UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

EKONOMIKA NALOŽB V INFORMACIJSKO VARNOST

V Ljubljani, maj 2007

Samo Gaberšček

Izjava

Študent Samo Gaberščček izjavljam, da sem avtor tega magistrskega dela, ki sem ga izdelal pod mentorstvom prof. dr. Mira Gradišarja ter somentorstvom prof. dr. Metke Tekavčič, in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____

Podpis: _____

Kazalo

Kazalo slik

Kazalo tabel

1 UVOD

1.1 Opredelitev področja informacijske varnosti

Informacije so eden temeljnih virov sodobnega poslovanja in ključno orodje za odločanje. Dostop pravim osebam do pravih informacij ob pravem času prinaša ne le konkurenčno prednost, ampak lahko tudi omogoča osnovno preživetje organizacije.

V dobi informacijske družbe smo z razvojem informacijskih tehnologij priče vedno novim grožnjam in tveganjem, ki zahtevajo velike napore za njihovo obvladovanje. Brez celovitega pristopa in delujočega sistema upravljanja informacijske varnosti ter upravljanja tveganj so organizacije obsojene na gašenje požarov in manj učinkovite ad-hoc ukrepe, kar ima za posledico manj učinkovito rabo sredstev v organizaciji in v izjemnih primerih celo propad prizadetih organizacij.

V Sloveniji pot k sistemskemu pristopu informacijske varnosti v skladu z mednarodno sprejetimi standardi utirajo banke, ki jih k temu zavezuje II. baselski sporazum v okviru zahtev za kapitalsko ustreznost. Z vključitvijo operativnih tveganj in tveganj, povezanih z uporabo informacijskih tehnologij, v sporazum se področju namenja vedno več pozornosti, banke uvajajo funkcijo varnostnih inženirjev, tveganja postajajo obvladovana, namenjena finančna in druga sredstva pa se povečujejo in merijo. Bankam počasi sledijo ostale organizacije, s čimer informacijska varnost tudi širše pridobiva vse večji pomen, kar se kaže v povečani pozornosti organizacij in rasti naložb na tem področju.

V magistrski nalogi bom zagotavljanje informacijske varnosti obravnaval z vidika upravljanja s tveganji. Poudaril bi, da je izraz upravljanje sicer rezerviran za nadzorno funkcijo, izvajalska funkcija pa s tveganji ravna ali jih obvladuje (Mohorčič, 2007, str. 15). V nalogi sicer uporabljam izraze, ki so trenutno najbolj razširjeni v strokovni sferi, za manj znane pa navajam tudi njihove angleške izvorne izraze. Tako v nadaljevanju dela uporabljam izraz upravljanje s tveganji (ang. risk management), kljub primernejšima izrazoma ravnanje ali obvladovanje tveganj.

1.2 Opis problematike

Naložbe v informacijsko varnost dosegajo že tudi petnajst odstotkov proračunov služb za informatiko varnostno bolj ozaveščenih organizacij. Posledica te rasti je višina naložb, ki postajajo predmet ostrejšega nadzora. Predlagatelji teh naložb

morajo vse bolj upoštevati vpeljane kriterije izbora naložb v organizacijah in posledično poskušati ovrednotiti razmerja stroškov in koristi oziroma donosnosti naložb – zgolj kvalitativno naštevanje razlogov in potencialnih groženj ne zadostuje več (Briney, 2001, str. 4), kajti v poslovnem svetu je ekonomska korist tista, ki upravičuje naložbo.

Težave pri izračunih donosnosti naložb v informacijsko varnost nastajajo pri izračunih koristi teh naložb, saj običajno ni neposrednega povratnega denarnega toka. Koristi se zato poskuša bolj ali manj uspešno meriti na različne načine, ki so predmet obravnave in razvoja zadnjih nekaj let, ki hkrati praktično predstavljajo mlado obdobje novega področja, imenovanega ekonomika informacijske varnosti.

Dodatno težavo pri upravičevanju teh naložb predstavlja dejstvo, da je zagotavljanje informacijske varnosti primarno umeščeno v podporne službe informacijskih tehnologij. Tudi razvoj merjenja koristi naložb v informacijske tehnologije je še v razvoju in po svetu neodvisno nastaja veliko metod in tehnik, za katere se predvideva, da se bodo sčasoma povezovale v smislu najboljše prakse. To pa pomeni, da današnjim tipičnim predlagateljem naložb v informacijsko varnost izkušnje na njihovem primarnem področju dela ne morejo biti v pomoč pri izračunih donosnosti naložb.

Težave, ki izhajajo iz teh dejstev, so v zadnjem času razvidne iz poudarjenih vprašanj upravljavcev organizacij o smotrnosti in učinkovitosti naložb v našteta področja.

1.3 Namen in cilji dela

Osnovna namena magistrske naloge Ekonomika naložb v informacijsko varnost sta dva. V teoretičnem delu želim predstaviti okvir (informacijskih) tveganj in ekonomske vidike področja z namenom celovitega pregleda in predstavitve težav na tem mladem področju. V praktičnem delu magistrske naloge se posvečam izvedbi konkretnega načina pristopa k upravljanju informacijskih tveganj s posebnim poudarkom na izvedbi načina izračuna donosnosti naložb v informacijsko varnost.

Izhajajoči cilji teoretičnega dela naloge so sledeči:

- pregled relevantne literature in virov s področij upravljanja tveganj ter informacijske varnosti,
- umestitev področja informacijske varnosti v okvir celovitega upravljanja tveganj,

- predstavitev lastnosti ekonomike področij upravljanja tveganj ter informacijske varnosti,
- predstavitev naraščajočega pomena informacijske varnosti,
- predstavitev okvira k celovitemu upravljanju informacijske varnosti.

Izhajajoči cilji praktičnega dela naloge so sledeči:

- pripraviti metodologijo upravljanja informacijskih tveganj, ki omogoča njihovo kvantifikacijo,
- predstaviti uporabnost metodologije izračuna koristi naložbe na primeru,
- na primeru predstaviti izračune donosnosti naložb v informacijsko varnost.

1.4 Metode dela

Pri magistrskem delu bom uporabil znanja, pridobljena na podiplomskem študiju na Ekonomski fakulteti v Ljubljani, in izkušnje pridobljene z delom na področjih informatike in informacijske varnosti. Pri proučevanju področij upravljanja tveganj, informacijske varnosti ter analize donosnosti naložb se bom opiral na domačo in tujo literaturo ter internetne vire.

Pri izdelavi magistrske naloge bom uporabil sledeče metode in tehnike:

- študij obstoječe literature in virov,
- metodo analize,
- metodo sinteze,
- izvedeno metodo določanja ključnih aktivnosti in virov poslovanja,
- izvedeno metodo izračuna vpliva na poslovanje,
- izvedeno metodo kvantifikacije tveganj,
- metodo celotnih stroškov lastništva,
- metode analize donosnosti naložb (neto sedanja vrednost, notranja stopnja donosnosti, doba povračila, indeks donosnosti).

1.5 Povzetek vsebine po poglavjih

Prvi del magistrske naloge predstavljajo poglavja dva do štiri. V drugem poglavju bom predstavil področje upravljanja tveganj ter povezavo s področjem informacijske varnosti. Tretje poglavje opisuje lastnosti področja informacijske varnosti, njegov naraščajoči pomen ter okvir pristopa k celovitemu sistemskemu upravljanju informacijske varnosti. Četrto poglavje predstavlja načine pristopov pri uvajanju ali nadgrajevanju sistema upravljanja informacijske varnosti.

Drugi del magistrske naloge je usmerjen v praktičen primer možnega pristopa s poudarkom na kvantificiranih uporabljenih metrikah, tehnikah in metodah. V petem poglavju je tako ponazorjen pristop k identifikaciji informacijskih tveganj, ki

postavlja podlago za kvantitativne izračune. Šesto poglavje je namenjeno ponazoritvi uporabe izvedenih metod izračuna verjetnosti uresničitve grožnje ter ocene njene potencialne škode, ki določata višino tveganja. Izračunana višina tveganja predstavlja osnovo za njegovo ovrednotenje, kot je opisano v sedmem poglavju. V osmem poglavju je predstavljen postopek nadaljnje obravnave tveganj z namenom njihovega zmanjševanja. Deveto poglavje predstavlja izbor in uporabo nekaterih metod analize donosnosti naložb, ki so lahko podlaga za izbor učinkovitega zmanjševanja tveganj. Ta pa predstavlja odgovor na problematiko, ki je predmet obravnave magistrske naloge.

2 UPRAVLJANJE TVEGANJ

Informacijska varnost je posledica procesa varovanja podatkov in je sestavni del upravljanja informacijskih tveganj. Področje upravljanja informacijskih tveganj oziroma tveganj zaradi vključenosti informacijskih tehnologij (v nadaljevanju IT) pa umeščamo kot del upravljanja (operativnih) tveganj (ZBS, 2006, str. 59).

V literaturi najdemo veliko definicij tveganja (Vidic, 2001, str. 3), pri čemer se te od avtorja do avtorja nekoliko razlikujejo, vsem pa je skupno, da je govora o negotovi prihodnosti – to je, o različnih verjetnostih različnih izidov, ki niso vsi enako zaželeni. V splošnem torej lahko rečemo, da tveganje sestavljata dve komponenti, in sicer:

- negotovost in
- izpostavljenost (ang. exposure).

Če obstaja za dano situacijo le en možen izid, tveganje ne obstaja, ker ni negotovosti glede morebitnega razvoja dogodkov v prihodnosti. Kot metrika negotovosti se najpogosteje uporablja verjetnost, pri čemer pa je njena uporabnost omejena, saj v najboljšem primeru kvantificira zaznano oziroma dojeto negotovost. Glede metrik za kvantificiranje izpostavljenosti velja enaka ugotovitev (Holton, 2004, str. 22). Kot metrike izpostavljenosti se uporabljajo različne metrike ocene potencialnih posledic uresničitve tveganja.

V nadaljevanju dela je pojem tveganje uporabljen v smislu definicije kot jo je opredelila organizacija International Standards Organization (v nadaljevanju ISO), in sicer, da je tveganje kombinacija verjetnosti dogodka in njegovih posledic (ISO Guide 73, 2002, str. 2). Glede na definicijo tveganja in njegovo komponento posledic je razvidno, da je tveganje lahko pozitivno ali negativno, v odvisnosti od posledic uresničitve dogodka. Dogodki, katerih uresničitve imajo pozitivne posledice, imenujemo priložnosti, tiste z negativnimi posledicami pa grožnje (IRM, 2002, str. 2).

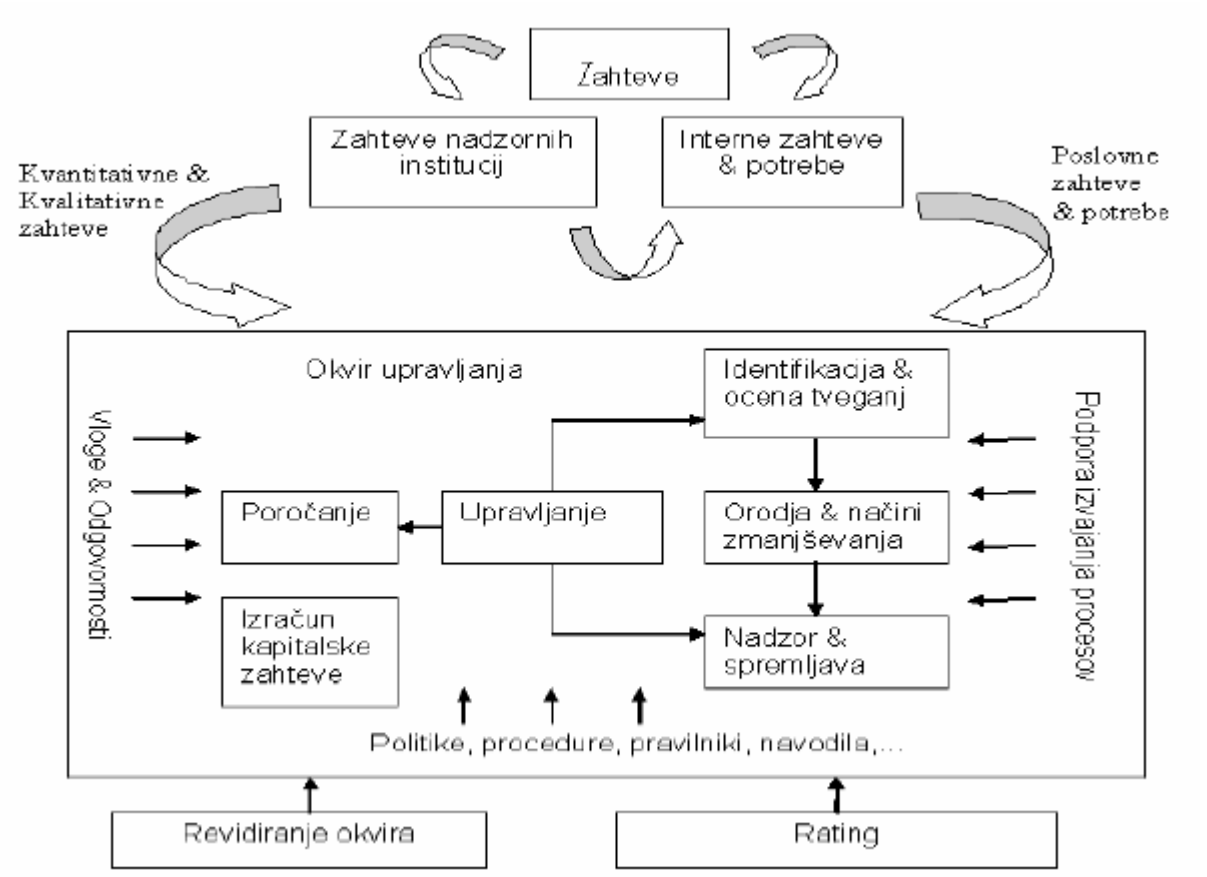
Z vidika varnosti v splošnem, torej tudi informacijske varnosti, so predmet obravnave predvsem grožnje (potencialni dogodki z negativnimi posledicami) in upravljanje tveganj, ki so povezana z njimi. Uresničitve groženj oziroma dogodki z negativnimi posledicami so pogosto imenovani tudi škodni dogodki, glede na to, da imajo za posledico nastanek škode.

Upravljanje tveganj je osrednji del strateškega upravljanja v vsaki organizaciji. Je proces, s katerim organizacija metodično raziskuje tveganja, povezana s svojim poslovanjem, tako da sistemsko prepoznava in razume potencialne pozitivne ter negativne posledice dejavnikov, ki lahko vplivajo na poslovanje organizacije. Namen upravljanja tveganj je dodajanje vrednosti vsem aktivnostim organizacije v smislu zagotavljanja njihove trajnosti, povečevanja verjetnosti uspeha in zmanjševanja tako verjetnosti neuspeha kot negotovosti glede doseganja ciljev organizacije. Povzamemo lahko, da je namen upravljanja tveganj iskanje točke minimalnega vlaganja v strategije zmanjševanja tveganj z zmanjševanjem morebitnih negativnih posledic na sprejemljiv nivo.

Nekatere industrije, ki sestavljajo kritično infrastrukturo držav in širše, upravljajo z nekaterimi svojimi tveganji v strogo regulirani obliki. Primeri so letalstvo, nuklearna energija in energetika nasploh, zdravstvo, bančništvo in drugje, kjer ima uresničitev grožnje oziroma škodni dogodek kot posledice, ki ne prizadenejo zgolj organizacijo, ampak tudi širši okvir v katerem deluje. V Sloveniji, denimo, je v zadnjem času bolj izpostavljeno področje bančništva.

Učinkovit okvir upravljanja tveganj sestavlja več komponent, predvsem pa razvoj ustreznega okolja upravljanja tveganj (vloge in odgovornosti, politike, procedure, pravilniki, podpora izvajanju procesov) ter uvedba procesa upravljanja tveganj.

Slika 1: Okvir upravljanja tveganj



Vir: Prirejeno po Kralj, 2005, str. 14.

Posamezne komponente lahko dopolnjujemo in dodatno členimo, denimo na področju bančništva glede na deset načel, ki izhajajo iz spremljevalnih dokumentov Novega baselskega kapitalskega sporazuma.

Z upravljanjem tveganj varujemo in dodajamo vrednost organizaciji in njenim deležnikom (ang. stakeholders) oziroma udeležencem v širšem smislu z zagotavljanjem podpore ciljem organizacije, tako da:

- varujemo imetje organizacije,
- varujemo in povečujemo ugled organizacije,
- zmanjšujemo nestanovitnosti v manj ključnih področjih delovanja organizacije,
- razvijamo, organiziramo in nadgrajujemo bazo znanja deležnikov in organizacije,
- prispevamo k bolj učinkoviti uporabi kapitala in drugih virov znotraj organizacije,
- izboljšujemo operativno učinkovitost,
- izboljšujemo odločanje, načrtovanje in določanje prednosti in

- postavljamo osnovo organizaciji za izvedbo bodočih aktivnosti na kontroliran način (IRM, 2002, str. 4).

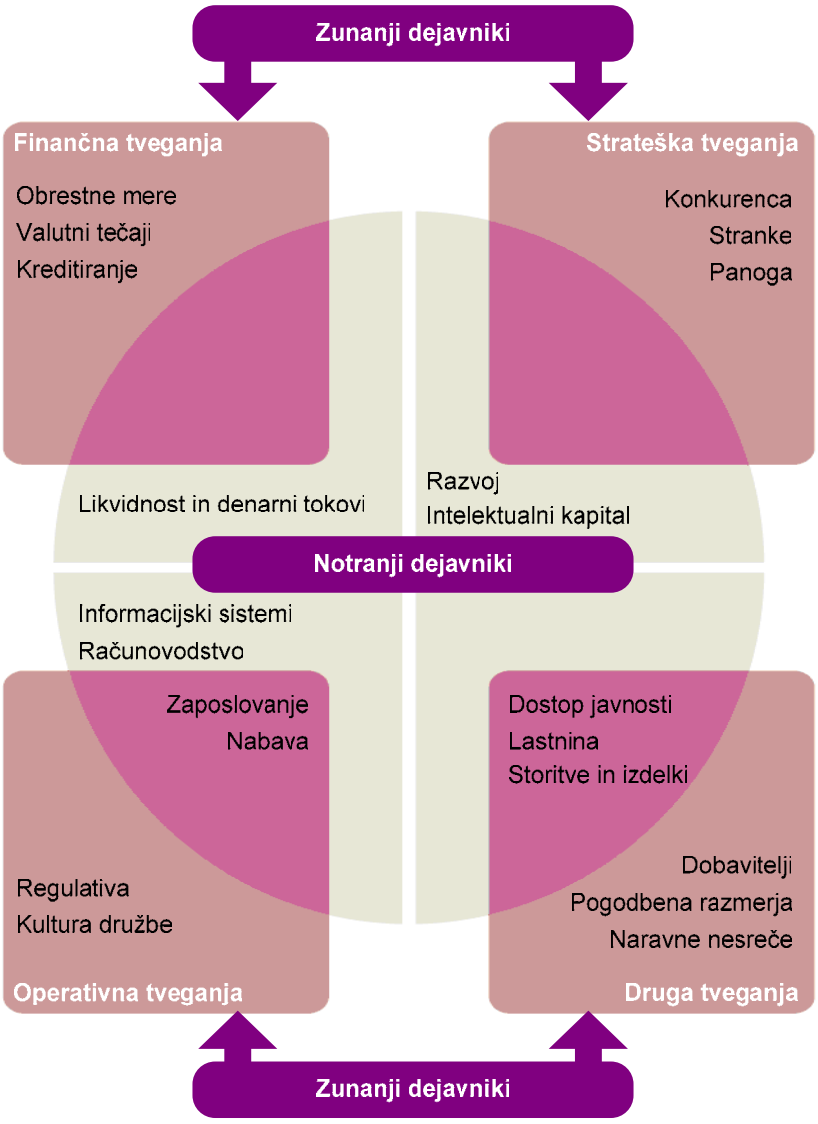
2.1 Delitve tveganj

Kot že omenjeno, obstajajo tako različne definicije samega tveganja, kot posledično tudi različne klasifikacije v skupine ali področja tveganj. Primarno tveganja delimo na čista in špekulativna. O čistem tveganju govorimo, ko obstaja zgolj možnost izgube ne pa dobička – primer je tveganje, povezano z grožnjo potresa, kajti če do njega pride, bo organizacija utrpela škodo, sicer pa ne bo ne škode ne dobička. Kadar obstaja poleg možnosti izgube tudi možnost dobička, govorimo o špekulativnem tveganju – enostaven primer je tveganje, povezano z nakupom delnice, kjer v primeru rasti zabeležimo dobiček, v primeru padca pa izgubo (Vidic, 2001, str. 5).

Podrobnejše klasifikacije običajno temeljijo na združevanju tveganj glede na vzroke uresničitev groženj, kot na primer združevanje groženj potresa in poplave v kategorijo tveganj, povezanih z uresničitvijo naravnih nesreč.

Tveganja, ki jim je izpostavljena organizacija, lahko izhajajo iz notranjih in zunanjih dejavnikov. Na sliki 2 je prikazan primer pomembnejših tveganj, ki jim je organizacija lahko izpostavljena, ter delitev glede na notranje in zunanje dejavnike. Nekatera tveganja imajo lahko izvor tako v zunanjih kot notranjih dejavnikih in so prikazana v presekih. Tveganja so lahko nadalje klasificirana v denimo strateška, finančna, operativna tveganja in podobno.

Slika 2: Dejavniki tveganj



Vir: IRM, 2002, str. 3.

Ker so tveganja značilnost posamezne organizacije ali vsaj njene panoge in (geografske, geopolitične) lokacije, je težko opredeliti splošno shemo tveganj. V bančništvu, na primer, je predvsem govor o kreditnih, tržnih, obrestnih ter operativnih tveganjih, ki so lastna njihovi obliki poslovanja ter uporabljenim prvinam.

Pomembno za vsako organizacijo je, da za lastne potrebe opredeli svojo klasifikacijo tveganj, tako da so posamezna njej lastna tveganja nedvoumno umeščena in definirana. Na ta način organizacija točno opredeli, s katerimi tveganji se ukvarja sistematično in so predmet natančne obravnave ter katera niso predmet obravnave.

2.2 Ekonomika upravljanja tveganj

Kot že omenjeno, so tveganja sestavni del poslovanja vsake organizacije. Tveganja lahko predstavljajo poslovne priložnosti, ki jih organizacija izkorišča za dosego donosnosti, druga tveganja pa so povezana z načinom izvajanja poslovnih procesov, ki jih organizacija izvaja. Vsaka organizacija je torej izpostavljena tveganjem, razlog pa tiči v tem, da so tveganja spremljajoči faktor za dosego ciljev organizacije.

Napor in sredstva, ki jih organizacije vlagajo v obvladovanje tveganj, so odvisni od marsičesa. Mlajša in manjša podjetja, denimo, so običajno zelo izpostavljena tveganjem, saj je sama narava njihovega poslovanja taka, da hitreje izkoriščajo poslovne priložnosti kot večja podjetja oziroma je to celo osnovni pogoj za njihov nastanek in razvoj. V manjših podjetjih, kjer so razpoložljiva sredstva redka dobrina, so procesi upravljanja tveganj slabše definirani, če o njih sploh lahko govorimo, in je razporejanje kapitala glede na tveganost v rokah ozkega kroga upravljavcev, ki hitro lahko podcenijo tveganja. Posledica je velika smrtnost mladih podjetij, v primerjavi z večjimi podjetji, ki smo ji priča na globalni ravni brez izjeme.

Večja podjetja si lažje privoščijo celovito upravljanje tveganj. Običajno so večja podjetja konservativnejša v svojih odločitvah glede tveganj in so posledično redkeje toliko izpostavljena, da bi lahko posamezno uresničeno tveganje ogrozilo njihov obstoj. V vsakem primeru obstaja meja ekonomske upravičenosti vlaganja v upravljanje tveganj, ki pravi, da je višina namenjenih sredstev lahko največ enaka vrednosti, ki je izpostavljena tveganju.

V nekaterih panogah, ki predstavljajo kritično infrastrukturo, pa je upravljanje tveganj predmet zahtev regulatorja in njihovega nadzora. Banke ob svojem poslovanju pretežno razpolagajo z denarjem svojih deponentov, kar pomeni, da upravljajo s tujim denarjem; na drugi strani pa ta denar dalje posojajo kreditojemalcem. Vse te aktivnosti so povezane z različnimi tveganji. Banke bi se lahko tveganjem izognile le v primeru, če bi prenehale s svojimi aktivnostmi, kar pa ne bi imelo poslovnega smisla. Obvladovanje ključnih tveganj je temeljito regulirano tudi z bančnimi predpisi. Poslovanja bank namreč ni možno v celoti prepustiti delovanju zgolj tržnih zakonitosti, saj lahko propad ene banke hitro povzroči propad drugih in s tem vpliva na zmanjšanje zaupanja v celoten bančni sistem in razpad sistema. To je tako imenovano sistemsko tveganje, ki ima lahko daljnosežne posledice za celotno narodno in širše gospodarstvo. Zato je v večini držav bančno poslovanje urejeno s posebno regulativo in nadzorom. Banke morajo tveganja sistemsko nadzirati in obvladovati (Slak, 2005, str. V).

Poslovanje bank v Sloveniji v glavnem opredeljujeta dva zakonodajna okvira: smernice Evropske unije in domača zakonodaja. Kot nova članica Evropske unije mora Slovenija pospešeno prilagajati in usklajevati svojo notranjo zakonodajo z evropsko, in sicer z uvajanjem evropskih smernic in priporočil. Dokument Baselskega odbora za reguliranje bank in nadzorne prakse s sedežem v uradu Banke za mednarodne poravnave v Baslu, Švici, z nazivom Novi baselski kapitalski sporazum, znan tudi pod nazivom Basel II, katerega vsebina bo prenesena v nove evropske bančne direktive, opredeljuje metodologijo merjenja kapitalskih zahtev glede na kategorije bančnih tveganj. Namen te kapitalske regulative je zagotoviti trdnost finančnih institucij in finančnega sistema nasploh, koncept t.i. kapitalske ustreznosti, ki določa, da mora banka vedno zagotoviti razpoložljivost določene višine kapitala glede na obseg in vrsto storitev, ki jih opravlja, ter tveganja, ki jim je izpostavljena pri opravljanju teh storitev. Pomembna novost je vključitev operativnih tveganj, ki po nekaterih podatkih predstavljajo drugo največjo kategorijo tveganj v bančnem poslovanju. Pravila, ki določajo minimalne kapitalske zahteve, so banke vzpodbudila k izboljšanju upravljanja tveganj, saj omogočajo večjo razpoložljivost prostega kapitala in boljšo poslovno učinkovitost ter posledično donosnost.

