Univerza v Ljubljani
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VLOGA INFORMATIKE PRI ZAGOTAVLJANJU NEPREKINJENEGA POSLOVANJA V SLOVENSKIH PODJETJIH

Ljubljana, oktober 2006 Borut Žnidar

IZJAVA

Študent Borut Žnidar izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom doc. dr. Aleša Groznika in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 27. oktobra 2006

Podpis:_____

Kazalo

1. Uvod

Poslovna okolja v današnjem svetu vse bolj zaznamujejo hitre in nepredvidljive spremembe. Te so lahko pozitivne, če prinašajo nove poslovne priložnosti, ali negativne v primeru nepredvidenih problemov ali ogrožanja poslovanja. Ne glede na predznak teh sprememb mora management podjetja zagotoviti pravočasen in ustrezen odziv nanje. Odziv podjetja na spremembo mora na eni strani ublažiti nastalo tveganje in na drugi strani znati čim bolje izkoristiti novo nastalo poslovno priložnost.

Za zagotavljanje delovanja podjetja v primeru nepredvidljivih sprememb se uvaja program neprekinjenega poslovanja. Njegova naloga je vzdrževati minimalni nivo storitev za stranke, medtem ko se obnavlja običajno delovanje. Izkušnje so pokazale, da je reaktivno delovanje na tem področju tvegano početje. Organizacije, ki ne uspejo vzdrževati minimalnega nivoja storitev za stranke, morda ne bodo imele česa obnavljati: stranke gredo lahko h konkurenci, financiranje se preneha, ponovno preverjanje potreb po storitvi podjetja se lahko izkaže kot nepotrebno. Zato se je proaktivno delovanje uveljavilo kot prevladujoč model pri obvladovanju neprekinjenega poslovanja (Harris, 2003, str. 691-693).

Cilj neprekinjenega poslovanja podjetja je ščitenje treh področij: poslovnih funkcij za zagotavljanje storitev in produktov, kritičnih podpornih funkcij (npr. informacijske tehnologije) in podpornih funkcij na nivoju podjetja (financ, človeških virov). Informacijska tehnologija predstavlja pomemben element zaradi svoje podpore poslovanju podjetja, omogočanja konkurenčnosti poslovanja ter zagotavljanja podatkov, informacij in informacijskih sistemov za izvajanje poslovnih aktivnosti in poslovnega odločanja (Hilles et al., 2004, 1. poglavje).

Neprekinjeno poslovanje sloni na obvladovanju tveganja in informacijski varnosti. Kot tako vključuje naslednja področja: obnovitev informacijske tehnologije, zagotavljanje razpoložljivosti, programe za neprekinjeno poslovanje, usklajenost z zakonodajo ter pobude varnosti in zasebnosti (Gallagher, 2002).

Pri vpeljevanju neprekinjenega poslovanja ima informatika običajno zelo pomembno vlogo. Velikokrat se celo zgodi, da se celoten program prepusti v izvajanje informatikom, kar pa pripelje do nepopolnih rezultatov. Takrat so običajno slabo obdelana tri pomembna področja zagotavljanja neprekinjenega poslovanja: strategija, poslovni procesi in organizacija (Harris, 2003, str. 693-697, Gallagher, 2002, str. 3).

V nalogi se ukvarjam z odnosom med informatiko in managementom podjetja ter podporo slednjega pri zagotavljanju neprekinjenega poslovanja. Zanimajo me načini, kako management aktivno pritegniti k oblikovanju poslovnih zahtev,

vpeljavi in upravljanju ter preverjanju neprekinjenega poslovanja. Še posebej pa me zanimajo ta razmerja v slovenskih podjetjih in primerjava z izkušnjami v tujini.

Ugotoviti in potrditi želim kritične faktorje in njihove medsebojne odvisnosti pri uvajanju neprekinjenega poslovanja v slovenskih podjetjih. Začetni tezi, ki jih bom poskusil dokazati, sta naslednji:

1. Sodelovanje managementa pri načrtovanju, izvajanju in nadzoru bistveno vpliva na dosežen nivo neprekinjenega poslovanja in presega vlogo informatike v tem procesu,

2. Do vpeljave neprekinjenega poslovanja v slovenskih podjetjih prihaja predvsem zaradi zunanjih zahtev. Dva glavna dejavnika, ki odločilno vplivata na višji nivo neprekinjenega poslovanja v slovenskih podjetjih, sta:

    - Zakonodaja (npr. v bančništvu, zavarovalništvu, farmaciji),

    - Zahteve partnerjev zaradi poslovnih povezav z razvitimi trgi.

Namen naloge je pokazati pomembnost vzpostavitve in izvajanja programa neprekinjenega poslovanja podjetja ter opozoriti na nujnost aktivnega sodelovanja managementa in informatike pri upravljanju tega programa, saj je v nasprotnem primeru lahko vpeljava programa neuspešna.

2. Neprekinjeno poslovanje podjetja

Ekonomist Peter F. Drucker (Drucker, 1972) je kot glavno nalogo podjetja postavil preživetje in kot vodilni princip poslovne ekonomije ne povečanje dobička, temveč izogibanje izgubi. Pri uresničevanju naloge preživetja vidimo izogibanje izgubi na dveh področjih: v okviru običajnega poslovanja kot management kontrole izgube in v primeru katastrofe kot krizni management. V nalogi se osredotočam na zagotavljanje neprekinjenega poslovanja na drugem področju – ob katastrofi, incidentu, izpadu proizvodnje.

Eden od načinov nastajanja izgube v podjetju je torej izpad poslovanja. Razlogov za izpad poslovanja je lahko veliko: naravna nesreča, človeška napaka, sabotaža ali tehnična napaka. Marsikatera od njih lahko povzroči katastrofalne posledice za poslovanje podjetja. Rezultat so lahko poškodovano premoženje, prekinjen poslovni proces, izguba prihodka, konkurenčni položaj. Vse te posledice neposredno ali posredno vplivajo na poslovanje podjetja, s tem pa na njegovo finančno stanje in možno izgubo.

Kot pravi Wallace (Wallace et al., 2004), lahko katastrofo pomeni vse od izpada ključnega strežnika do naravne nesreče, ki uniči celotno poslovno enoto. Vse kar

lahko povzroči prekinitev normalnega poslovanja, lahko posledično postane tudi katastrofa. Brez skrbnega načrtovanja večina organizacij ne more preživeti večje prekinitve poslovanja.

Zato je pomembno (Fulmer, 2005), da je podjetje sposobno tudi v primeru hudih prekinitev poslovanja čim prej vzpostaviti nadzor nad dogajanjem in pričeti z obnovo poslovanja ter vzpostavitvijo delovanja kritičnih funkcij v najkrajšem času. V času izpada je največji sovražnik podjetja čas. Izgubljen čas se prevede v nezadovoljne stranke, izgubljen prihodek, kazni in še bi lahko našteval.

Tradicionalno so se podjetja pri pripravi obnove poslovanja v primeru katastrofe osredotočala na informacijsko infrastrukturo. Čeprav je le-ta zelo pomemben element pri obnovi poslovanja, pa običajno ni edini. Poskrbeti je potrebno tudi za rezervni prostor za delo, telefonske linije, prevoz, nujna finančna sredstva, ... Kritične funkcije podjetja so navadno zelo povezane z delovanjem informacijske tehnologije in je zato njeno hitro okrevanje zelo pomembno, vseeno pa imajo lahko malo vrednosti, če ne poskrbimo za širše okrevanje ključnih poslovnih procesov.

Fulmer tako priporoča, da priprava načrta neprekinjenega poslovanja vsebuje naslednje ključne korake:

- Določitev vseh računalniških sistemov, aplikacij, ljudi, opreme in zalog, potrebnih za okrevanje,
- Priprava rezervnega postopka za kritične datoteke in sisteme ter varen podatkovni podsistem na oddaljeni lokaciji,
- Določitev ene ali več rezervnih lokacij, kjer se lahko izvaja obdelava podatkov in poslovne operacije,
- Priprava učinkovite kontrole nad izvajanjem obnove,
- Določitev zunanjih sredstev in partnerjev, ki lahko pomagajo pri procesu okrevanja,
- Testiranje načrta, ki pokaže zmožnost zagotovitve zahtevanega nivoja storitve za ključne poslovne procese in obnovo poslovanja,
- Vzdrževanje načrta. Zastarel načrt je lahko slabša možnost, kot biti brez načrta.

Seveda je potrebno poudariti (Kajić, 1999, str. 401), da je na prvem mestu prioritet varovanje in reševanje človeških življenj, čemur sledi nacionalna varnost. Sledi zavarovanje in zaščita občutljivih podatkov in šele nato strojna in programska oprema.

Kot ugotavlja Claunch (Claunch, 2004), načrtovanje neprekinjenega poslovanja ni nov koncept; če bi pogledali daleč nazaj v zgodovino, bi ga našli že pri Noetovi

barki. Sicer pa je v novejšem času velika prelomnica načrtovanja neprekinjenega poslovanja leto 2000. Zaradi možnih težav z informacijskimi sistemi ob prehodu iz leta 1999 v leto 2000 se je veliko podjetij, ustanov in institucij s pomočjo pregleda, načrtovanja in testiranja pripravljalo na ta prehod. Postopki, ki so v tistem času delovali bolj kot enkratno dejanje, so dobili novo energijo ob katastrofi 11. septembra 2002 v New Yorku, ko se je uresničil eden najbolj črnih scenarijev načrtovanja neprekinjenega poslovanja. Če so postopki pred letom 2000 obravnavali večdnevni čas obnove poslovanja, so se postopki pred letom 2000 prilagodili na obnovo v urah in po septembru 2002 na minute v posebnih primerih pa je izpad celo popolnoma nesprejemljiv (npr. pri podjetjih, ki poslujejo v realnem času).

Zainteresirane stranke (angl. stakeholders) pri programu neprekinjenega poslovanja obsegajo široko množico udeležencev poslovanja podjetja, od zaposlenih in managementa do partnerjev in državnih institucij. Noakes-Fry ugotavlja (Noakes-Fry et al., 2004, str. 4-5), zainteresirane stranke pričakujejo obnovo poslovnih sistemov, če pride do problemov. Zato ni mogoče reči, da »zahteve izgledajo neizvedljive«, temveč le da »izvedba zahtev ni izvedljiva«. Zahteve in pričakovanja pritiskajo na organizacijo z vseh strani, upravljavci neprekinjenega poslovanja pa morajo poskrbeti, da je stanje neprekinjenega poslovanja v ravnovesju. Pričakovanja zainteresiranih strank so prikazana v spodnji tabeli:

Stranke	Izdelki in storitve so na voljo (brez prevelikih zamud) v vseh situacijah.
Lastniki	Nespremenjen nadzor managementa skozi vsako krizo.
Zaposleni	Zavarovanje življenj in preživetja.
Poslovni partnerji	Brez prekinitve poslovne mreže v primeru krize.
Dobavitelji	Nepoškodovana dobavna mreža za zagotavljanje dobave.
Regulatorji	Izpolnjevanje zahtev ne glede na okoliščine.
Zavarovalnice	Skrbnost pri izvajanju poslovanja (angl. due care)

Tabela 1: Pričakovanja zainteresiranih strank (Noakes-Fry et al., 2004, str. 5).

Učinkovite rešitve so lahko le tiste, pri katerih vse zainteresirane stranke sodelujejo že pri načrtovanju ter imajo podporo, udeležbo in odgovornost najvišjega vodstva podjetja. Pri takem pristopu k načrtovanju in izvedbi neprekinjenega poslovanja je mogoče pričakovati izgradnjo strateškega pristopa, ki spremeni kulturo podjetja v smeri zmanjševanja tveganj zaradi: izpada poslovnega procesa, izgube sredstev, regulative, izpada storitve, izgube ugleda znamke.

2.1 Definicija neprekinjenega poslovanja podjetja

Neprekinjeno poslovanje definirajo procesi, postopki, odločitve in aktivnosti, ki zagotavljajo neprekinjeno poslovanje podjetja v primeru prekinitev delovanja. To zahteva izdelavo proaktivnih in reaktivnih načrtov, ki pomagajo pri izogibanju kriznih situacij in katastrof, ter omogočajo hitro obnovo poslovanja v kolikor do slednjih pride (Continuity Central, 2006).

Načrtovanje neprekinjenega poslovanja podjetja (angl. business continuity planning – BCP) je metodologija, ki se uporablja za izdelavo načrta delne ali popolne obnove delovanja kritičnih oz. ključnih poslovnih funkcij podjetja v primeru katastrofe. Aktivnosti izdelave načrta neprekinjenega poslovanja obsegajo naslednje:

1. Analizo,
2. Pripravo rešitve,
3. Vpeljavo rešitve,
4. Testiranje in potrditev,
5. Vzdrževanje.

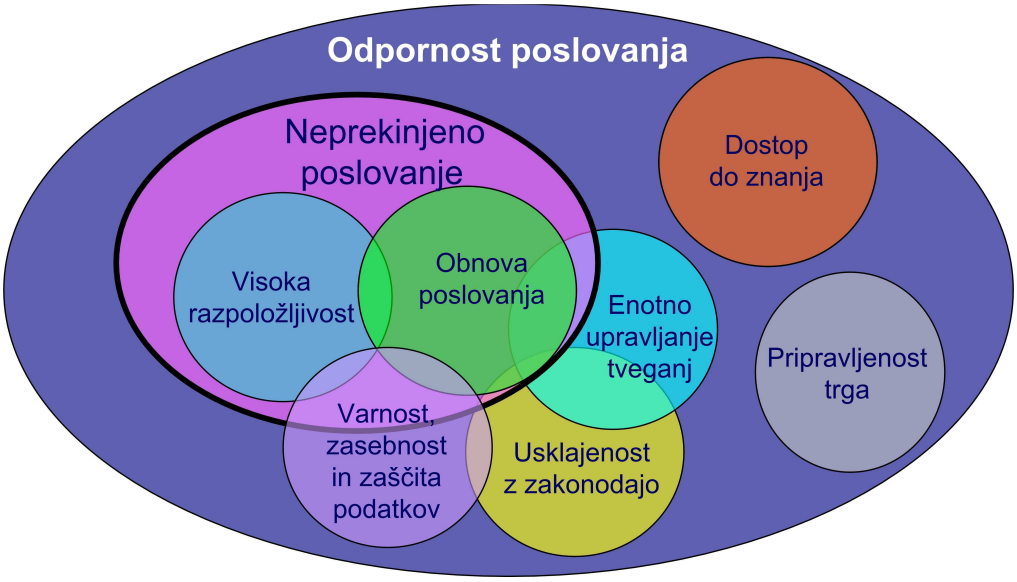
Rezultat tega cikla je načrt neprekinjenega poslovanja, ki se kot referenčni dokument uporablja pred, med in po katastrofi kakor tudi pri testiranju. Načrt pomaga v primeru krizne situacije ali katastrofe zadovoljivo hitro obnoviti kritične poslovne procese (Wikipedia, 2006).

Upravljanje neprekinjenega poslovanja (angl. business continuity management – BCM) sestavljata dva elementa. Prvi predstavlja proces upravljanja načrta neprekinjenega poslovanja, s čimer zagotovimo njegovo pravilnost in veljavnost. Drugi element predstavlja upravljanje operativne odpornosti in razpoložljivost ključnih procesov v podjetju, pri čemer želimo doseči minimalne motnje poslovanja podjetja (Continuity Central, 2006).

2.2 Odpornost poslovanja

Odpornost poslovanja je širši pojem od neprekinjenega poslovanja. Pomeni zmožnost podjetja ali organizacije, da trpi posledice prekinitve poslovanja, obnovi in nadaljuje poslovanje na določenem minimalnem nivoju zagotavljanja storitev.

V študiji odpornosti poslovanja je Gordon (Cocchiara, 2005, str. 5) določil šest ključnih področij, ki jih mora obsegati odpornost poslovanja:



Slika 1: Ključna področja Odpornosti poslovanja (vir: IBM, 2005).

1. Neprekinjenost poslovanja – postati bolj prilagodljivi in robustni – od informatike preko vseh poslovnih procesov.

2. Usklajenost z zakonodajo – hitrejša in cenovno učinkovitejša usklajenost z novo in spreminjajočo se državno zakonodajo.

3. Enotno upravljanje tveganj za zmanjševanje stroškov – ostati konkurenčen z učinkovitejšim upravljanjem tveganja.

4. Varnost, zasebnost in zaščita podatkov – zaščita pred notranjimi in zunanjimi grožnjami ter pomoč pri razvoju politike upravljanja informacij.

5. Dostop do znanja – razvoj okolja, ki omogoča enostavno pridobivanje in obvladovanje znanja s področja neprekinjenega poslovanja.

6. Pripravljenost trga – predvidevati in odgovoriti na spremenjene pogoje na trgu ter pospešiti raziskave in razvoj, ki bodo omogočili pripravo pravega izdelka za pravega kupca ob pravem času.

Na zgornji sliki (Slika 1) so prikazana ključna področja odpornosti poslovanja in njihova povezanost z neprekinjenim poslovanjem.

2.3 Poslovni vidik neprekinjenega poslovanja

Po Claunchu je upravljanje neprekinjenega poslovanja v podjetju nujno, če želimo zagotoviti njegovo dolgoročno delovanje. V zadnjih letih je prišlo tudi do širšega gledanja na zagotavljanje delovanja podjetij. Tako so se postopku obnove po

katastrofi (angl. disaster recovery) pridružili še drugi elementi, ki jih lahko razdelimo v pet komponent (Claunch, 2004):

- *Obnova po katastrofi* obravnava dogodke, ki povzročijo izpad informacijskih komponent ali celotnega sistema,

- *Obnova poslovanja* (angl. business recovery), obravnava možne zunanje dogodke, ki lahko povzročijo izpad poslovanja (npr. izpad električne energije),

- *Vzdrževanje poslovanja* (angl. business resumption) obravnava situacije, ko se zaradi izpada aplikacije poskuša nadaljevati poslovanje na pomožen način (npr. z ročnimi postopki),

- Načrtovanje odzivov in rezerve za nepredvidene dogodke (angl. contingency planning),

- *Krizni management* predstavlja upravljanje dejavnosti v primeru kriznega dogodka in je podlaga za preostale štiri naštete elemente.

Podlago za vzpostavitev in upravljanje neprekinjenega poslovanja v podjetju vidi Claunch v močni podpori višjega managementa ter v sodelovanju in vključitvi neprekinjenega poslovanja v kulturo podjetja, tako da postane to del življenjskega cikla projektov in procesa sprememb.

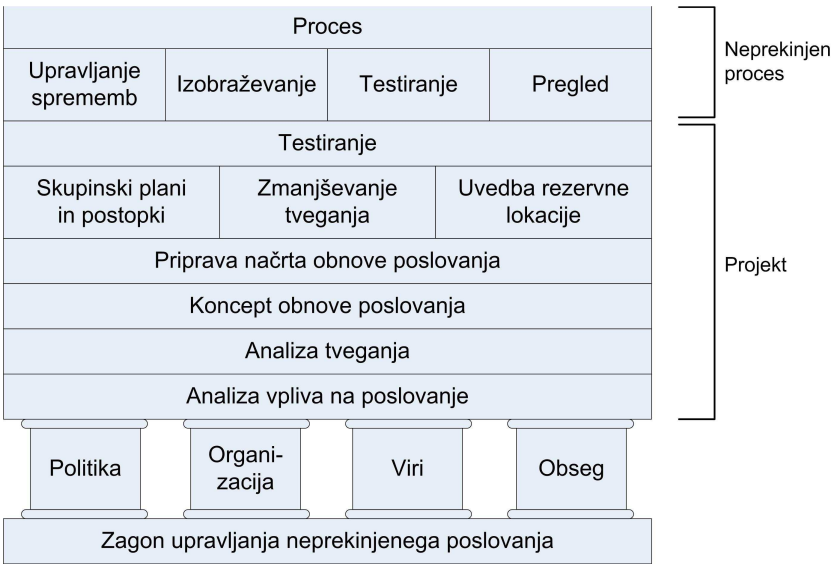
Pomembnejši koraki pri izdelavi učinkovitega načrta neprekinjenega poslovanja po mnenju Clauncha obsegajo (Slika 2):

- *Analiza vpliva na poslovanje* (BIA) ugotovi kaj je v podjetju izpostavljeno tveganju in kateri poslovni procesi so najbolj kritični, s čimer se določi prednostni seznam odpravljanja tveganj in obnovitvenih investicij. Preučijo se neposredne in posredne posledice prekinitve poslovanja, s čimer se lahko določi največji čas nedelovanja poslovnega informacijskega sistema.

