnosti IS (»SWOT« analiza):

Povzetek:

9.12 Poročilo – Status IS

UISDDFW - Poročilo o statusu IS
(ob zaključku pregleda na lokaciji)

zaupno

Naslov pregledovane organizacije:

Cilji obiska:

1. Splošno
2. Revizija IT
3. Organizacija IT in načrtovanje
4. Sredstva IT
    a. Strojna oprema
        i. Centralni sistem
        ii. Strežniki
        iii. Testno okolje
        iv. Delovne postaje
        v. Ostalo
        vi. Komunikacijska oprema
    b. Programska oprema
        i. Sistemska programska oprema
        ii. Anti virusna zaščita
        iii. Aplikativna programska oprema
    c. Kadri v IT
    d. Prostori IT
        i. Sistemski prostor
        ii. Sekundarna lokacija (»DRL«)
        iii. Oddaljena hramba medijev
        iv. Ostali prostori
5. Varovanje informacij
    a. Stališče vodstva pregledovane organizacije
    b. Pooblaščenec za varovanje informacij
    c. Politike
    d. Avtorizacija in avtentičnost
    e. Klasifikacija podatkov

   f. Dostop do sistemov
      i. Fizična zaščita
      ii. Logična zaščita
      iii. Oddaljeni dostop
      iv. Identifikacija
      v. Spremembe produkcijskih podatkov
   g. Požarna pregrada
   h. Dnevniški zapisi

   i. Pomožni programi
   j. Upravljanje z mediji
   k. Uničevanje medijev
   l. Revizijska sled

6. Upravljanje neprekinjenega poslovanja in upravljanje okrevanja po katastrofi
   a. Upravljanje okrevanja po katastrofi
   b. Upravljanje neprekinjenega poslovanja

7. Razvoj, nabava, vzdrževanje in implementacija aplikacij

8. Upravljanje procesov in upravljanje tveganj IS

9. Dokumentacija
   a. Strategija
   b. Načrtovanje
   c. Uporabniška navodila
   d. Postopki
   e. Standardi
   f. Obrazci
   g. Obstoječa tehnična dokumentacija

10. Namesto zaključka

11. Nekatere povezave

12. Priporočila

13. Naslednje aktivnosti

14. Zahvala

9.13 Poročilo – Kratko poročilo

UISDDFW – Kratko poročilo o IS
(ob zaključku analize)

zaupno

Naslov pregledovane organizacije:

1. Povzetek poročila,
2. Povzetek ugotovitev (s priporočili[6]),
3. Analiza tveganj,
4. Analiza prednosti, slabosti, priložnosti in nevarnosti IS (»SWOT analiza«),
5. Stališče,
6. Zaključek.

Izvajalec pregleda:

Kraj in datum:

[6] V primeru splošnega skrbnega pregleda IS

9.14 Poročilo – Odločitev

UISDDFW – Odločitev skrbnega pregleda IS
(ob zaključku odločitve)

strogo zaupno

Naslov pregledovane organizacije:

Izvajalec pregleda:

Izračunane vhodne vrednosti v model(v sklopu faze Analize):

- Trenutna vrednost IS (se izpiše izračunana trenutna vrednost IS, ki je od nekaj 10.000 DE do nekaj mio. DE),
- Investicije v IS v naslednjih petih letih (se izpiše izračunana vrednost investicij v IS od nekaj 100.000 DE do nekaj mio DE),
- Stroški IS v naslednjih petih letih (se izpiše izračunana vrednost stroškov IS od nekaj 100.000 DE do nekaj mio DE),
- Zahtevano število svetovalnih dni investitorja (se izpiše izračunana vrednost človek dni (FTE) svetovalcev za naslednje štiri leta),
- Maksimalno odstopanje na področju Prednosti in slabosti IS (se izpiše izračunana vrednost odstopanja Prednosti in slabosti IS od 1 do 5),
- Stopnja tveganja IS (se izpiše izračunana vrednost stopnje tveganja od 0 in 10),
- Odstopanje produktov in storitev (se izpiše izračunana vrednost % odstopanja produktov in storitev od 0 % do 100 %).

Izračunana numerična vrednost odločitve:

Kraj in datum:

9.15 Poročilo – Odločitev

UISDDFW – Končno poročilo skrbnega pregleda IS
(ob zaključku odločitve ali ob zaključku analize)

strogo zaupno

Naslov pregledovane organizacije:

1. Povzetek za poslovodstvo
2. Povzetek ugotovitev (s priporočili[7]),
3. Osnova za pregled,
4. Ugotovljene podrobnosti,
5. Analiza pogovorov,
6. Trenutna vrednost osnovnih sredstev informacijske tehnologije[8],
7. Analiza tveganj (zelo visoka, visoka, srednja, nizka, zelo nizka),
8. Analiza prednosti, slabosti, priložnosti in nevarnosti IS (»SWOT analiza«),
9. Investicije in finance (*pri splošnem pregledu*) ali Ocena stroškov in investicij ter vključenost strokovnjakov banke (lastnika) za predhodno obdobje 3-5 let (*pri začetnem skrbnem pregledu ali skrbnem pregledu zunanjega izvajanja*)
10. Stališče
11. Priporočila
12. Zaključek

Priloge

Izvajalec pregleda:

Kraj in datum

[7] V primeru splošnega skrbnega pregleda IS
[8] V primeru začetnega skrbnega pregleda IS