V preteklosti so se tveganja tudi v bankah obvladovala v okviru posameznih operativnih enot. Ker je osnovni motiv teh enot dobiček, so se tveganja sistematično podcenjevala oziroma se jim ni posvečalo pretirane pozornosti – razen, če so se tveganja realizirala v nepričakovano velikih izgubah. Sodobni koncepti obvladovanja tveganj uvajajo strokovnjake specialiste, ki neodvisno tveganja spremljajo, merijo, nadzorujejo in pripravljajo predloge usmeritev za vodstvo. Obvladovanje tveganj v bankah se je najprej razvilo na področju zakladništva (pri trgovanju z vrednostnimi papirji, devizami in kasneje izvedenimi instrumenti) in upravljanja z bilanco banke (ang. asset and liability management oziroma s kratico ALM). Kasneje se je razvilo upravljanje s kreditnimi tveganji. V smislu najnovejših priporočil oziroma Basel II pa naj bi banke obvladovale vsa tveganja, vključno z operativnimi, na enem mestu, pri čemer mora biti ta funkcija ali organizacijska enota neodvisna oziroma izločena iz operativnih enot. Tendenca je, da ta funkcija ali enota poroča neposredno najvišjemu vodstvu, podobno kot služba notranje revizije.

Banke trenutno izpostavljajo naslednje najpomembnejše strateške cilje pri obvladovanju tveganj (Mohorčič, 2007, str. 27):

- spremljanje poslovanja in sistema razporejanja kapitala glede na višino tveganja,

- vpeljava metod merjenja višine tveganja oziroma izpostavljenosti (denimo metoda Value at Risk – v nadaljevanju VaR),
- merjenje kreditnih in operativnih tveganj,
- razvoj in povezovanje informacijskega sistema za podporo obvladovanju tveganj v celoto,
- okrepitev nadzora (npr. notranja revizija, kontrolni sistemi, sistemi limitov in odgovornosti).

Iz navedenega je razvidno, da imajo banke velik interes za razvoj metod ugotavljanja višine izpostavljenosti tveganjem ter razporejanja kapitala in drugih sredstev glede na ugotovljeno višino tveganj. Pogoj je, da se izmerijo vsa tveganja, pri čemer je velik poudarek na področju tveganj, s katerimi so se banke pričele sistematično ukvarjati nazadnje, to je operativnimi tveganji. Povezan s tem je tudi celovit sistematičen nadzor glede uresničevanja škodnih dogodkov. Posebej je izpostavljeno, da trenutno prevladujejo kvalitativne metrike za merjenje operativnih tveganj, medtem ko se izpostavljenost drugim, kot so obrestna, kreditna in tržna tveganja, že meri z kvantitativnimi metrikami.

2.3 Operativna tveganja in informacijska varnost

Tako kot ne obstaja enotna definicija tveganja tudi ne obstaja enotna definicija operativnih tveganj. Definicija operativnih tveganj se je s časom spreminjala in dograjevala (Gornik, 2004, str. 20). Oprl se bom na definicijo, kot jo je postavil Baselski odbor za nadzor bank, ki je naslednja (Basel Comitee on Banking Supervision - The Joint Forum, 2006, str. 3):

»Operativno tveganje predstavlja tveganje izgube zaradi neustreznih ali neuspešnih notranjih postopkov, ravnanj ljudi, delovanja sistemov ali zaradi zunanjih dogodkov.«

Kot je razvidno iz definicije, je področje zelo široko zastavljeno in vsebuje številne oblike tveganj.

Glede na cilj dela bo nadaljevanje osredotočeno na naslednja operativna tveganj, ki jih lahko neposredno povežemo s cilji informacijske varnosti (Mohorčič, 2007, str. 60):

- tveganje delovanja informacijskega sistema, ki ga predstavlja tveganje nedelovanja in napak pri delovanju komponent informacijskega sistema, ki se kaže v njegovi nerazpoložljivosti,
- tveganje izgube materialnega premoženja zaradi izgube, uničenja ali poškodovanja stavb in opreme zaradi namernih ali nenamernih vzrokov

(kraje, vandalizem, naravne nesreče), ki lahko vpliva na razpoložljivost, celovitost in zaupnost komponent informacijskega sistema,
- tveganje podatkov, ki vključuje:
    - tveganje izgube podatkov, ki se izkaže v izgubi zaupnosti ali razpoložljivosti podatkov,
    - tveganje točnosti podatkov, ki se izkaže kot izguba celovitosti podatkov (nepopolnost, nepravilnost ali neažurnost).

Nekatera druga operativna tveganja, ki niso predmet obravnave v tem delu in jih navajam kot omejitev, so:
- tveganje informacijske tehnologije, ki obsega:
    - tveganje nezdružljivosti strojne in programske opreme zaradi hitrega razvoja informacijske tehnologije,
    - tveganje odvisnosti od dobaviteljev in proizvajalcev,
- tveganje projektov in novih produktov,
- tveganje postopkov dela, ki vsebuje tveganje, da navodila ne obstajajo, so nepopolna ali neustrezna, ali da se postopki (navodila in pooblastila) izvajajo nepravilno,
- tveganje v zvezi z zaposlenimi, ki vključuje tveganja usposobljenosti, tveganje izkoriščenosti, tveganje prevare in tveganje (ne)zadostne informiranosti zaposlenih,
- tveganje strategije, kar lahko predstavlja prevzemanje prevelikih tveganj ali pa tveganje neustreznosti strategije glede na tržne in druge okoliščine,
- tveganje organizacije vključuje tveganje nefunkcionalne organizacije, neučinkovite izrabe virov, neustrezne strukture informacijskih tokov, neustreznih pooblastil, tveganje konfliktov, in tako dalje, ter
- tveganje vodenja kot tveganje neizvajanja sprejete strategije, nedelovanja sprejete organiziranosti ali neustreznega vodenja.

Kot je razvidno iz navedenega, je namen dela osredotočiti se na tveganja, katerih uresničitev predstavljajo potencialni škodni dogodki, denimo poškodbe, nedostopnosti ali izgube nadzora nad informacijskimi viri ter posledičnega vpliva na poslovanje.

Eden večjih izzivov pri upravljanju operativnih tveganj v primerjavi z drugimi, ki so že upravljana, predstavlja razvoj metod za vrednotenje le-teh. Težava nastaja pri zbiranju podatkov tako o pogostosti oziroma verjetnosti uresničitve takih groženj kot pri samem ocenjevanju vpliva na poslovanje, ki bi ga uresničitev imela. Nekatere od teh groženj se tako redko uresničijo (npr. potres določene stopnje moči), da je njihovo prihodnjo verjetnost težko oceniti. Enako težko je oceniti dejanski vpliv uresničitve take grožnje drugače, kot da predpostavimo popolno

izgubo virov organizacije na nekem območju. Drugo težavo predstavlja časovna odvisnost uresničenja groženj in njihovega trajanja. Ni namreč vseeno ali lokacija poslovanja organizacije doživi prekinitev dobave električne energije ponoči ali med delovnim časom, kot tudi ne na primer v bankah ali pride do prekinitve v dopoldanskih urah, ali v popoldanskih, ko se poslovanje s strankami zaključuje in izvajajo pomembne zaključne aktivnosti.

Operativna tveganja so v zadnjem času pridobila na pozornosti in pomembnosti predvsem v bankah z vključitvijo v kapitalski sporazum Basel II.

3 INFORMACIJSKA VARNOST

Informacijska varnost je področje, ki se ukvarja z varovanjem podatkov pred nepooblaščenim dostopom, uporabo, razkritjem, uničenjem, spremembo ali nerazpoložljivostjo. Termini informacijska varnost, računalniška varnost ter varnost informacijskih sistemov (ang. information assurance) se pogosto uporabljajo izmenično. Čeprav vsa tri področja delijo mnoge skupne lastnosti oziroma imajo vsa skupen cilj v varovanju zaupnosti, celovitosti ter razpoložljivosti informacij, obstajajo med njimi razlike glede vidika, s katerega pristopajo k tem ciljem in načinov zagotavljanja le-teh. Informacijska varnost se ukvarja z varovanjem informacij ne glede na obliko: elektronsko, papirno ali v drugi obliki. Definicija informacijske varnosti po ISO 17799:2005 se glasi:

»Informacijska varnost zagotavlja ohranitev zaupnosti, celovitosti in razpoložljivosti informacij; dodatno so lahko vpletene tudi druge lastnosti, kot so istovetnost, odgovornost, preprečevanje nepriznavanja (ang. non-repudiation) in zanesljivost.«

Varnost informacijskih sistemov pristopa nekoliko drugače, tako da upošteva predvsem varovanje sistemov, ki omogočajo hrambo, procesiranje, predstavitev ali prenos informacij. Dodatno daje poudarek na vprašanja glede zasebnosti, upoštevanja zakonskih in drugih določil, neprekinjeno poslovanje ter okrevanje po katastrofi. Računalniška varnost se osredotoča na zagotavljanje varne uporabe računalnikov. Osnovni pristop je izdelava računalniških platform, jezikov in programov z vgrajenimi omejitvami, tako da agenti (denimo uporabniki ali drugi računalniški programi) lahko izvedejo le dovoljene akcije.

Danes je na voljo večje število standardov, ki se ukvarjajo s področjem varovanja informacij. Nekateri so splošnejši in namenjeni vsem organizacijam, drugi so bolj specializirani. Med vsemi referenčnimi sistemi za to področje je verjetno najbolj celovit, zagotovo pa najbolj priznan ISO 17799, ki ga je izdala Mednarodna

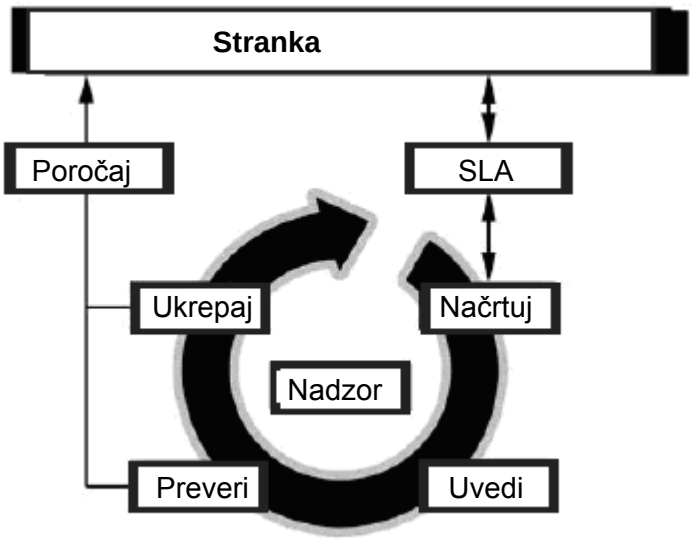
organizacija za standarde (ang. International Standards Organization – v nadaljevanju ISO). Zgodovina tega standarda se prične z delom Centra za komercialno računalniško varnost (ang. Commercial Computer Security Center) v okviru Ministrstva za trgovino in industrijo Velike Britanije (ang. UK Department of Trade and Industry). Ena od njegovih nalog je bila priprava kodeksa varovanja informacij, ki je izšel leta 1989. V nadaljevanju je kodeks izšel kot British Standard BS 7799:1995. V februarju 1998 je bil dodan drugi del pod imenom British Standard BS 7799-2:1998, ki opredeljuje zahteve za sistem varovanja informacij. V nadaljevanju je ISO po hitrem postopku sprejel omenjena standarda in jih izdal pod imenom ISO 17799-1:2000 ter ISO 17799-2:2002. V okviru zadnje izdaje je prišlo do razširitev teh standardov v tako imenovano družino standardov ISO 27000, katerih prvi je leta 2005 izšel pod imenom ISO 27001:2005 – Specification for an Information Security Management System. Ta standard bo v nadaljevanju dela uporabljen kot osnova za prikaz načina uvedbe sistema upravljanja informacijske varnosti.

IT Infrastructure Library (v nadaljevanju ITIL) je drugi primer dobre prakse, ki se je uveljavil in izšel v obliki standarda ISO 20000. ITIL opisuje okvir najboljših praks upravljanja storitev informacijskih tehnologij (ang. IT Service Management - v nadaljevanju ITSM). ITIL sestavlja večje število sklopov in en od njih je upravljanje IT varnosti, ki naj omogoča in zagotovi, da:

- so uvedeni in izvajani procesi varovanja,
- so varnostni incidenti ustrezno obravnavani,
- rezultati revizij in pregledov prikazujejo (ne-)primernost kontrol in aktivnosti
- so izdelana poročila poslovodstvu, ki prikazujejo stanje informacijske varnosti.

Na sliki 3 je prikazan ITIL proces upravljanja IT varnosti. Proces predstavlja pot od zajema poslovnih zahtev, preko načrtovanja, uvedbe, ocene ustreznosti in vzdrževanja, s stalnim nadzorom izvedbe teh aktivnosti do zaključka s poročanjem.

Slika 3: ITIL proces upravljanja IT varnosti



Vir: itSMF, 2004, str. 32.

Aktivnosti procesa upravljanja IT varnosti po ITIL-u so tesno povezane z drugimi procesi upravljanja storitev, še posebej izrazito s procesi upravljanja razpoložljivosti ter procesi upravljanja neprekinjenosti IT storitev.

Še en primer je nabor najboljših praks za upravljanje informacij oziroma IT, ki ga je mednarodno združenje Information Systems Audit and Control Association (v nadaljevanju ISACA) skupaj z inštitutom IT Governance Institute izdalo pod imenom Control Objectives for Information and Related Technology (v nadaljevanju CobiT). Glavna tema CobiT je poslovna naravnanost. CobiT predstavlja nabor kontrol, meril, indikatorjev in procesov, ki so lahko upravljavcem, revizorjem, IT strokovnjakom in uporabnikom v pomoč pri optimizaciji koristi, pridobljenih z uporabo IT, ter razvoja primernih kontrol in primernega upravljanja IT (ang. IT governance). V četrti izdaji COBIT iz decembra 2005 sestavlja 34 kontrolnih ciljev, ki vsebujejo 215 kontrol, kategoriziranih v štiri domene: Načrtovanje in organizacija, Nabava in uvedba, Dobava in podpora, Nadzor in ocenjevanje (ITGI, 2005, str. 25).

Navedene najboljše prakse na področju upravljanja IT morajo biti usklajene tako s poslovnimi zahtevami kot med samimi sabo. Težave nastajajo zlasti, kjer se pristopi prekrivajo. Z namenom čim lažje in čim bolj učinkovite uvedbe se pojavljajo matrike povezav (ang. mappings) med njimi. Te matrike omogočajo pregled nad močnejšimi stranmi posameznih pristopov ter povezave med njimi (ITGI et al, 2005, str. 21).

Tabela 1: Prednosti in slabosti ISO 17799, ITIL in CobiT

	ISO 17799	**ITIL**	**CobiT**
Prednosti	- Seznam varnostnih kontrol	- Opredeljuje procese dobavnih in podpornih procesov - Opredeljuje kako strukturirati procese na operativnem nivoju	- Usmerjen v kontrole in metrike
Slabosti	- Ne vsebuje smernic uvedbe - Ne nakazuje povezav s procesi upravljanja IT	- Slabo opisuje procese varnosti in varnostne kontrole	- Slabo opredeljuje elemente področja varnosti

Vir: Avtor.

V nadaljevanju dela bo področje informacijske varnosti obravnavano v širšem smislu in sicer, kot sistematično varovanje informacij in informacijskih virov pred širokim naborom groženj z zmanjševanjem njihovih ranljivosti za zmanjševanje poslovnih tveganj na uspešen in učinkovit način.

3.1 Kategorije informacijske varnosti

V prejšnjem poglavju smo omenili tri kategorije varnosti, ki jih dandanašnji standardi izpostavljajo, in sicer zaupnost, celovitost in razpoložljivost. To se pogosto povzema kot podajanje pravih informacij pravim osebam ob pravem času. Kategorije so atomične v smislu, da niso deljive v nadaljnje podkategorije, ter niso prekrivajoče, kar pomeni da opredeljujejo posamezne unikatne vidike informacij, med katerimi ni presečnih množic.

Vsaka informacija je potencialno predmet varnostnega incidenta, ko pride do kršitve navedenih kategorij. To se v primeru informacij v elektronski obliki lahko zgodi ob uresničitvi grožnje informacijskemu viru, kjer je informacija hranjena, je prikazana, procesirana ali po katerem se informacija prenaša. Vsak varnostni incident lahko vpliva na eno ali več kategorij informacijske varnosti.

Varovanje zaupnosti informacije pomeni varovanje informacijskega vira pred nepooblaščenimi dostopi in razkritjem informacije osebam, ki jim niso namenjene. Informacije, ki so klasificirane pod določeno stopnjo zaupnosti, so predmet dostopa le po potrebi in s strani oseb, ki so avtorizirane za dostop, uporabo, prepis ali razkritje. Kršitev zaupnosti predstavlja vsak dogodek, ko oseba, ki nima primerne avtorizacije, izvede neavtorizirano aktivnost. Varovanje zaupnosti je pogoj za ohranjanje zasebnosti oseb, katerih osebne podatke ima organizacija v posesti.

Celovitost (ali neoporečnost) informacije predstavlja njeno pravilnost in zagotavlja, da ni prišlo do nepooblaščenih ali nekontroliranih aktivnosti, to je kreiranja, spremembe ali izbrisa v informacijskem viru. To tudi pomeni, da so podatki v enem delu podatkovnih baz v skladu z podatki v drugem delu, kar je posebej izpostavljeno v primerih nepopolnih prenosov podatkov med podatkovnimi bazami. Oporečne spremembe informacij so lahko namerne v primeru zlorab ali nenamerne v primeru nesreč.

Razpoložljivost informacij in informacijskih virov predstavlja dosegljivost, ko se pojavi potreba ali zahteva po njih in to v zahtevani oziroma pričakovani obliki, ki omogoča njeno uporabo. Nerazpoložljivost v večji meri, kot je pričakovana ali zahtevana za storitev, predstavlja kršitev. Razpoložljivost je prav tako ključna, saj nam najboljše informacije ne pomagajo, če niso dosegljive, ko jih potrebujemo.

Več kot dvajset let so te tri kategorije predstavljale jedro informacijske varnosti. V zadnjem času pa se med strokovnjaki povečuje zavedanje, da zgolj te tri kategorije niso zadostne. Različni viri dodajajo različne nove kategorije. Tudi v zadnji izdaji standarda ISO 17799 iz leta 2005 že obstaja omemba naslednjih dodatnih kategorij: istovetnost, odgovornost, preprečevanje nepriznavanja in zanesljivost.

Istovetnost se nanaša na pravilno označevanje informacij. Primer kršitve te kategorije predstavlja namerno ponarejanje podatkov izvira, kot, na primer, ko zlonamerna oseba opremi elektronsko pošto z nepravimi podatki pošiljatelja. Kršitev tega tipa, morda nenamerno, predstavlja tudi zamenjava pri izpolnjevanju polj obrazca in posledično napačnih zapisih v podatkovni bazi (npr. zapis imena v polje predvideno za priimek ter zapis priimka v polje predvideno za ime).

Odgovornost se nanaša na primerno ravnanje z informacijami.

Preprečevanje nepriznavanja pomeni, da lahko po opravljeni aktivnosti, denimo poslovni transakciji, obe strani nedvoumno dokažeta opravljeno transakcijo. Primer take kontrole je digitalno podpisovanje.

Zanesljivost predstavlja mero zaupanja v pravilno delovanje sistema. Sistem je lahko ustrezno razpoložljiv (znotraj meja zahtev glede skupnega časa izpadov), a je zaradi pogostih kratkih izpadov nezanesljiv.

Gartner po drugi strani denimo opredeljuje osem zahtev in sicer poleg že opisane osnovne trojke še nevmešavanje (ang. non-interference), overjanje, odobritev, zasebnost ter preprečevanje nepriznavanja (Gartner, 2001, str. 10).

Nevmešavanje predstavlja nezmožnost dostopa in uporabe sredstev organizacije s strani nepooblaščenih oseb. Primer je preprečevanje internetnih vdorov, ki imajo v nadaljevanju običajno posledice za ostale kategorije varnosti.

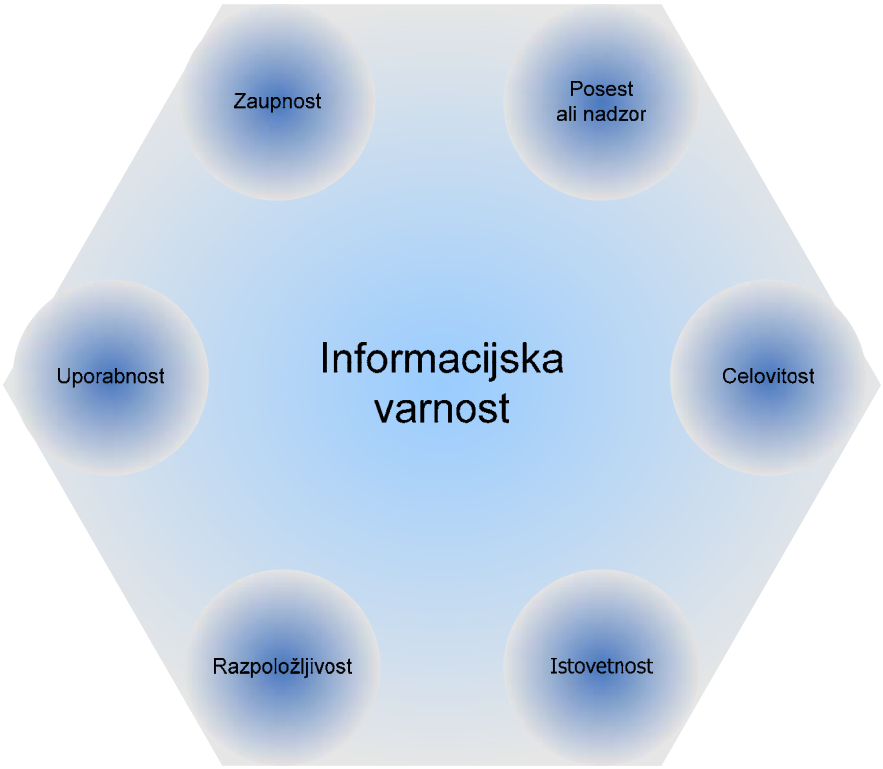
Overjanje pomeni, da so osebe in drugi agenti primerno identificirani pred dovolitvijo dostopa do informacijskih virov.

Odobritev pomeni, da se vsakokratni dostop overjene osebe primerja s seznamom dovoljenih pravic in dovoljuje le na tej podlagi.

Varovanje zasebnosti predstavlja uporabo osebnih podatkov zgolj v namen, za katerega so bili pridobljeni.

V zadnjem času pridobiva na popularnosti tako imenovana Parkerjeva šesterica (ang. Parkerian hexad), ki ima tako kot osnovna trojica kategorij lastnosti atomičnosti in neprekrivanja kategorij (Wikipedia). Poleg osnovne trojice so dodatne tri kategorije, ki sestavljajo šesterico, še posest, istovetnost in uporabnost.

Slika 4: Parkerjeva šesterica



Vir: Prirejeno po Wikipedia.

Posest ali nadzor preprosto pomeni preprečevanje izgube nadzora nad informacijo. Izguba posesti ne pomeni v prvem koraku kršitve drugih kategorij, lahko pa so te posledica. Primer je lahko izguba zaupnega seznama, ki ne predstavlja razen kršitve posesti druge kršitve v primeru, da ga nihče ne najde in zlorabi.

Uporabnost pa pomeni zagotavljanje oblike informacij, kot je potrebna za njeno uporabo. Primer, ko pozabimo geslo za dostop do varovane datoteke, predstavlja kršitev uporabnosti, saj ni kršena nobena od drugih kategorij, vendar pa nam je onemogočen dostop do informacij v varovani datoteki.

3.2 Ekonomika informacijske varnosti

Najpogosteje se soočamo s pogledom na informacijsko varnost, ki pravi, da je le-ta odvisna od tehničnih ukrepov. Problem naj bi bil rešljiv z uporabo boljših kriptografskih metod, boljšimi mehanizmi odkrivanja poskusov vdorov in delovanja zlonamerne programske opreme, boljšimi orodji za preverjanje varnosti sistemov in tako dalje. Vendar pa lahko marsikatero težavo zagotavljanja informacijske varnosti lahko enostavneje in bolj prepričljivo opišemo z jezikom ekonomike. (Anderson, 2006, str. 610).

V raziskavi o prevarah pri uporabi bankomatov je bilo ugotovljeno, da so vzorci prevar odvisni od tega, kdo od vpletenih nosi njihove posledice. V Združenih državah Amerike (v nadaljevanju ZDA) mora na strankino pritožbo banka dokazati strankino laž ali zmoto, medtem ko v Veliki Britaniji, na Norveškem in Nizozemskem leži breme dokazovanja na stranki – banka ima prav, dokler stranka ne dokaže nasprotno. Ker je tako dokazovanje praktično nemogoče, so banke v slednjih državah postale malomarne. V nadaljevanju so banke v navedenih evropskih državah utrpele več prevar kot banke v ZDA, čeprav so za varnost namenjale celo več denarja. Težava je bila v tem, da so denar uporabile manj učinkovito. To je primer težave, ki nastane, ko oseba, ki v osnovi skrbi za varnost (npr. dobavitelj storitve), ne nosi tudi posledic oziroma utrpi škode, temveč jo utrpi nekdo drug (npr. uporabnik storitve). Učinkovitost zahteva, da se odgovornost za tveganje dodeli tistemu vpletenemu, ki lahko najbolje upravlja z njim.

Naslednji dejavnik so mrežne eksternalije (ang. network externalities). Pri pojavu mrežnih eksternalij je značilno, da več oseb ko uporablja mrežo, bolj vredna le-ta postaja za vse udeležene. To se dogaja tudi pri določenih IT produktih. Kot tipičen primer se pogosto navaja telefonsko omrežje, kjer vrednost omrežja (npr. kot število možnih različnih povezav) narašča s številom priključenih telefonskih priključkov in oseb, ki jih uporabljajo. Nič drugače ni na področju programske opreme, namenjene širši javnosti in (številčnosti) skupnosti njenih uporabnikov. Glede trgov IT produktov obstajajo tri posebno pomembne lastnosti:

- vrednost produkta za uporabnika je odvisna od števila drugih uporabnikov,
- tehnologija ima pogosto visoke fiksne stroške z izdelavo prvega produkta in nižje variabilne z izdelavo vseh naslednjih,
- uporabniki imajo visoke stroške ob morebitni menjavi, kar vodi v trajnejšo navezavo uporabnikov na produkt.