- *Analiza tveganja* ugotovi ranljivosti in tveganja, ki jim je izpostavljeno podjetje, da bi jih po potrebi lahko ustrezno zmanjšali pri pripravi nove rešitve.

- *Koncept obnove* določi strategijo in postopke, ki se bodo uporabljali za obnovo poslovanja. Koncept je zasnovan na potrebah poslovanja, izraženih preko BIA analize in na finančni omejitvi investicije, kar zahteva njuno usklajevanje.

- *Priprava načrta obnove* obsega izdelavo načrtov in postopkov obnove poslovanja v primeru izpada poslovanja.



Slika 2: Elementi vzpostavitve in upravljanje neprekinjenega poslovanja podjetja (vir: Claunch, 2004).

- *Testiranje postopka obnove*, s čimer se preveri ustreznost zapisanih načrtov in postopkov.

- *Proces* zagotavlja ažurnost načrta obnove z vključitvijo popravkov ob vsaki spremembi poslovnih procesov ali sistemov.

Prvi korak izdelave načrta neprekinjenega poslovanja je analiza vpliva na poslovanje, kjer sodelujejo informatiki, poslovodstvo in upravljavci varnosti pri določanju ključnih poslovnih procesov in cene izpada poslovanja glede na čas izpada.

Rezultate te analize uporabljamo za izdelavo strategije in postopka obnove. Definirati je potrebno poslovne zahteve za posamezne aplikacije glede dosegljivosti in hitrosti ter načina obnove ob izpadu. Gre za uskladitev poslovnih potreb na eni strani, tehničnih možnosti na drugi strani in cene rešitve na tretji strani. V primeru neupoštevanja poslovnih zahtev v zgodnji fazi razvoja načrta lahko pride do neprimerne arhitekture končne rešitve, ki ima z odlašanjem v nadaljevanju projekta vse hujše posledice.

Za oceno dosežene stopnje neprekinjenega poslovanja je Mingay (Mingay, 2002) objavil model zrelosti (angl. maturity model), ki deli podjetja v šest razredov oz. nivojev:

Nivo 0 – Neobstoječ načrt. Minimalno zavedanje o potrebah in procesih za neprekinjeno poslovanje ne obstaja. Manjši deli organizacije imajo morda pripravljene posamezne elemente, vendar ni centralnega pristopa

in sprejete obveze za izvedbo. Na neprekinjeno poslovanje se gleda kot problem informatike.

Nivo 1 – Začetni načrt. Del višjega managementa prepozna potrebo, vendar še ni formalne organiziranosti, obveznosti in zadolžitev. Obstajajo lokalni poskusi reševanja problema brez uporabe metodologije. V oddelku informatike se izvajajo določene aktivnosti na to temo in tudi manjša finančna sredstva so bila odobrena v ta namen. Manjka revizija, poročila in nadzor.

Nivo 2 – Ponovljiv načrt. V managementu obstaja razumevanje in pripravljenost, da se problem neprekinjenega poslovanja reši. V okviru projekta je opravljena analiza in upravljanje tveganj, analiza vpliva na poslovanje, razvoj načrta. Neprekinjeno poslovanje se obravnava kot (enkraten) projekt. Glavni poudarek načrta je v obnovi informatike po katastrofi, kjer so tudi zagotovljena finančna sredstva. Občasno se izvaja testiranje načrta na nivoju informatike.

Nivo 3 – Definiran načrt. Postopki in procedure so standardizirani in dokumentirani, vendar brez revizije in nadzora. Obstaja organizacija za nadzor nad izvajanjem razvoja neprekinjenega poslovanja s sponzorjem iz višjega managementa, vendar s slabim sodelovanjem preostalih višjih managerjev.

Testiranje se izvaja redno, z vpeljanim učenjem na podlagi rezultatov. Tveganja in ranljivosti se sproti identificira in oceni. Prav tako se redno analizira vpliv izpada na poslovanje. Glavni poudarek in financiranje je na obnovi informatike in kritičnih poslovnih procesov.

Nivo 4 – Upravljan načrt. Ves management vidi načrtovanje neprekinjenega poslovanja kot del celovitega upravljanja tveganj. Mogoče je nadzorovati in meriti usklajenost glede na kontrole, postopke, politike in standarde. Neprekinjeno poslovanje se obravnava kot program in ne kot projekt. Testiranje in nadzor se izvajata redno. Ob odkritih napakah se sprožijo ukrepi za njihovo odpravo. Postopki se pregledujejo in poskušajo izboljšati ter so v glavnem usklajeni z najboljšo prakso.

Stroški, povezani z neprekinjenim poslovanjem, so zajeti in obvladovani. Glavni poudarek je neprekinjeno poslovanje na nivoju poslovnih procesov. Do neke mere se poskuša analizirati in zmanjševati tveganja ter obvladovati neprekinjeno poslovanje, povezano s poslovanjem izven podjetja.

Nivo 5 – Optimiziran načrt. Višji management zna razložiti strategijo neprekinjenega poslovanja in ga vidi kot dodano vrednost pri poslovanju

podjetja. Uprava redno obravnava, ocenjuje in upravlja neprekinjeno poslovanje. Upravljanje tveganja je del kulture podjetja. Poslovni procesi so optimizirani glede na najboljšo prakso. Glavni poudarek neprekinjenega poslovanja je na poslovnih procesih in okrepitvi oskrbovalne verige. Nadzor je vzpostavljen in postopki se izvajajo. Neprekinjenost poslovanja se upošteva v zgodnjih fazah načrtovanja informacijskih projektov. Neprekinjeno poslovanje je vzpostavljeno med podjetji in se redno testira.

2.4 Standardi na temo neprekinjenega poslovanja

Z uvajanjem in upravljanjem neprekinjenega poslovanja se ukvarjajo tudi različni standardi, ki poskušajo definirati primerne načine in postopke uvajanja in upravljanja neprekinjenega poslovanja v podjetjih.

2.4.1 BSI priporočilo PAS 56

PAS 56 predstavlja priporočila za postopek, principe in terminologijo upravljanja neprekinjenega poslovanja, ki sta jih pripravila angleški institut za standarde (BSI) in Insight Consulting. Priporočilo opisuje aktivnosti in rezultate v programu upravljanja neprekinjenega poslovanja. Podaja priporočila dobre prakse in opisuje kriterije za vrednotenje programa.

Življenjski cikel priporočila PAS 56 obsega pet korakov, ki se ciklično ponavljajo:

1. Razumevanje poslovanja,
2. Priprava strategije neprekinjenega poslovanja,
3. Razvoj in implementacija načrta in rešitev neprekinjenega poslovanja,
4. Razvoj in vpeljava kulture neprekinjenega poslovanja,
5. Izvajanje, vzdrževanje in pregled.

PAS 56 je kot javno dostopen dokument izšel leta 2003.

2.4.2 BSI standard BS 25999

Angleški standard BS 25999 je standard v nastajanju, ki naj bi bil objavljen leta 2007. Nasledil bo že omenjeni PAS 56 dokument, iz katerega izhaja in je z njim tudi tesno povezan. Namenjen je vsem v podjetjih in organizacijah, ki so zadolženi za poslovne aktivnosti in njihovo neprekinjeno poslovanje. Standard obsega dva dela:

BS 25999-1:2006 obravnava minimalne zahteve in dobro prakso pri upravljanju neprekinjenega poslovanja. Podaja osnovo za razumevanje, razvoj in vpeljavo neprekinjenega poslovanja znotraj organizacije.

BS 25999-2:2006 določa zahteve za vzpostavitev, izvajanje, kontrolo, pregled, vzdrževanje in izboljševanje sistema neprekinjenega poslovanja v povezavi s celotnim poslovnim tveganjem organizacije. Dokument vsebuje tudi izjave o ustreznosti, ki določa potrebne elemente za usklajenost s standardom.

2.4.3 Mednarodni standard ISO/IEC 17799

ISO17799 je mednarodni standard za sistem upravljanja varnosti informacij. Omogoča določanje, upravljanje in zmanjševanje tveganj, ki so jim izpostavljene informacije v podjetju. Prva izdaja standarda je iz leta 2000. Druga izdaja je izšla leta 2005, razdeljena je na 11 domen, med katerimi je tudi upravljanje neprekinjenega poslovanja.

V enem od enajstih domen standarda je torej obravnavano upravljanje neprekinjenega poslovanja oz. vidiki informacijske varnosti znotraj tega. Njen namen je preprečiti prekinitve poslovnih aktivnosti in zaščititi kritične poslovne procese pred posledicami hujših izpadov informacijskih sistemov ali katastrof ter zagotoviti njihov pravočasen ponovni zagon.

Cilji domene so zagotoviti naslednje:

- Vpeljavo procesa upravljanja neprekinjenega poslovanja za zmanjšanje posledic na poslovanje in obnovitev informacijskih sredstev na zadovoljiv nivo s pomočjo preventivnih in obnovitvenih postopkov.

- S pomočjo Analize vpliva na poslovanje se ugotovijo posledice katastrof, varnostnih incidentov, izpada storitev.

- Izdela in vpelje se načrt neprekinjenega poslovanja, ki omogoča pravočasno obnovitev ključnih procesov in operacij.

- Informacijska varnost mora biti integralni del celotnega procesa neprekinjenega poslovanja in ostalih upravljavskih procesov v podjetju.

- Upravljanje neprekinjenega poslovanja mora vsebovati postopke za določitev in zmanjšanje tveganj v okviru širšega procesa analize in upravljanja tveganj. Postopek mora zmanjšati posledice škodljivih incidentov in zagotoviti, da so poslovne informacije vedno na voljo.

Mednarodni standard ISO/IEC 17799 se je razvil iz angleškega standarda BS 7799-1. Predvideno je, da se bo ta standard v prihodnosti prestavil v okvir varnostnih standardov pod nazivom ISO/IEC 27002.

2.4.4 Mednarodni standard ISO/IEC 27001

ISO/IEC 27001 predstavlja standardno specifikacijo za sistem nadzora informacijske varnosti (angl. information system management system – ISMS). Leta 2005 je bil razvit iz angleškega standarda BS 7799-2, ki je bil objavljen leta 2002.

Glavni cilj standarda je pomoč pri vzpostavitvi in upravljanju učinkovitega sistema nadzora informacijske varnosti z uporabo pristopa stalnih izboljšav. Vsebina standarda je podobna vsebini BS 7799-2 in vključuje:

- Navzkrižne reference na kontrole standarda ISO/IEC 17799 ,
- Uporabo PDCA cikla,
- Upravljalni sistem,
- Izraze in definicije.

Standard ISO/IEC 27001 je prvi izmed serije standardov, ki so povezani z informacijsko varnostjo. Preostali predvideni standardi iz te serije so naslednji:

ISO 27002 bo nadomestil naslednjo verzijo ISO/IEC 17799,

ISO 27003 bo vseboval navodila za implementacijo sistemov nadzora informacijske varnosti,

ISO 27004 bo pokrival varnostne mere in merjenje,

ISO 27005 naj bi obravnaval upravljanje tveganja v sistemu nadzora informacijske varnosti,

ISO 27006 naj bi obravnaval upravljanje neprekinjenega poslovanja in obnovo po katastrofi.

2.4.5 ITIL

Knjižnica informacijske infrastrukture (ITIL) predstavlja okvir postopkov dobre prakse, ki spodbuja kvalitetne informacijske storitve na področju informacijske tehnologije. ITIL obravnava potrebno organizacijsko strukturo in znanja ter potrebne upravljavske postopke, s katerimi lahko organizacija upravlja svoje informacijske storitve. Postopki omogočajo poslovnemu delu podjetja, da na

področju informacijskih storitev doseže kvaliteto in ustrezno vrednost za vložen denar.

ITIL je v začetku nastal kot zbirka knjig, ki so pokrivala posamezna področja prakse pri upravljanju informacijske tehnologije. V drugi izdaji se je ta zbirka uredila v logična področja, ki kažejo različne vidike upravljanja sistemov, aplikacij in storitev informacijske tehnologije. ITIL ogrodje je sestavljeno iz naslednjih petih delov:

1. *Podpora storitev* (angl. service support) se usmerja na uporabnika IKT storitev in poskuša zagotoviti, da ima dostop do ustreznih storitev za zagotavljanje poslovnih funkcij. Ta del obsega naslednja področja:
    - Storitveni pult (angl. service desk),
    - Obvladovanje incidentov,
    - Upravljanje problemov,
    - Upravljanje konfiguracije,
    - Upravljanje sprememb,
    - Upravljanje izdaj (angl. release management),
2. *Izvajanje storitev* (angl. service delivery) se ukvarja s proaktivnimi storitvami, ki jih poslovni del pričakuje od izvajalca IKT storitev za zagotavljanje ustrezne podpore poslovnim uporabnikom. Obsega naslednja področja:
    - Upravljanje ravni storitev,
    - Upravljanje zmogljivosti,
    - Upravljanje neprekinjenega izvajanja IT storitev: pomaga zagotavljati razpoložljivost in hitro obnovo informacijskih storitev v primeru izpada. Aktivnosti, ki jih obravnava, so: analiza in upravljanje tveganja ter upravljanje in testiranje načrta postopkov ob izpadih,
    - Upravljanje razpoložljivosti: omogoča organizaciji zagotavljanje razpoložljivosti informacijskih servisov za podporo poslovanju glede na opravičljive stroške. Obravnavane aktivnosti so: določitev zahtev, priprava načrta, merjenje razpoložljivosti in vzdrževalnih obveznosti,
    - Finančno upravljanje za IT storitve,
3. *Upravljanje IKT infrastrukture* predlaga najboljšo prakso za pridobivanje zahtev, analizo, načrtovanje, zasnovo, postavitev, upravljanje in tehnično podporo informacijski infrastrukturi. Sem spadajo naslednje teme:
    - Načrtovanje in planiranje IKT,

- Uvajanje IKT,
- Operativno upravljanje IKT,
- Tehnična podpora IKT,

4. *Upravljanje aplikacij* vsebuje seznam dobrih praks, ki so predlagane za izboljšanje kvalitete razvoja in vzdrževanja programske opreme, skozi življenjski cikel projekta razvoja programske opreme. Poseben poudarek je namenjen zbiranju in definiciji poslovnih zahtev.

5. *Upravljanje varnosti* opisuje strukturirano prileganje informacijske varnosti v upravljanje organizacije in temelji na standardu ISO/IEC 17799. Glavni cilj je zagotavljanje varnosti informacij, ki jih ščitimo pred tveganji. Pri tem nas zanimajo zaupnost, celovitost in razpoložljivost ter dodatno še zasebnost, anonimnost in preverljivost.

Med petimi deli sta najbolj popularna prva dva – podpora in izvajanje storitev. Tem petim osnovnim delom pa so dodane še trije za pomoč pri implementaciji:

1. Poslovni pogled je seznam dobrih praks, ki se ukvarjajo s poslovnimi zahtevami upravljanja informacijske infrastrukture ter obsega naslednje izzive: upravljanje neprekinjenega poslovanja, preživetje sprememb, radikalna transformacija poslovne prakse, zunanje izvajanje, …

2. Načrtovanje za uvajanja upravljanja storitev,

3. Implementacije v manjšem obsegu.

Čeprav se knjižnica ITIL ukvarja s širšo oz. drugačno tematiko, pa se v treh podpoglavjih prekriva z obravnavano tematiko tega dela: upravljanje neprekinjenega delovanja IT storitev, upravljanje razpoložljivosti in upravljanje varnosti.

V letošnjem letu naj bi bila pripravljena verziji 3 ITIL knjižnice, ki bo vsebovala pet novih glavnih področij:

- Strategija IT storitev,
- Načrtovanje IT storitev,
- Uvajanje IT storitev,
- Izvajanje IT storitev,
- Izboljšave IT storitev.

Glavna sprememba v novi verziji knjižnice bo poudarek na poravnavi vidika informatike in poslovanja, ter na upravljanju informacijske tehnologije skozi celoten življenjski cikel.

2.4.6 COBIT

COBIT (cControl objectives for information and related technology) obsega množico dobrih praks za upravljanje informacijske tehnologije, ki sta jih leta 1996 pripravila ISACA in ITGI. Sedaj je v uporabi četrta verzija, katere pomen se je povečal predvsem zaradi uvajanja zakona Sarbanes-Oxley.

COBIT daje managerjem, reviziji in uporabnikom IKT na voljo splošno sprejete mere, indikatorje, procese in dobro prakso pri uporabi IKT in razvoju primernega nadzora in kontrole informacijske tehnologije v podjetju.

V zadnji verziji ima COBIT 34 zahtev (angl. high level objectives), ki obsegajo 215 kontrolnih zahtev in so uvrščene v štiri domene:

1. *Načrtovanje in organizacija* pokriva uporabo tehnologije za zagotavljanje ciljev in zahtev podjetja. Obenem prikaže še primerno organizacijsko in infrastrukturno obliko IKT-ja za doseganje optimalnih rezultatov,
2. *Nabava in implementacija* obsega identifikacijo, nabavo in implementacijo IKT tehnologije znotraj poslovnih procesov podjetja. Domena vsebuje tudi izdelavo načrta vzdrževanja za nabavljeno IKT tehnologijo.
3. *Izvajanje in podpora* obsega izvajanje aplikacij na IKT ter podporni proces, ki omogoča njihovo učinkovito izvajanje. Pod to domeno sodi tudi varnost in izobraževanje.
4. *Nadzor in ocenjevanje* preverja, če IKT še izpolnjuje zahteve, zaradi katerih je bil postavljen glede na potrebe in strategijo podjetja ter zahteve regulative. Obravnava tudi zagotavljanje neodvisnega pregleda učinkovitosti IKT pri izpolnjevanju poslovnih zahtev.

Cilj COBIT-a je razvoj, objava in promocija mednarodno priznanih kontrol za informacijsko tehnologijo, ki so uporabni tako za management podjetja, kakor tudi za revizorje. Vsem pa omogoča boljše razumevanje IKT ter pomaga pri odločitvah o potrebnih kontrolah in stopnji varnosti za zaščito sredstev podjetja.

Celoten paket COBIT obsega šest publikacij:

1. Povzetek,
2. Ogrodje (angl. framework),
3. Zahteve nadzora,
4. Navodila za pregled (angl. audit guidelines),

5. Orodja za implementacijo,
6. Navodila za upravljanje.

Ogrodje COBIT je usklajeno z ITIL-om. COBIT nadzira zahteve in dobro prakso, ITIL pa natančno razlaga dobro prakso.

2.5 Elementi neprekinjenega poslovanja

2.5.1 Analiza vpliva na poslovanje

Analiza vpliva na poslovanje (angl. business impact analysis) je metoda za opredelitev poslovne vrednosti posameznih delov informatike (procesi, aplikacije, podatki). Običajno se uporablja kot začetni korak pri pripravi načrta obnovitve poslovanja v primeru izpada celotne informatike ali njenega dela, lahko pa jo uporabimo tudi za analizo vrednosti in usklajenosti informatike s poslovnimi procesi.

Analiza ugotovi ključne potrebe, ki so pomembne za vzpostavljanje in zagotavljanje nemotenega delovanja poslovanja:

1. Zagotovi finančne in druge podatke o posledicah na poslovanje v primeru nepredvidenih dogodkov, ki vplivajo na delovanje informatike,
2. Določi pomembnost informacijskih procesov, aplikacij in podatkov,
3. Določi ciljni čas vzpostavitve delovanja sistema (RTO) in ciljno točko obnavljanja podatkov (RPO),
4. Zagotovi seznam informacijskih sredstev z določeno njihovo poslovno vrednostjo,

Analiza vpliva na poslovanje je običajno sestavljena iz treh načinov pridobivanja podatkov za izvedbo analize:

1. Določitev poslovnih funkcionalnosti in procesov, nanje vezane aplikacije in podatke ter pomembnost slednjih za poslovanje,
2. Analiza posledic za poslovanje v primeru obstoječih izpadov informatike,
3. Ugotavljanje posledic na posamezne poslovne procese v primeru hipotetičnega izpada informatike za daljše časovno obdobje.

V vseh treh delih je potrebno sodelovanje nosilcev poslovnih procesov v podjetju in močna podpora vodstva podjetja, sicer se težko zagotovi kvalitetne rezultate. Spodaj opisani trije koraki pridobivanja potrebnih informacij se v praksi običajno

združijo v en vprašalnik oz. intervju, da bi se zmanjšala obremenitev nosilcev poslovnih procesov ter zagotovila učinkovitost celotne analize.