Te lastnosti vodijo k strukturi trga tipa »zmagovalec vzame vse«, kar pomeni, da je za proizvajalce izjemnega pomena, da so hitro na trgu. To pa predstavlja težavo in omejitev pri poteku razvoja produkta z vidika varnosti oziroma manjši poudarek na preverjanju in testiranju produkta, kot bi bilo z vidika uporabnika zaželeno. Tipičen primer ne najbolj varnega IT produkta je operacijski sistem Microsoft Windows in nenazadnje se včasih tudi uporablja naziv »Microsoftova filozofija« za njihov domnevni pristop »Odpošlji v torek in popravi do verzije 3«. Vendar pa je ta pristop popolnoma razumski na mnogih trgih, kjer prihaja do učinkov ekonomije mrež. Zato proizvajalec v prvih fazah zanemarja varnostne vidike, po osvojitvi vloge prvega pa dodaja varnostne mehanizme, ki so pretirani ali pa ne služijo primarnemu namenu varnosti, temveč služijo trdnejši navezavi uporabnikov na produkt s povečevanjem stroškov menjave.

Težavo glede uporabe varnejših IT produktov predstavlja tudi težavno razločevanje slabih produktov od dobrih oziroma zakaj se tudi na konkurenčnih trgih dogaja, da slabši produkti prevladajo. Odgovor ponuja teorija asimetričnih informacij. V principu bo višja kakovost produktov vedno zahtevala višje proizvodne stroške in višja ceno kot pri slabših oziroma manj kakovostnih produktih. Ko kupci nimajo enakih informacij glede kakovosti produktov, kot jih imajo prodajalci, bo posledica pritisk navzdol na cene in kakovost. To bo imelo za posledico zgolj prodajo slabših produktov in obstoj njihovih proizvajalcev ter propad tistih, ki jih kupci ne nagradijo s plačevanjem višje cene za kvaliteto, ki je ne morejo ugotoviti. Ena od možnosti razločevanja je certificiranje produktov, storitev ali spletnih strani. Vendar pa se zaenkrat ta možnost ni izkazala za posebej zanesljivo, še posebej v primerih, ko je certificiranje zaupano komercialnim konkurenčnim ustanovam, namesto da ga izvaja sam nosilec tveganja uporabe.

Vse naštete težave vplivajo na razvoj boljših produktov z vidika varnosti. Razvoj produktov tako ne upošteva ciljev, ki bi jih narekoval idealističen pristop k upravljanju tveganj, ampak je za proizvajalce v danih okoliščinah pač bolj smiseln prenos tveganj na uporabnika. Nadaljevanje dela torej obravnava upravljanje tveganj z vidika uporabnika IT.

Poslovni uporabniki oziroma lastniki in upravljavci organizacij so vedno imeli težave tako pri IT naložbah v širšem smislu kot pri naložbah v informacijsko varnost. Gonilna sila teh naložb je bil hiter razvoj področja, nedoločena konkurenčna prednost oziroma nek način zavarovanja položaja organizacije. Zelo malo pozornosti pa je bilo posvečene pravi prioriteti - finančni odgovornosti za zagotavljanje učinkovite uporabe sredstev organizacije oziroma upravičenosti IT naložb. V času, ko se proračuni krčijo in je vsaka naložba pomembna, se vse več pozornosti usmerja prav sem. Vse poslovne funkcije organizacije tekmujejo z IT za svoj delež pri proračunu organizacije in upravljavci želijo nalagati v tja, kjer lahko pričakujejo največje učinke (Devaraj, Kohli, 2002, str. 5).

Pojavlja se vse večje število metod za kvantitativno merjenje učinkov IT naložb, ki naj bi omogočale poslovnim uporabnikom ustrezno primerjavo med naložbami v IT in ostalimi naložbami, ki so že do sedaj bile predmet kvantitativne ocene učinkov.

Večja razlika med IT naložbami v splošnem ter tistimi usmerjenimi v zagotavljanje informacijske varnosti je težavnost merjenja koristi zagotavljanja informacijske varnosti. V metodah uporabljene metrike za merjenje učinka IT naložb so usmerjene predvsem v tri kategorije: dobičkonosnost, produktivnost in kvaliteto storitve oziroma zadovoljstvo strank. Težava pri uporabi teh metod tudi na

področju informacijske varnosti je merjenje koristi – kolikšna je korist, če se grožnje nikoli ne uresničijo?

Kategorija naložb v varnost je bila običajno obravnavana kot obvezni izdatek za zagotavljanje usklajenosti z regulatornimi ali zakonskimi zahtevami, s sprejetimi obveznostmi do zaposlenih ali sklenjenih zavarovalnih dogovorov. Naložbe so bile povezane s kategorijo naložb za vzdrževanje poslovanja. Odločitev o naložbi je temeljila na odločitvi, ali bo podjetje še izvajalo operacije, ki zahtevajo naložbo, in niso bile predmet detajlnega procesa ocenjevanja naložb (Brigham, 2004, str. 374). To je bil tako imenovan strošek poslovanja (ang. cost of doing business).

V spremenjenih razmerah pa se enako kot pri IT naložbah pojavlja potreba po metodah kvantitativne analize učinkovitosti naložb v zagotavljanje varnosti (Berinato, 2002, str. 2). V primeru naložb v informacijsko varnost so to lahko metode, ki se glede izračuna koristi varovanja naslanjajo na izračun pričakovanih letnih izgub (ang. annualized loss expectancy).

V letih 2000 in 2001 so na univerziteti v Idahu pričeli s poskusi na področju informacijske varnosti, katerih cilj je bil dokazati, da je preventiva tudi na tem področju boljša od odpravljanja posledic. Glavna težava je bilo seveda merjenje koristi varovanja. Beležili so vse stroške, povezane z uvajanjem kontrol, pogostostjo uresničevanja groženj, ceno posledic uresničevanja, in prišli do enačbe izračuna pričakovane letne izgube kot zmnožka pričakovane enkratne izgube ob uresničitvi grožnje ter frekvenco njene uresničitve. Izračun koristi je postal tako preprost kot izračun razlike med pričakovano letno izgubo pred in po uvedbi kontrol. Pričujoče magistrsko delo temelji na tej osnovi ter praktičnem prikazu njene uporabe.

3.3 Pomen informacijske varnosti

Vse večja uporaba podatkov, informacij in informacijsko-komunikacijskih sistemov IT v poslovanju organizacij narekuje, da pri svojem poslovanju organizacije upoštevajo tudi specifična in vse večja tveganja, povezana s podatki, informacijami ter njihovo obdelavo in izmenjavo. V zadnjih dveh desetletjih smo bili priča ogromnim vložkom v IT, a so se le-ti v zadnjem času zniževali. To pa ne velja za vložke, povezane s področjem informacijske varnosti, ki pravzaprav v zadnjih letih šele pridobiva na pomenu in prepoznavnosti z razkrivanjem informacij o uresničevanju groženj.

3.3.1 Odvisnost organizacij od IT

Razmere v organizacijah so se v zadnjih desetletjih precej spremenile. Z razvojem informacijskih in telekomunikacijskih tehnologij s konca 20. stoletja se je pričel prehod v razmere informacijske družbe. Poleg tradicionalnih dobrin, kot so kapital in material, so sedaj postali strateški viri tudi znanje, intelektualni kapital in informacijski viri (Patru et al, 2003, str. 16).

Vloga in pomen informacijskih tehnologij v sodobni družbi tako nenehno narašča. Danes se lahko v veliki večini organizacij brez uporabe IT izvaja le malo kritičnih aktivnosti. Vprašanje ni več uporaba tehnologij, temveč usklajevanje poslovnih potreb in ustrezne IT podpore, saj še vedno ostajajo ocene o velikem deležu delno ali v celoti neuspelih IT projektov.

IT se uporablja kot orodje za prenovo procesov z namenom večje ekonomičnosti, racionalizacije in za doseganje konkurenčnih prednosti in v sodobnih organizacijah podpira praktično vse poslovne procese in funkcije. Informacijske tehnologije so postale kritični element poslovanja. Kot orodje, ki podpira večino poslovnih procesov, mora delovati zanesljivo in biti sposobno prilagajati se spremembam v okolju.

3.3.2 Porast groženj in škode varnostnih incidentov

Pri tem uporabnikom IT ne morejo biti v tolažbo podatki o zgodovini varnosti njihove uporabe. Vsak nov val tehnologij ima za posledico zastarelost obstoječih varnostnih ukrepov in se pojavi izpostavljenost novim grožnjam. Na primer:

- osebni računalnik je zahteval popolnoma drugačen pristop k varnosti kot princip osrednjega računalnika,
- omrežno povezovanje je izbrisalo dosežke pri varovanju posameznih osebnih računalnikov,
- brezžična omrežja so olajšala nepooblaščen dostop v omrežja, saj ni bil več potreben fizični priključek na komunikacijski vod, ..

Vsak nov val tehnologij povzroča težave pri opredelitvi in ocenjevanju tveganj ob uporabi teh tehnologij. Ocenjevanje tveganj v veliki meri temelji na podajanju ocen izkušenih strokovnjakov z določenega področja, ki jih pa takrat še ni.

Spremembe okolij, ki smo jih doživeli ob prihodih osebnega računalnika, omrežij, tehnologije odjemalec/strežnik, brezžičnih povezav, mobilnih naprav in tako naprej, nakazujejo zakaj bo varnost uporabe novih tehnologij vedno znova ostajala ena glavnih skrbi njihovih uporabnikov (Gartner Research, 2004, str. 3).

Po eni od raziskav (PriceWaterhouseCoopers, 2006a, str. 3), ki je raziskovala stanje informacijske varnosti v Veliki Britaniji, je v zadnjem letu 62 odstotkov anketiranih podjetij utrpelo varnostne incidente. 52 odstotkov jih je bilo tarča namernega napada. Velike organizacije so verjetnejše žrtve in utrpijo večje število varnostnih incidentov. Utrpela škoda se je glede na prejšnjo raziskavo iz leta 2004 v povprečju povišala za polovico.

Tabela 2: Škoda največjega varnostnega incidenta v letu 2005

Izvor škode	**Povprečno**	**Velika podjetja**
Škoda zaradi motnje v poslovanju	9.000 do 18.000 Eur v trajanju 1 do 2 dneva	75.000 do 150.000 Eur v trajanju 1 do 2 dneva
Stroški časa odpravljanja posledic	900 do 1.800 Eur v trajanju 2 do 4 človek-dneva	2.700 do 5.000 Eur v trajanju 5 do 10 človek-dni
Neposredni stroški povezani z odpravljanjem posledic	1.500 do 3.000 Eur	7.500 do 15.000 Eur
Neposredna finančna izguba (izguba sredstev, kazni,..)	750 do 1.500 Eur	5.000 do 7.500 Eur
Izguba ugleda	150 do 600 Eur	7.500 do 15.000 Eur
Skupna cena največjega varnostnega incidenta	12.000 do 25.000 Eur	100.000 do 200.000 Eur

Vir: PriceWaterhouseCoopers, 2006a, str. 3.

Medtem ko se je denimo stanje glede protivirusne zaščite izboljšalo, četrtina anketiranih organizacij nima uvedenih kontrol glede vohunskih programov – tukaj lahko iščemo tudi razlog, da je kar sedmina utrpelih največjih zlonamernih napadov povezanih z vohunskimi programi. Najslabše je stanje na področju preprečevanja kraje identitete, kjer jih le en odstotek poroča o uvedenih celovitih pristopih k preprečevanju. Tri petine organizacij dovoljuje oddaljen dostop do intraneta, pri čemer se vsebine komunikacij ne šifrirajo. Enak delež tudi ne preprečuje dostopa iz lastnih omrežij do neprimernih vsebin na internetu. Šestina ima uvedene kontrole pregleda izhodne elektronske pošte, skoraj tretjina pa ne šifrira vsebine komunikacij ob spletnih transakcijah. Več kot polovica organizacij

nima uvedenih kontrol glede uporabe prenosnih medijev tipa USB ključkov in MP3 predvajalnikov.

Iz tega je razvidno, da organizacije počasi sledijo pojavom novih groženj ob rastoči uporabi novih tehnologij. Tudi zato je opazen pesimizem, saj je skoraj 60 odstotkov anketiranih organizacij odgovorilo, da v prihodnosti pričakujejo porast števila varnostnih incidentov in njihovo težje zaznavanje.

3.3.3 Informacijska varnost kot prioriteta

Zaradi porasta groženj in škode varnostnih incidentov, predstavljenih v predhodnem poglavju, informacijska varnost pridobiva na pomenu. Vidna škoda je razvidna vsaj iz kategorij, navedenih v tabeli 2, medtem ko se običajno ob varnostnih incidentih pojavljajo tudi skriti stroški in težje zaznana škoda, kot na primer:

- izguba posla zaradi nerazpoložljivih informacijskih virov,
- padec produktivnosti ali popolna ustavitev dela zaposlenih v podpornih službah organizacije, ki odpravljajo posledice varnostnih incidentov,
- oportunitetni stroški finančnih sredstev, namenjenih odpravi posledic varnostnih incidentov, in tako naprej.

Zaradi teh vplivov (ne-)ustrezne informacijske varnosti, bo le-ta tudi v prihodnje ostajala med glavnimi prioritetami. Gartner vsako leto izvaja raziskave med direktorji informatike z namenom ugotavljanja prioritet glede poslovanja in uporabe tehnologij. V nadaljevanju so predstavljeni rezultati raziskave o glavnih prioritetah direktorjev informatike v letu 2004 (Gartner Research, 2004, str. 3). V tej raziskavi je sodelovalo 956 direktorjev informatike z vsega sveta in vseh panog.

Tabela 3: Glavne prioritete direktorjev informatike

	Uvrstitev		
	2004	**2003**	**2002**
Varnostni incidenti / prekinitve poslovanja	1	2	-
Stroški poslovanja / proračuni	2	1	1
Varovanje podatkov in zasebnosti	3	10	4
Potreba po rasti prihodkov	4	-	-
Uporaba informacij v produktih in storitvah	5	-	-
Ekonomska obnovitev	6	-	-
Inovacije	7	3	5
Poenoten pogled na kupca	8	5	3
Transparentnost poročanja	9	7	-
Celovito upravljanje tveganj v organizaciji	10	4	-

Vir: Gartner Research, 2004, str. 3.

Na prvem in na tretjem mestu najdemo potrditev, da v letu 2004 predstavlja informacijska varnost najvišjo prioriteto na področju informatike. Na desetem mestu po prioriteti najdemo tudi celovito upravljanje tveganj v organizaciji, ki se sicer ne nanaša samo na informacijsko varnost, a slednja vendarle predstavlja pomemben del celovitega upravljanja tveganj.

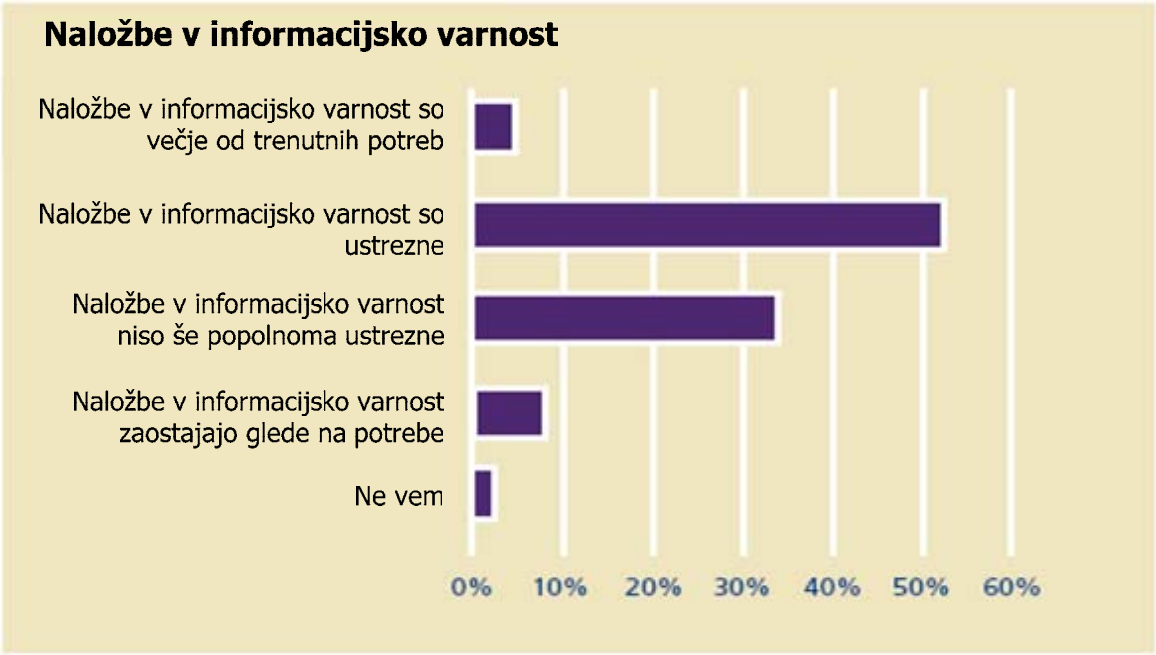
Drugo mesto med prioritetami zasedajo stroški poslovanja, iz česar lahko sklepamo o pomenu čim boljšega odločanja o naložbah tudi v informacijsko varnost. V naslednjem poglavju je predstavljen naraščajoč trend naložb v informacijsko varnost, kar še bolj izpostavlja pomen pravilnega odločanja tudi o teh naložbah in povezanih stroških.

3.3.4 Trendi naložb v informacijsko varnost

Rezultati raziskave (Deloitte, 2006, str. 24), ki je zajemala največje svetovne finančne organizacije s področij, kot so zavarovalništvo, bančništvo, upravljanje z vrednostnimi papirji in podobno, govorijo, da se višina proračuna za informacijsko varnost zelo povečuje. Kar 95 odstotkov organizacij, ki so odgovarjale na anketo, je poročalo o povečanju. Pri tem jih je več kot petina javila povečanje namenjenih

sredstev za več kot 10 odstotkov, pri čemer jih veliko meni, da so naložbe v pravi višini ali pa je celo še prostor za rast, kot je prikazano na sliki 5.

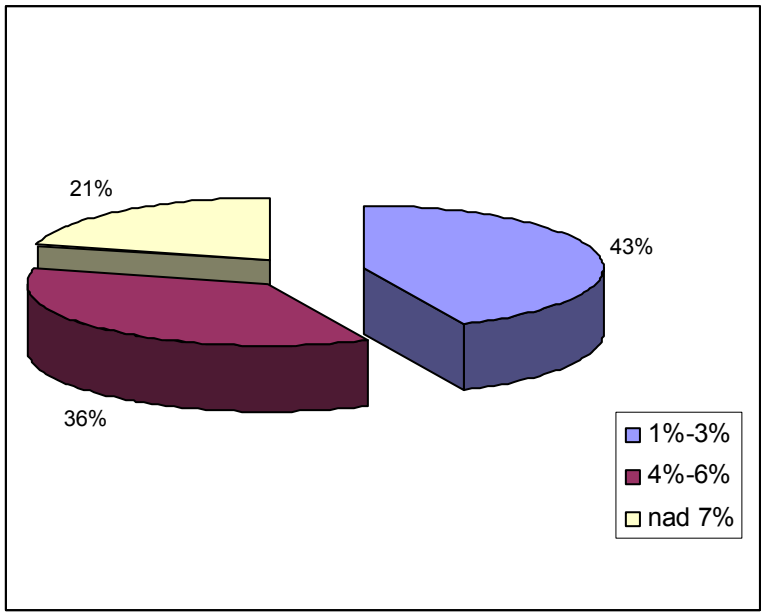
Slika 5: Naložbe v informacijsko varnost



Vir: Deloitte, 2006, str. 25.

Rezultati tudi nakazujejo, da več kot polovico finančnih organizacij informacijsko varnost vidi v okviru IT, kakor nakazuje opredelitev sredstev znotraj IT proračunov. Drugo največje področje, ki zagotavlja sredstva za informacijsko varnost, so v 23 odstotkih primerov organizacijske enote, ki izvajajo temeljne poslovne procese. Na sliki 6 so prikazani podatki o porazdelitvi organizacij glede na višino sredstev za informacijsko varnost v okviru IT proračunov.

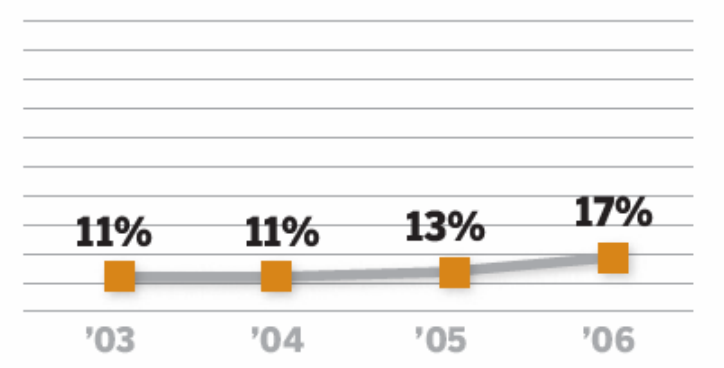
Slika 6: Porazdelitev finančnih organizacij glede na višino sredstev, namenjenih informacijski varnosti znotraj IT proračuna



Vir: Prirejeno po Deloitte, 2006, str. 25

Druga anketa, ki so jo izvedle reviji CIO, CSO ter PriceWaterhouseCoopers je zajela skoraj 8000 organizacij iz 50 držav in iz najrazličnejših področij, vključno z neprofitnimi organizacijami. Več kot polovica jih predvideva povečanje proračunov tudi za naslednje leto (PriceWaterhouseCoopers, 2006, str. 4), pri čemer jih petina predvideva dvomestno odstotno povečanje. Povečevanje višine teh sredstev je večje kot pa povečevanje IT proračuna in se torej njihov delež povečuje, kot je razvidno iz slike 7.

Slika 7: Delež sredstev, namenjenih informacijski varnosti znotraj IT proračuna



Vir: PriceWaterhouseCoopers, 2006, str. 4.

3.4 Sistem upravljanja informacijske varnosti

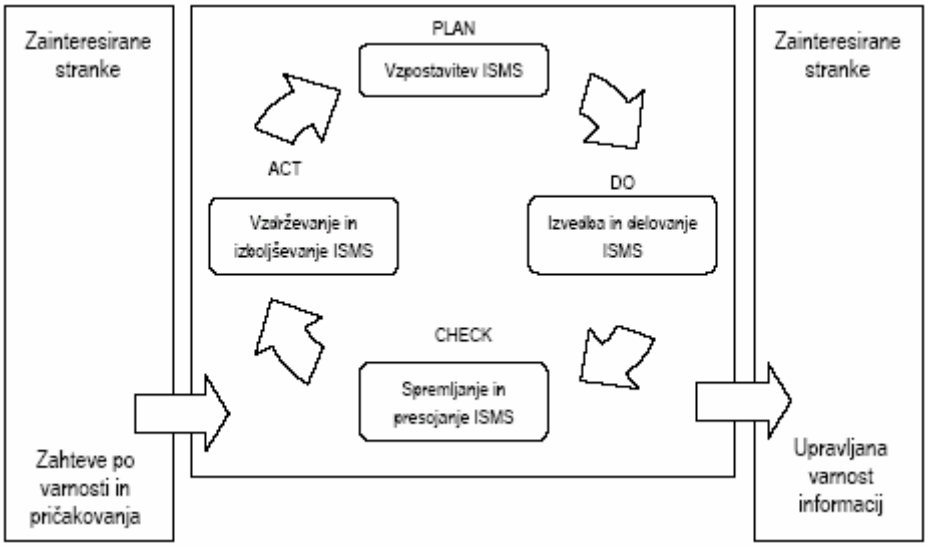
Sistem predstavlja organiziran način, kako organizacija upravlja informacijsko varnost. V svetu se je kot najbolj priznan koncept sistema uveljavil standard, ki je v svoji zadnji različici poznan kot ISO 27001:2005 – Specification for an Information Security Management System. Standard opredeljuje specifikacije sistema upravljanja informacijske varnosti (v nadaljevanju SUIV) in je kot prvi izšel iz družine standardov ISO 27000, ki posamično opredeljujejo elemente SUIV.

Trenutno znani člani družine standardov ISO 27000 so naslednji:

- ISO 27000: Vocabulary and Definitions,
- ISO 27001: Specification for an Information Security Management System,
- ISO 27002: Code of Practice for Information Security Management,
- ISO 27003: Implementation guidance,
- ISO 27004: Information Security Management Metrics and Measurement.,
- ISO 27005: Guidelines for information security risk management,
- ISO 27006: Guidelines for information and communications technology disaster recovery services.

ISO 27001 temelji na »Plan-Do-Check-Act« (v nadaljevanju PDCA) procesnem modelu izboljševanja kvalitete. PDCA procesni model definira cikel aktivnosti pri načrtovanju in vzpostavitvi ISMS, izvedbo in operativno uporabo ISMS, redni nadzor in preglede ISMS, ter izboljševanje in dopolnjevanje ISMS na osnovi sprememb in novih zahtev okolja. Koncept procesnega cikla PDCA zagotavlja implementacijo učinkovitega varovanja informacij in učinkovitost vzpostavljenega varovanja informacij skozi stalno izboljševanje. PDCA (Demingov krog) predstavlja strategijo nadzora in upravljanja kakovosti s štirimi koraki. PDCA uporabljamo ponavljajoče, v najkrajših možnih ciklih, v navidezni spirali, ki nas pripelje do končnega cilja. V vsakem ciklu smo bližje končnemu cilju. Ta pristop je zasnovan na spoznanju, da so naše znanje in sposobnosti omejene, vendar jih stalno izboljšujemo. Pogosto nimamo na voljo vseh informacij, ki bi jih potrebovali. Namesto, da bi se ujeli v smrten objem neskončnih analiz in iskanja takojšnje popolnosti, je bolje, da napredujemo s približno popolnostjo. Čez čas bomo pridobili več znanj, ki nam bodo omogočala boljše definiranje ciljev, in spretnosti, ki nam bodo pri doseganju ciljev pomagale.

Slika 8: PDCA in sistem upravljanja informacijske varnosti



Vir: prirejeno po ISO 27001:2005 .

PDCA procesni model v ISO 27001 zajema nabor procesov upravljanja tveganj. Namen teh procesov je identifikacija tveganj, njihovo vrednotenje in obvladovanje z različnimi upravljavskimi možnostmi.

Kljub ustreznemu izvajanju vseh opredeljenih načinov za zniževanje informacijskih tveganj še vedno lahko pride do udejanjanja določenih tveganj. Zato je potrebna povezava procesa upravljanja informacijskih tveganj s procesom upravljanja informacijskih incidentov. Z ustreznim ravnanjem v primeru informacijskih incidentov organizacija zagotovi, da škoda zaradi udejanjenih tveganj ostane čim nižja in da imajo taki dogodki čim manjši negativen vpliv na poslovanje organizacije.

Za primere katastrofalnih dogodkov, ki od celotne organizacije ali katerega od njenih poslovno kritičnih delov zahtevajo prehod v krizni način delovanja, je predvidena povezava upravljanja informacijskih tveganj ter incidentov na eni strani s procesom upravljanja neprekinjenega poslovanja na drugi strani. Urejen proces upravljanja neprekinjenega poslovanja zvišuje možnost, da bo organizacija preživela katastrofalen dogodek.

V skladu s PDCA principom postopek vzpostavitve in upravljanja SUIV razdelimo v štiri faze:
1. Vzpostavitev sistema
2. Implementacija in delovanje
3. Nadzor in pregled
4. Vzdrževanje in izboljševanje

Vzpostavitev sistema

V okviru faze vzpostavitve definiramo obseg sistema varovanja informacij v kontekstu poslovanja in organizacijske sheme organizacije, lokacije, virov in tehnologije. Po določitvi obsega moramo definirati varnostno politiko organizacije. Varnostna politika opredeljuje splošno usmeritev glede varovanja informacij, razne zahteve v zvezi z varovanjem informacij, strateški organizacijski kontekst in kontekst upravljanja tveganj, kriterije za vrednotenje tveganj. Varnostno politiko mora potrditi vodstvo organizacije.

Po opredelitvi varnostne politike moramo definirati sistematični pristop k obvladovanju tveganj. Pri definiciji pristopa k obvladovanju tveganj določimo metodo ocenjevanja tveganj, politiko zmanjševanja tveganj na sprejemljivo raven, kriterije za sprejem tveganj in nivoje sprejemljivega tveganja.

Določitvi sistematičnega pristopa k obvladovanju tveganj sledi analiza tveganj v okviru katere identificiramo vire, grožnje, ki so jim izpostavljeni, ranljivosti, ki bi jih grožnje lahko izkoristile, in vpliv groženj na sredstva oziroma vire. Nadalje sledi ocena tveganj, pri kateri ocenimo verjetnost dogodka, ki bi povzročil škodo ter potencialno poslovno škodo. Sledi izdelava profila tveganj ter na njegovi osnovi ovrednotenje tveganj glede sprejemljivosti.

Na osnovi pridobljenih informacij identificiramo in ovrednotimo možnosti za obvladovanje tveganj. Izberemo ustrezne kontrole, zavestno sprejmemo tveganja, se tveganjem izognemo ali pa jih prenesemo na nekoga drugega.

Ko smo za posamezna tveganja izbrali način obvladovanja in pripravili predloge izbranih kontrol, pripravimo izjavo o trenutnih implementiranih kontrolah in v njej dokumentiramo vse implementirane in izbrane kontrole in razloge zanje, kot tudi za kontrole, ki niso izbrane.

Vodstvo mora potrditi sprejem preostanka (ang. residual) tveganj in dati soglasje k implementaciji in delovanju sistema upravljanja varovanja informacij.

Implementacija in delovanje

V prvih korakih implementacije moramo poskrbeti za formulacijo načrta obvladovanja tveganj, ki vsebuje aktivnosti vodstva, odgovornosti in prioritete pri upravljanju tveganj.

Formulaciji načrta obvladovanja tveganj sledi implementacija načrta, ki ima za cilj identifikacijo ciljev kontrol z opredelitvijo virov in odgovornosti za njihovo izvedbo.

Sledi implementacija izbranih kontrol, usposabljanja in izobraževanja za dvig zavesti. Nato nastopi upravljanje sistema in virov ter implementacija postopkov in drugih kontrol za ustrezen odziv na varnostne incidente.

Nadzor in pregled

V tej fazi skrbimo za pravočasno odkrivanje napak pri procesiranju informacij, identifikacijo neuspešnih in uspešnih vdorov v sistem in določamo aktivnosti za obvladovanje incidentov. Vodstvo organizacije spremlja, ali se aktivnosti v okviru sistema varovanja informacij odvijajo po pričakovanjih.

Izvajamo tudi redne preglede učinkovitosti delovanja sistema upravljanja varovanja informacij. Pri tem se poslužujemo rezultatov presoj, incidentov, predlogov in povratnih informacij vseh zainteresiranih strank.

Preverjamo stopnjo ostanka tveganj in sprejemljivega tveganja. Pri tem upoštevamo spremembe v organizaciji, tehnologiji, poslovnih ciljih in procesih, identificiranih grožnjah in zunanjih dogodkih.

Izvajamo načrtovane interne presoje in vodstvene preglede. Beležimo aktivnosti in dogodke, ki bi lahko imeli vpliv na učinkovitost sistema upravljanja varovanja informacij.

Vzdrževanje in izboljševanje

Organizacija, ki je vzpostavila sistem upravljanja varovanja informacij bi morala redno razvijati in implementirati izboljšave sistema in zagotavljati, da izboljšave dosežejo predvidene cilje, izvajati korekcijske in preventivne ukrepe, sporočati informacije o stanju sistema vsem zainteresiranim strankam.

3.5 Procesi upravljanja (informacijskih) tveganj

PDCA procesni model SUIV iz ISO 27001 zajema nabor procesov upravljanja tveganj. Namen teh procesov je identifikacija in ocenjevanje tveganj in vplivov tveganj z namenom obvladovanja ugotovljenih tveganj z različnimi upravljavskimi možnostmi.

Eden od ciljev naloge je prikaz načina izvedbe nekaterih od teh aktivnosti. Procesi in njihove aktivnosti, ki so predmet nadaljnje obravnave v magistrski nalogi so naslednji:

V fazi »Načrtuj« (ang. plan):
- določitev obsega SUIV in pristopa k oceni tveganj,
- analiza tveganj:
    - identifikacija tveganj:
        - opredelitev ključnih aktivnosti,
        - opredelitev virov ključnih aktivnosti,
        - identifikacija groženj
    - ocena tveganj:
        - ocena verjetnosti uresničitve grožnje,
        - izdelava profila tveganj.
- obravnava tveganj:
    - ovrednotenje oziroma opredelitev sprejemljivosti tveganj.
    - identifikacija predlogov obravnave tveganj in njihova analiza.
    - izbor ukrepov obravnave tveganj.

Procesi in njihove aktivnosti, ki niso predmet nadaljnje obravnave, so torej naslednji:

V fazi »Načrtuj« (ang. plan):
- pridobitev odobritve ostanka tveganj in odobritve implementacije SUIV,
- priprava izjave o skladnosti.

V fazi »Izvedi« (ang. do)
- načrt implementacije in implementacija kontrol,
- merjenje učinkovitosti kontrol,
- programi izobraževanja in zavedanja,
- upravljanje izvajanja SUIV in potrebnih virov,
- upravljanje informacijskih incidentov.

V fazi »Preveri« (ang. check)
- nadzor in pregled vseh komponent SUIV.

V fazi »Ukrepaj« (ang. act)
- vzdrževanje in izboljševanje SUIV.

V nadaljevanju dela bo predstavljen način implementacije teh aktivnosti, ki predstavlja sistematičen in ekonomsko učinkovit način upravljanja informacijskih

tveganj v organizaciji, s poudarkom na razlagi tistih aktivnosti, ki neposredno prispevajo k učinkoviti in pregledni obravnavi naložb v informacijsko varnost.

Predstavljeni način temelji na interno razviti metodologiji v podjetju, kjer sem zaposlen, in predstavlja osnovo za izvajanje svetovalnih storitev tako v gospodarskih družbah kot v javni upravi.

4 DOLOČITEV OBSEGA IN PRISTOPA

V okviru faze vzpostavitve definiramo obseg sistema varovanja informacij v kontekstu aktivnosti poslovanja in organizacijske sheme organizacije, lokacij, virov in tehnologije.

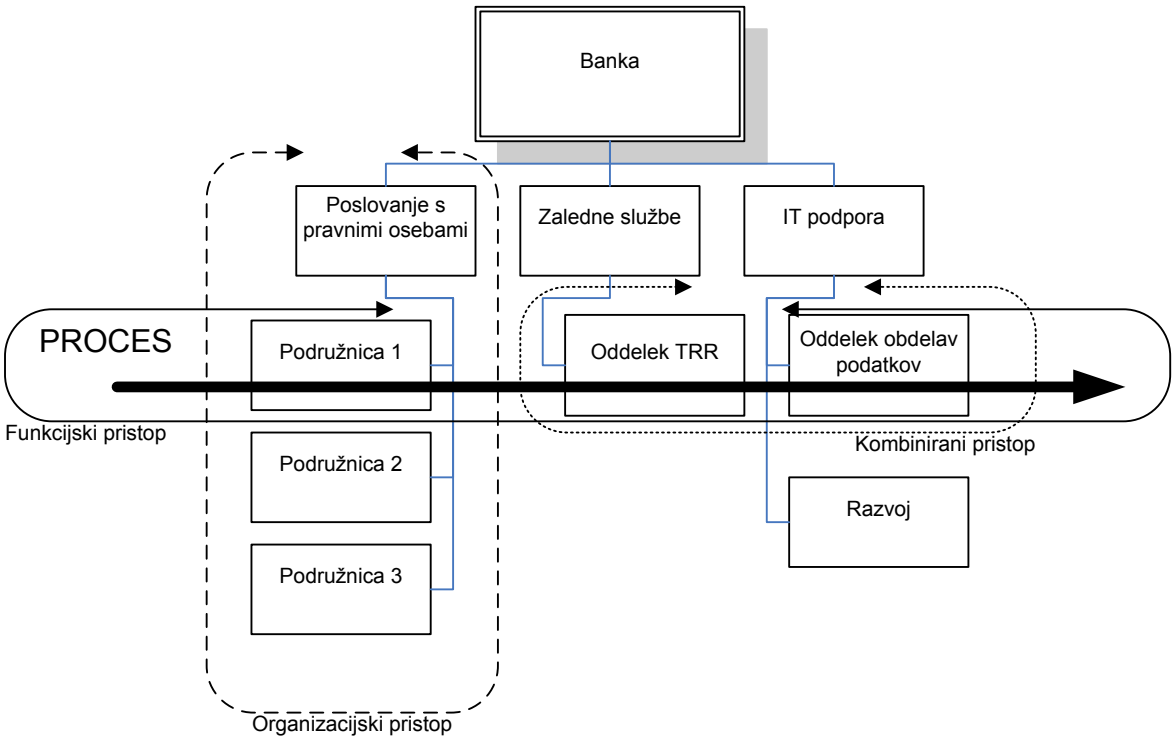
4.1 Obseg

Pomen določitve obsega SUIV je v omejitvi področja upravljanja in identificiranju povezanih tveganj. V smislu PDCA cikla in spiralnega izboljševanja je priporočljivo, da organizacija ob vpeljavi sistema omeji obseg SUIV, tako da vključuje prioritetno določena področja. Kasneje ga postopoma širi.

Tipično se lahko organizacija odloča med naslednjimi pristopi, ki izhajajo iz vidika opravljanja poslovnih aktivnosti in združevanja le-teh v skupine:

- organizacijski – organizacija omeji obseg SUIV na osnovi organizacijske sheme (npr. na sliki 9 s črtkano črto predstavljena zamejitev obsega na organizacijske enote Podružnic v okviru Poslovanja s pravnimi osebami),
- funkcijski – organizacija omeji obseg SUIV na osnovi poslovnih procesov (npr. na sliki 9 s polno črto predstavljena zamejitev obsega na proces, ki poteka skozi organizacijske enote Podružnica 1, Oddelek TRR ter Oddelek obdelav podatkov),
- kombinirani – organizacija kombinira oba pristopa glede na želeni ciljni obseg SUIV (npr. na sliki 9 s pikčasto črto predstavljena zamejitev obsega na zgolj aktivnosti procesa, ki se izvajajo v organizacijskih enotah Oddelek TRR ter Oddelek obdelav podatkov).

Slika 9: Možni pristopi k določitvi obsega SUIV



Vir: Avtor

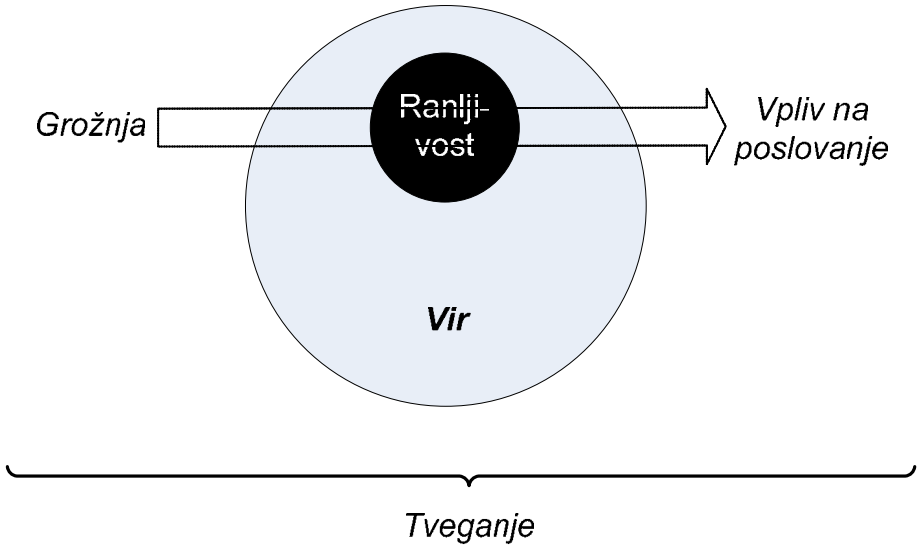
Predstavljena metodologija dopušča poljubno možnost izbire pristopa. Registra organizacijske sheme in poslovnih procesov sta predvidena kot temelj za nadaljnje delo, vendar pa je vsebina in njena omejitev poljubna glede na izbrani pristop in ciljni obseg SUIV.

4.2 Metodologija analize tveganj

Drugi del te faze predstavlja izbira ali opredelitev metodologije analize tveganj. Metodologija analize tveganj je predstavljena v poglavjih 5, 6 in 7 ter služi kot proces za izvedbo obravnave primera ekonomike naložbe v informacijsko varnost. Metodologija temelji na konceptih, ki so predstavljeni v nadaljevanju tega poglavja.

Tveganja, ki izhajajo iz uporabe IT virov, običajno ponazarjamo, kot je prikazano na sliki 10.

Slika 10: Tveganje kot grožnja viru z vplivom na poslovanje



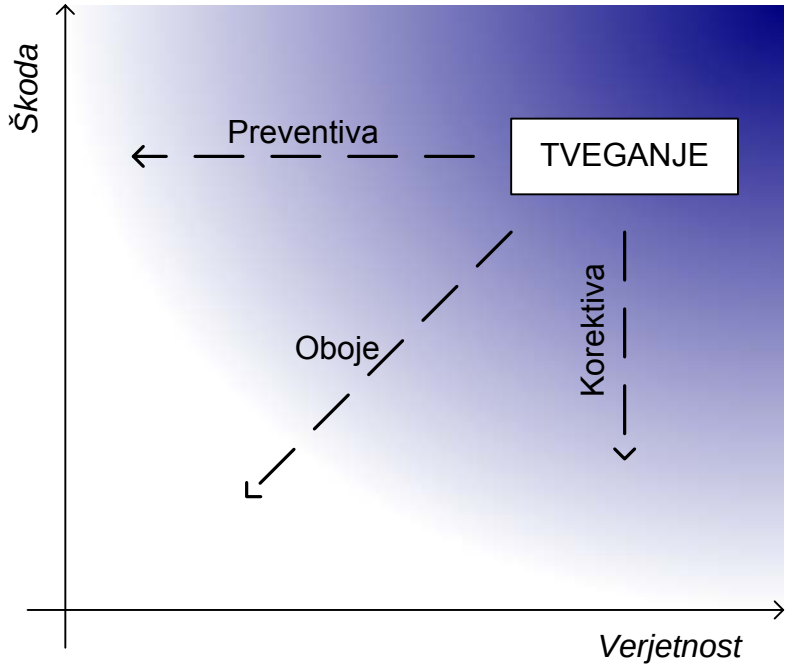
Vir: Avtor.

Grožnjo predstavlja možni vzrok uresničitve neželenega dogodka, ki lahko povzroči škodo (ISO 17799, 2005, str. 3). Stopnja grožnje lahko izvira iz geografskega položaja, političnega stanja, vabljivosti za napadalce in podobno. Ranljivost na drugi strani je lastnost oziroma slabost vira, ki jo lahko izkoristi grožnja ali več groženj. Stopnjo ranljivosti določa nivo uvedenih kontrol. Verjetnost uresničitve grožnje je določena s stopnjo grožnje in stopnje ranljivosti.

Verjetnost uresničitve grožnje rušenja stavbe zaradi potresa, na primer, določa funkcija, ki upošteva stopnjo grožnje viru (ta izvira predvsem iz lokalne tektonske dejavnosti) in stopnje ranljivosti (ta lahko izvira iz ranljivosti zaradi neuvedenih kontrol protipotresne gradnje). Grožnja tako pomeni vir potencialnega varnostnega incidenta, vendar pa ni nujno, da iz njega le-ta nastane, saj je poleg grožnje viru potrebna tudi ranljivost vira - šele tedaj lahko nastane možnost varnostnega incidenta (ZBS, 2006, str. 39 – 42) oziroma, kot jo imenujemo v nadaljevanju, verjetnost uresničitve grožnje viru.

Kontrole predstavljajo ukrepe za zmanjševanje tveganja in jih pogosto imenujemo tudi z izrazoma protiukrepi in varovanja. Kontrola je lahko administrativne, tehnične, vodstvene ali zakonske narave. Ima en ali dva vpliva na tveganje – lahko zmanjšuje verjetnost uresničitve grožnje ali zmanjšuje potencialno škodo v primeru, da pride do uresničitve grožnje, lahko pa oboje. Kontrole, ki primarno zmanjšujejo verjetnost uresničitve grožnje, tipično označujemo kot preventivne, če primarno zmanjšujejo potencialno škodo, pa kot korektivne. Mnogo kontrol pa vpliva na oba elementa tveganj in jih ne moremo strogo razvrščati v določeno vrsto.

Slika 11: Vpliv kontrol na tveganja



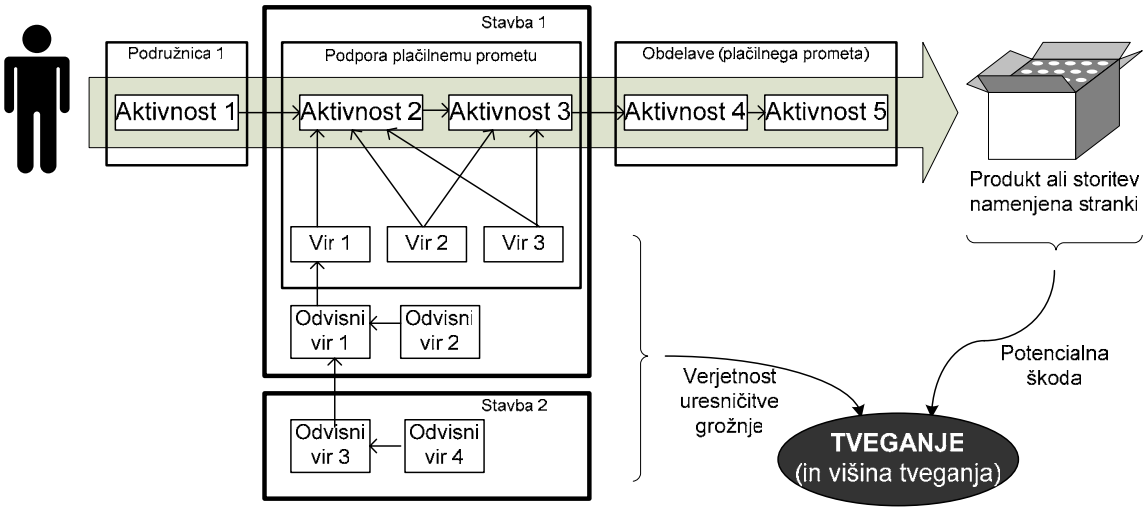
Vir: Avtor.

Uresničitev grožnje predstavlja škodni dogodek, ki ima lahko z vidika obravnavanih kategorij varnosti IT vira naslednje posledice:

- razkritje zaupnih IT virov (informacijski viri v hrambi ali prenosu),
- napaka v celovitosti (pravilnosti) informacij (informacijski viri v hrambi ali prenosu),
- izpad razpoložljivosti IT virov.

Posledice oziroma potencialno škodo poskušamo ocenjevati z oceno vpliva na poslovanje. Neposredno škodo predstavljajo direktni stroški za odpravo posledic po incidentu. Posredna škoda nastane zaradi motenj ali izpadov delovnih procesov.

Slika 12: Povezave procesa, aktivnosti in uporabe virov



Vir: Avtor.

Tveganje je kombinacija verjetnosti pojava dogodka in njegovih posledic, škode. Vsak od teh dveh elementov tveganja pa vsebuje neko mero negotovosti. IT tveganje (ang. IT related risk) je neto vpliv na poslovno poslanstvo, kjer je upoštevana verjetnost, da bo določen vir grožnje (naključno ali namerno) izkoristil določeno ranljivost informacijskega sistema in bo s tem povzročena škoda.

4.2.1 Pristopi k oceni tveganj

Glede samega pristopa k ocenjevanju tveganj poznamo dve skrajni meji kategorizacij metrik in tehnik za ocenjevanje tveganj, ki ju imenujemo kvalitativni in kvantitativni pristop. V praksi se pri uporabi raznih tehnik skoraj vedno nahajamo nekje med skrajnostma in gre iz praktičnih razlogov za kombinacijo med pristopoma.

Če so vse v metodologiji ocenjevanja tveganj uporabljene kategorije – potencialna škoda, stopnja grožnje, učinkovitost kontrol oziroma stopnja ranljivosti, negotovost in cena varovanja – kvantificirane, se proces označuje kot popolnoma kvantitativen. Kot omenjeno, je v praksi skoraj nemogoče izvajati popolnoma kvantitativno upravljanje tveganj, saj je potrebno izvajati kvantitativne meritve tudi glede kvalitativnih lastnosti, kot je recimo opis ranljivosti (primer tipičnega kvalitativnega opisa ranljivosti je lahko »slabo upravljanje z dostopnimi gesli«). Je pa mogoče izvajati popolnoma kvalitativno upravljanje tveganj, ko vse kategorije ocenjujemo opisno, ima pa ta pristop veliko slabosti, katerih največja je velika stopnja subjektivnosti pri podajanju ocen.

Prvi poskusi kvantitativnega ocenjevanja tveganj sodijo že v sedemdeseta leta prejšnjega stoletja (Tipton et al, 2004, str. 807). Vendar so se hitro pojavile težave zaradi naslednjih razlogov:

- ni bilo skupne iniciative za vzpostavitev neodvisnih in zanesljivih shem, metrik ter statistik in je vsakdo izdeloval svoje,
- proces, sicer preprost v svoji zasnovi, je bil kompleksen za izvajanje,
- potrebna je bila velika količina podatkov, ki jih je bilo potrebno povezovati in na njihovi osnovi izdelovati veliko izračunov,
- vso to delo je bilo, ob pomanjkanju oziroma neobstoju osebnih računalnikov, opravljeno ročno.

Posledično so bili rezultati zelo nezanesljivi in se je večina usmerila h kvalitativnemu pristopu, ki je preprostejši. V tabeli 4 je predstavljen enostaven primer kvalitativnega pristopa k ocenjevanju tveganj, in sicer na način, ko je vrednost razpoložljivosti IT vira in verjetnost uresničitve grožnje opisana s tristopenjskima lestvicama, in sicer z vrednostmi »nizko«, »srednje« in »visoko«. Te vrednosti naj bi predstavljale ocene vodstvenih kadrov na poslovni strani, ki imajo znanje o potrebni razpoložljivosti IT vira z vidika poslovnih procesov, ter strokovnjakov, ki lahko najbolje ocenijo verjetnost uresničitve grožnje, ki preti IT viru, in ki so bile pridobljene z uporabo vprašalnikov ali izvajanjem intervjujev. Združitev obeh komponent, kot je prikazano v tabeli 4, predstavlja združitev ocen v oceno tveganja.

Tabela 4: Primer kvalitativne ocene tveganj

Tveganje povezano z uporabo IT sredstva glede na pretečo grožnjo				
		Vrednost razpoložljivosti IT sredstva		
		Nizka	Srednja	Visoka
Verjetnost uresničitve grožnje	Nizka			
	Srednja			
	Visoka			

Vir: Avtor.

Ko se odloča za ta pristop, se običajno izbere strategija po kateri področja z najvišjimi ocenami tveganj (najbolj temna področja) zahtevajo takojšnjo pozornost, področja s srednjimi ocenami tveganj (svetlejša področja) zahtevajo

načrte za korektivne ukrepe, področja z najnižjimi ocenami tveganj (svetla področja) pa so sprejemljiva.

Kot že omenjeno, ima kvalitativen pristop določene slabosti in prednosti v primerjavi z kvantitativnem pristopom in te so navedene v nadaljevanju v tabeli 5.

Tabela 5: Primerjava prednosti in slabosti kvalitativnega in kvantitativnega pristopa k ocenjevanju tveganj

	Kvalitativni pristop	**Kvantitativni pristop**
Za	• Izračuni, če sploh so, so preprosti in lahko razumljivi. • Ni potrebno ugotavljati denarnih vrednosti IT virov (glede razpoložljivosti, zaupnosti in zanesljivosti). • Ni potrebno ugotavljati kvantitativnih pogostnosti groženj in potencialne škode. • Ni potrebno ugotavljati stroškov varnostnih ukrepov in izvajati analizo stroškov in koristi. • Običajno so s strani vodstva podana področja, ki zahtevajo posebno pozornost ob ugotavljanju tveganj.	• Vrednotenje in rezultati so osnovani na neodvisnih in objektivnih procesih in metrikah. To omogoča smiselne statistične analize. • Denarna vrednost IT virov (glede razpoložljivosti, zaupnosti in zanesljivosti) predstavlja lažje razumljivo osnovo za ovrednotenje potencialnih izgub. • Ustvarjena je verodostojna osnova za analizo stroškov in koristi ob vrednotenju ekonomske upravičenosti varnostnih ukrepov za izogibanje tveganjem. Na ta način je podprt sistem odločanja za odločanje o proračunu za informacijsko varnost. • Ocenjevanje izvajanja procesov upravljanja tveganj je lahko objektivno. • Rezultati vrednotenja tveganj so izraženi v jeziku vodstva – denarne vrednosti, odstotki in verjetnosti. Na ta način vodstvo tveganja bolje razume.
Proti	• Vrednotenje tveganj je izrazito subjektivno. • Viri se ovrednotijo denarno in posledično subjektivna ocena vrednosti vira ne vodi k realnemu ovrednotenju tveganj.	• Izračuni so kompleksni. Če jih vodstvo ne razume ali mu niso učinkovito predstavljeni, se pojavi dvom v rezultate. • Algoritmi običajno ne upoštevajo razlike med tveganji tipa velika pogostnost-majhna škoda in majhna pogostnost-velika škoda

	• Ni osnov za izvajanje analize stroškov in koristi, kar lahko vodi k prevelikim vlaganjem v varovanje nekaterih virov ter premajhno v varovanje drugih. • Nemogoče je objektivno ocenjevati izvajanje upravljanja tveganj, če so vse ocene subjektivne.	in ne omogočajo ustrezne predstavitve tveganj. • Izvajanje kvantitativnega vrednotenja tveganj brez uporabe avtomatiziranih orodij ni praktično in je dolgotrajno. Zlahka pride do napak pri preračunavanju rezultatov. • Potrebno je zbirati znatno količino podatkov o vsakem viru in njegovem okolju. • Ne obstaja še standardna in neodvisno sestavljena podatkovna baza groženj in pogostnosti njihovega pojavljanja. Zato se morajo uporabniki zanesti na zanesljivost podatkov proizvajalca orodij ali pa narediti lastno raziskavo groženj.