Analiza poslovnih funkcij, procesov, aplikacij in podatkov

Ta del obsega določitev in analizo kritičnih poslovnih procesov, aplikacij in podatkov. Najprej se določijo poslovni procesi, nakar se zanje določijo aplikacije in podatki, ki so potrebni za delovanje poslovne funkcije. Na podlagi ocene časa, ki ga posamezen poslovni proces lahko preživi brez ustreznih aplikacij in podatkov se nato določi pomembnost posameznih poslovnih procesov.

Analiza obstoječih izpadov informatike

Drugi del obsega popis znanih izpadov informatike v podjetju ter analizo poslovnih posledic teh izpadov. Pri tem nas zanimajo tako finančne kot tudi nefinančne posledice. Pridobljeni podatki se uporabijo za kontrolne podatke pri preverjanju ostalih dveh delov metode.

Analiza na primeru hipotetičnega izpada

Tretji del metode pridobi podatke o vrednosti posameznih delov informatike s pomočjo namišljenega scenarija izpada informatike. Scenarij običajno opiše stanje po popolnem izpadu informacijske tehnologije za daljše časovno obdobje (npr. nekaj tednov). V tem okviru se za posamezne poslovne procese ugotovi finančne in nefinančne posledice. Med finančne posledice štejemo:

- Izpad prihodka ali dobička,
- Kazni in penale,
- Dodatne stroške dela, delo izven delovnega časa,
- Dodatne logistične stroške.

Med nefinančne posledice štejemo:

- Izgubo ugleda,
- Zmanjšanje kvalitete storitve,
- Izgubo tržišča,
- Odziv javnosti in medijev,
- Zmanjšanje zaupanja delničarjev,
- Tveganje za zdravje ali varnost ljudi.

Navedene posledice niso urejene po neki prioriteti, ker je ta različna za različna podjetja. Če je v nekaterih podjetjih (skoraj) edini kriterij izpad dobička, je v večjih in medijsko bolj izpostavljenih ali državnih podjetjih odziv javnosti lahko še pomembnejši.

Prikaz postopka izvedbe opisane analize običajno obsega tri korake:

1. Priprava vprašalnikov,
2. Izvedba intervjujev
3. Delavnica.

Intervju

Informacije v okviru tega dela analize se običajno zbirajo s pripravljenim vprašalnikom na intervjuju s posameznimi nosilci poslovnih procesov. Zaradi večje učinkovitosti je priporočljivo vprašalnike vsaj delno prirediti za vsak intervju – npr. izključitev nepomembnih vprašanj, poslovnih procesov, aplikacij, ...

Vprašalnik je običajno sestavljen iz naslednjih delov:

1. Splošna vprašanja o poslovnem procesu – v »ogrevalnem« delu opredelimo položaj in pomembnost poslovnega procesa za poslovanje podjetja, njeno splošno odvisnost od informacijske tehnologije ter možnost izvajanja poslovnih procesov brez delujoče informacijske infrastrukture,
2. Pomembnost posameznih aplikacij za delovanje poslovnega procesa
3. Izgube poslovnega procesa ob izpadu informacijske infrastrukture – obravnavamo finančne in nefinančne posledice, kot so bile že naštete zgoraj.

   V primeru finančnih posledic izberemo (za celotno podjetje) tip finančne posledice, ki ga je smiselno opazovati (dobiček, prihodek). Poskušamo čim bolje oceniti finančne posledice izpada poslovnega procesa ob izpadu celotne informacijske infrastrukture po določenih časovnih intervalih: po 1 uri, 4 urah, 8 urah, 1 dnevu, 1 tednu, ...

   Podobno v primeru nefinančnih posledic opazujemo, kdaj se posamezna od njih pojavi. Časovni intervali so običajno enaki kot pri finančnih posledicah.

4. Dodatni podatki – evidentira se ostale, potencialno pomembne informacije o poslovnem procesu: obdobja največje odvisnosti od informacijske tehnologije, povezava z ostalimi procesi, ...

Iz vsebine vprašalnika je razvidno, da je potrebno dobro motivirati sodelujoče pri intervjuju, da se vsebini posvetijo in poskušajo po svojih najboljših močeh dati kvalitetne odgovore.

Delavnica za sintezo intervjujev

Posamezni intervjuji lahko predstavljajo individualen pogled posameznih nosilcev poslovnih procesov na vlogo in pomen poslovnega procesa znotraj podjetja. Če se je med intervjuji pričakovalo, da bodo intervjuvanci odgovarjali predvsem s stališča posameznega poslovnega procesa, pa je cilj delavnice bolj usmerjen v enoten, širok pogled na celotno podjetje. Pri združevanju vseh intervjujev v enotno zgodbo je zato potrebno »soočenje« nosilcev pomembnih poslovnih procesov, kjer se zbrani rezultati ovrednotijo, utežijo, uskladijo in po potrebi tudi popravijo. Rezultat delavnice je enoten dokument za celotno podjetje, v katerem so ocene odvisnosti posameznih poslovnih procesov od informacijske tehnologije.

Pogoji za uspešno izvedbo analize

Uspešna izvedba Analize vpliva na poslovanje ni enostavna, je pa izvedljiva. Najpomembnejši element vidim v močni podpori in sodelovanju poslovodstva podjetja. Nosilci poslovnih procesov, ki sodelujejo v analizi, morajo biti pripravljeni polno sodelovati v intervjuju in posredovati poslovne podatke o posledicah scenarija po svojih najboljših močeh.

Za vodenje celotne analize je najbolj primeren poslovni svetovalec, ki zna govoriti tako poslovni jezik, kot jezik informatike. Priporočljivo je tudi, da je neodvisen od glavnih poslovnih procesov v podjetju. Zato analizo velikokrat izvajajo zunanji poslovni svetovalci.

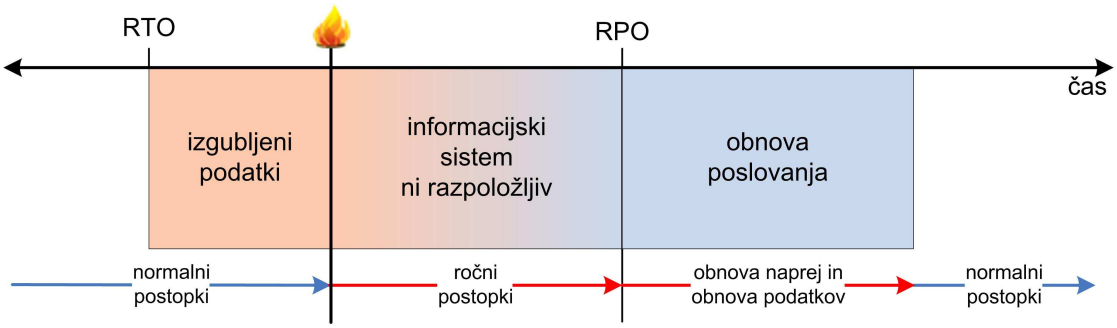
Sodelovanje oddelka informacijske tehnologije pri celotni analizi je ključno, saj zagotovi podatke za pripravo materiala analize in intervjujev, sodeluje pri izvajanju intervjujev in pomaga pri interpretaciji rezultatov ter pripravi končnega poročila.

Rezultati analize vpliva na poslovanje

Glavni cilj BIA analize je določitev poslovnih zahtev pri vzpostavljanju neprekinjenega poslovanja ali obnovi poslovanja. Na podlagi opravljene analize se določijo poslovne zahteve in s tem tudi način obnove poslovnega informacijskega sistema. Dva glavna parametra, ki predstavljata pomemben rezultat analize, sta:

- *Ciljni čas vzpostavitve delovanja sistema* (angl. recovery time objective – RTO) je najdaljše trajanje izpada informacijskega sistema, ki ga podjetje še lahko dopusti, ne da bi resneje ogrozili svoje poslovanje.

- *Ciljna točka obnavljanja podatkov* (angl. recover point objective – RPO) določa (časovno) količino podatkov, ki jih organizacija ob izpadu informacijske tehnologije še lahko izgubi brez resnejših posledic.



Slika 3: Časovni prikaz parametrov RTO in RPO v analizi vpliva na poslovanje (lasten vir).

Opisana parametra sta časovno prikazana na zgornji sliki (Slika 3). Občasno se uporablja še Tretji parameter – Ciljna točka obnavljanja omrežja (angl. recovery network objective – RNO) določa najdaljše trajanje izpada mrežne infrastrukture, ki ga podjetje še lahko dopusti, ne da bi resneje ogrozili svoje poslovanje.

Za pripravo načrta obnove poslovnega informacijskega sistema so potrebni tudi ostali rezultati Analize vpliva na poslovanje:

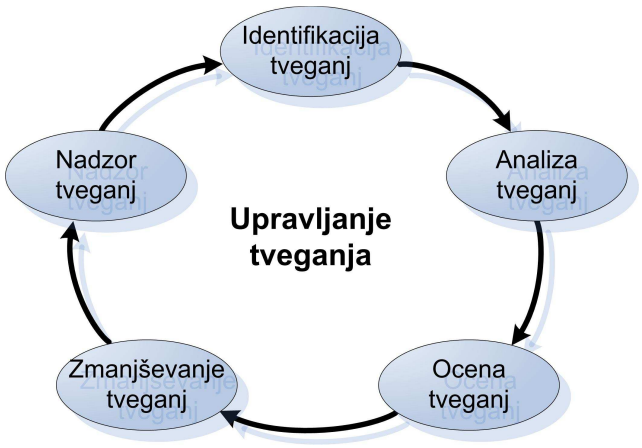
- Seznam in prioritete aplikacij, podatkov in sistemov,
- Ocenjene finančne in nefinančne posledice izpada informacijskega sistema na posamezne poslovne procese,
- Seznam in prioritete poslovnih procesov ter pripadajočih aplikacij.

2.5.2 Analiza in upravljanje tveganj

V informacijski varnosti so tveganja sestavni del vsakodnevnega dela. Namestitev popravkov, spremembe gesel, vklop požarne pregrade, preverjanje varnostnih zapisov – skoraj vsaka kontrola v okviru informacijske varnosti je namenjena zmanjševanju tveganj.

Obvladovanje tveganja je proces v okviru informacijske varnosti, ki se ukvarja z določanjem, analizo in oceno varnostnih tveganj ter pripravo ustreznih rešitev za zmanjšanje le-teh (Slika 4). Prvi del obvladovanja tveganja predstavlja določanje možnih varnostnih tveganj. Sledi analiza in ocena tveganj, ki poskuša za vsako tveganje določiti možno škodo in verjetnost, da se bo tveganje zgodilo. Temu sledi postopek zmanjšanja tveganja, kar dosežemo z enim od naslednjih štirih načinov: izogibanje tveganju, zmanjšanje tveganja, prenos tveganja ali sprejem tveganja.

Izbor načina za zmanjšanje tveganja in njegova implementacija zaključi en cikel obvladovanja tveganja. Vendar pa je potrebno celoten postopek obvladovanja tveganja stalno pregledovati, ocenjevati in predvsem redno ponavljati cikel določanje – analiza – zmanjševanje tveganj (PDCA cikel).



Slika 4: Elementi in postopki v procesu upravljanja tveganja. (lasten vir)

Del zahtevnosti, ki jo predstavlja proces obvladovanja tveganja leži v postopku določanja dveh vrednosti, ki tveganje določata (škoda in verjetnost). Ocena je lahko nezanesljiva, zato jo je potrebno redno pregledovati in po potrebi popraviti.

Na tem mestu obravnavam obvladovanje in analizo tveganja s stališča informacijske varnosti. Kljub temu pa se je potrebno zavedati, da precej tveganj prihaja iz splošnega področja informacijske tehnologije in tudi iz področij, ki niso direktno povezana z informacijsko tehnologijo, npr. računski center, stavbe, naravne nesreče ...

Tveganje (angl. risk) pomeni možnost, da pride zaradi znane nevarnosti do finančne škode na elementu informacijske infrastrukture (vključujoč ugled, vpliv javnosti, izguba tržišča ...). Elementi informacijske infrastrukture so lahko strežniki, omrežje, programska oprema...

Analiza in ocena tveganja predstavlja težji del tega postopka *obvladovanja tveganj*, ki je zelo izpostavljen napakam. Ko so tveganja določena in ocenjena, je postopek nadaljnjih aktivnosti dobro definiran in utečen.

Analiza tveganja v osnovi oceni dve vrednosti za vsako tveganje: grožnjo in potencialno škodo. V nadaljevanju bomo pogledali posamezne elemente postopka, ki nam omogočajo analizo tveganja in določitev njegove ocene.

Prvi korak pri določanju velikosti tveganja je določitev potencialnih groženj. To določanje ni enostavno opravilo in zahteva vztrajnost, kreativnost, sodelovanje strokovnjakov za posamezna področja in tudi skupinsko delo. Paziti pa je potrebno tudi na drugo skrajnost – če posvetimo identifikaciji tveganj preveč časa, lahko pride do dajanja pretiranega poudarka in verodostojnosti malo verjetnim tveganjem.

Grožnja (angl. threat) predstavlja dogodek, ki nam lahko povzroči škodo. Pogosto se dogaja, da se ta definicija zamenjuje s tveganjem, ki je definiran kot *možnost za škodo*.

Pomembno je razumeti razliko med grožnjo in tveganjem. *Grožnja* predstavlja nekaj, kar je izven našega neposrednega nadzora. S tem povezano *tveganje* pa dobimo iz kombinacije grožnje dogodka, verjetnosti, da se le-ta zgodi, in škode, ki jo povzroči. Primeri groženj so: bolezen, potres, požar, poplava, internetni napad, hurikan, izpad napajanja, terorizem.

Del tveganja je **možna škoda** (angl. potential damage), ki jo lahko pričakujemo, če se zgodi obravnavani dogodek.

Opisani pristop (izračun na podlagi znanih vrednosti) se imenuje *kvantitativni*.

Predvidena posamezna izguba (angl. single loss expectancy – SLE) poskuša določiti škodo, vendar se ne omeji le na finančne posledice. Kakšne so posledice, če nekdo vdre preko spletne strani in pride do baze strank s podatki o kreditnih karticah. V takih primerih je škodo težko finančno oceniti, zato uporabljamo kvantitativni pristop.

Pri tem pristopu uporabljamo opisne termine, npr. lestvico izgube (od 1 do 4): *zelo malo*, *malo*, *srednje*, *veliko*. Lahko uporabljamo številke ali opise, potrebno pa je paziti, da se oznake uporabljajo dosledno.

Kvantitativna in kvalitativna analiza se načeloma lahko uporabljata skupaj, vendar je običajno lažje, če ju ne mešamo.

Poleg ocene škode, ki jo povzroči obravnavani dogodek, je potrebno ugotoviti še verjetnost, da se bo le-ta v resnici zgodil. **Letna verjetnost dogodka** (angl. annualized rate of occurrence – ARO) je verjetnost, da se bo grožnja uresničila v enem letu. To vrednost je velikokrat težko določiti.

Letno verjetnost dogodka nam običajno pomagajo določiti strokovnjaki za posamezna področja. Natančnost ocene verjetnosti dogodka je zelo pomembna, saj lahko napačen ARO pripelje do bistvenih napak pri analizi tveganja. Zanimivo je, da so ocene letne verjetnosti dogodka običajno prej previsoke kot prenizke.

Tudi pri letni oceni verjetnosti je možno uporabljati kvalitativni in kvantitativni pristop. V kolikor imamo na voljo statistične podatke, je lažje delati s prvim pristopom. Če nam pomaga specialist s svojo oceno, pa je običajno lažje delati kvantitativno z definirano lestvico, npr.: *zelo nizka*, *nizka*, *srednja*, *visoka*.

Predvidena letna izguba (angl. annualized loss expectancy – ALE) predstavlja povprečno izgubo, ki jo imamo zaradi obravnavanega tveganja v enem letu. Pri

kvantitativnem pristopu naredimo le izračun ALE = ARO * SLE, pri kvalitativnem pristopu pa uporabimo tabelo, ki nam ALE določi na podlagi opisnih terminov kvalitativne lestvice.

Cilj vseh dosedanjih izračunov je **Indeks obvladovanja tveganj** (angl. risk management index – RMI). To je število med 1 in 100, ki nam pove pomembnost, in s tem določi, o kakšnem tveganju govorimo.

Najprej se bomo osredotočili na kvantitativni rezultat predvidene letne izgube in pogledali, kako lahko to pretvorimo v indeks obvladovanja tveganj (RMI).

Določiti moramo količino sredstev, ki si jo lahko privoščimo izgubiti brez resnih posledic za normalno poslovanje (*max*). Za izračun kvantitativnega RMI delimo ALE z maksimalno vrednostjo, ki jo lahko letno izgubimo in množimo s 100: RMI = ALE / *max* * 100.

Zmanjševanje tveganja

Ko smo končali z analizo tveganja in določili Indeks obvladovanja tveganj (RMI), pridemo do točke, ko se je potrebno odločiti o nadaljnjih aktivnostih.

Temu sledi postopek zmanjšanja tveganja, kar običajno dosežemo na enega od naslednjih štirih načinov:

1. *Izogibanje tveganju* (angl. risk avoidance) pomeni, da se izognemo dogodku, ki bi lahko povzročil tveganje; npr. ne uporabljamo brezžične povezave, da se izognemo tveganju brezžičnih povezav ali preprečimo uporabo P2P programov (Kazaa, eMule ...),

2. *Zmanjšanje tveganja* (angl. risk reduction / mitigation) pomeni, da vpeljemo ukrepe, ki posledično zmanjšajo letno verjetnost dogodka (ARO) in s tem tudi tveganje; npr. nadgradimo protokol WEP v WPA za zmanjšanje nevarnosti vdora v brezžično omrežje,

3. *Prenos tveganja* (angl. risk transfer) pomeni, da zmanjšamo predvideno posamezno izgubo (SLE), tako da se proti tveganju zavarujemo pri zavarovalnici,

4. *Sprejem tveganja* (angl. risk acceptance / retention) pomeni, da se s tveganjem sprijaznimo in ne naredimo nič za njegovo odpravo.

Četrta možnost ne zmanjša tveganja in se običajno uporabi le za zelo majhna tveganja (RMI manjši od 10). Pri večjih tveganjih pa se mora odgovorni manager odločiti, na kakšen nivo bo spustil RMI.

Če hočemo ugotoviti, ali so izbrani ukrepi zadostovali, moramo postopek *analize tveganja* ponoviti. Glede na to, da se večina podatkov ne spremeni, je ponovljeni postopek običajno krajši in hitrejši.

2.5.3 Koncept obnove poslovanja

Cilj priprave koncepta obnove je določitev najboljše finančno ustrezne rešitve za postavljene zahteve neprekinjenega poslovanja podjetja. Zahteve dobimo iz faze analize, predvsem iz Analize vpliva na poslovanje. V primeru informacijske tehnologije so ključni podatki naslednji:

- Potreben obseg aplikacij in podatkov za nadaljevanje poslovanja,
- Največji možen čas nedelovanja posameznega sistema,
- Količina podatkov, ki jih organizacija ob izpadu informacijske tehnologije še lahko izgubi brez resnejših posledic.

Koncept obnove poslovanja se običajno osredotoča predvsem na informacijsko tehnologijo; ta vidik je opisan v tretjem poglavju. Obstajajo pa tudi druga področja, ki potrebujejo načrtovanje obnove v primeru katastrofe, kot je npr. hranjenje dokumentov v papirni obliki ali obnavljanje tehnologije v proizvodnem procesu. V splošnem pa mora Koncept obnove poslovanja določiti naslednje element (Wikipedia, 2006):

- Struktura kriznega managementa,
- Rezervna lokacija (če je potrebna),
- Komunikacijska arhitektura med primarno in rezervno lokacijo,
- Način kopiranja podatkov med primarno in rezervno lokacijo,
- Potrebna programska in aplikacijska oprema na rezervni lokaciji,
- Potrebni podatki na rezervni lokaciji.