Vir: Tipton et al, 2004, str. 805.

Obstaja sicer še en pristop k upravljanju tveganj, in sicer pristop osnovnih zahtev (ang. baseline approach), ki je dokaj pogost med manjšimi ali mlajšimi organizacijami. Ta pristop temelji na identifikaciji v praksi izvedenih kontrol in ukrepov, ki jih izvaja konkurenca ali sorodne organizacije, in privzame to kot standard, kateremu želi zadostiti. Potrebno pa je opozoriti, da ta pristop, ki ne raziskuje sistematično groženj v svojem specifičnem okolju, niti ne vrednosti lastnih virov, zlahka nenamerno spregleda tveganja. Dodaten problem predstavlja, da organizacije zaradi izgube dobrega imena ne oglašujejo javno svojih varnostnih incidentov in se posledično standard osnovnih zahtev na nekem področju ali v neki industriji dviguje počasneje, kot bi se sicer glede na količino in ceno pojavov incidentov. V bistvu ta pristop sam po sebi predstavlja veliko tveganje.

4.2.2 Uporabljene kvantitativne metrike

Glede na namen dela so v metodologiji uporabljene metrike in tehnike izbrane tako, da omogočajo kvantitativen pristop k oceni tveganj pri oceni uporabljenih kategorij. Osnovne kategorije, katerim je potrebno določiti kvantitativne metrike so najmanj naslednje: škoda uresničitve grožnje, verjetnost uresničitve grožnje in cena varovanja. Posamezne od teh osnovnih kategorij so lahko nadalje dodatno razdeljene. Ozier, denimo, govori o naslednjih kategorijah, ki jim pravi šest osnovnih (ang. primitive) elementov (Tipton et al, 2004, str. 809):

- vrednost vira,

- faktor izpostavljenosti vrednosti vira grožnji,
- pogostost uresničitve grožnje,
- učinkovitost kontrol (oziroma stopnja ranljivosti),
- cena varovanja in
- negotovost.

Kategorije, ki so del predstavljene metodologije, temeljijo na istih osnovnih kategorijah, a so zastavljene nekoliko drugače, in sicer, kot je predstavljeno v tabeli 6.

Tabela 6: Primer kategorij kvantitativnega pristopa k oceni IT tveganj

Osnovna kategorija	**Kategorija**	**Metrika**
Škoda uresničitve grožnje		Eur
	Cena nadomestitve vira	Eur
	Škoda zaradi vpliva na poslovanje	Eur
Verjetnost uresničitve grožnje		Verjetnost na letni ravni
	Stopnja grožnje	Verjetnost na letni ravni
	Stopnja ranljivosti (glede na nivo vpeljanih kontrol)	Številčni faktor
Cena varovanja		Eur na letni ravni
	Fiksni stroški	Eur na letni ravni
	Tekoči stroški	Eur na letni ravni

Vir: Avtor.

Škoda uresničitve grožnje je torej izražena v denarni vrednosti in je vsota posameznih vrednosti treh kategorij. Ceno nadomestitve vira lahko predstavlja nakup nadomestnega vira ali stroški, povezani z obnovitvijo celovitosti podatkov. Zaradi uresničitve grožnje se zmanjša obseg poslovanja za čas trajanja okrevanja in ima ponavadi za posledico negativne finančne učinke v odvisnosti od tipa poslovanja in kategorije strank. V kategorijo drugo lahko umeščamo na primer pogodbeno dogovorjene kazni ter kazni regulatorja in podobno.

Verjetnost uresničitve grožnje je sestavljena iz dveh kategorij. Stopnjo grožnje določimo kot verjetnost na letni ravni, pri čemer stopnja 0,5/leto predstavlja verjetnost uresničitve enkrat na 2 leti. Stopnjo grožnje se določi na osnovi okoliščin in lastnosti obravnavanega vira organizacije. Stopnja grožnje okvare strojne opreme se denimo določi na osnovi podatkov o njeni zanesljivosti, stopnja grožnje potresa pa na osnovi geografske lokacije stavbe in podobno. Stopnja ranljivosti je določena kot faktor, ki korigira stopnjo grožnje glede na nivo vpeljanih preventivnih kontrol.

Cena varovanja je izražena kot strošek vpeljave in vzdrževanja kontrol. Strošek vpeljave predstavljajo fiksni stroški, ki jih lahko porazdelimo glede na predvideno življenjsko dobo kontrole, in tako dobimo strošek na letni ravni. Strošek vzdrževanja predstavljajo tekoči stroški v enem letu.

5 IDENTIFIKACIJA TVEGANJ

V okviru identifikacije tveganj identificiramo vire v uporabi v ključnih aktivnostih, ki so potencialen izvor tveganj. Nadalje identificiramo grožnje, ki so jim ti viri izpostavljeni, ranljivosti virov, ki bi jih grožnje lahko izkoristile, in vpliv uresničitev groženj na vire glede njihove razpoložljivosti, zaupnosti ter celovitosti.

5.1 Opredelitev ključnih aktivnosti

Za opredelitev ključnih aktivnosti bomo uporabili predstavljeni kombinirani pristop k določitvi obsega SUIV ter določeni obseg analize zamejili na organizacijsko enoto (v nadaljevanju OE) Oddelek TRR in proces vodenja transakcijskega računa pravnih oseb.

Proces vodenja transakcijskega računa je torej sestavljen iz več aktivnosti, ki se odvijajo v različnih OE, nekatere od njih v Oddelku TRR. Izmed identificiranih aktivnosti procesa je potrebno določiti tiste, ki so ključne za izvajanje poslanstva organizacije.

5.1.1 Identifikacija aktivnosti

Identifikacijo aktivnosti izvedemo z analizo aktivnosti v zadanem obsegu SUIV. Na sliki 13 je predstavljen primer možnih identificiranih aktivnosti procesa vodenja transakcijskega računa v Oddelku TRR.

Slika 13: Primer identificiranih aktivnosti procesa

	Opravilo	Opis	Nosilec	Ime in priimek
▶	000860	Kreiranje plačilnih nalogov		
	000870	Spremljanje plačilnega prometa po TRR PO		
	000900	Podajanje informacije o TRK (stanje promet izvršbe...)		
	001000	Reševanje reklamacij - TRR PO		
	001010	Vodenje izvršb po TRR PO		
	001020	Zapiranje računa TRR		

Vir: Avtor.

5.1.2 Določitev kriterijev teže aktivnosti glede vpliva na poslovanje

Za objektivno določitev vpliva škodnih dogodkov na poslovanje na nivoju aktivnosti potrebujemo kriterije, ki jih bomo poimenovali kriteriji teže aktivnosti. Teža aktivnosti bo osnova, na kateri bomo lahko določili aktivnosti, ki jih imamo za ključne.

Kriteriji teže aktivnosti morajo biti zastavljeni tako, da vpliv kršitve informacijske varnosti lahko celovito ovrednotimo. V naslednjem podanem primeru kriterijev, leti izhajajo neposredno iz kategorij informacijske varnosti:

- razpoložljivost - Vpliv omejenega obsega poslovanja zaradi IT virov in njihove nerazpoložljivosti,
- celovitost - Vpliv uporabe nepravilnih podatkov pri izvajanju aktivnosti,
- zaupnost - Vpliv kršenja zaupnosti podatkov.

V primeru vpliva omejenega obsega poslovanja zaradi nerazpoložljivosti IT virov oziroma kriterija razpoložljivosti je potrebno tudi upoštevati, ali se opravilo izvaja zgolj na eni lokaciji ali v eni organizacijski enoti in lahko predstavlja edino točko izpada (ang. single point of failure) zaradi svoje unikatnosti v procesu ali ne.

5.1.3 Določanje teže aktivnostim

Za določanje teže aktivnostim po sprejetih kriterijih je pomembno poznavanje posamezne aktivnosti glede načina rokovanja s podatki (vpogled, izpis, vnos, modifikacija in izbris) ter poznavanje vpliva na poslovanje v primeru nepravilne izvedbe ali neizvedbe aktivnosti.

Pri oceni vpliva na poslovanje po posameznih kriterijih je potrebno upoštevati značilnosti organizacije in okolja v katerem posluje (konkurenca, regulator, stranke, itd). Te značilnosti opredeljujejo izvor vpliva na poslovanje ter količino oziroma težo posledic. V bančnem okolju bi izvori vpliva na poslovanje lahko bili naslednji:

- kratkoročen izpad prihodkov zaradi omejenega obsega poslovanja,
- dolgoročen izpad prihodkov zaradi izgube strank,
- pogodbene kazni,
- kazni regulatorja, ki lahko vplivajo tudi na dolgoročen izpad prihodkov v primeru odvzema licence.

Težo aktivnosti predstavlja trojček ocenjenih vrednosti po posameznih kriterijih in jo lahko ponazorimo z naslednjim izrazom:

Aktivnost (Teža razpoložljivosti, Teža celovitosti, Teža zaupnosti)

Medtem ko lahko vrednosti kriterijev celovitosti in zaupnosti opredelimo kot eno vrednost, je vrednost kriterija razpoložljivosti časovno odvisna oziroma narašča s časom trajanja omejenega obsega ali prekinitve poslovanja. To pomeni, da je potrebno vrednosti kriterija oceniti na časovni premici, kot je predstavljeno na spodnjem primeru.

Tabela 7: Primer teže aktivnosti

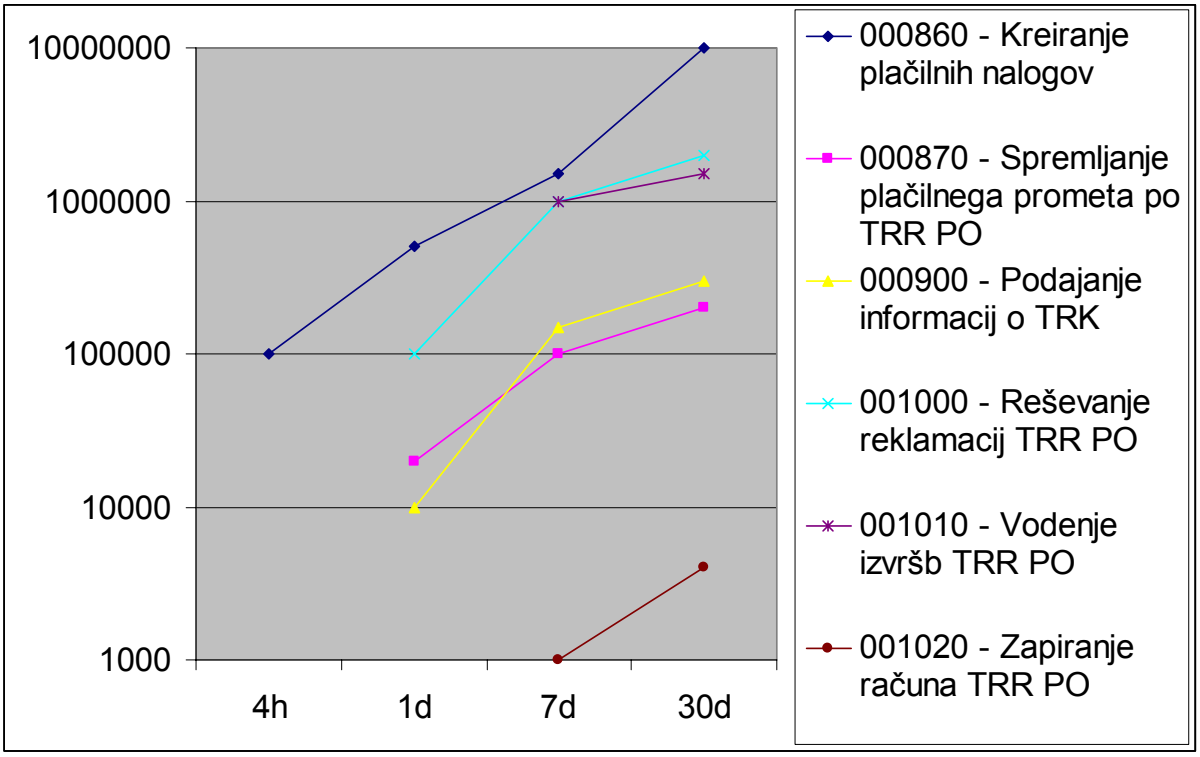
Aktivnost:	001000 – Reševanje reklamacij TRR PO			
Kriterij Celovitost	100.000 Eur	Stroški povezani z izrednimi reklamacijami zaradi uporabe napačnih podatkov		
Kriterij Zaupnost	0 Eur			
Kriterij Razpoložljivost	4h	1 dan	7 dni	1 mesec
	0 Eur	100.000 Eur	10 mio Eur	20 mio Eur

Vir: Avtor.

5.1.4 Izbor ključnih aktivnosti

Izbor ključnih aktivnosti izvedemo s pregledom tež aktivnosti. Izvajamo ga tako, da se osredotočimo na aktivnosti z največjimi ocenami vrednosti po posameznih kriterijih, ki jih določimo kot ključne. Na sliki 14 je prikazan primer, ko izbiramo na podlagi kriterija razpoložljivosti.

Slika 14: Primer ponazoritve izbora ključnih aktivnosti – kriterij razpoložljivosti



Vir: Avtor.

Primeri izbora so lahko sledeči – ključne aktivnosti so tiste, katerih vpliv omejenega obsega poslovanja:

- je v enem dnevu enak ali večji od 10.000 Eur ali
- je v sedmih dneh večji od 1 mio Eur.

5.2 Opredelitev virov za ključne aktivnosti

Vir ali sredstvo je vse, kar je potrebno za izvedbo posameznega opravila. Vir je vse, kar ima vrednost za organizacijo. Vire združujemo v skupine, imenovane tipi, glede na njihove skupne lastnosti, kar nam omogoča učinkovitejši pregled nad njimi. Standard ISO 17799:2005 glede na sorodnost lastnosti virov identificira naslednje tipe:

- informacijski viri (v elektronski in tiskani obliki),
- programska oprema,
- fizični viri, kot so strojna računalniška oprema, komunikacijska oprema, prenosni mediji in drugo,
- storitve,
- ljudje,
- neotipljivi viri, kot sta ugled in javna podoba organizacije.

Večini fizičnih virov lahko opredelimo lokacijo nahajanja. Na osnovi teh informacij gradimo mrežo lokacij, njihovih povezav ter virov na lokacijah, ki skupaj sestavljajo infrastrukturo. Slika 15 predstavlja infrastrukturo lokacije Oddelka transakcijskih računov v poslovni stavbi z identifikacijsko oznako 00011 Stavba 1 in IT centra z identifikacijsko oznako 00012 Stavba 2 – IT center.

Slika 15: Primer lokacij in infrastrukture

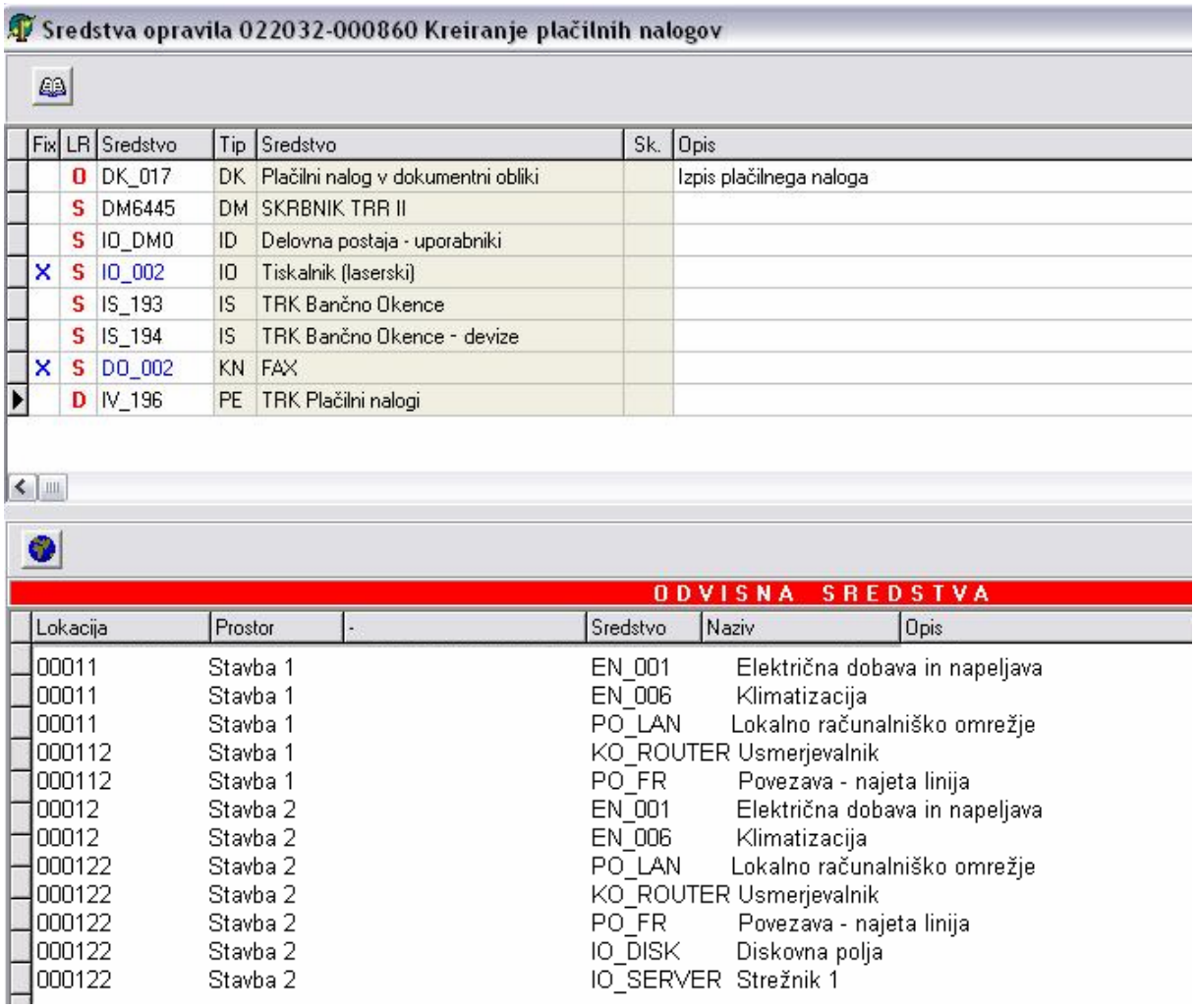
LOKACIJE in LOKACIJSKA SREDSTVA

Lokacija/Sredstvo	Naziv	PTT	Kraj
000		-	-
0001	Banka		
00011	Stavba 1		Nova Gorica
-->EN_001	S1-Električna dobava in lokalna napeljava (Stavba 1)		00
-->EN_006	S4-Klimatizacija (Stavba 1)		00
-->PO_LAN	KN-Lokalno računalniško omrežje (Stavba 1)		00
000111	Delovni prostori		
0001112	Pisarna Oddelka TRR		
000112	Sistemski prostor		
-->KO_ROUTER	SW-Usmerjevalnik (Stavba 1)		00
-->PO_FR	KZ-Povezava - najeta linija (Stavba 1)		00
00012	Stavba 2 - IT center		Ljubljana
-->EN_001	S1-Električna dobava in lokalna napeljava (Stavba 2)		00
-->EN_006	S4-Klimatizacija (Stavba 2)		00
000122	Sistemski prostori		
-->IO_DISK	IS-Diskovna polja		00
-->IO_SERVER	IS-Strežnik 1		00
-->KO_ROUTER	SW-Usmerjevalnik (Stavba 2)		00
-->PO_FR	KZ-Povezava - najeta linija (Stavba 2)		00
-->PO_LAN	KN-Lokalno računalniško omrežje (Stavba 2)		00

Vir: Avtor.

Uporaba ostalih virov je opredeljena preko neposredne navedbe njihove uporabe v posameznih aktivnostih, kot so prikazani v zgornjem okencu na sliki 16.

Slika 16: Primer virov opravila



Vir: Avtor.

Uporaba teh virov je običajno odvisna od razpoložljivosti virov, ki tvorijo infrastrukturo, ki so na sliki 16 razvidni iz spodnjega okenca kot odvisna sredstva oziroma viri.

Povezavo med viri aktivnosti na prvem nivoju ter viri infrastrukture določimo z opredelitvijo njihovih odvisnosti, kot je razvidno iz primera na sliki 17. Na njej je prikazana odvisnost vira informacijski sistem IS_193 TRK Bančno Okence, ki se uporablja na lokaciji 0001112 Pisarna Oddelka TRR, od strežnika in skupnega diskovnega prostora lociranih na lokaciji z oznako 000122 Sistemski prostori IT centra.

Slika 17: Primer določitve odvisnosti virov oziroma sredstev

ODVISNA SREDSTVA

Število zapisov: 84

Vir: IS_193 - TRK Bančno Okence

Lokacija	Opis lokacije	Rabi sredstvo	Opis sredstva	Na lokaciji	Opis lokacije
0001112	Pisarna Oddelka TRR	IO_DISK	Skupni diskovni prostor	000122	Sistemski prostori
0001112	Pisarna Oddelka TRR	IO_SERVER	Strežnik	000122	Sistemski prostori

Vir: Avtor.

5.3 Identifikacija groženj

Namen aktivnosti je opredelitev groženj, katerim so ti viri izpostavljeni, ranljivosti virov, ki bi jih grožnje lahko izkoristile, in vpliv uresničitev groženj na vire glede njihove razpoložljivosti, zaupnosti ter celovitosti. Grožnje in ranljivosti sta lahko dve od lastnosti, po katerih vire združujemo v tipe virov.

Naloga je zahtevna, saj lahko nameren ali nenameren spregled grožnje izniči trud in rezultate celotnega procesa, saj so povezana tveganja tako nehote sprejeta. Glede na to, da ne obstaja neodvisen, celovit in verodostojen seznam groženj, povezanih ranljivosti in kontrol, lahko ta aktivnost zahteva precej raziskovanja in terja veliko časa. Trenutno je najboljša rešitev uporaba orodja, ki že vsebuje seznam. Vendar imajo tudi orodja omejitve in je običajno priporočljiv razmislek o morebitnih dopolnitvah seznama glede na okolje in specifične lastnosti organizacije.

V tabeli 8 je prikazan primer identificiranih groženj viru in njegovih ranljivosti ter vpliv na obravnavane kategorije varnosti vira.

Tabela 8: Primer groženj viru, ranljivosti vira ter vpliva ranljivosti na vir

Sredstvo: Strežnik 1		**Vpliv na..**		
Grožnja	**Ranljivost**	**Razpoložljivost**	**Zaupnost**	**Celovitost**
G1 Izpad	***R1*** Tehnična okvara	X		
	R2 Nenačrtovano vzdrževanje			
	R3 Preobremenitev			
	R4 Odsotnost kontrol neprekinjenega delovanja			
G2 Napačno delovanje na nivoju programske opreme	***R5*** Neažurna nameščena programska oprema	X	X	X
	R6 Nepravilni ali neupoštevani postopki nameščanja programske opreme			
	R7 Okužba z zlonamerno programsko opremo			
	R8 Odsotnost ali nedelovanje sistema obveščanja o izrednih dogodkih			
G3 Vdor	***R5*** Neažurna nameščena programska oprema		X	X
	R7 Okužba z zlonamerno programsko opremo			
	R9 Slabe logične kontrole			
	R10 Slabe fizične kontrole			

Vir: Avtor.

Razvidno je, da nekatere grožnje, na primer »Napačno delovanje na nivoju programske opreme« ter »Vdor« lahko izkoristijo iste ranljivosti, na primer »Neažurno nameščeno programsko opremo« ali »Okužbo z zlonamerno programsko opremo«. To v nadaljevanju pomeni, da uvedba kontrol, ki zmanjšujejo ali odpravljajo te ranljivosti, zmanjšuje verjetnost uresničitve obeh navedenih groženj.

Pomembno je izpostaviti, da so v primeru navedene le grožnje, ki pretijo neposredno obravnavanemu viru. Vir je kot del celovitega informacijskega sistema na primer z vidika izpada nudenja svojih storitev ranljiv tudi na prekinitev električne energije ali na prekinitev komunikacijskih povezav. V okviru opisanega načina povezav odvisnih sredstev, ki skupaj tvorijo (informacijski) sistem, so te grožnje in ranljivosti obravnavane na virih, ki jim neposredno grozijo, torej v danih primerih električnemu napajanju in komunikacijski povezavi.

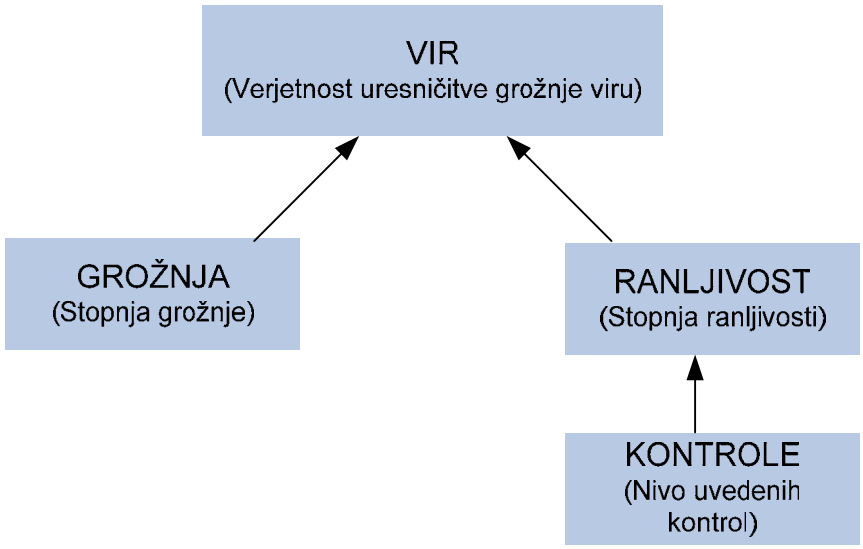
6 OCENA TVEGANJ

V tej fazi opredelimo kvantificirano oceno za oba elementa tveganja, to je verjetnost uresničitve grožnje ter potencialno škodo. Na osnovi teh dveh elementov lahko razporejamo in predstavljamo tveganja v enotni sliki profila organizacije izpostavljenosti tveganjem, ki v nadaljevanju služi kot osnova za razmejitev sprejemljivih in nesprejemljivih tveganj.

6.1 Ocena verjetnosti uresničitve grožnje

Ocena verjetnosti uresničitve grožnje je sestavljena iz dveh komponent in sicer stopnje grožnje in stopnje ranljivosti vira, kot je predstavljeno na sliki 18.

Slika 18: Verjetnost uresničitve grožnje, ki preti viru



Vir: Avtor.

V prvem koraku določamo stopnjo posamezne grožnje, ki preti viru. Stopnja grožnje je nekaj, na kar organizacija težko vpliva. Stopnja grožnje je odvisna od zunanjih dejavnikov, kot so nivo aktivnosti virov groženj (glede stopnje grožnje

potresa denimo seizmološka aktivnost geografske lokacije vira), mamljivost napadalcem (glede grožnje vdora denimo pridobitev strogo zaupnih podatkov konkurenčnih podjetij) in podobno. Stopnja grožnje predstavlja predvideno stopnjo uresničitve grožnje v primeru, ko niso uvedene nobene kontrole za ranljivosti vira, kateremu preti grožnja.

Stopnje grožnje bomo opredelili kot verjetnost na letni ravni. Za osnovo in v pomoč lahko vzamemo v tabeli 9 predlagane vrednosti, izvedene na osnovi kvalitativnih stopenj, pri čemer seveda lahko na osnovi drugačnih podatkov določimo tudi katerokoli v tabeli nezabeleženo vmesno stopnjo.

Tabela 9: Primer stopenj groženj

Kvalitativna ocena	**Opis**	**Kvantitativna ocena**
Zanemarljiva	Ni verjetno	0,05/leto
Zelo nizka	Do dvakrat, trikrat na pet let	0,5/leto
Nizka	Do enkrat na leto	1/leto
Srednja	Dvakrat na leto	2/leto
Visoka	Enkrat na mesec	12/leto
Zelo visoka	Dvakrat, trikrat na mesec	30/leto
Ekstremna	Dnevno	350/leto

Vir: Prirejeno po OICT, 2005, str. 11.

Identificiranim grožnjam vira Strežnik 1 lahko stopnje opredelimo na primer takole:

- izpad: 0,5/leto,
- napačno delovanje na nivoju programske opreme: 2/leto,
- vdor: 30/leto.

Druga kategorija, ki vpliva na verjetnost uresničitve grožnje, je, kot rečeno, stopnja ranljivosti vira. Stopnjo ranljivosti ocenjujemo na osnovi nivoja uvedenih kontrol oziroma ocene njihove učinkovitosti.

Primer ocene stopnje uvedenih kontrol je predstavljen v tabeli 10. Posamezna kontrola lahko varuje pred več ranljivostmi in je razporejena glede na ranljivosti, na katere vpliva.

Tabela 10: Primer ocene stopnje uvedenih kontrol za posamezne ranljivosti

Sredstvo: Strežnik 1			
Grožnja	**Ranljivost**	**Kontrole**	**Ocena kontrole**
G1 Izpad	***R1*** Tehnična okvara	***K1*** Skrbništvo	DA
		K2 Periodično vzdrževanje	DELNO
		K3 Redundanca komponent vira	DELNO
		K4 Podvojevanje vira	NE
		K5 Vzdrževalne pogodbe (SLA)	DA
		K18 Zanesljivost vira	DELNO
	R2 Nenačrtovano vzdrževanje	***K1*** Skrbništvo	DA
		K5 Vzdrževalne pogodbe (SLA)	DA
		K6 Načrtovanje vzdrževanja	NE
		K7 Testno okolje	DA
		K8 Upoštevanje postopkov testiranja	DELNO
	R3 Preobremenitev	***K1*** Skrbništvo	DA
		K7 Testno okolje	DA
		K9 Nadzor obremenitev	NE
		K10 Načrtovanje kapacitet	NE
		K11 Testiranje obremenitev	NE
	R4 Odsotnost kontrol neprekinjenega delovanja	***K1*** Skrbništvo	DA
		K3 Redundanca komponent vira	DA
		K4 Podvojevanje vira	NE
		K5 Vzdrževalne pogodbe (SLA)	DA
		K12 Rezervna oprema na dosegu	NE
		K13 Proizvajalčeva dokumentacija vira	DA
		K14 Načrt obnovitve sredstva	
		K15 Rezervne kopije nastavitev	NE
		K16 Rezervne kopije programske opreme	DA
		K17 Rezervne kopije podatkovnih baz	DA
			DA
Čas obnovitve funkcionalnosti vira po uresničitvi grožnje			1 dan

Vir: Avtor.

S pomočjo identificiranega nivoja uvedenih kontrol lahko za posamezno ranljivost določimo stopnjo ranljivosti in tudi ugotovimo čas, potreben za obnovitev funkcionalnosti vira. Stopnjo ranljivosti podamo kot faktor stopnje ranljivosti, s katerim prilagodimo stopnjo grožnje, da določimo ocenjeno verjetnost uresničitve grožnje. Verjetnost uresničitve grožnje torej izračunamo glede po naslednji enačbi:

Verjetnost uresničitve grožnje = Stopnja grožnje x Stopnja ranljivosti

Na primer za ranljivost R1 Tehnična okvara imamo podatek o stopnji grožnje 3/leto. Nivo uvedenih kontrol opisuje stanje delnega zadovoljstva o zanesljivosti opreme, delne redundance komponent vira, ter podatka o vzdrževanju, ki je deloma načrtovano. Poleg tega vir ni podvojen oziroma del gruče. Na osnovi teh podatkov določimo faktor. Z zmnožkom faktorja s stopnjo grožnje določimo boljšo oceno verjetnosti uresničitve grožnje. Primer možnih izračunov za navedene ranljivosti je podan v tabeli 11.

Tabela 11: Primeri izračuna verjetnosti uresničitve grožnje izpada

Ranljivost	**Stopnja grožnje izpada**		**Stopnja ranljivosti**		**Verjetnost uresničitve grožnje z izrabo ranljivosti**
R1 Tehnična okvara	0,5/leto	X	1	=	0,5/leto
R2 Nenačrtovano vzdrževanje	1/leto	X	0,25	=	0,25/leto
R3 Preobremenitev	1/leto	X	0,25	=	0,25/leto

Vir: Avtor.

Za določitev verjetnosti uresničitve grožnje seštejemo verjetnosti uresničitve grožnje z izrabo posameznih ranljivosti zaradi neodvisnosti posameznih ranljivosti med sabo. Tako za grožnjo izpada vira Strežnik 1 dobimo verjetnost uresničitve grožnje enako (0,5 + 0,25 + 0,25)/leto oziroma sešteto 1/leto. Čas trajanja uresničitve grožnje je en dan.

6.2 Potencialna škoda uresničitve grožnje

Potencialno škodo uresničitve grožnje določimo kot seštevek cene nadomestitve vira ter škode zaradi vpliva na poslovanje. Škodo zaradi vpliva na poslovanje ocenimo kot seštevek tež aktivnosti, ki so prizadete zaradi uresničitve grožnje.

Seštevek cene nadomestitve vira in vpliva na poslovanje z vidika zaupnosti in celovitosti predstavlja fiksni del škode. V primeru, da uresničitev grožnje vpliva na poslovanje tudi zaradi nerazpoložljivosti virov, je seštevek spremenljiv v času in predstavlja dinamični del škode.

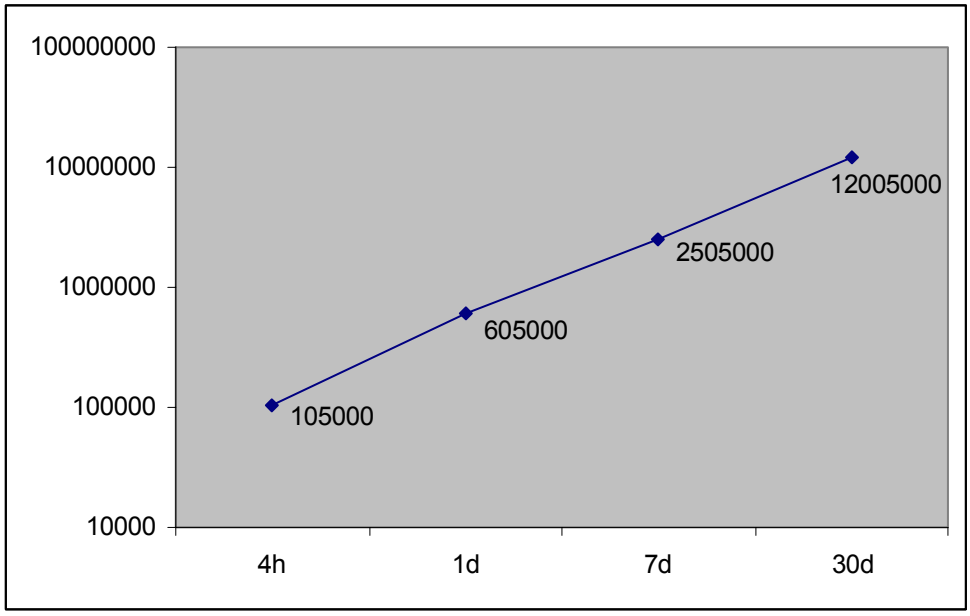
Tabela 12: Primer potencialne škode uresničitve grožnje

Grožnja:	Izpad			
Vir:	Strežnik 1			
Prizadete aktivnosti:	001000 – Reševanje reklamacij TRR PO 000860 - Kreiranje plačilnih nalogov			
Cena nadomestitve vira	5000 Eur			
Kriterij Razpoložljivost	**4h**	**1 dan**	**7 dni**	**1 mesec**
	0 Eur + 100.000 Eur	100.000 Eur + 500.000 Eur	1 mio Eur + 1,5 mio Eur	100 mio Eur + 20 mio Eur

Vir: Avtor.

Na sliki 19 je predstavljen primer ocene potencialne škode zaradi uresničitve grožnje izpada vira Strežnik 1, ki povzroči prekinitev izvajanja aktivnosti 001000 – Reševanje reklamacij TRR PO in 000860 - Kreiranje plačilnih nalogov za vse opredeljene časovne intervale. Cena obnovitve strežnika je ocenjena na 5000 Eur. Škoda zaradi vpliva na poslovanje je seštevek tež navedenih dveh aktivnosti po kriteriju razpoložljivosti. Na sliki 19 je predstavljena ocena potencialne škode za vse opredeljene časovne intervale.

Slika 19: Ocena potencialne škode uresničitve grožnje



Vir: Avtor.

Kot je razvidno iz tabele 10, je podana ocena časa obnovitve funkcionalnosti vira po uresničitvi grožnje, in sicer en dan. To pomeni, da je največja potencialna škoda iz vidika zmanjšanega obsega poslovanja glede na nivo uvedenih kontrol tista, ki nastane v enem dnevu. Višina te celotne škode je v zgornjem grafikonu navedena pri ustreznem časovnem intervalu in torej znaša 605.000 Eur.

6.3 Profil tveganj

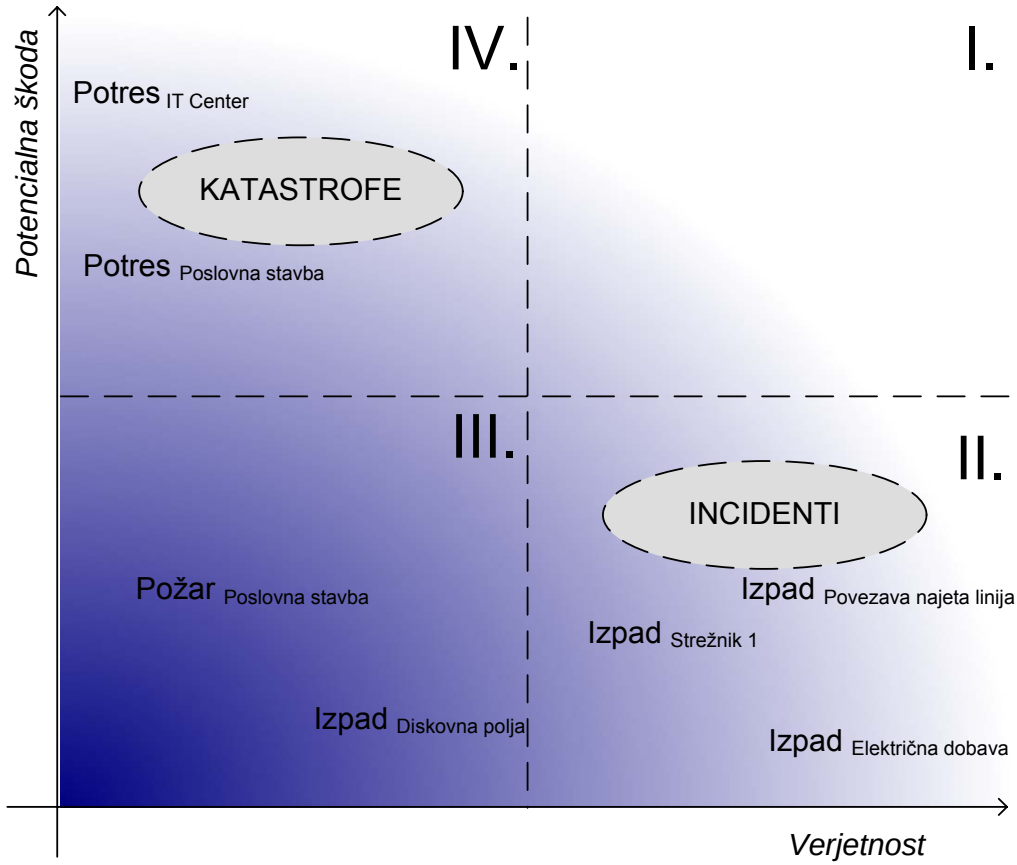
Končni rezultat ocene tveganj je profil tveganj, na osnovi katerega je mogoča primerjalna analiza tveganj glede njihove pomembnosti. Pomembnost je iz profila razvidna iz višjih ocen vrednosti ocen tveganja glede na izbrane kriterije in omogoča pregledno razvrščanje.

Tveganje je torej sestavljeno iz dveh elementov in ga lahko predstavimo z naslednjim izrazom:

Tveganje = (Verjetnost uresničitve grožnje viru, Potencialna škoda)

Posledično profil tveganj običajno predstavljamo z grafikonom, kjer na abscisi predstavljamo verjetnost uresničitve grožnje, na ordinati pa potencialno škodo. V primeru, ki ga obravnavamo, bi grafikon profila tveganj izgledal, kot je predstavljen na sliki 20.

Slika 20: Profil tveganj



Vir: Avtor.

Pozicija tveganja v grafikonu odraža njegove karakteristike glede na elementa, ki ga določata:

- tveganj v kvadrantu I praktično ne sme biti, saj predstavljajo relativno pogosto uresničevanje groženj z relativno veliko škodo,
- tveganja v kvadrantu II imajo večjo verjetnost uresničitev groženj, ki pretijo določenim virom, a je potencialna škoda ocenjena kot relativno majhna – običajno jih imenujemo kot manjše izpade oziroma incidente,
- tveganja v kvadrantu III predstavljajo manjša tveganja, saj se te grožnje relativno redko uresničujejo in imajo relativno manjšo škodo,
- tveganja v kvadrantu IV predstavljajo tako imenovane katastrofe – relativno redko uresničevanje groženj, ki pa imajo za posledico veliko škodo organizaciji.

Pomembno je, da so vsa tveganja predmet nadzora, saj se njihova pozicija lahko hitro spremeni glede na spremembe v okolju oziroma zaradi spremenjene verjetnosti uresničitve grožnje viru ali pa zaradi spremenjenega pomena vira za

organizacijo zaradi večje odvisnosti poslovnih aktivnosti organizacije od uporabe vira.

Glede na dosedanjo dosledno uporabo kvantitativnih metrik pa lahko tveganje tudi izračunamo in sicer z uporabe naslednje enačbe:

Tveganje = Verjetnost uresničitve grožnje viru x Potencialna škoda

V tabeli 13 je podan primer izračuna nekaterih tveganj.

Tabela 13: Primer kvantitativnega izračuna tveganja

Grožnja	**Verjetnost uresničitve grožnje**	**Potencialna škoda**	**Tveganje**
Izpad $_{\text{Električna dobava}}$	6/leto	20.000 Eur	120.000 Eur/leto
Izpad $_{\text{Strežnik 1}}$	1/leto	605.000 Eur	605.000 Eur/leto
Požar $_{\text{Poslovna stavba}}$	0,1/leto	700.000 Eur	70.000 Eur/leto
Potres $_{\text{IT center}}$	0,05/leto	200 mio Eur	10 mio Eur/leto

Vir: Avtor.

Vrednost tveganja v zadnjem stolpcu tabele 13 predstavlja potencialno škodo opredeljeno na letni ravni glede na verjetnost uresničitve grožnje viru in čas potreben za okrevanje.

7 OVREDNOTENJE TVEGANJ

Po izvedeni oceni tveganja izvedemo ovrednotenje tveganj, s katerim opravimo pregled tveganj na osnovi izdelanega profila tveganj, glede na kriterije sprejemljivosti, in ugotovimo, ali so sprejemljiva ali pa je potrebno določanje strategij obravnave nesprejemljivih tveganj.

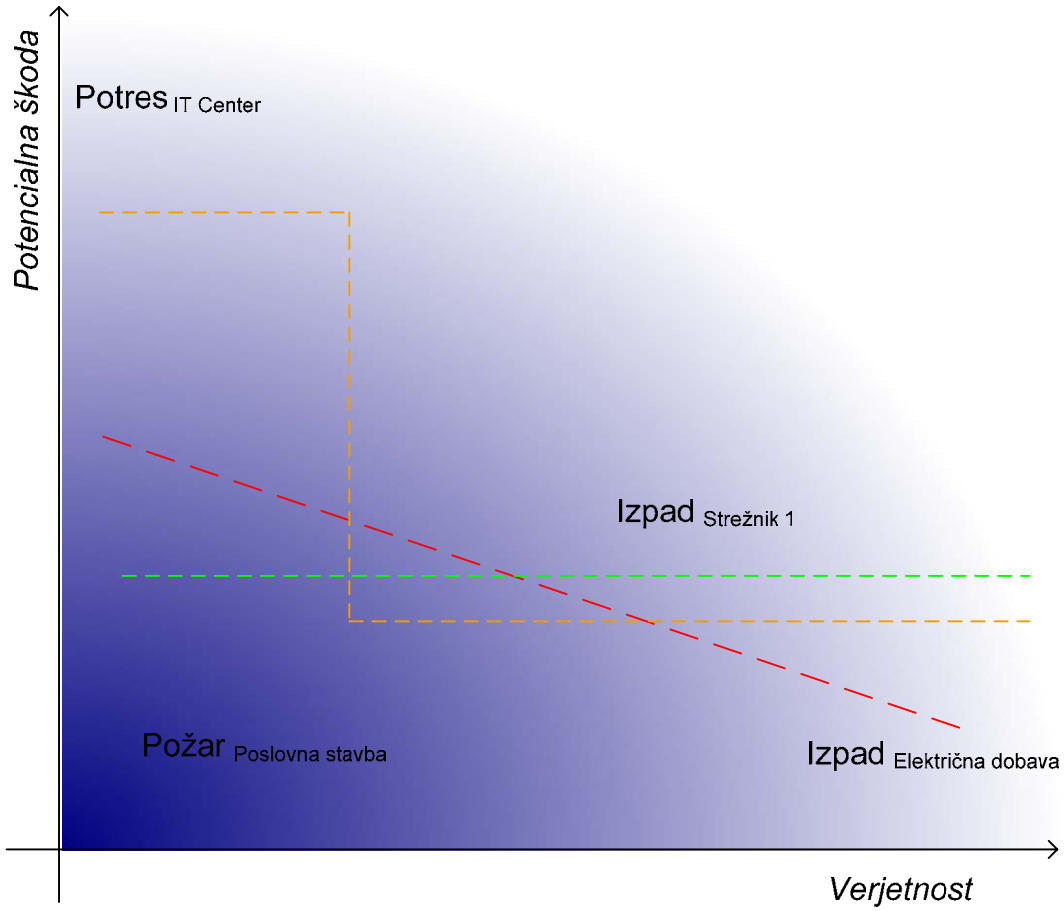
Kriterije sprejemljivosti lahko določamo na različni globini elementov, ki sestavljajo tveganja. V našem primeru lahko v prvem koraku glede na kvantitativni izračun tveganja opredelimo sprejemljivo mejo potencialne škode na letni ravni glede na tabelo 13. Tako določena sprejemljiva meja tveganja na denimo 500.000 Eur/leto določi kot nesprejemljivi tveganji:

- potres na lokaciji IT centra z oceno tveganja 10 mio Eur/leto,

- izpad Strežnika 1 z oceno tveganja 605.000 Eur/leto.

Tako določena sprejemljiva meja tveganja je na sliki 21 prikazana s črtkano rdečo črto. V nadaljevanju dela se bom glede sprejemljivosti tveganj navezoval na to mejo sprejemljivosti.

Slika 21: Meja sprejemljivosti tveganj



Vir: Avtor.

Naslednji, drugi korak v globino ovrednotenja tveganj bi bil pregled po verjetnosti uresničitve grožnje ter potencialne škode. Ta pogled nam v prvi vrsti omogoča razlikovanje med tveganji tipov »velika verjetnost – majhna škoda« ter »majhna verjetnost – velika škoda«, kar nam kvantitativni izračun zamegli. Kriterije sprejemljivosti tveganj lahko določamo ločeno glede na verjetnosti uresničitve grožnje in potencialne škode. Ovrednotenje tveganj na tem nivoju nam lahko predvsem postavi osnovo za izbor strategij ovrednotenja tveganj glede delitve na omenjena tipa, oziroma na katastrofe ter incidente in na ločene kriterije sprejemljivosti. Nekatere tipične lastnosti obeh vrst tveganj so predstavljene v tabeli 14.

Tabela 14: Lastnosti tveganj katastrof v primerjavi z incidenti

Lastnost	**Katastrofa**	**Incident**
Potencialna škoda	Zelo velika	Omejena na manjši del poslovanja
Verjetnost uresničitve grožnje	Manjša verjetnost, redkejša uresničitev	Večja verjetnost, pogostejša uresničitev
Čas obnovitve	Zelo dolg	Kratek
Stopnja prizadetosti virov	Večje število virov	Posamezen vir

Vir: Avtor.

V našem primeru bi torej lahko na primer določili dva kriterija sprejemljivosti in sicer:

- meja sprejemljivosti za škodne dogodke z verjetnostjo manjšo od 0,1/leto je 5 mio Eur,
- meja sprejemljivosti za škodne dogodke z verjetnostjo večjo od 0,1/leto je 500.000 Eur.

Kriterija sprejemljivosti tveganj sta na sliki 21 predstavljena z oranžno črto.

Primer nesprejemljivega tveganja po prvem kriteriju sprejemljivosti je potres na lokaciji IT centra z oceno potencialne škode 200 mio Eur. Primer nesprejemljivega tveganja po drugem kriteriju sprejemljivosti je izpad Strežnika 1 z oceno potencialne škode 605.000 Eur.

Drugi primer določitve kriterija sprejemljivosti na tej globini ovrednotenja tveganj bi lahko bil kriterij vezan zgolj na enega od elementov tveganj, na primer na potencialno škodo, in bi izgledal takole:

- meja sprejemljivosti za škodne dogodke je 600.000 Eur (ne glede na verjetnost uresničitve grožnje).

Ta kriterij sprejemljivosti tveganj je na sliki 21 predstavljen z zeleno črto.

V tretjem koraku globine ovrednotenja tveganj bi lahko oceno potencialne škode razstavljali glede na izvore vpliva na poslovanje, in sicer na primer glede na kršenje zahtev regulatorja ter izpad prihodkov. Uresničitvam groženj, katerih

posledice predstavljajo kršitev zahtev regulatorja, bi lahko dali poseben pomen ter prioriteto obravnave in podobno.

8 OBRAVNAVA TVEGANJ

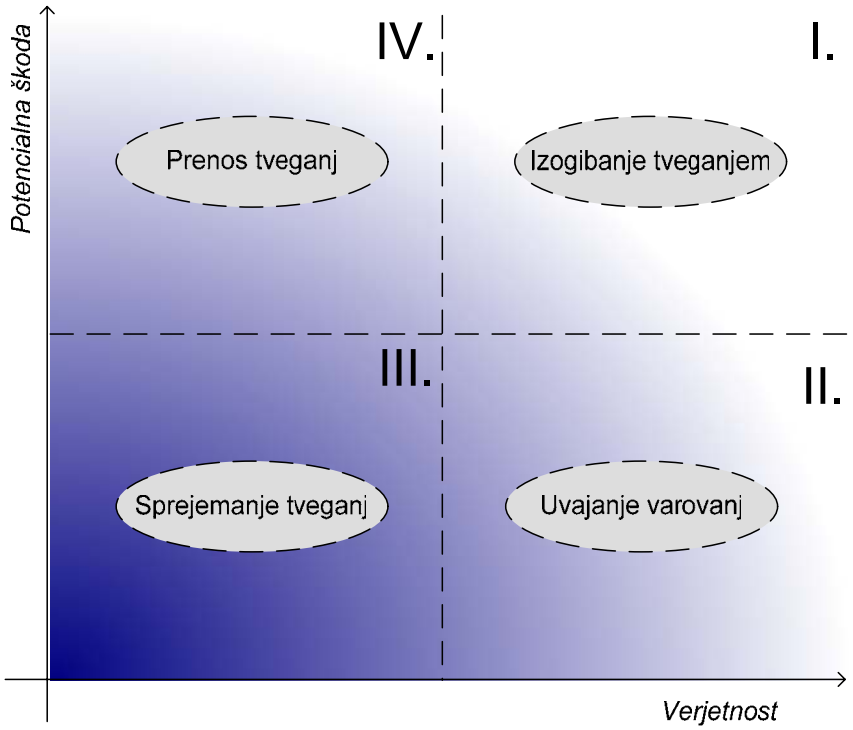
Naslednji korak po oceni ter ovrednotenju tveganj je njihova obravnava glede identifikacije možnosti ravnanja ter ocene primernosti in učinkovitosti teh možnosti.

Štiri temeljne strategije ravnanja pri obravnavi tveganj so (ISO 27001, 2005, str. 5):

- uvajanje kontrol z namenom zmanjševanja tveganj,
- sprejemanje tveganj na osnovi znanih ocen, v skladu s sprejetimi politikami in v mejah kriterijev sprejemljivosti,
- izogibanje tveganjem,
- prenos tveganj, na primer s sklenitvijo dogovora z zavarovalnico ali partnerjem.