Claunch (Claunch, 2004) predlaga izdelavo klasifikacijske sheme podprtih servisnih nivojev in pripadajoče cene, ki določajo aplikacijsko arhitekturo ter način operativnega izvajanja storitev. Poslovni managerji na podlagi tega za vsako informacijsko storitev določijo, kam jo bodo uvrstili v klasifikacijski shemi. Primer klasifikacijske sheme s štirimi razredi je:

Razred	Storitve za poslovne procese	Nivo storitve (SLA)
Razred 1	• Stik s strankami in parterji • Generiranje prihodka	24x7, RTO = 2 uri, RPO = 0 99,9% razpoložljivost

Razred	Storitve za poslovne procese	Nivo storitve (SLA)
Razred 2	• Manj kritične funkcije pri generiranju prihodka • Oskrbovalna veriga	24x6, RTO = 8-24 ur, RPO = 4 ure 99,5% razpoložljivost
Razred 3	• Poslovne zaledne funkcije	18x7, RTO = 3 dni, RPO = 1 dan 99% razpoložljivost
Razred 4	• Oddelčne funkcije	24x6, RTO = 5 dni, RPO = 1 dan 98% razpoložljivost

Taka razporeditev se najlažje izvede v okviru Analize vpliva na poslovanje. Na podlagi definiranih razredov storitve (angl. service level agreement – SLA) se določi potrebna strategija obnove poslovanja podjetja:

1. Za servise Razreda 1 je običajno potrebna podvojena arhitektura na rezervni lokaciji,

2. Servisi Razreda 2 običajno zahtevajo kopiranje podatkov na rezervno lokacijo,

3. Za storitve razreda 3 zadostuje standardne varnostne kopije na traku. To storitev se lahko da v zunanje izvajanje,

4. Daljši čas obnove za storitve razreda 4 omogoča pogodbeno ureditev hitre dobave opreme v primeru katastrofe.

2.5.4 Načrt neprekinjenega poslovanja

Načrt neprekinjenega poslovanja (angl. business continuity plan) je proces, ki zagotovi neprekinjeno poslovanje podjetja (Wikipedia, 2006).

Osnovne komponente načrta neprekinjenega poslovanja vključujejo:

- Načrtovanje in vpeljava vseh aktivnosti, ki preprečujejo ali zavarujejo pred tveganji, ki jih pričakujemo pred kritičnim dogodkom,

- Načrtovanje aktivnosti, ki se izvajajo v primeru nevarnosti ali katastrofe,

- Načrt evakuacije,

- Krizni management,

- Komunikacijski načrt,

- Rezervni postopki in načrt odziva na nepredvidene dogodke,

- Strateško in taktično načrtovanje z viri in pomembnimi informacijami,
- Dokumentiranje aktivnosti obnove in vzpostavitve delovanja,
- Vzpostavitev poslovanja, tako fizično kot logično,
- Testiranje in obnova načrta,
- Izvajanje načrtovanja.

Lahko bi rekli, da načrt neprekinjenega poslovanja določa načrtovanje in izvajane aktivnosti pred, med in po katastrofi. Vključuje načrte za potrebe po ljudeh, tehnologijo in poslovanje. Priporočljivo je, da imajo tveganja z veliko verjetnostjo ali hudimi posledicami ustrezne načrte za odziv na dogodek in obnovo poslovanja.

Harris v (Harris, 2003) priporoča posebno pozornost naslednjim štirim ključnim informacijam, ki jih mora načrt jasno opredeliti:

- *Odgovornost* – vsi udeleženi pri obnovi poslovanja morajo poznati svojo funkcijo v primeru kaotične situacije. Vsak posameznik mora vedeti, kaj se od njega pričakuje in to lahko dosežemo s pomočjo urjenja, komuniciranja in dokumentiranja.
- *Pooblastila* – v primeru krize je pomembno da vemo, kdo je odgovoren za kaj. Skupinsko delo je pomembno v kritičnih situacijah, prav tako pa je pomembno, da ima skupina primernega in sposobnega vodjo. Odločen vodja lahko pomaga pri zmanjšanju zmede in povečanju sodelovanja.
- *Prioritete* – v primeru kritične situacije je pomembno vedeti, katere poslovne funkcije so kritične za delovanje podjetja in katere manj pomembne. Podobno je potrebno pogledati tudi pomembnost aplikacij, sistemov in informacij. Glede na postavljene prioritete, ki jih pripravi poslovodstvo, se lahko pripravi načrt neprekinjenega poslovanja, ki zagotavlja ustrezno obnovo kritičnih poslovnih funkcij.
- *Vpeljava in preizkušanje* – izdelava načrta brez njegove uporabe in testiranja običajno ne prinese pričakovanih koristi podjetju. Načrt je potrebno preizkusiti; ljudi je potrebno naučiti kako bodo opravili pričakovane aktivnosti. Te aktivnosti je potrebno izvajati vsaj enkrat letno, načrt pa je potrebno stalno posodabljati in izboljševati.

Nekatera podjetja imajo izdelan načrt neprekinjenega izvajanja operacij (angl. continuity of operations plan – COOP), ki pokriva del obsega načrta neprekinjenega poslovanja, poleg tega pa še širša področja poslovanja podjetja:

zaščita znamke, ugleda podjetja, deleža na tržišču, zaupanja delničarjev, zaščita oskrbovalne verige, strank in zaposlenih.

Poleg omenjenega načrta lahko obstaja v podjetjih še Načrt obnove po katastrofi, ki se včasih zamenjuje z načrtom neprekinjenega poslovanja. Načrt obnove po katastrofi predstavlja dokument, ki vsebuje navodila za obnovo podatkov, tehnologije, informacijske infrastrukture in podpornih orodij. Ta načrt je del načrta neprekinjenega poslovanja podjetja in mora biti vanj tudi vključen.

Načrt obnove po katastrofi vsebuje vse aktivnosti, ki so potrebne za uspešno obnovo poslovnega informacijskega sistema v primeru katastrofe. Pokriva naslednja področja:

- Procedure za sprožitev alarma
- Sprejemanje odločitev
- Določitev narave katastrofe
- Obnova centralnega informacijskega sistema
- Obnova informacijskih podsistemov v območnih enotah
- Obnova omrežja (LAN in WAN)
- Obnova infrastrukture
- Notranje in zunanje informacije
- Arhiviranje podatkov in nosilcev podatkov
- Organizacijski vidiki
- Testiranje in vzdrževanje načrta obnove

2.5.5 Krizni management

V širokem pogledu je cilj kriznega managementa pogledati nevarnosti v oči: prepoznati možno krizo, jo poskusiti preprečiti in ukrepati hitro ter učinkovito, če do krize pride (Crisis Management & Disaster Recovery, 2006).

Krizni management tako predstavlja sistematični odgovor na nepričakovane dogodke, ki lahko ogrozijo ljudi, lastnino in poslovanje organizacije. Je formalni odziv na vsak dogodek, ki lahko ogrozi finančno ali operativno stabilnost organizacije. Osnovo kriznega managementa predstavlja ekipa managerjev, strokovnjakov, tehnikov in ostalega osebja, ki so usposobljeni za:

1. Analizo in oceno tveganja,
2. Razvoj in izvedbo možnih odzivov,

3. Pravilen prenos informacij in odločitev vpletenim,

4. Koordiniranje pri prehodu v normalno delovanje, ko se kriza zaključi.

Metoda kriznega managementa poskuša uporabiti znanje (ne pa emocije in intuicijo) v primerih, ki zahtevajo hitre odločitve v trenutkih krize, stresa in pritiska.

Cilji, ki jih mora doseči krizni management je zmožnost, da:

- Je skupina za krizni management pripravljena na odziv in upravljanje vsake krizne situacije ali katastrofe,
- Ima vzpostavljene in usposobljene skupine za nepredvidene situacije in obnovo, ki ukrepajo ob izbruhu katastrofe,
- Pomiri zaposlene in njihove družine, delničarje, dobavitelje in stranke,
- Upravlja kaotično in stresno situacijo v prvih treh dneh krize,
- Pripravi usklajen odziv in informacije za medije,
- Začne pripravljene postopke za vzdrževanje stabilnosti storitev,
- Izvaja postopke za obnovo ključnih informacijskih in komunikacijskih sistemov,
- Zagotavlja osredotočanje management in zaposlenih na akcije za vzpostavitev normalnega poslovanja podjetja.

V (Crisis Management & Disaster Recovery, 2006) so navedeni štirje ključni razlogi za vpeljavo kriznega managementa v podjetje:

1. *Zmanjšanje osebne odgovornosti*.

   Osebna odgovornost vodilnih v podjetju za dejanja ali nedejanja v zvezi s poslovanjem podjetij je večinoma znana in sprejeta. Manj pa je znano, da se ta odgovornost lahko prenese tudi na ostale nivoje managementa in celo na ostale zaposlene. Če pride do velike izgube v podjetju zaradi katastrofe, se lahko ugotavlja odgovornost posameznikov za izgubo, če bi z ustreznimi dejanji lahko preprečili ali zmanjšali posledice katastrofe, pa jih niso izvedli.

   Zaposleni, ki delajo za podjetje, so v odnosu zaupanja s tem podjetjem. Tega morajo upravljati in ščititi v interesu delničarjev oz. lastnikov podjetja. Če odgovorna oseba prekine odnos zaupanja, je lahko za to odgovorna lastnikom podjetja.

2. *Zmanjšanje negativne reakcije.*

   Zgodovina je potrdila dejstvo, da v primeru nastanka krizne situacije v podjetju več dolgoročne škode naredijo zunanje osebe kakor sama krizna situacija. Požar, naravna katastrofa ali podobno imajo očiten in hiter vpliv na zmožnost delovanja podjetja. Odziv delničarjev in strank je zaskrbljenost za njihovo investicijo ali dobavo materiala, storitev. Posledica te zaskrbljenosti je njihova čim boljša zaščita interesov, brez upoštevanja koristi podjetja. Te posledice lahko preprečijo podjetju uspešno obnovo poslovanja, lahko za daljši čas ali pa tudi za stalno.

3. *Zavarovanje sredstev podjetja.*

   V primeru krizne situacije je lahko večina sredstev podjetja – produkti, sredstva, oprema, ljudje – izpostavljena tveganju. Brez vpeljanega kriznega managementa je v kaotičnem ozračju in stresnem okolju težko zagotoviti organiziran in takojšen odziv na situacijo. Situacija se s časom le poslabšuje. Samo takojšnje ukrepanje organizacije lahko zmanjša škodo in dostopnost sredstev podjetja.

4. *Zmanjšanje finančnih izgub.*

   Le manjši del možnih finančnih izgub je mogoče zaščititi preko zavarovalnic. Direktna izguba prodaje, začasna izguba proizvodnje ali nezmožnost izvajanja storitev so lahko skoraj zanemarljive v primerjavi z možnimi dolgoročnimi posledicami, kot so izguba tržišča, strank, zmanjšana privrženost strank produktu ali storitvi.

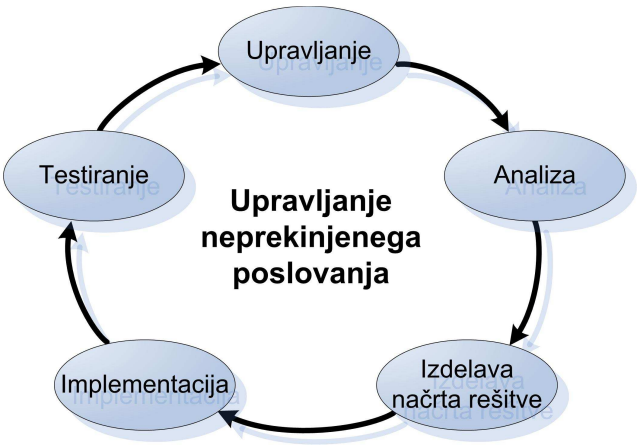
   Zavarovanje tako lahko pokrije kratkoročne posledice izpada, preprečevanje dolgoročnih posledic pa je naloga kriznega managementa in programov za odziv na krizo.

2.6 Uvajanje programa neprekinjenega poslovanja

Enciklopedija Wikipedia opisuje program neprekinjenega poslovanja v podjetju kot razvoj načrta neprekinjenega poslovanja, ki poteka v petih fazah: analiza, izdelava načrta rešitve, implementacija, testiranje in upravljanje (Slika 5).

Uvajanje programa neprekinjenega poslovanja v podjetje običajno poteka v dveh korakih:

1. Izvedba (enkratnega) projekta uvedbe neprekinjenega poslovanja v okviru katerega se izvede analiza, izdelava načrta rešitve, implementacija in na koncu testiranje uvedenega načrta,



Slika 5: Življenjski cikel upravljanja neprekinjenega poslovanja podjetja (vir: Wikipedia, 2006).

2. Po zaključku projekta, ki obsega skoraj celoten, zgoraj opisani cikel, se projekt zaključi oz. nadaljuje v program upravljanja neprekinjenega poslovanja, ki obsega celoten cikel neprekinjenega poslovanja podjetja.

Hiles v (Hiles et al., 2000) bolj natančno definira klasične korake cikla uvajanja neprekinjenega poslovanja v podjetje:

1. Razumevanje in predstavitev izzivov neprekinjenega poslovanja – dviganje zavedanja o problemu in prevzemanje obveznosti,
2. Načrtovanje projekta neprekinjenega poslovanja,
3. Izvajanje Analize tveganj in zmanjšanja tveganj,
4. Izvajanje Analize vpliva na poslovanje,
5. Definiranje strategije neprekinjenega poslovanja,
6. Izdelava načrta neprekinjenega poslovanja,
7. Razvoj in implementacija postopkov za vzdrževanje načrta neprekinjenega poslovanja,
8. Razvoj in implementacija izobraževanja skupine za neprekinjeno poslovanje ter načrtovanje programov testiranja.

Za uspešen začetek in vodenje projekta neprekinjenega poslovanja navaja kot ključne naslednje faktorje:

- Definicija in predstavitev potreb – razvoj in implementacija programa za dvig zavedanja v problematiki neprekinjenega poslovanja,

- Pridobitev podpore višjega managementa, po možnosti z izjavo ali politiko o neprekinjenem poslovanju podjetja,
- Vzpostavitev nadzorne komisije,
- Jasna določitev, razumevanje in sprejetje terminov, obsega in predpostavk,
- Obravnavanje upravljanja neprekinjenega poslovanja najprej kot projekt in nato kot program,
- Popolna vzpostavitev discipline in metod projektnega vodenja,
- Priprava začetnih finančnih zahtev,
- Poročanje višjemu managementu in uporaba drugih motivacijskih sredstev za ohranjanje momenta.

Iz naštetih faktorjev je posebej izpostavljen pomen dobre predpriprave na projekt, ki mora predstaviti problem, vzpostaviti sponzorstvo in sodelovanje s ključnimi udeleženci projekta ter kvalitetno definiranje ciljev in okvira projekta.

Noakes-Fry ponuja v (Noakes-Fry et al., 2004, str. 5-6) podoben način uvajanja neprekinjenega poslovanja, le da ga razdeli v tri faze:

1. faza – *Vzpostavitev osnove*, ki vsebuje tri elemente:
    - Vključitev vseh. S pristopom in zavezanostjo projektu od zgoraj navzdol je potrebno zagotoviti čas, denar in človeške vire za celoten projekt neprekinjenega poslovanja.
    - Analiza vpliva na poslovanje. Zahteve projekta temeljijo na ocenah stroškov in posledic izpada, ki jih podjetje pridobi z izvedbo analize vpliva na poslovanje, ter analizo tveganj.
    - Poslovna potreba. Na podlagi opisane analize je za poslovni načrt mogoče pridobiti sponzorstvo višjega managementa, vključujoč potrebne vire za izvedbo projekta.
2. faza – *Razvoj in implementacija načrta*, ki se nanaša na akcije, potrebne za razvoj načrta (ali načrtov) neprekinjenega poslovanja:
    - Analiza potreb in virov. Na podlagi analize vpliva na poslovanje se definirajo potrebni viri znotraj podjetja in po potrebi tudi zunanji viri.
    - Razvoj primernega načrta. Pri pripravi načrta je potrebno sodelovanje vseh zainteresiranih strank. Načrt mora vsebovati politiko obnove, obseg, ciljni čas vzpostavitve delovanja sistema, ciljno točko obnavljanja podatkov in natančne postopke.

3. faza – *Vzdrževanje načrta*, ki vsebuje dve akciji:
    - Posodobitev. Novi poslovni procesi, nova tveganja, nove tehnologije, spremembe telefonov, naslovov in drugo zahteva spremljanje in redno obnavljanje načrta neprekinjenega poslovanja.
    - Testiranje. Načrt je potrebno testirati, da se zaposleni z njim dobro seznanijo in da se sam načrt preveri v praksi.

2.6.1 Analiza

Prvo fazo cikla upravljanja neprekinjenega poslovanja predstavlja analiza trenutnega stanja, ki se po enciklopediji Wikipedia deli v štiri dele:

1. Analiza vpliva na poslovanje (glej 2.5.1).

2. Analiza tveganj (glej 2.5.2).

3. Definicija scenarijev posledic.

    Po definiciji možnih tveganj je priporočljivo definirati možne scenarije posledic. Priporoča se izdelava širših scenarijev katastrof, ki običajno vsebujejo tudi manjše, bolj omejene scenarije. Primer scenarija je npr. lahko »izguba glavne stavbe podjetja«, ki bo verjetno zajel vse glavne poslovne funkcije podjetja.

4. Izdelava dokumentacije o zahtevah obnove.

    Ob zaključku faze analize se poslovne in tehnične zahteve dokumentirajo za začetek izvajanja faze implementacije. Tipične zahteve za podjetja, ki intenzivno uporabljajo informacijsko tehnologijo in imajo pisarniško orientirano delovanje, bi lahko vključevala naslednje elemente:

    - Število in vrste delovnih mest, potrebnih na rezervni lokaciji,
    - Posamezniki, potrebni za obnovo poslovanja,
    - Programi in podatki, potrebni za delovanje kritičnih funkcij na rezervni lokaciji,
    - Rezervni postopki v primeru nedelovanja določenih poslovnih ali informacijskih funkcij,
    - Največji dovoljen izpad za posamezne poslovne funkcije, aplikacije,
    - Potrebna oprema na rezervni lokaciji: faks naprave, telefoni, papir, tiskalniki, kopirni stroji, pisala,...

Različna podjetja morajo glede na specifiko svoje dejavnosti v navedeni seznam dodati elemente, ki omogočajo opravljanje ključnih poslovnih funkcij na rezervni lokaciji.

2.6.2 Priprava načrta rešitve

Priprava načrta rešitve je sestavljena iz dveh delov, ki sta opisana v 2.5.3 in 2.5.4.

2.6.3 Vpeljava programa neprekinjenega poslovanja

Pri vpeljavi programa neprekinjenega poslovanja v podjetje je posebnega pomena vključevanje celotne organizacije v proces neprekinjenega poslovanja, kjer neprekinjeno poslovanje lahko postane del poslovnega procesa in ne le njegov dodatek. Šele na tej točki se lahko pričakuje, da bo neprekinjeno poslovanje pokazalo pravo poslovno vrednost. Sikich predlaga uporabo devetih postopkov, tehnik in orodij, s katerimi lahko dosežemo poslovno vrednost neprekinjenega poslovanja ali pripravimo poslovno priložnost za izvedbo načrta neprekinjenega poslovanja (Sikich, 2004):

1. Sistematično osredotočanje na človeški faktor. Kadar pride do krize v podjetju, se soočamo s človeškimi problemi in njihovo reševanje za nazaj ne prinese pozitivnih posledic. Zato je potrebno že vnaprej vzpostaviti ustrezne komunikacijske kanale.
2. Od zgoraj navzdol – od spodaj navzgor. Po eni strani je potrebno zagotoviti enotno komunikacijo vodstva podjetja po hierarhiji navzdol, po drugi strani pa prisluhniti in pomagati posameznikom v stresnem času.
3. Vključitev vseh nivojev. V proces priprave je potrebno vključiti vse nivoje podjetja in preko tega določiti ključne ljudi, ki so potrebni v primeru odpravljanja posledic katastrofe.
4. Vzpostavitev Ponudbe vrednosti (angl. value proposition). Poleg opredelitve zavezanosti vodstva podjetja programu neprekinjenega poslovanja je potrebno formalno vzpostaviti vire za izvedbo in nastaviti Ponudbo vrednosti, ki na vseh nivojih podjetja stimulira izvedbo.
5. Način izvajanja poslovanja, ne le dodatek k poslovanju. Potrebno je vpeljati lastništvo neprekinjenega poslovanja ter ga vpeti v poslovni proces in ne le kot dodatek k poslovanju.
6. Sporočanje zavezanosti. Odgovorni za izvajanje morajo zagotoviti prenos odločenosti vodstva podjetja o vpeljavi neprekinjenega poslovanja. To sporočilo je potrebno redno obnavljati med zaposlenimi.
7. Analiziranje kulture podjetja. Analiza kulture podjetja lahko pomaga pri izvedbi projekta. S prilagoditvijo kulturi podjetja se lahko povečajo koristi in zmanjša nasprotovanje pri vpeljavi.