Nekateri viri priporočajo uporabo navedenih strategij oziroma možnosti ravnanja v skladu s profilom tveganj, kot je predstavljeno na sliki 22.

Slika 22: Povezave profila tveganj s strategijami obravnave



Vir: Prirejeno po Andersen, 1998, str. 119.

Očitna težava tega pristopa je razvidna denimo pri priporočeni uporabi strategije prenosa tveganj za tveganja v kvadrantu IV. Medtem ko je materialno škodo ob uresničenju recimo grožnje naravne nesreče danes v Sloveniji mogoče zavarovati, je nemogoče skleniti zavarovanje za izpad prihodkov organizacije, povezanimi s to ali drugo grožnjo. Posledično nam v tem primeru prenos tveganj ne pomaga dosti in se organizacije poslužujejo tudi strategije uvajanja kontrol, kot je predstavljeno na sliki 11. Primer uvedbe take kontrole je denimo vzpostavitev nadomestne lokacije poslovanja. Smiselno je vsaj hkratno obravnavati uporabo strategij prenosa tveganj in uvajanja kontrol glede na posamično tveganje iz kvadrantov II in IV, verjetno pa celo širšo uporabo vseh možnih strategij glede na učinkovitost konkretnih aktivnosti v okviru posamezne strategije ter kriterijev sprejemljivosti tveganj organizacije.

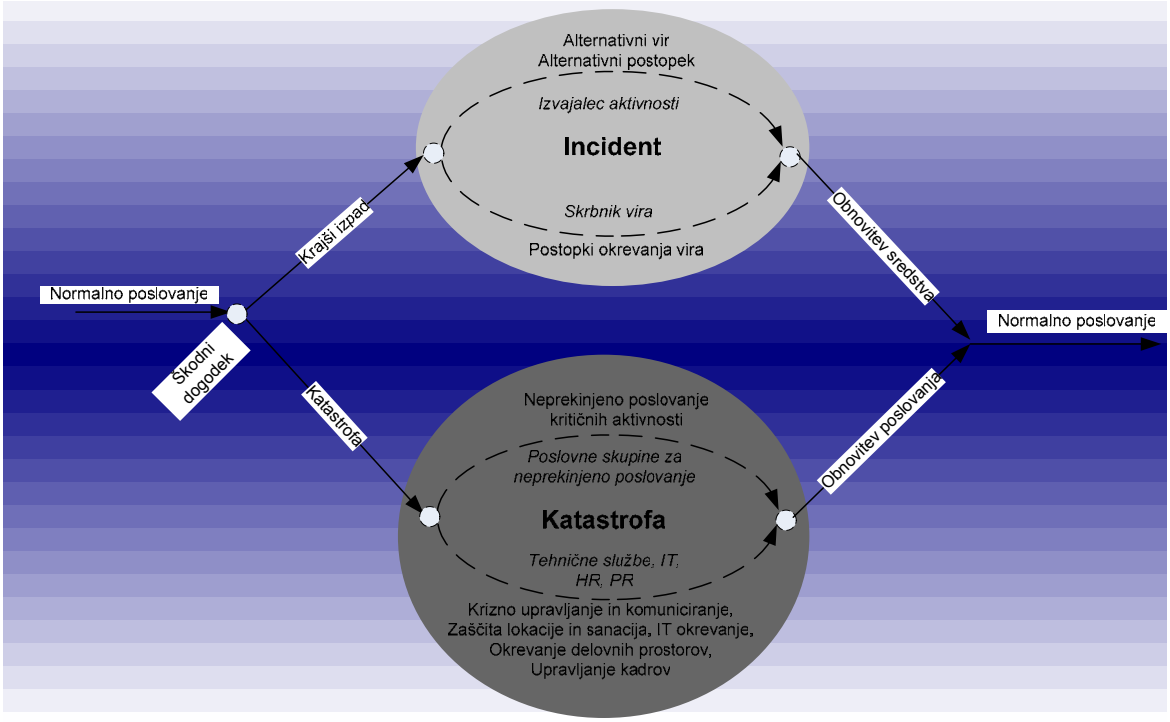
Pri razvoju strategij lahko upoštevamo naslednje možnosti strategij, ki so razvite iz že omenjenih temeljnih strategij:

- sprejem tveganja: v primeru, da so tveganja znotraj meja sprejemljivosti in v skladu s potrjeno politiko, morda niso potrebne dodatne aktivnosti glede zmanjševanja tveganja,
- prekinitev (dela) poslovanja: v primeru, da je del poslovanja povezan z višjimi tveganji, kot so koristi, obstaja možnost odločitve o prekinitvi izvajanja tega dela poslovanja,
- prenos aktivnosti: v primeru uresničitve grožnje lahko izvedemo prenos aktivnosti na zunanjega izvajalca ali prenos v skladu s sklenjenim recipročnim dogovorom,
- prenos tveganja z zavarovanjem: cilj uporabe te možnosti je delna finančna nadomestitev nastale škode in ne preprečuje samega nastanka škode,
- izogibanje nastanku škode: nastanek škode preprečujemo ali omejujemo z uvajanjem ukrepov varovanj,
- upravljanje neprekinjenega poslovanja: aktivnosti upravljanja neprekinjenega poslovanja omogočajo izboljševanje odpornosti organizacije z načrtovanjem neprekinjenega poslovanja v minimalnem zahtevanem obsegu. Ta pristop omogoča, da strategije UNP vseh treh nivojev tvorijo uspešno in učinkovito sposobnost organizacije za neprekinjeno poslovanje.

V nadaljevanju dela se bomo posvetili predvsem strategijam izogibanja nastanka škode z uvedbo dodatnih kontrol. Uvedba kontrol ima lahko dve vrsti pozitivnih učinkov, in sicer lahko zmanjšujejo verjetnost uresničitve grožnje ali pa zmanjšujejo potencialno škodo. Medtem ko v primeru nekaterih groženj, kot so na primer naravne nesreče, lahko predvsem vplivamo na zmanjševanje potencialne škode, denimo z že omenjeno vzpostavitvijo nadomestne lokacije poslovanja lahko z uvajanjem kontrol vplivamo v obeh smereh na druga tveganja.

Glede na razlike v lastnostih med katastrofami in incidenti je tudi izbor strategij obravnave in obseg uvajanja dodatnih kontrol zelo različen.

Slika 23: Kontrole v primeru katastrof in incidentov



Vir: Avtor.

Na sliki 23 je predstavljen obseg aktivnosti in kontrol, ki so potrebne za zmanjševanje tveganj z vidika neprekinjenega poslovanja. Medtem ko v primeru krajšega izpada oziroma incidenta raziskujemo predvsem možnosti alternativnih postopkov in virov, gre v primeru katastrof za obsežnejše aktivnosti celovitega načrtovanja okrevanja poslovanja po katastrofi (ang. disaster recovery).

8.1 Identifikacija in izdelava predlogov obravnave tveganj

Cilj uvajanja dodatnih kontrol je povišan nivo varnosti izvajanja aktivnosti, ki ga dosežemo tako, da zmanjšamo verjetnost uresničevanja groženj ali potencialno škodo.

Predlogi kontrol lahko temeljijo na podlagi pomanjkljivosti varovanja vira, ki so bile identificirane pri oceni ranljivosti vira. Na podlagi tabele 10 lahko izdelamo seznam pomanjkljivih kontrol varovanja vira Strežnik 1 in sicer tako, da povzamemo tiste kontrole, ki so označene kot delno ali v celoti neuvedene.

Tabela 15: Primer identifikacije predlogov uvedbe kontrol

Sredstvo: Strežnik 1	
Pomanjkljive kontrole	**Ocena uvedenosti kontrole**
K2 Periodično vzdrževanje	DELNO
K3 Redundanca komponent vira	DELNO
K4 Podvojevanje vira	NE
K6 Načrtovanje vzdrževanja	NE
K8 Upoštevanje postopkov testiranja	NE
K9 Nadzor obremenitev	NE
K10 Načrtovanje kapacitet	NE
K11 Testiranje obremenitev	NE
K12 Rezervna oprema na dosegu	NE
K14 Načrt obnovitve sredstva	NE
K18 Zanesljivost vira	DELNO
Čas obnovitve funkcionalnosti vira po uresničitvi grožnje	1 dan

Vir: Avtor.

Konkreten cilj uvajanja dodatnih kontrol za Strežnik 1 je zmanjšanje tveganja pod mejo sprejemljivosti tveganj, to je pod 500.000 Eur/leto. To lahko naredimo tako, da:

- uvedemo kontrole za zmanjševanje verjetnosti uresničitve grožnje izpada strežnika (npr. izboljšanje periodičnega vzdrževanja, popolna redundanca komponent vira, uporaba vira z višjo stopnjo zanesljivosti, itd.),
- zmanjšamo potencialno škodo z zmanjšanjem časa, potrebnega za obnovitev funkcionalnosti vira (npr. s podvojevanjem vira, rezervno opremo na dosegu, pripravo celovitega načrta obnovitve sredstva, itd.).

Takoj je razvidno, da lahko tvorimo predloge treh tipov uvedbe kontrol. Prvi se usmerja na zmanjševanje verjetnosti uresničitve grožnje, drugi na zmanjšanje časa potrebnega za obnovitev funkcionalnosti vira, tretji tip pa ima lahko učinek na oboje. Možna je izdelava več predlogov znotraj posameznega tipa.

Denimo, da se odločimo za izdelavo predloga, ki zmanjšuje čas obnovitve funkcionalnosti vira z enega dneva na štiri ure. Glede na trenutno stanje bi

potrebovali uvesti nekatere dodatne kontrole, na primer tiste, navedene v tabeli 16.

Tabela 16: Primer predloga uvedbe kontrol z vplivom na čas obnovitve

Sredstvo: Strežnik 1	
Predlog uvedbe dodatnih kontrol	
K4 Podvojevanje vira ***K12*** Rezervna oprema na dosegu ***K14*** Načrt obnovitve sredstva	
Čas obnovitve funkcionalnosti vira po uresničitvi grožnje	4 ure

Vir: Avtor.

Z uvedbo tega predloga bi torej lahko skrajšali čas izpada ob uresničitvi grožnje na štiri ure in potencialno škodo na 105.000 Eur, kot je razvidno iz slike 19. Pri nespremenjeni verjetnosti uresničitve grožnje 1/leto to predstavlja tveganje v višini 105.000 Eur/leto.

8.2 Izbor ukrepov obravnave tveganj

Izdelane predloge, ki vsebujejo opis potrebnih aktivnosti za uvedbo kontrol ter ocenjen vpliv na zmanjšanje tveganja, je nato potrebno obravnavati in izbrati najučinkovitejše. Podrobneje so nekatere aktivnosti izbora predstavljene v poglavju 9, ki govori o ekonomika naložb v informacijsko varnost.

Končni rezultat obravnave tveganj so akcijski načrti za zagotavljanje primernega in učinkovitega nivoja varovanja glede na oceno tveganj ter kriterije sprejemljivosti tveganj.

9 EKONOMIKA NALOŽB V INFORMACIJSKO VARNOST

Za organizacije kot osnovne nosilce odločitev o naložbah le-te predstavljajo odločujoč element v njihovem razvoju in rasti. Sprejete dolgoročne odločitve danes bistveno opredeljujejo pogoje gospodarjenja v prihodnje in s tem uspešno ali neuspešno gospodarjenje. Zato so naložbene odločitve med najbolj

pomembnimi poslovnimi odločitvami, ki jih sprejemajo organizacije (Stepko, 1980, str. 2).

Informacije so temelj za sprejemanje pomembnih poslovnih odločitev. Zaposleni v organizacijah uporabljajo informacije v pomoč pri odločanju, tako da se lahko odločajo bolje, kot bi se, če teh informacij ne bi posedovali.

Vodstvo na višjih ravneh odloča o zadevah, ki imajo dolgoročne posledice na donosnost, medtem ko se vodja na nižjih nivojih odloča o operativnih zadevah, ki imajo vpliv na vsakodnevno poslovanje. V obeh primerih je vrednost informacij razlika med neto koristmi (koristmi, zmanjšanimi za stroške) odločitev, sprejetih na podlagi dodatnih informacij za zmanjševanje negotovosti, in koristmi odločitev, ki so sprejete brez teh informacij. To je eden od razlogov, da morajo biti informacije kakovostne. Zagotoviti morajo zanesljivo presojo uspešnosti poslovanja in omogočiti, da bodo aktivnosti, ki bodo temeljile na teh informacijah, logične in dolgoročno ekonomsko učinkovite (Tekavčič v Možina et al, 2002, str. 665).

S predstavljenim povečevanjem groženj na področju informacijske varnosti ter povečevanjem sredstev, ki jih organizacije posledično namenjajo za naložbe na tem področju, se povečuje tudi pritisk oseb, odgovornih za naložbe, po dodatnih informacijah, ki bi zmanjševale negotovost glede njihovih donosov.

Drugo pomembno dejstvo, ki se ga moramo zavedati pri sprejemanju naložbenih odločitev je, da gre praviloma vedno za omejena finančna sredstva, ki so lahko namenjena za naložbe. V primerih izbire med alternativnimi naložbenimi možnostmi pri omejenih finančnih sredstvih je izredno važno, da je mogoča medsebojna primerljivost različnih naložb. Temu pogoju mora zadostiti tudi metoda ali merilo, na osnovi katere ocenjujemo uspešnost različnih naložbenih možnosti (Stepko, 1980, str. 3). V nadaljevanju bodo predstavljene nekatere metode, ki predstavljajo podlago za zmanjševanje negotovosti glede vrednosti in primerljivosti potencialnih naložbenih možnosti oziroma učinkovite uporabe virov organizacije. Metode lahko različno ocenijo isto naložbeno možnost med več potencialnimi možnimi glede na lastnosti metode, kar pomeni, da vse metode in merila ne morejo imeti enake uporabne vrednosti. Vendar je pravilno izbrano merilo prvi indikator, ki kaže zaželenost določene naložbe. Merilo in metoda sta lahko pravilno izbrana le z zavedanjem njegovih lastnosti in omejitev uporabnosti.

Preden lahko ocenjujemo naložbene možnosti je potrebno vsaki od njih opredeliti njene osnovne značilnosti – denarne tokove v posameznih časovnih obdobjih. V nadaljnjih dveh poglavjih so le-ti opredeljeni, in sicer v okviru identifikacije

stroškov kot negativnih denarnih tokov ter identifikacije koristi kot pozitivnih denarnih tokov.

Identifikacija stroškov naložbe

Stroški uvedbe kontrol na področju informacijske varnosti vključujejo začetne stroške vzpostavitve in tekoče stroške vzdrževanja kontrol. Stroški lahko izhajajo iz podobnih kategorij kot stroški uvedbe IT tehnologij, in sicer:

- strojna oprema,
- programska oprema,
- podpora uporabnikom,
- IT podpora,
- ostalo.

Pomembno je, da identificiramo vse povezane stroške, tako neposredne kot posredne. Slednji se v večini primerov realizirajo kot strošek zmanjšane produktivnosti zaradi časa, potrebnega za priučitev zaposlenih na spremembo (Curley, 2002, str. 62). Uvajanje kontrol ima pogosto posledice, ki se odražajo v zmanjšani produktivnosti uporabnika, še posebno kadar se kontrole uvajajo na pristopnih točkah informacijskih sistemov. Če dejansko pride do zmanjševanja uporabnikove produktivnosti, moramo te posledice upoštevati kot posredni strošek uvedbe kontrol.

9.1.1 Celotni stroški lastništva

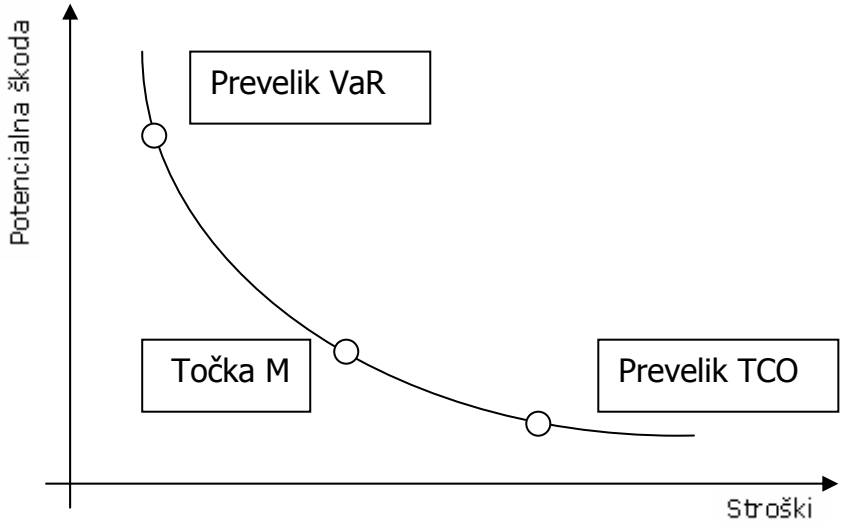
Koncept celotnih stroškov lastništva (ang. total cost of ownership, v nadaljevanju TCO) je bil s strani institucije Gartner Group uveden v osemdesetih letih prejšnjega stoletja, ko so podjetja imela težave pri razumevanju stroškov, povezanih z uporabo informacijskih tehnologij. TCO je sistem merjenja ter oblika pristopa k upravljanju in zmanjševanju stroškov. Dejansko je prav ta pristop pokazal na vzdrževalni del kot na del rešitve, ki ima največji prispevek k stroškom rešitev in pripomogel k iniciativam po poenotenju oziroma konsolidaciji rešitev z namenom znižanja stroškov organizacije.

Za manjša in srednje velika podjetja ima izračun TCO rešitve še drug pomen. Pri njih ima velikost naložbe in časovna razporeditev denarnih tokov naložbe velik vpliv ob odločanju, saj jim je težko rezervirati ali pridobiti ustrezna sredstva za večje naložbe, ne glede na potencialne velike koristi večje naložbe za podjetje (Bradbury, 2005). Višina TCO je torej lahko kriterij izbora predlogov uvedbe kontrol sam po sebi – ali zaradi omejitev finančnih virov organizacije ali kot dodatni kriterij pri predlogih s podobnimi vrednostmi analiz stroškov s ciljem izbora stroškovno ugodnejših.

Tipično TCO analiza rešitve zavzema pregled treh ključnih področij, in sicer: v rešitev vključeni ljudje, procesi in tehnologije. Druga delitev stroškov je po času nastanka, in sicer na stroške vzpostavitve ter na stroške vzdrževanja rešitve. Vrednost TCO je vsota identificiranih stroškov v celotni predvideni življenjski dobi rešitve.

Čeprav je cilj uporabe koncepta TCO čim nižji strošek rešitve, ima svoje omejitve. Profesor Paul Tallon iz Boston College je to prikazal s povezavo s konceptom VaR (ang. value at risk). VaR v našem primeru predstavlja potencialno škodo v primeru uresničitve grožnje informacijskemu viru. Tallon zagovarja, da lahko nizke vrednosti TCO vodijo k izredno velikim ter nesprejemljivim vrednostim VaR in tudi obratno. Povezava med Var in TCO je prikazana na sliki 24.

Slika 24: Povezava med TCO in VaR



Vir: Curley, 2001, str. 65.

V primeru zagotavljanja varovanja informacij imamo lahko v eni skrajnosti preveliko vrednost VaR, ko smo z namenom zmanjševanja TCO nesprejemljivo zmanjševali tudi sposobnost varovalnih ukrepov. Na drugi strani smo v želji po zmanjševanju VaR poiskali rešitev, ki ima nesprejemljivo ceno oziroma TCO, ki ne upravičuje zmanjšanja tveganj. Namen usklajevanja sprejemljivih vrednosti VaR in TCO je poiskati rešitev, ki je čim bližje točki M, saj naj podjetje ne bi namenjalo več sredstev za varovanje (TCO), kot so vredna varovana sredstva (VaR).

Ocena TCO, na osnovi v tabeli 13 podanega predloga uvedbe kontrole, je prikazana v spodnji tabeli in povzema potrebne aktivnosti za izvedbo kontrole ter oceno stroškov teh aktivnosti.

Tabela 17: Primer TCO izračuna uvedbe kontrole

Kategorija stroška	Opis stroška	Začetni strošek	Tekoči stroški
Strojna oprema	Nabava novega strežnika	5.000 Eur	-
Programska oprema	Licence dodatne programske opreme	10.000 Eur	3.000 Eur
IT podpora	Namestitev in konfiguracija	3.000 Eur	-
IT podpora	Izdelava načrta obnovitve sredstva	10.000 Eur	-
IT podpora	Vzdrževanje načrta obnovitve sredstva	-	1.000 Eur/leto
IT podpora	Vzdrževanje strežnika	-	4.000 Eur/leto
Ostalo	Stroški infrastrukturnih storitev	-	1.000 Eur/leto
Skupaj		28.000 Eur	9.000 Eur/leto

Vir: Avtor.

TCO obravnavanega primera uvedbe kontrole predstavljajo začetni stroški v višini 28.000 Eur ter tekoči letni stroški za potrebe vzdrževanja uvedene kontrole v višini 9.000 Eur na leto. Ti stroški predstavljajo negativni denarni tok naložbe v uvedbo kontrole.

9.2 Identifikacija koristi naložbe

Identifikacija koristi naložb v informacijsko varnost je do javne predstavitve izračuna pričakovane letne izgube predstavljala trd oreh vsem, ki so koristi poskušali kvantitativno opredeliti. Danes je izračun koristi tako preprost, kot je izračun razlike potencialne škode uresničitve grožnje pred uvedbo kontrole in po tem.

Predstavljeni izračun koristi temelji na osnovi podatkov primera grožnje izpada Strežnika 1 pred uvedbo kontrole v tabeli 16 ter po uvedbi predloga uvedbe kontrol, predstavljenega na strani 53.

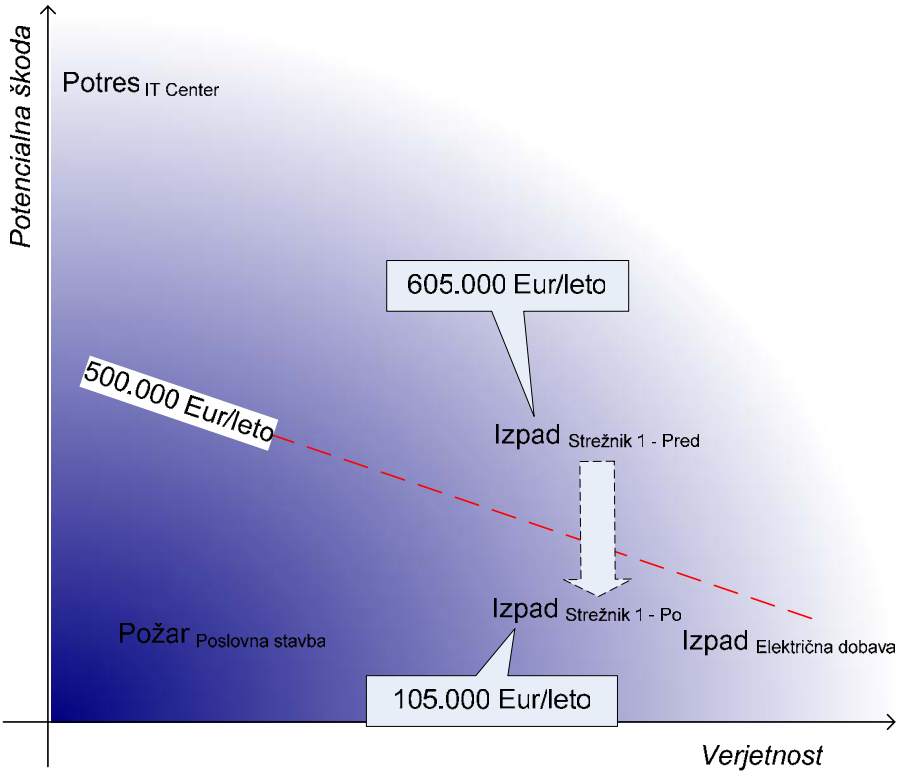
Tabela 18: Primer izračuna koristi uvedbe kontrole

Grožnja: Izpad Strežnik 1	**Verjetnost uresničitve grožnje**	**Potencialna škoda**	**Tveganje**
Pred uvedbo predloga kontrole	1/leto	605.000 Eur	605.000 Eur/leto
Po uvedbi predloga kontrole	1/leto	105.000 Eur	105.000 Eur/leto
Koristi		500.000 Eur	500.000 Eur/leto

Vir: Avtor.

Korist zmanjšanja tveganja se na profilu tveganj odrazi, kot je predstavljeno na sliki 25, kjer je izpostavljeno zmanjšanje tveganja izpada Strežnika 1 in povezano znižanje pozicije tveganja po uvedbi predloga kontrol. Razvidno je tudi, da bi glede na trenutno zadano mejo sprejemljivosti tveganj zadostovalo že manjše znižanje, kot izhaja iz predloga uvedbe kontrole, podanega kot primer.

Slika 25: Primer koristi kontrole oziroma zmanjšanja tveganja



Vir: Avtor.

Vsota koristi kot razlike v pričakovani letni izgubi predstavlja pol milijona evrov na leto in predstavlja pozitivni denarni tok naložbe v uvedbo kontrole.

9.3 Metode ocenjevanja naložb

V nadaljevanju bom izvedel primere ocenjevanja naložbe z uporabo nekaterih najbolj pogosto uporabljanih metod. Namen je ugotoviti uspešnost naložbe v smislu njene ekonomičnosti.

Ekonomičnost opredelimo z razmerjem med ustvarjeno količino poslovnih učinkov in zanjo potrebnimi stroški ali z ustreznim recipročnim kazalnikom (Tekavčič v Možina, 2002, str. 669). Kazalniki so relativna števila, ki jih dobimo s primerjavo dveh velikosti. Lahko so indeksi, koeficienti ali deleži. Razlikovati jih moramo od kazalcev, ki so širši pojem, saj vključujejo tudi informacije o poslovanju, ki so izražene absolutno (Tekavčič v Možina, 2002, str. 666). Primer kazalcev v našem primeru predstavljata izračun TCO in izračun koristi v predhodnih dveh poglavjih.

Obstajajo različne metode ocenjevanja naložb. Vsaka od njih ima svoje prednosti in slabosti, glede na vidik, s katerega ocenjuje naložbo. Posledično je težko najti univerzalno, ki bi vedno dajala najboljši rezultat ocene. V posameznih organizacijah se uporabljajo različne kombinacije le-teh, izbira pa je stvar politike organizacije in lastnosti procesa odločanja. V poglavju so podani primeri uporabe nekaterih najpogosteje uporabljanih metod.