8. Priprava na nepredvideno. Noben program neprekinjenega poslovanja ne more predvideti vseh možnosti, ki se lahko zgodijo v podjetju. Zato se je okviru programa in načrta neprekinjenega poslovanja potrebno razmišljati tudi o nepredvidenih dogodkih in reševanju stanja v tem primeru.
9. Osebno sporočilo. V primeru kriznega dogodka se posledice poznajo tako na celotni organizaciji kot na posameznih zaposlenih. Ljudje so pri uspešnosti programa neprekinjenega poslovanja ključni, zato je potrebno poleg načrtovanja samega procesa pozornost posvetiti tudi ključnim človeškim faktorjem.

2.6.4 Testiranje načrta neprekinjenega poslovanja

Namen testiranja je doseganje potrditve, da predlagana in implementirana rešitev neprekinjenega poslovanja ustreza zahtevam podjetja (Wikipedia, 2006).

Testiranje opredeljuje Šalehar-Kegl kot ključno fazo neprekinjenega delovanja. Ta omogoča preverjanje definiranih postopkov ter zmožnost vseh udeleženih zaposlenih in zunanjih izvajalcev za dosledno in učinkovito uporabo načrta. Testiranje je mogoče izvesti s preigravanjem scenarijev v obliki delavnic ali prek izvajanja simulacij. Temeljno pravilo testiranja je, da je vnaprej napovedano in da ne ovira rednih aktivnosti (Šalehar-Kegl et al., 2004).

Šele testiranje nam zares pokaže, ali smo načrt neprekinjenega poslovanja dobro pripravili. Seveda je vsak možni izpad različen in ni nujno, da ga načrt v celoti uspe obdelati, vseeno pa ima testiran načrt večjo možnost za uspeh kot načrt, ki ni testiran. Wallace (Wallace et al., 2004) navaja nekaj prednosti, ki jih testiranje prinaša:

- Pokaže, da načrt deluje,
- Identificira nepredvidene postopke, izdatke, zastoje,
- Preveri razpoložljivost virov,
- Ugotovi resničen čas trajanja obnove,
- Usposobi ljudi v njihovih vlogah pri obnovi
- Poveča zavedanje udeležencev o njihovi vlogi v načrtu neprekinjenega poslovanja.

Testiranje načrta neprekinjenega poslovanja lahko poteka na tri načine:

- Simulacija testiranja, kjer se umetno naredi krizno stanje in se potem na podlagi tega teoretično pregleda in preveri načrt. Ta način omogoča preverjanje načrta v primeru različnih scenarijev .

- Delno testiranje pomeni testiranje le določenega dela načrta neprekinjenega poslovanja. Omogoča testiranje načrta v bolj resničnih razmerah, vendar ga še vedno omejimo v tak okvir, da ob slabem delovanju načrta ne more povzročiti katastrofe.
- Polno testiranje pomeni testiranje celotnega načrta ob izpadu sistema ali prenosu produkcije na rezervno lokacijo. To testiranje da najboljšo sliko o kvaliteti načrta in upravljanja neprekinjenega poslovanja, vendar pa s seboj prinaša tveganje. Če se takega testiranja lotimo prezgodaj, lahko povzročimo težave ali celo izpad poslovanja.

Harris predlaga pet nivojev testiranja (Harris, 2003), ki se razlikujejo glede na obseg testiranja, vključenost produkcije in možne posledice v primeru neuspešnega testiranja. Teh pet nivojev je naslednjih:

- Testiranje s kontrolnim seznamom,
- Testiranje s strukturiranim pregledom (angl. structured walk-through),
- Simulirano testiranje,
- Vzporedno testiranje,
- Testiranje popolne prekinitve.

Priporoča se, da se testiranje izvaja zaporedoma po teh nivojih in da se nivoji testiranja ne preskakujejo. V nasprotnem primeru lahko pride do resnih motenj pri delovanju podjetij, ki lahko pripeljejo pod vprašaj celo obstoj podjetja.

2.6.5 Upravljanje programa neprekinjenega poslovanja

Povzeto po (Andolšek, 2001, str. 29) je ključna sestavina vzdrževanja načrta neprekinjenega poslovanja testiranje, ki sem ga že obdelal v prejšnjem podpoglavju. Upravljanje programa pa pomeni tudi njegovo vzdrževanje. Vse spremembe načrta morajo biti predstavljene odgovornim za izvajanje načrta. Andolšek še posebej poudarja, da je pri upravljanju programa neprekinjenega poslovanja pomembno k vzdrževanju in testiranju pritegniti neodvisne svetovalce. Ti na načrt ne gledajo z istega zornega kota kot njegovi razvijalci, zato lahko opazijo pomanjkljivosti, ki so jih slednji spregledali.

Wikipedia opredeljuje upravljanje načrta neprekinjenega poslovanja kot tri periodične aktivnosti, ki se morajo ponavljati vsaj letno:

1. Preverjanje in posodobitev informacij v načrtu. Organizacije se s časom spreminjajo in zato se mora načrt neprekinjenega poslovanja temu

prilagajati. Običajne so spremembe osebja, strank, dobaviteljev, včasih pa tudi spremembe v organizacija, npr. oddelkov.

2. Preverjanje tehničnih rešitev. Sem sodi redno vzdrževanje strojne opreme, aplikativne varnosti, virusnih definicij, delovanja aplikacij, pravilnosti podatkov.

3. Preverjanje postopkov za okrevanje organizacije. S spremembami delovnega procesa, ki se običajno dogaja skozi čas, morda organizacijski okrevalni postopki niso več primerni.

2.7 Spodbujevalci uvajanja neprekinjenega poslovanja

Ideja o vpeljavi neprekinjenega poslovanja v podjetje običajno ni ena prvih misli podjetja. Misli, energija in delovanje so, razumljivo, usmerjene predvsem v učinkovito, uspešno poslovanje podjetja, izdelovanje produkta ali storitve, uspešna prodaja in čim večji profit. Misel na »črni« scenarij, ko gre narobe vse, kar lahko sploh gre, se običajno odžene. Tako ni presenetljivo, da se neprekinjenega poslovanja v večini primerov uvaja na zunanjo iniciativo, kot je zakon, regulativa, delničarji, revizorji. Navkljub temu pa podjetja ugotavljajo, da uvajanje neprekinjenega poslovanja tudi podjetju prinese precej koristi, lahko tudi konkurenčno prednost. Upamo lahko, da bodo take pozitivne izkušnje pripeljale do večjega zanimanja in posnemanja med managementom, ki bi moral postati osnovni spodbujevalec vpeljave neprekinjenega poslovanja.

Noakes-Fry v svoji raziskavi (Noakes-Fry et al., 2004, str. 10) ugotavlja, da je največjo uporabo in uvajanje neprekinjenega poslovanja mogoče zaslediti v reguliranih dejavnostih. Državna uprava, finančna industrija, zdravstvo in javna podjetja ostajajo najmočnejši uporabniki storitev in produktov neprekinjenega poslovanja. Razvoj elektronskega prenosa in povezovanja med podjetji (B2B) ter podjetji in strankami (B2C) je razširil mrežo podjetij, kjer je potrebna vpeljava neprekinjenega poslovanja. Vključena so predvsem velika in srednja podjetja (za svetovne razmere), predvsem tista, ki potrebujejo usklajenost z industrijsko regulativo in ISO900x/IEC standardi.

2.7.1 Regulativa

V svetu obstaja precej zakonov, ki obravnavajo delovanje organizacij in med drugim od organizacij zahtevajo ali jim priporočajo vpeljavo neprekinjenega poslovanja ali njegovega dela. Noakes-Fry v (Noakes-Fry et al., 2005, str. 2-5) navaja zakone in regulativo, ki so v veljavi v ZDA:

Področje	Zakon in regulativa	Vpliv na neprekinjeno poslovanje
Zdravstvo	HIPAA, 1996	Zahteva načrt varnostnega kopiranja, obnove po katastrofi in načrt delovanja v izrednih razmerah.
	FDA CFR, Title XXI, 1999	Zahteva elektronski zapis in elektronski podpis.
Državna uprava	FISMA, 2002	Poudarek na varnosti podatkov. Zahteva po delovanju vlade med krizo.
	COOP and COG, 1999	Določa minimalne zahteve za načrt delovanja ameriške zvezne vlade.
	NIST SP 800-34, 2002	Zahteva načrt za nepredvidene dogodke, obnovo po katastrofi in neprekinjeno izvajanje operacij.
	NIST 800-53, 2005	Zahteva načrtovanje, načrt, izobraževanje, testiranje in obnovo za primer nepredvidenih dogodkov.
Finance	FFIEC Handbook, 2003-2004	Določi direktorje in management za odgovorne za načrtovanje ponovne vzpostavitve operacij po katastrofi.
	Basel II, 2003	Zahteva, da banke vzpostavijo neprekinjeno poslovanje in obnovo po katastrofi.
	Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 2003	Zahteva od bank, da v okviru neprekinjenega poslovanja obravnavajo tveganja, ki so bila odkrita ob napadu na WTC.
	EFA Act, 1989	Zahteva od zvezno pooblaščenih finančnih institucij, da imajo načrt neprekinjenega poslovanja.
Javna podjetja	GASB statement No. 34, 1999	Zahteva načrt neprekinjenega poslovanja.
	NERC 1200 (1216.1), 2003	Načrt neprekinjenega poslovanja zaenkrat še ni obvezen.
	FERC RM01-12-00, 2003	Zahteva načrt neprekinjenega poslovanja.

Področje	Zakon in regulativa	Vpliv na neprekinjeno poslovanje
	RUS 7 CFR Part 1730, 2005	Zahteva načrt obnove v izrednih razmerah.
	Telecommunications Act of 1996, Section 256, Coordination for Interconnectivity	Zahteva vzpostavitev postopkov za nadzor koordiniranega načrtovanja telekomunikacijskega omrežja.
	NERC Security Guidelines for the Electricity Sector, 2001	Zahteva neprekinjeno poslovanje in informacijsko varnost od podjetij, ki sodelujejo z vlado.

Tabela 2: Regulativa s področja neprekinjenega poslovanja v ZDA (vir: Noakes-Fry et al., 2005, str. 2-5).

Od naštetih je v Sloveniji prisoten le Basel II, zato ga v nadaljevanju natančneje opisujem. Dodatno sem opisal še HIPAA, ki ureja področje zdravstva. Na tem področju pri nas ni primerljive regulative.

Basel II

Konec leta 1974 je bil ustanovljen Baselski odbor za bančni nadzor, ki so ga sestavljali guvernerji centralnih bank desetih držav. Odbor je formuliral široke standarde in navodila za nadzor v bančnem sektorju, ki jih centralne banke potem vpeljejo v posameznih državah. Basel II, imenovan tudi Novi sporazum, predstavlja priporočila nadzornikov bank in guvernerjev centralnih bank trinajstih držav, ki so združena v mednarodni standard za merjenje primernosti bančnega kapitala.

Po Božiču (Božič, 2005, str. 5-7) naj bi nova pravila za ugotavljanje kapitalske ustreznosti bank bolje povezala regulativne kapitalske zahteve z dejanskim ekonomskim kapitalom, ki ga banke potrebujejo glede na obseg in tveganost svojih poslov. Osrednji poudarek je na obravnavanju minimalnih zahtev za kapitalsko ustreznost: na učinkovitejši obravnavi kreditnega tveganja ter dodanih zahtevah za operativno tveganje.

Cilj sporazuma je predvsem povečanje varnosti in stabilnosti v mednarodnem finančnem sistemu, povečanje konkurenčne enakosti med bankami iz različnih držav, razvoj bolj celovitega pristopa k merjenju tveganj in uporabnost novih kapitalskih pravil za vse banke po svetu. Dogovor spodbuja krepitev mednarodnega finančnega sistema in uveljavlja vzpodbude finančnim ustanovam za uvajanje učinkovitejših praktičnih rešitev za obvladovanje tveganja. V ta namen ima dogovor tri osnovne stebre:

1. steber: *Minimalne kapitalske zahteve* – obravnava minimalno zahtevo za kapitalsko ustreznost in ga sestavljata dva dela: način določanja uteži za naložbe in način določanja minimalnega zakonskega kapitala.

2. steber: *Regulativni nadzor* – vsebuje pravila nadzora nad uveljavljanjem pravil ustreznosti kapitala.

3. steber: *Tržna disciplina* – obravnava področje razkrivanja poslovanja bank tržnim udeležencem.

Pod prvi steber Minimalnih kapitalskih zahtev sodi upravljanje tveganja, ki obsega tržno, kreditno in operativno tveganje. *Operativno tveganje* je tveganje posredne ali neposredne izgube zaradi neprimernega ali izpadlega internega poslovnega procesa, ljudi ali sistemov ali zaradi zunanjega dogodka.

Kot analizira (Honey, 2002) se neprekinjeno poslovanje podjetij sreča z implementacijo Basel II v bančnem svetu na točki operativnega tveganja, ki lahko povzroči zmanjšanje količnika donosnosti sredstev (angl. return on equity – ROE).

Z vpeljavo celovitega načrta neprekinjenega poslovanja se zmanjša operativno tveganje za podjetje, s tem pa se zmanjša tudi alokacija kapitala za operativno tveganje (Božič, 2005, str. 7-12).

Za uskladitev operativnega tveganja in načrta neprekinjenega poslovanja vidi (Honey, 2002) naslednje točke oz. korake:

- Definicija okvira operativnega tveganja,
- Definicija politike operativnega tveganja,
- Identifikacija tveganj in ugotavljanje izgub,
- Samo-analiza tveganj s strani poslovanja (BIA),
- Vzpostavitev komunikacije in zavedanja o tveganjih med zaposlenimi,
- Izvajanje zmanjševanja tveganj,
- Poročilo o stanju tveganj in glavnih kazalcih tveganj,
- Razvoj metodologije upravljanja alokacije kapitala.

Zahteva po upravljanju neprekinjenega poslovanja je ena osnovnih zahtev in rezultatov Basel II dogovora. Glede na finančne posledice in posledično slabšo konkurenčnost pelje finančna podjetja v smeri vpeljave načrta in nato upravljanja neprekinjenega poslovanja podjetja.

HIPAA

HIPAA je predpis za zdravstvene organizacije v ZDA, ki določa standarde in postopke za elektronsko shranjevanje, uporabo in izmenjavo osebnih medicinskih podatkov in zdravstvenih podatkov. Leta 1996 ga je potrdil ameriški kongres (Harris, 2003).

Predpis je sestavljen iz dveh dokumentov:

1. dokument (angl. Title I: Health Care Access, Portability, and Renewability) varuje pokritje zdravstvenega zavarovanja za zdravniške delavce in njihove družinske člane, kadar menjajo ali izgubijo službo,

2. dokument (angl. Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform) zahteva vzpostavitev standardov za izmenjave zdravstvenih podatkov ter enotnih oznak za dobavitelje, zavarovalnice in zaposlene v zdravstvu. Obenem obravnava tudi varnost in zasebnost zdravstvenih podatkov. Namen vpeljave standardov je izboljšanje zmožnosti in učinkovitosti zdravstvenega sistema s spodbudo pri uvajanju elektronske izmenjave podatkov.

Za obravnavano temo te naloge je zanimiv predvsem 2. dokument, ki definira številne prestopke v povezavi z zdravstvom ter določata tudi kazenske sankcije v primeru nespoštovanja le-teh. Določa programe za nadzor nad prevarami in zlorabami znotraj zdravstvenih sistemov. V okviru HIPAA je bila postavljena tudi zahteva, da »Department of Health and Human Services« pripravi pravila, ki bodo omogočila učinkovitejšo uporabo zdravstvenih sistemov. Omenjena institucija je pripravila pet pravil:

1. Pravilo zasebnosti (angl. privacy rule) uvaja zaščito in nadzor nad varovanimi zdravstvenimi informacijami (angl. protected health information). Te obsegajo informacije o zdravstvenem stanju, ukrepih zdravljenja ali plačilu za zdravljenje, ki jih lahko povežemo na posameznega pacienta. Interpretacija je precej široka in obsega katerikoli del zdravstvenih podatkov pacienta ali plačilne zgodovine.

2. Pravilo o izmenjavi in obliki podatkov (angl. transactions and code sets rule) določa obliko prenosa podatkov, ki je kompatibilen z X12 in se označuje kot HIPAA/EDI.

3. Pravilo varnosti (angl. security rule) dopolnjuje pravilo zasebnosti in določa tri vrste varnostnih mehanizmov: administrativni, fizični in tehnični. Za vsakega od njih opredeli različne varnostne standarde in znotraj njih določi, kateri ukrepi so zahtevani in kateri le priporočeni.

4. Pravilo enoličnih identitet (angl. unique identifiers rule) vpeljuje sistem enotnih oznak za dobavitelje, zavarovalnice in zaposlene v zdravstvu.

5. Pravilo vpeljave (angl. enforcement rule) je bilo zadnje in določa 16. marec 2006 za datum, do katerega so morali biti vpeljani postopki povezani s HIPAA predpisom ter določa kazni v primeru njegovega nespoštovanja.

V okviru opisanega 3. pravila (Pravilo varnosti) obstajajo tudi varnostni mehanizmi, ki omogočajo in zahtevajo izvajanje neprekinjenega poslovanja zdravstvenih ustanov:

- Vzpostavljen mora biti načrt za nepredvidljive dogodke (angl. contingency plan), ki ga sestavljata rezervno kopiranje podatkov in vzpostavljen načrt obnove poslovanja. Celoten načrt mora določati prioritete podatkov, postopek analize dogodka, aktivnosti testiranja in postopke za spremembo kontrol.

- Izpeljana in dokumentirana mora biti analiza tveganja ter vpeljan program za nadzor tveganja. Obravnavana morajo biti tveganja, ki so pomembna za izvajanje poslovnih funkcij posamezne zdravstvene enote ter izvedena analiza in odločitev glede zmanjševanja tveganj na ustrezno raven.

- Vzpostavljeni morajo biti postopki za nadzor in odziv na varnostne incidente, ki so zaznani med normalnim delovanjem ali med izvajanjem nadzora delovanja.

- Notranji nadzor predstavlja ključno točko HIPAA usklajenosti s preverjanjem potencialnih varnostnih kršitev.

HIPAA postavlja ključne elemente zagotavljanja neprekinjenega poslovanja in predstavlja močan temelj za njegovo implementacijo. Žal je vpeljan le v ZDA, medtem ko na področju zdravstva v Sloveniji ta hip ni vpeljan primerljiv zakon ali standard.

2.7.2 Management

Management predstavlja osnovni spodbujevalec za vpeljavo programa neprekinjenega poslovanja. Brez polne podpore in sodelovanja managementa si je težko predstavljati uspeh takega programa. Da pa management to svojo vlogo sprejme in jo vzame za svojo, so včasih potrebne aktivnosti za predstavitev prednosti vzpostavitve programa.

Scott v (Scott et al., 2005, str. 2-4) ugotavlja, da se vpliv prekinitve na poslovanje bistveno povečal in s tem tudi zahteva po neprekinjenem poslovanju. Odgovornost za neprekinjeno poslovanje ne leži v oddelku informatike, temveč v vsaki poslovni

enoti. Zato mora višji management razumeti svojo udeležbo v procesu ter zahtevo po sponzorju v vrhu podjetja. Podjetja z najboljšo prakso na tem področju imajo neprekinjenost vtkano v kulturo podjetja in po drugi strani dobro razumevanje posledic izpada poslovnih funkcij.

V kolikor management podjetja ne razume vrednosti neprekinjenega poslovanja oz. ga jemlje kot nepotreben strošek, predlaga Scott nekaj pristopov, ki lahko izboljšajo pogled managementa na to področje:

1. Povečanje zavedanja o možnosti katastrofe. Dogodki v zadnjih letih – napad na WTC, izpad električne energije na severovzhodu ZDA, bombni napadi v Madridu in Londonu, orkana Katrina in Rita – lahko uporabimo za pogovor z višjim managementom o možnih nevarnostih, ki bi lahko resno prekinila poslovni proces. Možne posledice so lahko:

   - Prekinitev oskrbovalne verige,
   - Skrb za večjo skupino ljudi, ki ne morejo zapustiti delovnega mesta,
   - Pomanjkanje delovne sile, ker so morali zapustiti domove,
   - Izpad kritičnih aplikacij poslovnega procesa,
   - Pomanjkanje finančnih sredstev po katastrofi lahko povzroči še daljše čase obnove poslovanja.

   Zavedanje o možnih katastrofah pomaga dvigniti zavedanje višjega managementa o potrebi po neprekinjenem poslovanju in obnovi po katastrofi ter zagotoviti, da se enkraten projekt prelevi v trajen program. Management se mora zavedati tudi incidentov, ki so se zgodili v podjetju in na kakšen način so bili rešeni. Zagotoviti je potrebno evidentiranje teh dogodkov in redno poročanje. Pregled incidentov podjetij v sorodni dejavnosti ali iz iste regije lahko prikaže pomembnost načrtovanja neprekinjenega poslovanja.