Pri tem bom predvidel dve omejitvi, znotraj katerih bom proučeval ekonomičnost naložb. Prva omejitev so pogoji gotovosti, kar pomeni, da bodo vse posledice naložbe nastopile z gotovostjo v enakem obsegu, kot so bile predvidene. Nadalje bomo predpostavili, da je cilj, ki ga zasledujemo, z naložbo doseči čim večjo donosnost. Kot donosnost pojmujemo ustvarjeno količino poslovnih učinkov, zmanjšano za vse stroške razen za amortizacijo.

Pomembna razlika med metodami je upoštevanje časa kot bistvene komponente vsake naložbe. Glede na to, ali metode pravilno vključujejo časovno komponento ali ne, bi jih lahko razdelili na dve skupini, to je na statične, ki ne upoštevajo časovne komponente, in dinamične, ki jo upoštevajo. V nadaljevanju najprej obravnavamo naložbo z uporabo statičnih metod.

9.3.1 Doba vračanja

Doba vračanja (ang. payback period) je definirana kot tisto obdobje, ki je potrebno, da se stroški naložbe povrnejo z donosi. Enačba za izračun je sledeča:

$$DP = ŠLPP + (PP / CFi) \quad [1]$$

Kjer je:

DP = Doba vračanja
ŠLPP = Število let pred popolnim povračilom
PP = Preostanek do povračila
CF = Neto denarni tok v danem letu
i = Leto poplačila

Doba vračanja daje informacijo o tem, koliko časa bo trajalo, da se naložena sredstva povrnejo in so torej na nek način »vezana«. Iz tega sledi, da je zaželena čim krajša doba, ki predstavlja večjo likvidnost sredstev. Dodatno velja, da ker so običajno ocene denarnih tokov v bolj oddaljeni prihodnosti manj predvidljive, daljša doba povračila predstavlja tudi večjo tveganost naložbe.

V našem primeru, kjer koristi že v prvem letu presežejo stroške naložbe, lahko dobo povračila izračunamo iz razmerja med začetnimi stroški in denarnim tokom v prvem letu. Povračilna doba torej znaša 0,057 leta oziroma enaindvajset dni.

Prednost metode je, da lahko do določene mere sklepamo o tveganosti in likvidnosti naložbe.

Pomanjkljivosti in slabosti metode, ki so sicer skupne vsem statičnim metodam ocenjevanja naložb, so:

- največkrat ne upoštevajo skupnih donosov naložbe, kar pomeni, da zanemarijo tudi življenjsko dobo naložbe,
- ne upoštevajo časovne razporeditve donosov in stroškov naložbe ter
- ne vključujejo pravilno časovnega horizonta pri ocenjevanju uspešnosti naložb.

Navedene pomanjkljivosti imajo za posledico, da statične metode ocenjevanja naložbe ne upoštevajo alternativne uporabe omejeno razpoložljivih finančnih sredstev in zato pri izbiri med različnimi naložbenimi možnostmi odpovedo (Stepko, 1980, str. 13).

9.3.2 Metode sedanje vrednosti

Iz navedenih slabosti statičnih metod ocenjevanja naložb sledi, da je potrebno rešiti dva problema, in sicer, da upoštevamo različne časovne razporede stroškov naložbe in njenih donosov ter da upoštevamo celotno življenjsko dobo naložbe.

Problem primerljivosti časovno različno razporejenih denarnih tokov naložbe rešujemo s pomočjo metode sedanje vrednosti, ki predstavlja reduciranje vseh denarnih tokov na začetni termin, to je na začetek obdobja, ko nastopijo prvi stroški naložbe. Na osnovi te metode je ekonomska teorija izoblikovala dve metodi oziroma dva kriterija za sprejemanje naložbenih odločitev, in sicer neto sedanjo vrednost in notranjo stopnjo donosnosti (Stepko, 1980, str. 14).

9.3.2.1 Neto sedanja vrednost

Neto sedanja vrednost (v nadaljevanju NSV) odraža absolutno vrednost koristi v sedanjosti in prikazuje vrednost diskontiranih prihodnjih denarnih tokov (ang. discounted cash flow). Za uporabo tehnike moramo ugotoviti sedanjo vrednost vseh denarnih tokov, jih zmanjšati za ustrezni diskont glede na leto nastanka denarnega toka, ter jih sešteti. Enačba izračuna NSV je naslednja:

$$NSV = CF0 + CF1/(1-r) + CF2/(1-r)^2 + . \qquad [2].$$

Kjer je:

NSV = Neto sedanja vrednost

CF0, CF1, .. = Neto denarni tok v letošnjem letu, v naslednjem letu,..

r = faktor diskonta denarnih tokov v prihodnosti in predstavlja ceno kapitala

Neto denarni tok predstavlja razlika med donosi in stroški naložbe, torej med pozitivnimi in negativnimi denarnimi tokovi. Pozitivna NSV je znesek, za katerega je sedanja vrednost donosov naložbe večja od sedanje vrednosti stroškov naložbe. Če teh denarnih tokov ne bi diskontirali na sedanjost, to je izrazili v sedanji vrednosti, ti zneski ne bi bili primerljivi. Zaradi časovne vrednosti denarja le-ta nima enake vrednosti glede na obdobje realizacije denarnih tokov. Zato je po tem kriteriju sedanja vrednost časovno bližjih denarnih tokov večja od sedanje vrednosti enakih, a časovno bolj oddaljenih denarnih tokov. Poleg časovne razporeditve denarnih tokov pa metoda upošteva tudi denarne tokove v celotnem življenjskem obdobju naložbe.

Predpostavljeni faktor diskonta denarnih tokov, ki bo uporabljen v izračunih za ponazoritev primera ocenjevanja naložbe, je 0,1 oziroma 10 odstotkov. Primer

izračuna za naš primer uvedbe kontrole temelji na v tabelah 17 in 18 predstavljenih podatkih o predvidenih stroških in koristih.

Primer izračuna neto denarnega toka v trenutku naložbe je:

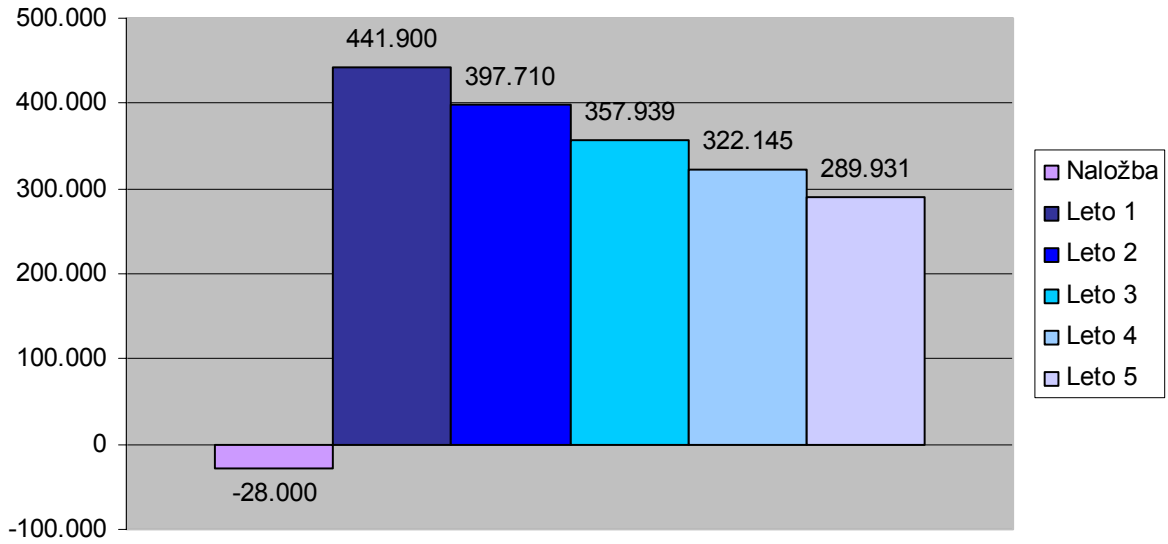
CF0 = Korist - Začetni strošek naložbe
= 0 - 28.000 Eur
= - 28.000 Eur

Ob zaključkih naslednjih let je izračun neto denarnih tokov naslednji:

CF1, CF2, CF3, CF4, CF5 = (Korist v danem letu – Tekoči stroški kontrole) x $(1 - \text{diskont})^{\text{leto}}$
= (500.000 Eur/leto – 9.000 Eur) x $0{,}9^{\text{leto}}$
= 491.000 Eur/leto x $0{,}9^{\text{leto}}$

Grafični prikaz neto denarnih tokov, zmanjšanih s faktorjem diskonta je predstavljen na sliki 27.

Slika 26: Primer neto denarnih tokov naložbe, zmanjšanih za faktor diskonta



Vir: Avtor.

Izračun NSV predstavlja seštevek za faktor diskonta zmanjšanih neto denarnih tokov naložbe, ki v obdobju petih let znaša okvirno 1,78 milijonov Eur.

Pozitivna vrednost NSV predstavlja doprinos naložbe, zmanjšan za vrednost diskonta, ki predstavlja ceno kapitala. Potencialna slabost metode je, da ne

prikaže velikostnega razreda naložbe in da izkazuje enako vrednost za naložbe, ki so različno občutljive na negotovost pozitivnih denarnih tokov.

9.3.2.2 Indeks donosnosti

Kadar izbiramo med naložbami, ki imajo različno življenjsko dobo in zahtevajo različne naložbene stroške, tedaj NSV niso primerljive. V takem primeru si pomagamo z indeksom donosnosti, ki namesto razlike med sedanjimi vrednostmi donosov in stroškov, obravnava razmerje med obema. Izračunamo ga kot razmerje med vsoto sedanjih vrednosti donosov oziroma koristi in vsoto sedanjih vrednosti stroškov. Enačba je torej naslednja:

$$\text{Indeks donosnosti} = \frac{\text{Sedanja vrednost donosov}}{\text{Sedanja vrednost stroškov}} \qquad [3]$$

Razmerje mora biti večje od 1, da bi bila naložba sprejemljiva. Zaželen je čim večji odstotek, ki ponazarja veliko donosnost in bi torej med dvema naložbama bila izbrana tista z večjim indeksom donosnosti.

Podatki o diskontiranih denarnih tokovih, uporabljenih za izvedbo primera ocene naložbe so navedeni v tabeli 19 in temeljijo na v tabelah 17 in 18 predstavljenih podatkih o predvidenih stroških in koristih.

Tabela 19: Primer diskontiranih denarnih tokov

Čas	Naložba	Leto 1	Leto 2	Leto 3	Leto 4	Leto 5
Diskontirani stroški	28.000 Eur	8.100 Eur	7.290 Eur	6.561 Eur	5.905 Eur	5.314 Eur
Diskontirani donosi	0 Eur	450.000 Eur	405.000 Eur	364.500 Eur	328.050 Eur	295.245 Eur

Vir: Avtor.

Vsota diskontiranih stroškov, ki predstavlja njihovo sedanjo vrednost, znaša 61.170 Eur, vsota diskontiranih donosov, ki predstavlja njihovo sedanjo vrednost, pa 1.842.795 Eur. Na tej osnovi izračunamo indeks donosnosti, ki za naš primer znaša preko 3000 odstotkov oziroma tridesetkratno povrnitev vloženih sredstev v naložbo.

Slabost te tehnike je predvsem, da nudi drugačne zaključke kot NPV, kadar gre za velike razlike v obsegu naložbe pri medsebojno izključujočih naložbah.

9.3.2.3 Notranja stopnja donosnosti

Alternativno uporabo koncepta NSV predstavlja notranja stopnja donosnosti (ang. internal rate of return – v nadaljevanju IRR). Definirana je kot stopnja diskonta r, pri kateri je sedanja vrednost pričakovanih denarnih tokov enaka sedanji vrednosti stroškov naložbe, oziroma z drugimi besedami, ko je NSV naložbe enaka nič. Razlika med NSV in IRR je, da uporablja prva od posamezne naložbene možnosti povsem neodvisno diskontno stopnjo, enako za vse naložbene možnosti, druga pa diskontne stopnje sploh ne pozna in jo na podlagi podatkov konkretne možnosti šele ugotavlja.

Namen tehnike je izračun pričakovane donosnosti naložbe, hkrati pa tudi ugotovimo mejo cene kapitala, pri kateri je naložba še upravičena. Sprejetje odločitve o naložbi, katere donosnost je večja od cene kapitala, bo povečala vrednost delničarjem. IRR izračunamo na osnovi sledeče enačbe:

$$0 = NSV = CF0 + CF1/(1-r) + CF2/(1-r)^2 + .. \quad [4]$$

Rešitev za IRR iščemo s poskušanjem ali z uporabo ustreznih orodij, kot je denimo Microsoft Excel. V našem primeru je razlika med ocenjenimi stroški naložbe in stroškov vzdrževanja ter ocenjenimi koristmi zelo velika, tako da izračunani IRR predstavlja več kot 1500 odstotkov. To pomeni, da je v našem primeru IRR 150-krat večji od uporabljene cene kapitala. Če je IRR večji od cene kapitala, uporabljenega pri naložbi, je odločitev za naložbo z danega vidika upravičena.

Problemi in omejitve uporabe metode so, da se IRR ne izkaže, če so denarni tokovi različne velikosti in/ali ob različnih terminih. V takih primerih obstaja več rešitev enačbe. Uporaba IRR je neprimerna tudi pri medsebojno izključujočih naložbah, ki se razlikujejo po obsegu in časovni razporeditvi denarnih tokov.

9.4 Izbor uvedbe kontrol

Učinkovita raba sredstev organizacije ni mogoča brez primerljivega prikaza koristi za organizacijo tako glede posamezne naložbe kot v okviru primerjave med potencialnimi naložbami. Osnovno omejitev naložb organizacije pa seveda postavlja tudi količina sredstev, ki jih lahko nameni zanje.

V magistrski nalogi smo prikazali uporabo različnih metod ocen naložb in izračunanih kazalcev, ki so organizaciji lahko v pomoč kot kriteriji izbire:

- višina tveganja,
- stroški (TCO),
- razmerja stroškov in koristi (NSV, IRR, doba povračila, indeks donosnosti).

Potrebno je izpostaviti, da izračuni metod niso nujno zadosten kriterij za odločanje in je potrebno upoštevati tudi druge morebitne dejavnike, kot so denimo regulatorne zahteve, zakonodaja in podobno.

Izbor uvedbe kontrol med predlogi zniževanja tveganj, ki je odvisen od ocene tveganj in ocene potrebnih naložb za njihova zmanjševanja, bo temeljil na izboru naložb, ki jih organizacija lahko financira glede na razpoložljiva in dosegljiva sredstva in ki najbolj ekonomično zmanjšujejo tveganja na sprejemljivo raven. Na tej osnovi lahko tudi določimo vrstni red uvedbe izbranih predlogov kontrol in dosego cilja zmanjševanja tveganj. Nadalje lahko merimo dejansko uresničevanje in vpliv groženj s spremljanjem škodnih dogodkov in primerjamo razliko glede na prvotno stanje.

10 ZAKLJUČEK

V preteklosti so bili predlogi in uvedbe kontrol velikokrat sprejeti in financirani na podlagi uspešnosti neformalnega prepričevanja odgovornih za varnost ter običajno tudi povezanega stanja v okolju, denimo uresničenja grožnje virom organizacije ali v okolici. Lažje je bilo pridobivanje sredstev za naložbe v varnost po okužbi z virusom kot pa preventivno pred škodnim dogodkom, čeprav je jasno, da bi imela naložba največjo korist ravno v primeru preventivno uvedenih kontrol. Nekoliko manj učinkovit je bil pristop, ki temelji na osnovi razširjanja strahu, negotovosti in dvoma in je med strokovnjaki pridobil poimenovanje FUD (okrajšava za ang. fear, uncertainty, doubt). Zagotovo pa ta dva načina pridobivanja sredstev za naložbe nista v dolgoročnem interesu ne strokovnjakov ne upravljavcev in lastnikov organizacij.

Danes težnja k učinkoviti uporabi sredstev ter upravljanju tveganj organizacij vodi k uporabi kvantitativnih analiz stroškov in koristi naložb. Podpora naložbam brez primerljivega prikaza koristi za organizacijo bo postajala vse redkejši primer.

Čeprav je področje ekonomike informacijske varnosti še mlado, pa že nudi nekatere tehnike in metode, ki omogočajo analize teh naložb ter posledično njihovo primerjavo na nivoju vseh naložb, med katerimi se organizacija odloča v skladu s svojimi strateškimi usmeritvami. Z razvojem tehnik in razširjanjem njihove uporabe lahko pričakujemo boljše razumevanje tega vidika poslovanja organizacij in izboljšano podlago za odločanje glede naložb v informacijsko varnost.

V okviru naloge sem v prvem delu, to je poglavjih 2 in 3, predstavil področja upravljanja tveganj in informacijske varnosti ter njun okvir. Predstavljeni so bili

osnovni elementi ter izpostavljeni ekonomski vidiki obeh področij, zaradi katerih organizacije vzpostavljajo ustrezne procese upravljanja. V poglavju 3 sem obsežneje predstavil informacijsko varnost kot naraščajočo prioriteto v organizacijah, ter posledičen porast naložb v to področje.

Te ugotovitve predstavljajo temelj, na osnovi katerega je opredeljena problematika, ki je predmet obravnave v praktičnem delu naloge. V poglavjih 4 do 7 je izveden konkreten primer metodologije analize tveganj, ki temelji na kvatifikaciranih ocenah, le-te pa predstavljajo osnovo za primerljiv prikaz koristi za organizacijo tako glede posamezne naložbe kot v okviru primerjave med potencialnimi naložbami. Poglavje 8 predstavlja fazo obravnave tveganj, katere sestavni del je analiza stroškov in koristi naložb, ki zmanjšujejo tveganja.

V poglavju 9 so predstavljene nekatere metode analize stroškov in koristi naložb v informacijsko varnost ter izveden primer njihove uporabe. S tem je dosežen namen praktičnega dela naloge, to je izvedba načina izračuna donosnosti naložb v informacijsko varnost ter iz tega izhajajoči cilji.

LITERATURA

1. Andersen Arthur: Operational Risk and Financial Institutions. London: Risk Publications, 1998. 187 str.

2. Anderson Ross, Moore Tyler: The Economics of Information Security. Science Magazine, 314 (2006), str. 610-613

3. Berinato Scott: Finally, a real return on security spending. [URL http://www.cio.com/archive/021502/security.html], 1.2.2007.

4. Bradbury Danny: Short-term planning drives IT purchases for SMEs. [URL http://www.silicon.com/research/specialreports/sme/0,3800004380,39128565,00.htm], 20.2.2007.

5. Brigham Eugene F., Houston Joel F.: Fundamentals of financial managament 10th ed. USA:Thomson/South Western, 2004, 831 str.

6. Briney Andy: 2001 Industry Survey, Information security magazine. [URL: http://infosecuritymag.com/articles/october01/images/survey.pdf], 22.2.2007.

7. Curley Martin G.: Managing information technology for business value. USA:Intel Press 2004, 350 str.

8. de Sutter Jan: The Power of IT – Survival Guide. North Charleston: Booksurge Publishing, 2004, 508 str.

9. Devaraj Sarv, Kohli Rajiv: The IT payoff. Upper Saddle River: FT Prentice Hall, 2002, 160 str.

10. Epstein Marc J., Rejc Adriana: Measuring the payofs of IT investments- [URL: http://www.managementmag.com/index.cfm/ci_id/2443/la_id/1], 22.2.2007.

11. Gornik Rado: Upravljanje operativnih tveganj v informatiziranih bankah – magistrsko delo. Maribor: Ekonomsko poslovna fakulteta, 2004, 119 str.

12. Gradišar Miro, Resinovič Gortan: Informatika v poslovnem okolju, 1. natis. Ljubljana: Ekonomska fakulteta, 2001, 508 str.

13. Grilj Matej: Varnost in tehnološka zaščita informacijskega sistema v banki – magistrsko delo. Ljubljana: Ekonomska fakulteta, 2003, 90 str.

14. Holton Glyn A.: Defining Risk. Financial Analysts Journal, 60 (2004), 6, str. 19–25

15. Kovacich Gerald D.: The Information Systems Security Officer's Guide. Burlington: Elsevier Science, 2003, 288 str.

16. Kralj Irena: Upravljanje z operativnimi tveganji v bankah – diplomsko delo., Ljubljana: Ekonomska fakulteta, 2005, 43 str.

17. Mihelčič Miran: Ekonomika poslovanja za inženirje. Ljubljana: Založba FE in FRI, 1997, 370 str.

18. Mohorčič Zobec Nataša: Notranje revidiranje operativnih tveganj v bankah. Ljubljana: ZBS, 2007, 57 str.

19. Možina Stane [et al]: Management, nova znanja za uspeh. Radovljica: Didakta, 2002, 872 str.

20. Patru Primož [et al]: Ukrepi v primeru informacijskih nesreč. Šempeter pri Gorici: Inštitut za informacijsko varnost, 2003, 148 str.

21. Potočnik Mark: Presojanje dologoročne naložbe podjetja – diplomsko delo. Ljubljana: Ekonomska fakulteta, 2005, 42 str.

22. Rebernik Miroslav: Ekonomika podjetja – 3. dopolnjena izdaja. Ljubljana: Gospodarski vestnik, 1997, 445 str.

23. Samuelson Paul A., Nordhaus William: Ekonomija – 14. izdanje. Zagreb: MATE, 1992, 784 str.

24. Slak Leon: Obvladovanje tveganj v bančnem poslovanju po novem kapitalskem sporazumu Basel II – magistrsko delo. Maribor: Fakulteta za podiplomske državne in evropske študije, 2005, 135 str.

25. Stepko Draga: Ekonomika naložb. Ljubljana: Ekonomska fakulteta Borisa Kidriča v Ljubljani, 1980, 74 str.

26. Tipton Harold F., Krause Micki: Information Security Management Handbook 5th Edition. Boca Ranton: Auerbach Publications 2004, 2036 str.

27. Turban Efraim [et al]: Information Technology for Management, 2nd Ed. USA: John Wiley & Sons, 1999, 700 str.

28. Vidic Andrej: Helios d.d.: Opis tveganj in načinov upravljanja z njimi – diplomsko delo. Ljubljana: Ekonomska fakulteta, 2001, 44.str.

VIRI

29. Basel Comitee on Banking Supervision: Sound Practices for the Management and Supervision of Operational Risk. Basel: BSI, 2003, 14 str. [URL http://www.bis.org/publ/bcbs96.pdf], 19.1.2007.

30. Basel Comitee on Banking Supervision, The Joint Forum: High level principles for business continuity. Basel: BIS, 2004, 38 str.

31. Deloitte [et al]: 2006 Global Security Survey. [URL: http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_2006%20Global%20Security%20Survey_2006-06-13.pdf], 12.12.2006.

32. Gartner Research: Management Update - The Future of Enterprise Security. 2004, 12 str.

33. Gartner Research: The Price of Information Security – Management Summary. 2001, 50 str.

34. IRM: Risk Management Standard. [URL: http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf], 15.1.2007.

35. Islovar. [http://islovar.org], 9.3.2007.

36. ISO 17799:2005 Information technology – Security techniques – Code of practice for information security management. Geneva:ISO/IEC, 2005, 115 str.

37. ISO 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. Geneva:ISO/IEC, 2005, 34 str.

38. ISO Guide 73:2002 Risk management - Vocabulary – Guidelines for use in standards. Geneva:ISO/IEC, 2002, 16 str.

39. ITGI: CobiT 4.0. Rolling Meadows, USA: ITGI, 2005, 194 str.

40. ITGI [et al].: Aligning CobiT, ITIL and ISO 17799 for Business Benefit. Rolling Meadows, USA: ITGI, 2005, 62 str.

41. itSMF: An Introductory Overview of ITIL, Version 2.0. Workingham, UK: itSMF, 2004, 40 str.

42. Metodologija analize informacijskih sistemov verzija 4.1. Ljubljana: SRC.SI, 2007, 40 str.

43. Metodologija analize tveganj verzija 3.3. Ljubljana: SRC.SI, 2006, 27 str.

44. Metodologija ocenjevanja in obravnave informacijskih tveganj v bankah verzija 2.0. Ljubljana: ZBS, 2006, 83. str.

45. Metodologija upravljanja neprekinjenega poslovanja verzija 3.0. Ljubljana: SRC.SI, 2006, 64 str.

46. PriceWaterhouseCoopers: Information security breaches survey 2002. [URL: http://www.security-survey.gov.uk], 20.2.2007.

47. PriceWaterhouseCoopers: Information security breaches survey 2004 – Executive summary. [URL: http://www.security-survey.gov.uk], 20.2.2007.

48. PriceWaterhouseCoopers: Information security breaches survey 2004 – Technical report. [URL: http://www.security-survey.gov.uk], 20.2.2007.

49. PriceWaterhouseCoopers: The Global State of Information Security. [URL: http://www.pwc.com/extweb/pwcpublications.nsf/docid/3929AC0E90BDB001852571ED0071630B], 20.2.2007.

50. Return on Investment in Information Security. [URL http://www.oict.nsw.gov.au/content/7.1.15.ROSI.asp], 17.1.2007.

SLOVAR

Tuji (angleški) izraz	Slovenski prevod
Act	Ukrepaj
Annualized loss expectancy (ALE)	Pričakovana letna izguba
Asset and liability management (ALM)	Upravljanje z bilanco banke
Baseline approach	Pristop osnovnih zahtev
Check	Preveri
Commercial Computer Security Center (CCSC)	Center za komercialno računalniško varnost
Cost of doing business	Strošek poslovanja
Disaster recovery (DR)	Okrevanje po katastrofi
Discounted cash flow (DCF)	Diskontirani denarni tokovi
Do	Izvedi
Exposure	Izpostavljenost
Information assurance	Varnost informacijskih sistemov
Information technology (IT)	Informacijska tehnologija
Internal rate of return (IRR)	Notranja stopnja donosnosti
International Standards Organization (ISO)	Mednarodna organizacija za standarde

IT governance	Upravljanje IT
IT related risk	IT tveganje
IT Service Management	Upravljanje IT storitev
Mappings	Matrike povezav
Network externalities	Mrežne eksternalije
Non-interference	Nevmešavanje
Non-repudiation	Preprečevanje ne-priznavanja
Parkerian hexad	Parkerjeva šesterica
Payback period	Doba povračila
Plan	Načrtuj
Primitive	Osnovno
Residual	Preostanek
Return on investment (ROI)	Donosnost naložbe
Risk management	Upravljanje tveganj Uravnavanje tveganj Obvladovanje tveganj
Single point of failure (SPoF)	Edina točka izpada
Stakeholders	Deležniki

Total cost of ownership (TCO)	Celotni stroški lastništva
UK Department of Trade and Industry (UK DTI)	Ministrstvo za trgovino in industrijo Velike Britanije
Value at risk (Var)	Potencialna škoda tveganja