2. Odgovornost managementa. V delniških družbah lahko zavedanje o tveganjih in odgovornosti podjetja povečajo notranji in zunanji revizorji ter finančni direktor. Pri javnih podjetjih, državnih inštitucijah ali bolnišnicah lahko dodatno pomaga tudi trening in priprava na komuniciranje z mediji po incidentu.

   Če ne gre drugače, Scott priporoča načrtovalcem neprekinjenega poslovanja in obnove po katastrofi, da previdno opozorijo višji management na zaupano odgovornost, da varujejo premoženje družbe. Če tega ne izpolnjujejo, tvegajo očitek malomarnosti in tudi možno odgovornost. Načrtovalci neprekinjenega poslovanja lahko v sodelovanju z oddelkom za upravljanje s človeškimi viri, pravnim oddelkom, interno revizijo in

oddelkom za skladnost in upravljanje tveganja pripravijo poslovni načrt, ki bi pokazal, da načrt neprekinjenega poslovanja dolgoročno cenejša možnost.

3. Izvedba neuradne analize vpliva na poslovanje, analize tveganj in namizni test. Načrtovalci neprekinjenega poslovanja lahko izvedejo pogovore s ključnimi poslovnimi managerji in ugotovijo vpliv izpada lokacije ali vira na poslovni proces. Ugotavljajo finančne in nefinančne posledice ter rezultate predstavijo višjemu managementu.

   Pri namiznem testu ljudje iz oddelka informatike in iz poslovnih enot za mizo izvajajo načrte obnove. To omogoča udeležencem iz poslovnih enot boljše razumevanje postopkov in oceno, če so le-ti izvedljivi v praksi. Taki testi lahko pomagajo pri pripravi poslovnih razlogov za odpravo odkritih neustreznosti pri načrtu.

   Stranski učinki neformalne analize učinka na poslovanje so še:

   - Boljše razumevanje vrzeli med poslovno zahtevano in trenutno možno obnovo poslovanja,
   - Boljša opredelitev in razvrstitev pomembnosti posameznih nalog v okviru neprekinjenega poslovanja,
   - Boljše razumevanje povezanosti med poslovnimi oddelki in zunanjimi ponudniki storitev. Izpad tega načrtovanja lahko posledično povzroči neuspešno obnovo poslovanja.

4. Povečanje zavedanja o regulativi, ki zahteva neprekinjeno poslovanje. Nekatere dejavnosti so uravnavane s regulativo, ki predpisuje neprekinjeno poslovanje in obnovo po katastrofi. V Sloveniji to velja predvsem za finančno industrijo, medtem ko v tujini sem sodi tudi zdravstvo, telekomunikacije, državna uprava. Seznanitev managementa z regulativo omogoči izogibanje možnim posledicam zaradi neusklajenosti.

5. Pravilno organiziranje. Če odgovornost za neprekinjeno poslovanje ostane v poslovnih enotah in ne v oddelku informatike, je tako zagotovljena boljša možnost za ustrezno podporo programu. Odgovornost za informacijsko opremo mora ostati v oddelku informatike. Osrednja koordinacija ekip na neprekinjeno poslovanje v poslovnih enotah in ekipe za obnovo po katastrofi v oddelku informatike pomaga zagotavljati ustrezno voden program.

Obstaja več načinov, kako pridobiti podporo višjega managementa za program neprekinjenega poslovanja. Povečanje zavedanja o možnih izpadih, o posledičnih

stroških ter o zahtevah zakonov in regulative predstavlja dobro osnovo za pridobitev njihovega sodelovanja.

Management podjetja je s strani lastnikov pooblaščen, da z imetjem podjetja upravlja kot dober gospodar in primerno skrbno (angl. due diligence / due care). Enciklopedija Wikipedija opredeljuje prvo geslo (Due diligence) kot odgovornost za raziskavo in identifikacijo spornih zadev, ter drugo geslo (Due care) kot odgovornost, da se glede izsledkov nekaj naredi. V zahodnem svetu to lahko pomeni, da je management podjetja kazensko odgovoren lastnikom, če ni naredil vsega potrebnega, da se določena škoda ne bi zgodila. Pri tem se dejanja opredeljuje glede na dobro prakso za posamezne dejavnosti. Vpeljava neprekinjenega poslovanja v podjetje se v čedalje večji meri šteje kot izvajanje dobre prakse.

2.7.3 Notranja in zunanja revizija

Revizija pomeni vrednotenje organizacije, sistemov, procesov ali produktov. Od revizorjev se pričakuje, da so kompetentni, neodvisni, objektivni in nepristranski. Cilj je izvedba neodvisne ocene finančnih razmer, računovodske prakse, internih kontrol, … Revizija vrednoti skladnost v sedanjosti in tudi v prihodnosti za razliko od inšpekcije, ki pregleduje skladnost v preteklosti (Wikipedia, 2006).

Pri izvajanju revizije neprekinjenega poslovanja in še posebej načrta obnove po katastrofi se pregledujejo vsaj naslednji elementi:

- Napisan in redno obnavljan načrt obnove po katastrofi,
- Določena vroča ali hladna rezervna lokacija,
- Zmožnost obnavljanja podatkov in sistemov,
- Postopek za redno izvajanje varnostnih kopij sistemov in podatkov,
- Testiranje in urjenje v postopkih ob katastrofi,
- Podatki in sistemske varnostne kopije so shranjene na oddaljeni lokaciji,
- Imenovana je komisija in njen vodja za obnovo ob katastrofi,
- Vidno navedene telefonske številke za primer nevarnosti,
- Ustrezno zavarovanje,
- Postopki za omogočanje učinkovite komunikacije med ekipo za obnovo in managementom,
- Vzdrževani podatki o sistemu in izvajanju operacij,
- Postopki za primer nevarnosti,
- Določene zamenjave za ključne funkcije,

- Seznam strojne in programske opreme,
- Izjava o poslanstvu v načrtu obnove po katastrofi,
- Vpeljani ročni in avtomatski postopki,
- Ustrezne pogodbe z zunanjimi agencijami in podjetji

Podjetja so podvrževa reviziji poslovanja zaradi zakonskih zahtev ali s strani lastnikov oz. delničarjev. V vseh primerih pa je revizija dejstvo za veliko slovenskih podjetij in s tem bo zahteva po vzpostavljanju in upravljanju neprekinjenega poslovanja dobila še dodatno težo v managementu podjetij.

2.7.4 Vpetost v proizvodne verige drugih podjetij

Podjetja, ki uvedejo program neprekinjenega poslovanja, poskušajo stabilnost in gibčnost svojega delovanja doseči tudi s širjenjem zahtev na zunanje partnerje. Na prvem mestu so običajno ponudniki storitev, npr. dostopa do interneta, zagotavljanjem elektronske pošte, varnosti. S temi ponudniki se običajno sklene pogodba o zagotavljanju nivoja storitve (angl. service level agreement).

Podobno velja za oskrbovalno verigo oz. za podjetja, ki sodelujejo v njih. Zahteve po uvedbi načrta neprekinjenega poslovanja se prenašajo izven podjetij na njihove dobavitelje in preko tega zagotavljajo neprekinjeno delovanje celotne oskrbovalne verige. Ta pristop se vpeljuje predvsem na razvitih trgih, kamor pa s sodelovanjem na njih segajo tudi slovenska podjetja.

2.8 Organizacija za upravljanje neprekinjenega poslovanja

Krischer (Krischer et al., 2005, str. 3-4) ugotavlja, da v veliko podjetjih obstaja prepričanje, da se neprekinjeno poslovanje konča z obnovo tehnološke infrastrukture, kot so omrežje, telekomunikacije, aplikacije in delovne postaje. V primeru katastrofe ali testiranja se nato lahko pokaže pomanjkljivost takega pristopa. Primer je lahko npr. drugačen telefonski sistem na rezervni lokaciji ali posebna delovna postaja, ki ni obnovljena na rezervni lokaciji. Do takih napak lahko prihaja, če se vse načrtovanje neprekinjenega poslovanja prepusti oddelku informatike brez sodelovanja poslovnega dela podjetja.

Če je priprava načrta neprekinjenega poslovanja prepuščena le oddelku informatike, se lahko zgodi, da poudarek načrta sloni na tehnično izvedljivih rešitvah in ne na poslovno potrebnih. Zato je pri pripravi, izdelavi, testiranju in izvajanju načrta neprekinjenega poslovanja nujno sodelovanje managementa podjetja, skupaj z oddelkom informatike.

Kovačič (Kovačič et al., 2004, str. 299) predlaga delitev službe za informatiko na štiri skupine: pomoč in storitve, načrtovanje razvoja, razvoj programskih rešitev in informatika poslovnih enot. V skupino Pomoč in storitve sodi tudi oddelek za zagotavljanje kakovosti, kamor sodijo aktivnosti skrbništvo podatkov, procesov, zagotavljanje varnosti, interna revizija. Informacijski del organizacije za upravljanje neprekinjenega poslovanja sodi verjetno v ta oddelek. Smiselno pa je, da je vrhnji del te organiziranosti v oddelku interne revizije.

Pogled na organiziranje s poslovne strani pokaže Krutz v (Krutz et al., 2003), kjer predlaga da se v organizacijo za upravljanje neprekinjenega poslovanja vključijo vsi bistveni deli podjetja v Komisijo za neprekinjeno poslovanje, v kateri morajo biti prisotni:

- Višji management,
- Funkcionalne poslovne enote,
- Informatika,
- Varnostno upravljanje.

Naloga in odgovornost te komisije je izdelava, vpeljava in preverjanje načrta neprekinjenega poslovanja.

Pomembno vlogo pripisuje Krutz višjemu managementu, ki mora s svojim sodelovanjem, podporo in nadzorom stalno sodelovati pri pripravi in upravljanju načrta. Pri testiranju načrta mora prevzeti vlogo upravljanja, med kritičnimi dogodki pa nadzor in izvajanje načrta. Sodelovanje višjega managementa je v programu neprekinjenega poslovanja nujno; brez njihove vključitve se verjetnost neuspeha celotnega projekta in programa bistveno poveča.

Krutz predlaga ustanovitev dve operativnih ekip za delovanje v primeru katastrofe:

1. *Ekipa za obnovo* skrbi za čim hitrejšo vzpostavitev delovanja na rezervni lokaciji. Z delom začne takoj, ko je razglašeno stanje katastrofe. Pri tem upošteva dogovorjene postopke za vzpostavitev poslovanja na rezervni lokaciji z upoštevanjem prioritet za ponovno vzpostavitev kritičnih poslovnih funkcij.
2. *Reševalna ekipa* (angl. salvage team) poskrbi za obnovo osnovne lokacije in vzpostavitev stanja, ki omogoča prehod iz rezervne lokacije v običajno delovanje. Ugotoviti mora stanje na osnovni lokaciji, poškodbe prostorov in opreme ter način obnove oz. vzpostavitve prvotnega stanja.

V okviru organiziranja neprekinjenega poslovanja mora podjetje zagotoviti upravljanje še treh področij, ki segajo preko meja podjetja:

1. *Sodelovanje z zunanjimi partnerji*, ki so po potrebi lahko vključene v obnovo poslovanja v primeru katastrofe, kot so npr. gasilci, policija, zdravstvena ustanova, varnostna služba. Sem sodijo tudi druge zunanje zainteresirane skupine, kamor sodijo zavarovalnica, stranke, dobavitelji, delničarji,... Za vse pomembne skupine mora biti določen postopek komuniciranja z njimi.

2. *Zaposleni in njihove družine* morajo biti obveščeni o okoliščinah v organizaciji, spremenjenih razmerah za delo in podobno. Ta komunikacija je nujno potrebna za uspešno obnovo poslovanja in sodelovanje zaposlenih v teh razmerah. Obenem mora organizacija za zaposlene zagotoviti tudi nujne življenjske potrebščine v primeru katastrofe – npr. izplačevanje plače.

3. *Komunikacija z mediji* je pomembno področje dela v primeru katastrofe. Organizacija mora zagotoviti primerne informacije za medije in javnost, pri tem pa paziti, da se pri tej komunikaciji ne sproži panika in širi negotovost. Običajno imajo podjetja za posebne razmere določeno osebo, ki bo komunicirala z mediji, pri tem pa mora vse informacije predhodno pogledati in potrditi višji management.

Za delovanje organizacije v primeru katastrofe morajo biti predhodno pripravljene in redno popravljane kontaktne informacije ključnih ljudi pri obnovi. Poleg tega mora biti vzpostavljen sistem za obveščanje udeleženih. Ker v primeru katastrofe lahko precejšen del infrastrukture izpade (npr. telefonske povezave), je potrebno za potrebe obveščanja izbrati tudi rezervne načine obveščanja.

2.9 Poslovna vrednost programa neprekinjenega poslovanja

Scott v (Scott, 1998) ugotavlja, da je zaradi močne integracije informacijske tehnologije v poslovne procese, vloga le-te postala kritična. Ob izpadu kritičnih aplikacij običajno ročni postopki niso smiselni. Rezultat je podoben kot ob izpadu telefonskih povezav ali električne energije, le da v primeru razpoložljivosti informacijske tehnologije le-te ne moremo enostavno kupiti ali zamenjati – zgraditi je potrebno ustrezno infrastrukturno in aplikacijsko arhitekturo ter vpeljati učinkovit informacijski proces za izvajanje razpoložljivosti.

Pri določanju vrednosti potrebne investicije mora podjetje najprej razumeti posledice izpada poslovanja. Glavne posledice izpada poslovanja so po Scottu naslednje:

1. *Prihodek*. Vsako zmanjšanje ali zaustavitev proizvodnje produktov in storitev ima posledice pri prihodkih. Izguba je odvisna od različnih faktorjev: tekmovalnosti v panogi, lojalnosti strank. Dodatno izgubo lahko vidimo v izgubi prihodnjih prihodkov zaradi zmanjšanega ugleda podjetja.

2. *Produktivnost*. Zaustavitev proizvodnje povzroči manjšo učinkovitost zaposlenih. Na nekaterih področjih, kot je npr. klicni center, je neučinkovitost lahko popolna, medtem ko je na drugih področjih lahko tudi zanemarljiva.

3. *Zmanjšan ugled*. Z zavarovalnimi policami lahko delno povrnemo izgubljen prihodek ob izpadu poslovanja, ne moremo pa zavarovati oz. povrniti dolgoročne posledice izgube ugleda in podobe podjetja pri strankah. Te izgube se ne poznajo le na bodočem prihodku, temveč tudi pri stikih s strankami, dobavitelji, poslovnimi partnerji, finančnimi institucijami.

4. *Finančna učinkovitost*. Posledica vseh naštetih učinkov izpada je zmanjšana finančna učinkovitost. Zakasnitve ali zmanjšani prihodki imajo lahko posledice pri računovodskih izkazih, denarnem toku, ceni delnice. Zamude pri plačilu dobaviteljem lahko povzročijo izgubo popustov ali izgubo kreditne ocene.

5. *Ostali stroški*. Glede na posledice in čas izpada poslovanja se lahko pojavijo še dodatni stroški, kot so npr. pravni postopki zaradi neizpolnjenih dogovorov in dodatni stroški za obnovitev poslovnega procesa.

Od naštetih posledic sta za podjetja običajno najpomembnejša prva dva faktorja.

Warrick v (Warrick et al., 2005, str. 5) določa naslednje poslovne probleme, ki jih podjetje rešuje tudi v okviru programa neprekinjenega poslovanja:

- *Neprekinjenost poslovnih operacij*. Podjetju pomaga pri doseganju prilagodljivosti in vzdržljivosti od informacijske tehnologije do poslovnih procesov.
- *Usklajenost z zakonodajo* in regulativo se izvaja hitreje in cenovno učinkovitejše.
- *Zmanjševanje stroškov upravljanja tveganja*. Podjetje lahko učinkoviteje upravlja s tveganji in s tem izboljšuje svojo konkurenčnost.
- *Varnost, zasebnost in zaščita podatkov*. Pomaga pri zaščiti podjetja pred tveganji in omogoča izdelavo strategije upravljanja kritičnih informacij.
- *Znanja in sposobnosti*. Podjetju omogočajo pridobitev potrebnih znanj za neprekinjeno izvajanje poslovnih operacij.

- *Vzdrževanje tržne pripravljenosti*. Podjetje lahko bolje predvidi in se hitreje prilagaja spremembam na trgu.
- *Postati boljši poslovni partner*. Podjetju se dvigne status in postane bolj zaupanja vredno v oskrbovalni verigi.

Zgoraj našteti faktorji omogočajo programu neprekinjenega poslovanja informatike dobro uskladitev s strateškimi načrti podjetja in s tem sodelovanje pri vzdrževanju rasti, boljši donosnosti in povečani vrednosti delničarjev.

Leta 2003 je skupina strokovnjakov z različnih področij v okviru Foruma vrednosti informatike (angl. IT value forum) izpostavila ključne elemente za opredelitev lete. Goldstein v svojem članku (Goldstein et al., 2003, str. 15-17) povzema glavne ugotovitve foruma v štirih točkah:

1. *Določanje vrednosti*. Če želimo vrednost informatike meriti, jo je potrebno najprej opredeliti. Definirati je potrebno želene koristi na eni strani in zmožnosti tehnologije na drugi strani.
2. *Zavedanje vrednosti*. Informacijska tehnologija sama po sebi nima resnične vrednosti. Pridobi jo šele z uporabo v poslovnih procesih in aktivnostih. Na eni strani je potrebno zagotoviti širše vrednotenje informacijskih projektov – poleg stroškov strojne in programske opreme je potrebno upoštevati še vzdrževanje, šolanje, spremembo poslovnih procesov. Na drugi strani pa je potrebno tudi na rezultate informacijskih projektov gledati širše – posledice se lahko pokažejo v kvalitetnejšem vodenju, izboljšanem ugledu podjetja, večjem zadovoljstvu zaposlenih in podobno.
3. *Strukturiranje razprave o vrednosti informatike*. Vrednost informatike je potrebno ocenjevati na treh nivojih:
    - *Strategija* – kako dobro informacijska tehnologija podpira strateške cilje,
    - *IT organizacija* – ali je oddelek informatike zmogljiv (angl. efficient) in učinkovit (angl. effective),
    - *Projekt* – ali je določeno tehnologijo smiselno slediti.
4. *Definicija metrike*. Za merjenje vrednosti informacijske tehnologije jo moramo biti sposobni meriti.

Rezultati foruma ne dajejo dokončnih odgovorov in receptov na osnovno vprašanje, vseeno pa razčlenjujejo način določanja vrednosti informacijske tehnologije in s tem omogočajo pristop k določanju njene vrednosti v podjetju.

2.9.1 Finančna opredelitev vrednosti

Tradicionalno se je ocenjevanje vrednosti informatike izvajala s finančno računovodskimi kazalci, pri katerih ima dobiček glavno vlogo. Slabost teh kazalcev je v ozki usmerjenosti v pretekla poslovna dogajanja, kar spodbuja kratkoročno usmerjenost organizacij (Kovačič et al., 2004, str. 32).

Donosnost investicije

Donosnost investicije (angl. return on investment – ROI) izraža finančni zaslužek, izražen kot odstotek finančnih sredstev, ki so bili potrebni za dosego tega zaslužka.

Skupni stroški lastništva

Skupni stroški lastništva (angl. total cost of ownership – TCO) predstavljajo metodo upravljanja s stroški, ki omogoča vsestransko oceno stroškov (npr. informatike) v podjetju skozi čas. Pripravljena je na način, da omogoča spremljanje stroškov delovanja in vzdrževanja po izvedeni nabavi. TCO se uporablja pri finančnih analizah koristi (npr. ROI) in predstavlja cenovno osnovo za določanje ekonomske vrednosti investicije.

Na področju informacijske tehnologije je TCO uporabna metoda za zmanjševanje tekočih stroškov s pomočjo izboljševanja upravljanja informacijske tehnologije. Pri oceni novih projektov oz. pri sprejemanju odločitev se ta metoda ne obnese enako dobro. Glavne pomanjkljivosti, ki jih je identificiral Dempsey (Dempsey, 1998) so: neupoštevanje ugodnosti, zanemarjanje strateških in mehkih faktorjev, pomanjkanje enotne osnove za primerjavo in težja primerjava ocene stroškov življenjskega cikla izdelka.

Skupna vrednost lastništva

Skupna vrednost lastništva (angl. total value of opportunity – TVO) je metodologija, ki jo je uvedel Gartner za izračun donosnosti investicije (ROI) na področju poslovnih projektov, podprtih z informacijsko tehnologijo. Mera določa poslovno vrednost investicije v informacijsko tehnologijo in vključuje tveganje, čas in faktor učinkovitosti zamenjave.

2.9.2 Modeli za celovito merjenje poslovne uspešnosti

Na področju managementa se uveljavljajo metode in modeli za ocenjevanje podjetij v širšem kontekstu, kot ga kažejo finančni kazalci. Iz teorije o družbeni odgovornosti podjetij izhajajo koncept organizacije kot skupnosti déležnikov (angl. stakeholder), preko njih pa novi modeli za celovito merjenje poslovne uspešnosti (Kovačič et al., 2004, str. 32-33).

Pri ocenjevanju vrednosti informacijskih naložb je potrebno obravnavati tako stroške, kot tudi koristi. Ugotavljanje stroškov je običajno precej enostavno, medtem ko je ugotavljanje koristi veliko težja naloga. Koristi lahko na en način

delimo na neposredne, ki izhajajo iz informacijske rešitve, in posredne, če izhajajo iz neke skupne organizacijske rešitve. Na drug način lahko koristi razdelimo na otipljive, ki jih lahko merimo, in neotipljive, ki jih lahko le ocenimo. Pri slednjih lahko govorimo o zadovoljstvu strank, boljši kakovosti informacij, večji prilagodljivosti poslovanja, večjem poslovnem ugledu podjetja (Groznik et al., 2005).

Med metode, ki skušajo koristi ocenjevati v širšem pomenu sodita dva modela, ki ju opisujem v nadaljevanju.

Celovit sistem kazalnikov

Sistem sta izdelala Kaplan in Norton kot koncept za merjenje dejavnosti podjetja, glede na njegovo strategijo in vizijo. Celovit pogled na poslovanje podjetja meri iz štirih zornih kotov:

1. *Finančni pogled* – meri finančno učinkovitost podjetja, npr. število dolžnikov, donosnost investicije.
2. *Pogled stranke* – merjenje direktnega vpliva na stranke, npr. čas za obdelavo naročila, rezultat ankete med kupci, število pritožb.
3. *Pogled na poslovni proces* – ocenjuje učinkovitost ključnih poslovnih procesov za uresničevanje interesov delničarjev in kupcev.
4. *Pogled učenja in rasti* – meri sposobnost učenja podjetja, npr. celotno število ur izobraževanj zaposlenih ali število predlogov zaposlenih.

Van Grembergen v članku (Van Grembergen, 2006, str. 2-3) predlaga uporabo celovitega sistema kazalnikov na področju informacijske tehnologije. Zanj predlaga merjenje iz naslednjih štirih zornih kotov:

1. *Usmerjenost uporabnikov* – ocenjuje, kako uporabniki vidijo oddelek informatike. Cilj oddelka je pridobitev položaja prednostnega dobavitelja informacijske tehnologije in storitev.
2. *Operativna odličnost* – meri zmogljivost in učinkovitost aplikacij in procesov na področju informacijske tehnologije.
3. *Prispevek k poslovanju* – meri pogled managementa na oddelek informatike. Cilj je doseči razumen nivo poslovnega prispevka investicij v informatiko.
4. *Usmerjenost v prihodnosti* – ocenjuje zmožnost informatike za doseganje bodočih potreb poslovanja in podjetja.

Za vsako od naštetih področij je potrebno definirati metrike in način merjenja. Avtor priporoča, da se pri določanju merjenja uporabljata dve vrsti meritev: merjenje rezultata (npr. število izdelanih funkcijskih točk /programerja / mesec) in merjenje učinka (npr. število izobraževalnih dni / osebo / leto). V vzročno-

posledičnem odnosu nam le en podatek ne pokaže celotne slike, zato je potrebna ustrezna mešanica obeh vrst meritev.

Poslovni celovit sistem kazalnikov se z opisanim celovitim sistemom kazalnikov na področju informacijske tehnologije povezuje preko »prispevka k poslovanju«. Po potrebi se celovit sistem kazalnikov za informatiko naprej deli na podpodročja (npr. razvoj in operativa).

Tallonov model

Model je poslovno usmerjen (Groznik et al., 2005; Tallon et al., 2000) in meri poslovno vrednost informatike skozi njen vpliv na izvajanje procesov v Porterjevi vrednostni verigi. Glede na način investiranja v informatiko deli podjetja v štiri skupine:

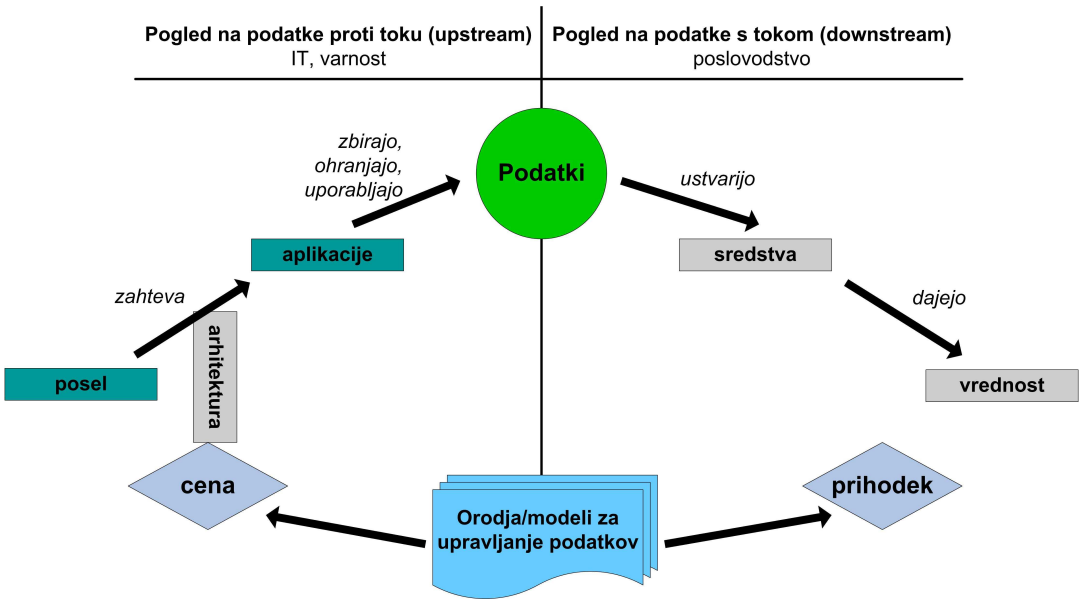
1. Brezciljno investiranje.
2. Investiranje v izboljšave na operativnem nivoju.
3. Investiranje v povezave navzven.
4. Strateško investiranje.

Raziskava je pokazala, da je v večini podjetij potrebna odobritev višjega managementa za naložbe v informatiko, po drugi strani pa je v večini podjetij malo vrednotenj uspešnosti teh naložb. V podjetjih z jasnimi cilji glede naložb v informatiko tudi veliko bolje zaznavajo njeno vrednost.

2.9.3 Poslovna vrednost podatkov

Eden od vidikov ocenjevanja poslovne vrednosti neprekinjenega poslovanja predstavlja ocena poslovne vrednosti podatkov, ki se nahajajo in uporabljajo v podjetju. Croy trdi (Croy, 2004), da obstaja neposredna povezava med zmožnostjo managementa, da odgovori na to vprašanje, in uspehom programa neprekinjenega poslovanja v podjetju. Odgovor na vprašanje vsekakor ni lahek, še posebej zaradi hitrih sprememb podatkov v hitro spreminjajočem se poslovnem okolju. Naloga odgovornih za neprekinjeno poslovanje je, da v sodelovanju z odgovornimi managerji in lastniki podatkov zagotovi ustrezno opredelitev, varovanje in možnost obnovitve podatkov na časovno in finančno primeren način.

Na začetku obravnavanja vprašanja poslovne vrednosti podatkov imamo običajno na eni strani zahtevo managementa po visoki razpoložljivosti podatkov, po drugi strani pa si večina podjetij tega ne more privoščiti za vse podatke. Ko se podatki starajo, običajno postajajo manj pomembni za poslovanje, s tem pa se tudi zmanjša potreba po njihovi hitri obnovi. Če je za določanje vrednosti podatkov pripravljeno ogrodje ali politika, je mogoče v primeru katastrofe veliko učinkoviteje in hitreje obnoviti najpomembnejše podatke za poslovanje podjetja. Pri določanju vrednosti je potrebno sodelovanje managementa in informatikov. Prvi imajo odgovornost, da



Slika 6: Pogled na podatke s stališča informatikov in poslovodstva (Adler, 2005).

določijo poslovno vrednost podatkov, drugi pa morajo zagotoviti ustrezno izvedbo hranjenja podatkov, ki bo v skladu z njihovo vrednostjo omogočala nemoteno poslovanje.

Zaradi vseh naštetih razlogov je učinkovito delo s podatki eden od ključnih delov načrta neprekinjenega poslovanja. Možna razvrstitev pomembnosti podatkov je po Croyu lahko naslednja:

1. Kritični podatki za poslanstvo,
2. Kritični podatki za poslovanje,
3. Bistveni podatki,
4. Pomembni podatki,
5. Nekritični podatki,
6. Nepomembni podatki,
7. Odstranljivi podatki.

Seveda tako obširna shema delitve podatkov ni nujno najbolj primerna za srednja in manjša podjetja, ki običajno uporabljajo enostavnejši način razvrstitve.

Zanimiv pogled na dvojnost podatkov, kot del informacijske infrastrukture, prikaže Adler (2005) in Slika 6. Na eni strani gre za pogled informatikov, kjer iz poslovanja pridejo zahteve za aplikacije, ki zbirajo, obdelujejo in uporabljajo podatke. Iz tega zornega kota vidimo podatke kot rezultat operacije, ki ima svojo ceno. Na drugi strani pa imamo poslovni pogled, ki izhaja iz podatkov. Podatki namreč lahko ustvarijo sredstva, ta pa nam dajo vrednost. Glede na to lahko na podatke gledamo

tudi kot na generatorje prihodka. Adler predlaga, da bi orodja in modeli za upravljanje podatkov morali vsebovati v sebi tudi informacije, ki bi omogočale določitev poslovne vrednosti podatkov, s katerimi podjetje upravlja.

Podobno, kot vidimo pri ocenjevanju vrednosti informatike, se nam tudi pri podatkih kažeta dve nasprotni vrednosti: cena in prihodek. Prvo lahko relativno enostavno izračunamo, medtem ko je določitev druge veliko težja. V prihodnosti se zato od orodij za upravljanje podatkov pričakuje večja možnost določanja, izračuna in vodenja vrednosti podatkov, tako na strani cene, kot tudi na strani prihodka.

2.9.4 Poslovna vrednost Analize vpliva na poslovanje

Analiza vpliva na poslovanje predstavlja del vpeljave neprekinjenega poslovanja in jo običajno izvajajo zunanji svetovalci v sodelovanju z oddelkom informatike in ključnimi nosilci poslovnih funkcij v podjetju. Mogoče pa jo je izvesti tudi v zmanjšanem obsegu interno v podjetju, če je le volja pri informatikih in poslovodstvu dovolj naklonjena temu. Sikich ugotavlja, da lahko Analizo vpliva na poslovanje z uporabo tehnike aktivne analize (angl. active analysis) uporabimo za uravnavanje treh ključnih managerskih območij (Sikich, 2004):

- *Zanimanje* – kjer sredstva in zmožnosti drugih lahko vplivajo na lastna dejanja,
- *Vpliv* – kjer lastna sredstva in zmožnosti lahko vplivajo na dejanja drugih,
- *Odgovornost* – poslanstvo, vizija in vrednosti organizacije.

Osnovni namen Analize vpliva na poslovanje je zagotavljanje podatkov za pripravo načrta obnovitve poslovanja v primeru izpada oz. ob pripravi rezervne lokacije informacijske infrastrukture. V okviru analize se poveže poslovne procese z aplikacijami, podatki in ostalo informacijsko infrastrukturo. V tem postopku lahko dobi poslovodstvo boljši vpogled v obseg uporabe informacijske tehnologije v okviru posameznih poslovnih procesov, informatika pa lahko bolje vidi, kakšne so poslovne zahteve in pomembnosti posameznih storitev, aplikacij in podatkov, ki so v njihovem upravljanju (Žnidar, 2005).

Med pomembne rezultate analize, ki lahko prispevajo k zbliževanju pogledov poslovodstva in informatike štejemo:

- Boljše razumevanje potencialnih finančnih in nefinančnih posledic izpadov informacijske infrastrukture,
- Postavitev prioritet in kritičnosti poslovnih procesov,
- Določitev potrebnih podatkov, aplikacij za izvajanje posameznih poslovnih procesov,

- Določitev poslovnih lastnikov ter skrbnikov aplikacij in podatkov,
- Definirani stroški izpada informacijskega sistema in njegovih delov v povezavi s poslovnimi procesi.

Metoda Analiza vpliva na poslovanje se od večine drugih metod merjenja vrednosti informatike v podjetju razlikuje po nekaj značilnostih, ki jih je potrebno upoštevati pri interpretaciji rezultatov:

- Dobljeni rezultati ne kažejo na vrednost informatike v podjetju, temveč na možno škodo, ki jo doživi podjetje ob nedelovanju informatike. Za izgubo ob nedelovanju ne moremo trditi, da je premo sorazmerna vrednosti ob delovanju. Vseeno pa nam dani rezultati dajo dober vpogled v zahteve poslovnih procesov ter vpetost informatike vanj.
- Dobljeni rezultati so ugotovljeni v danem trenutku in se s časom lahko bistveno spremenijo. Ob večjih spremembah v informacijski infrastrukturi je potrebno analizo (v omejenem obsegu) ponoviti.
- Glede na način pridobivanja rezultatov so le-ti samo delno natančni. Običajno gre za približne, vendar relevantne ocene s strani poslovodstva. Znano je, da so dobljene finančne in nefinančne ocene lahko tudi previsoke.

3. Neprekinjeno poslovanje informatike

V zadnjih desetih letih so se zahteve za neprekinjeno delovanje informatike v podjetju zelo povečale. Včasih so bile primerne in zadostne rešitve, ki so zagotavljale obnovo informacijske infrastrukture v nekaj dneh. Zahteve so se spremenile in večina podjetij ima sedaj vsaj nekatere procese, ki zahtevajo obnovo v času, manjšem od enega dne. Glede na povezanost poslovanja in informacijske tehnologije se v večini primerov izkaže informatika kot glavni faktor pri izpolnjevanju teh zahtev.

Na področju informatike je bilo razvitih precej novih tehnologij, postopkov in produktov, ki omogočajo izvedbo novih zahtev poslovanja po krajših časih nedelovanja v primeru katastrofe. Cene teh rešitev z zmanjševanjem RTO in RPO časa ne naraščajo linearno, temveč bliže eksponentnemu. Zato je potrebno precej pozornosti pred implementacijo nameniti analizi potreb poslovanja in šele za tem izbrati tehnološke rešitve.

Warrick v (Warrick et al., 2005, str. 7-8) neprekinjeno delovanje informatike obravnava s petimi vprašanji, ki nakazujejo pot izbire ustrezne rešitve:

1. Kakšne so poslovne posledice, če izpade informacijski sistem?

   Posledice so bile obširno obravnavane v predhodnih poglavjih.

2. Kakšni najverjetnejši razlogi za izpad?

   Opraviti je potrebno analizo tveganja in sestaviti prednostni seznam pomembnih informacijskih sredstev, ki lahko povzročijo izpad poslovanja.

3. Analiza trenutnega stanja.

   Analizira se trenutno stanje infrastrukture, aplikacij, podatkov, procesov, postopkov in nadzora nad sistemom.

4. Določitev sistema merjenja.

   Pred določitvijo in izvedbo potrebnih korakov za izvedbo prihodnjega stanja je potrebno določiti sistem merjenja, s katerim se bo lahko določilo napredek in uspeh oz. neuspeh projekta uvedbe neprekinjenega poslovanja podjetja. Običajno se za merjenje uporabljajo mere kot so: največji čas nedelovanja posameznega sistema, odzivni čas, čas obnove posameznih sistemov, RTO, porabljena finančna sredstva.

5. Določitev prihodnjega stanja

   Na podlagi analize razlike med trenutnim in končnim stanjem ter potrebami podjetja se določi način prehoda v izbrano prihodnje stanje informacijskega sistema za podporo zahtev neprekinjenega poslovanja podjetja.

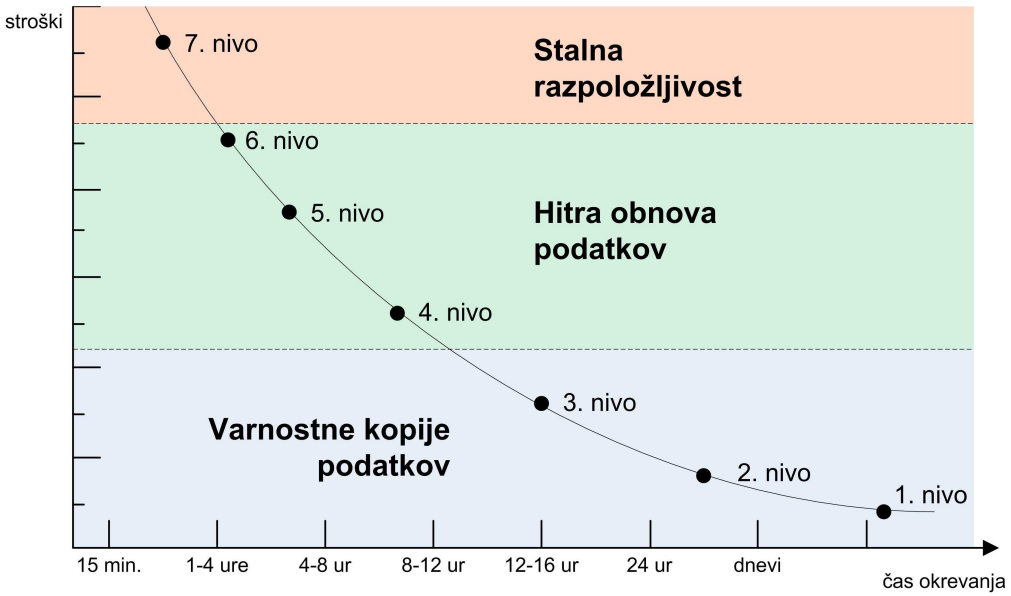
Opisani postopek je zelo podoben procesu uvajanja neprekinjenega poslovanja podjetja in je zato z njim lažje usklajen. Potrebno pa je vseeno paziti, da je neprekinjeno poslovanje informatike le del celovitega neprekinjenega poslovanja podjetja, ki se odvija na poslovnem nivoju podjetja.

Tehnologije implementacije neprekinjenega poslovanja na nivoju informatike se običajno opisujejo na osnovi sedem nivojev, ki jih je določila organizacija SHARE. Navkljub možnim subjektivnim ocenam uvrstitve podjetja na ustrezen nivo, se pokažejo kot ustrezno orodje za ocenitev trenutnega in pričakovanega stanja. Nivoji so naslednji (Slika 7):

Nivo 0 – *Ni podatkov na drugi lokaciji*: podjetje nima načrta neprekinjenega poslovanja. Prav tako ni shranjenih informacij ter dokumentacije, ni rezervne strojne opreme. Čas obnove ni mogoče predvideti, v slabem scenariju obnova sploh ni mogoča.

Nivo 1 – *Varnostno kopiranje na oddaljeni lokaciji*: podjetje izvaja varnostno kopiranje podatkov in prevoz na oddaljeno lokacijo. Podatki so na tej lokaciji, ni pa strojne opreme za njihovo obnavljanje in uporabo.

Nivo 2 – *Varnostne kopije podatkov na »vroči« lokaciji*: podjetje redno izvaja varnostno kopiranje in prevoz na rezervno »vročo« lokacijo, kjer se nahaja potrebna strojna oprema. V primeru potrebe je mogoče obnavljati podatke na tej lokaciji.



Slika 7: Nivoji neprekinjenega poslovanja (vir: SHARE, 1992).

Nivo 3 – *Elektronski prenos*: deluje podobno kot nivo 2, le da se del ključnih podatkov na rezervno lokacijo prenaša elektronsko. S tem zagotovimo manjšo izgubo podatkov ob katastrofi.

Nivo 4 – *Trenutne kopije* (angl. point-in-time): za prenos podatkov na rezervno lokacijo se uporabljajo naprednejše tehnologije, ki omogočajo hitrejši prenos podatkov, čeprav običajno brez preverjanja integritete podatkov.

Nivo 5 – *Transakcijska integriteta*: običajno obsega rešitve podatkovnih baz, pri čemer se pri prenosu na rezervno lokacijo zagotavlja celovitost na nivoju transakcije. Rešitve temeljijo na uporabniški programski opremi, ki zagotavlja minimalno izgubo podatkov in varuje pred logičnimi napakami v podatkih (delna transakcija).

Nivo 6 – *Zrcalno kopiranje brez izgube podatkov*: obsega rešitve na nivoju diskovnih podsistemov, ki zagotavljajo visoko stopnjo vrednosti podatkov z zagotovljeno podatkovno celovitostjo. Uporabljajo ga podjetja, ki potrebujejo minimalno izgubo podatkov in hitro obnavljanje v primeru katastrofe.

Nivo 7 – *Visoko avtomatizirana poslovno integrirana rešitev*: je podobna nivoju 6 z dodatno integracijo avtomatizacije vseh strežnikov, omrežja in diskovnih podsistemov. Rešitve na tem nivoju omogočajo skoraj neprekinjeno razpoložljivost z avtomatsko obnovo delovanja aplikacij.

Povzeto po (Warrick et al., 2005) so trije glavni vidiki neprekinjenega poslovanja informatike. Po eni strani so si sorodni, po drugi pa se med seboj dopolnjujejo:

- Visoka razpoložljivost,
- Neprekinjeno izvajanje operativnih del,
- Obnova po katastrofi.

3.1 Visoka razpoložljivost

Visoka razpoložljivost (angl. high availability – HA) pomeni zmogljivosti in postopke, ki zagotovijo dostop do poslovnih aplikacij ne glede na lokalne napake. Napake so lahko v poslovnih procesih, opremi ali informacijski strojni in programski opremi. S stališča informacijske infrastrukture se visoka razpoložljivost običajno zagotavlja s pomočjo zanesljive, podvojene strojne in programske opreme, ki običajno tečejo v okolju gruč (angl. clustering solution). Cilj je odstranitev možnih posameznih točk napake (Warrick et al., 2005).

3.2 Neprekinjeno izvajanje operativnih del

Neprekinjeno izvajanje operativnih del pomeni zmožnost, da informacijski sistem ni potrebno zaustavljati zaradi izvajanja načrtovanih opravil, kot so npr. izdelava varnostnih kopij ali redni servisi strojne opreme. Tehnologije za neprekinjeno izvajanje operativnih del zagotavljajo možnost izvajanja ponavljajočih, potrebnih infrastrukturnih opravil ob istočasnem zagotavljanju visoke razpoložljivosti.

Običajno so komponente sistema, ki zagotavljajo neprekinjeno izvajanje operativnih del, postavljene v istem računalniškem prostoru. Ta prostor oz. stavba tako postane možna posamezna točka napake. Neprekinjeno poslovanje tako še ne pomeni, da rešitev omogoča obnovo delovanja po katastrofi (Warrick et al., 2005).

3.3 Obnova delovanja po katastrofi

Obnova delovanja je zmožnost obnovitve delovanja računalniškega centra na drugi lokaciji in z drugo strojno opremo, če katastrofa uniči ali onesposobi računalniški center na primarni lokaciji. Situacije, kot je na primer pokvarjena ključna baza podatkov, ne sodijo v to kategorijo, razen če je rešitev situacije izvedljiva le s prenosom delovanja na rezervno lokacijo in drugo strojno opremo.

V okviru programa neprekinjenega poslovanja je običajno pripravljenih več načrtov obnove delovanja po katastrofi. To so bolj tehnični načrti za posamezne skupine znotraj organizacije, ki omogočajo obnovo delovanja posamezne poslovne aplikacije. Najbolj znan primer je načrt obnove za informacijsko tehnologijo, drugi

primeri pa so npr. za klicni center, distribucijski center, skladišče, … (Warrick et al., 2005).

Noakes-Fry vidi tri glavne vidike, ki določajo in omogočajo obnovo delovanja po katastrofi. Glede na zahteve poslovanja določimo ustrezne rešitve za rezervno lokacijo, zamenjavo opreme in shranjevanje podatkov (Noakes-Fry et al., 2004, str. 6-8).

3.3.1 Rezervna lokacija

Rezervna lokacija omogoča podjetju nadaljevanje računalniških in mrežnih dejavnosti v primeru izpada računalniškega sistema ali opreme. Poznamo štiri vrste rezervne lokacije (Rihar, 2003, str. 49-51; Noakes-Fry et al., 2004, str. 6-8):

1. *Vroča lokacija* (angl. hot site). Organizacija ima na voljo dve lokaciji (lahko tudi več) s popolnoma podvojeno strojno opremo. V posebnih primerih se obremenitev lahko enakomerno razporedi med obema sistemoma in v teh primerih ob izpadu enega od obeh sistemov celotno breme prevzame drugi sistem. Prenos je lahko izveden tako, da ga uporabniki sploh ne zaznajo. Čas prehoda na rezervno lokacijo je sicer pri vroči lokaciji dolg od nekaj minut do nekaj ur.
2. *Topla lokacija* (angl. warm site). Na voljo je rezervna lokacija s celotno strojno opremo in telekomunikacijskimi povezavami do svojih uporabnikov, pri čemer pa je računalniški sistem na nadomestni lokaciji v stanju pripravljenosti in se samodejno zažene le ob načrtovanem ali nenadnem izpadu primarnega sistema. Podatki se stalno kopirajo na rezervni sistem. Možna izguba podatkov (RPO) znaša od nekaj minut do nekaj ur, prehod na novo lokacijo (RTO) pa je en dan.
3. *Hladna lokacija* (angl. cold site). Organizacija ima na razpolago primerne prostore za namestitev strojne opreme. V primeru katastrofe podjetje lahko namesti svojo strojno opremo, programsko opremo in podatke ter nadaljuje s poslovanjem. Običajen čas obnove take lokacije je en teden ali več.
4. *Premična lokacija* (angl. mobile or portable site). Organizacija ima pripravljeno prikolico, na kateri je na voljo pripravljena strojna oprema. Obravnavamo jo lahko podobno kot toplo lokacijo, le da lahko tako pripravljeno strojno opremo prepeljemo na ustrezno lokacijo, npr. bližje končnim uporabnikom. Bistvena razlika od običajne tople lokacije je predvsem v omejeni velikosti opreme, ki jo lahko pripravimo. Čas obnove take lokacije je lahko po potrebi zelo nizek.

3.3.2 Zamenjava opreme

Pri pripravi strojne opreme moramo predvideti eno od štirih možnosti:

1. *Nakup strojne opreme vnaprej*. Ta možnost je najdražja, vendar nudi najhitrejši čas obnove poslovanja.
2. *Zavarovanje proizvajalca*, ki s posebno pogodbo zajamči dobavo ustrezne strojne opreme v primeru okvare v določenem času.
3. *Hitra dobava* (angl. quickship), ko ponudnik v določenem času dobavi opremo, ki mora biti shranjena in pripravljena za ta namen pri ponudniku.
4. *Posredna dobava* (angl. dropship), ko ponudnik storitve v primeru okvare izvede naročilo, tega pa opravi zunanji dobavitelj. Čas dobave v tem primeru je običajno daljši kot en teden, razen za standardno opremo, npr. namizni računalnik.

Običajno podjetja kombinirajo navedene metode nabave opreme glede na pomembnost poslovnih aplikacij, ki tečejo na posamezni strojni opremi.

3.3.3 Shranjevanje podatkov

Podatki predstavljajo pomembno komponento informacijskega sistema, ki mora biti v primeru izpada glavne lokacije primerno obnovljen na rezervnem sistemu. Pri tem je potrebno zagotoviti dosegljivost, celovitost in zaščito podatkov za uporabo na rezervni lokaciji. V grobem imamo na voljo tri mehanizme:

1. *Shranjevanje na rezervni lokaciji* (angl. physical vaulting). Pomembni podatki se na osnovni lokaciji shranjujejo na pomnilniške medije (npr. trakove), ki se nato prepeljejo v hrambo na rezervno ali varno lokacijo. V primeru izpada osnovne lokacije se zadnji mediji na rezervni lokaciji uporabijo za obnovo podatkov. Izguba podatkov v teh primerih je lahko tudi dan ali več.
2. *Elektronsko kopiranje* (angl. electronic vaulting). Podatki se elektronsko pošiljajo na rezervno lokacijo, kjer se shranjujejo na namenskih diskovnih sistemih. Ta način zagotavlja kratke čase obnove sistema (RPO) in možno majhno izgubo podatkov (RTO).
3. *Zrcalni prenos* (angl. remote disk mirroring). Ta način je podoben predhodnemu, le da se prenos podatkov vrši stalno in je tako usklajen s podatki na osnovni lokaciji. Na ta način se odpravi izguba podatkov in omogoča kratke čase obnove sistema v primeru izpada, zahteva pa zmogljivejše linije povezave in je tudi zato dražja možnost.

3.4 Zunanje izvajanje

Za veliko srednjih in manjših podjetij pomeni vzpostavitev in upravljanje neprekinjenega poslovanja informatike velik izziv ter finančno in organizacijsko velik zalogaj. Zato se postavlja vprašanje zunanjega izvajanja te funkcije ali le njenega dela.

Claunch meni (Claunch, 2004), da velikega dela procesa neprekinjenega poslovanja ni mogoče zunanje izvajati, lahko pa se to naredi z opremo in delom. Zunanje izvajanje je cenovno učinkovito, saj je v Evropi oprema v povprečju dodeljena 6 do 35 podjetjem, v ZDA pa celo 100 podjetjem. Vendar pa je potrebno paziti, da tveganje zaradi deljene opreme med več podjetij ni preveliko.

Adams vidi naslednja možna področja za zunanje izvajanje razvoja, vpeljave ali upravljanja neprekinjenega poslovanja podjetja (Adams, 2003):

1. *Obnova po katastrofi*. Zunanje izvajanje obsega nudenje lokacije, prostora in opreme za obnovo poslovanja v primeru katastrofe na rezervni lokaciji.
2. *Vzdrževanje poslovanja* (angl. business resumption). Storitev obsega svetovanje strategije, ki omogoča pripravo načrta obnove poslovnega informacijskega sistema v primeru izpada.
3. *Krizni management*. Predstavlja dodelitev funkcij in odgovornosti v pripravi na katastrofo ter vzpostavitev prioritet med poslovnimi funkcijami. Obsega celotno podjetje in ne le oddelek informacijske tehnologije.
4. *Načrtovanje odzivov in rezerve za nepredvidene dogodke* (angl. contingency planning). Predstavlja načrtovanje za primer daljnosežnih posledic, ki lahko doletijo podjetje. Običajno se izvaja s pomočjo orodij in predlog ter s pomočjo zunanjih svetovalcev pri uporabi teh orodij in vpeljavi v podjetje.
5. *Obnova poslovanja*. Vključuje načrtovanje obnove poslovnih aktivnosti in funkcij v primeru prekinitve. Sem sodi dodelitev funkcij, procesov in lokacij ter priprava načrta prednostnih aktivnosti za ponovno vzpostavitev poslovanja.

Adams v omenjenem delu (Adams, 2003) analizira tudi izkušnje strank pri zunanjem izvajanju storitev neprekinjenega poslovanja. Izkazalo se je, da je stopnja zadovoljstva predvsem rezultat ocene, kako dobro investicija zagotavlja kljubovanje znanim tveganjem in nevarnostim. Kvaliteta izvedbe in prihranki imajo po tej raziskavi majhno težo.

4. Analiza stanja vpeljave neprekinjenega poslovanja v slovenskih podjetjih

4.1 Raziskovanje s pomočjo ankete

Anketa je popularno raziskovalno orodje v družbenih vedah zaradi svoje prilagodljivosti, primernosti in uporabnosti v različnih situacijah. Pri kvantitativni analizi, ki sem jo uporabljal v tej nalogi, se ankete uporabljajo predvsem za

zbiranje podatkov. Kot navaja Hutchinsonova (2004, str. 285), lahko raziskava s pomočjo ankete doseže naslednje cilje:

- Vplivanje na poslušalce,
- Sprememba storitve ali produkta,
- Razumevanje ali predvidevanje človeškega obnašanja.

Informacije, ki jih na ta način lahko pridobimo, obsegajo mnenja, odnos in dejstva.

Izvedba socialne raziskave, kamor spada tudi raziskava s pomočjo ankete, običajno ne omogoča ponovitve v primeru neuspešne prve izvedbe. Zato je potrebno izbrati pravilno metodo in način izvedbe, ter pozitivno odgovoriti na naslednja vprašanja (Denscombe, 1998, str. 4-5):

Pomembnost – ali je pomembno, če se raziskava izvrši?

Izvedljivost – ali je raziskava izvedljiva časovno, stroškovno?

Pokritost – ali so z anketo pokrita vsa vprašanja, ki nas zanimajo?

Zanesljivost – ali lahko pričakujemo natančne, celovite, poštene odgovore?

Objektivnost – ali bo raziskava prikazala pošteno in uravnoteženo sliko?

Etika – ali bodo spoštovane pravice in čustva udeležencev v raziskavi?

Navedena vprašanja lahko raziskovalcu pomagamo pri preverjanju, ali je način in vsebina raziskave na pravi poti. Cilj mora biti suveren pozitiven odgovor na večino navedenih vprašanj oz. tematik.

Raziskava s pomočjo ankete (Hutchinson, 2004, str. 287-288) predvideva nekatere predpostavke in principe, ki jih je potrebno upoštevati ali se jih zavedati, da lahko zagotovimo ustrezne rezultate in tudi možnost nadaljnje analize:

Zaupanje v odgovore vprašanih. Predpostavljamo, da bo vprašani v normalnih okoliščinah »odgovoril tako kot je« oz. da bo odgovoril točno in resnično.

Odgovori na anketo so relevantni v trenutku izpolnjevanja ankete.

Vsi vprašani razumejo vprašanja na enak način, kar pomeni, da imajo uporabljeni izrazi, zveze in vprašanja isti pomen za sodelujoče. Do razlik lahko pride zaradi dvoumnosti, kulturnih razlik, bralnih sposobnosti, jezikovnih razlik in podobno.

»Resnica« in »realnost«, ki sta v odgovorih vprašanih in ju prikaže anketa, ni nujno objektivna resnica, temveč je lahko subjektivna resnica (ali pogled na svet) vsakega posameznega udeleženca v anketi.

V nekaterih primerih oz. vprašanjih lahko obstaja »pravilni« odgovor in v teh primerih je potrebno zagotoviti, da bodo vprašani odgovorili točno in ne tako, kot mislijo, da se od njih pričakuje. Primer bi lahko bilo vprašanje v šoli:

»Kolikokrat tedensko se učiš?«, kjer bi učenci mislili, da morajo odgovoriti npr. »vsak dan«.

V raziskavi vpeljave neprekinjenega poslovanja v slovenskih podjetjih, ki jo obravnavam v tej nalogi, sem anketo uporabil za zbiranje dejstev in pridobivanje mnenja o tej temi. Anketo sem pripravil na način, da bi zagotovil čim večjo možnost, da bodo udeleženi po svojih najboljših močeh odgovarjali točno in resnično ter da bi subjektivni odgovori skupaj dali odgovor na postavljena vprašanja in teze te naloge.

4.2 Priprava ankete

Kot že povedano v prejšnjem poglavju, imamo za najpomembnejši kriterij pri oceni vrednosti ankete dejstvo, koliko anketni odgovori odražajo resnico ali realnost. Ta kriterij zahteva tri okoliščine odgovarjanja, ki so po mnenju Batesona (Hutchinson, 2004, str. 288-289) ključne pri izdelavo ankete: razumevanje, zmožnost in pripravljenost.

Razumevanje pomeni, da udeleženec ankete lahko razbere in si razloži vprašanje in možne odgovore. Zmožnost, kot drugi pogoj pomeni, da mora biti udeleženec sposoben točno podati zahtevano informacijo. Ne razumevanje, ne zmožnost pa nam ne koristita, če udeleženec ni voljan oz. pripravljen sodelovati v anketi (Hutchinson, 2004, str. 289).

V obravnavani anketi sem poskušal zagotoviti vse tri ključne komponente, glede na pričakovano publiko in okoliščine izvajanja ankete. Glede na profil udeležencev ankete sem uporabljal jezik, ki na tehničnem nivoju obsegajo uveljavljene slovenske izraze. Vprašanja sem postavil v preprosti obliki, ki onemogoča različno ali napačno interpretacijo in omogoča preprosto izbiro primernega odgovora.

Ciljna publika ankete so podjetja ter informacijski strokovnjaki in managerji, ki so udeleženi v procesu neprekinjenega poslovanja v podjetju. Anketa je vsebinsko prirejena tej ciljni skupini, s čimer je lahko prišlo do manjše zainteresiranosti udeležencev ankete iz podjetij, kjer se z neprekinjenim poslovanjem ne ukvarjajo ali pa udeleženci niso zadosti vključeni v ta proces, da bi ga lahko ocenjevali. Pričakoval sem, da v teh primerih morda ne bom dobil izpolnjenih anket. Zato tudi na podlagi rezultatov ne morem ocenjevati deleža vpeljave neprekinjenega poslovanja v slovenskih podjetij. Analizo sem usmeril v ocenjevanje stopnje, načina, spodbujevalcev vpeljave neprekinjenega poslovanja v tistih podjetjih, kjer se nekaj na tem področju že dogaja.

Pri dolžini in vsebini ankete (glej 8.1, str. 1) sem se omejil na eno stran ter enajst vprašanj, razdeljenih v tri področja: profil podjetja in udeleženca, načrt neprekinjenega poslovanja podjetja in zaznane motnje poslovanja. Posebno

pozornost sem posvetil grafični obliki posameznih vprašanj in celotne strani, da bi delovala po eni strani resno, po drugi strani pa privlačno ter razgibano in brez občutka pretirane napolnjenosti z informacijami.

Anketa obravnava tri področja. Prvo področje opredeljujejo podjetje glede na velikost ter panogo in položaj udeleženca ankete v podjetju.

Za oznako dejavnosti podjetja sem napravil poenostavitev dejavnosti v skupine, ki ustrezajo pričakovanjem glede rezultatov. Skupine so prikazane v spodnji tabeli (Tabela 3), skupaj z ustrezno klasifikacijo, ki jo uporablja Statistični urad RS.

Pri velikosti podjetij sem pričakoval odgovore, primerne za obdelavo, predvsem od srednje velikih in velikih podjetij z več kot 100 zaposlenimi.

Dejavnost podjetja	Klasificirana dejavnost podjetja
Finančna inštitucija	J. Finančno posredništvo
Gospodarska dejavnost	D. Predelovalne dejavnosti
Storitve	K72 Obdelava podatkov, podatkovne baze in s tem povezane dejavnosti
Javna uprava	L. Dejavnost javne uprave in obrambe, obvezno socialno zavarovanje
Zdravstvo	N. Zdravstvo in socialno varstvo
Trgovina	G. Trgovina, popravila motornih vozil in izdelkov široke porabe
Telekomunikacije	I64 Pošta in telekomunikacije
Ostalo	A. Kmetijstvo, lov, gozdarstvo B. Ribištvo in ribiške storitve C. Rudarstvo E. Oskrba z električno energijo, plinom in vodo F. Gradbeništvo H. Gostinstvo I. Promet, skladiščenje in zveze K. Poslovanje z nepremičninami, najem in poslovne storitve M. Izobraževanje O. Druge javne, skupne in osebne storitvene dejavnosti P. Zasebna gospodinjstva z zaposlenim osebjem Q. Eksteritorialne organizacije in združenja

Tabela 3: Uporabljene dejavnosti podjetij v anketi glede na standardno klasifikacijo dejavnosti (Statistični urad RS, 2002).

Velikost podjetja	mikro	majhno	srednje	veliko
Število zaposlenih v podjetju	do 9	10 – 49	50 – 249	nad 250
Število podjetij	87.315	4.898	1.179	305

Tabela 4: Velikost in število podjetij podjetij (Statistični urad RS, 2005).

4.3 Izvedba ankete

V anketi sem skušal zajeti čim več srednjih in velikih podjetij v Sloveniji, v katerih je zavedanje po vpeljavi neprekinjenega poslovanja večje oz. nadpovprečno.

Anketo sem izvedel na dveh poslovnih dogodkih v aprilu 2006 in sicer na IBM Forumu in na Konferenci o neprekinjenem poslovanju.

IBM Forum se je odvijal v začetku aprila 2006 v Portorožu. Udeležujejo se ga IBM stranke in partnerji iz Slovenije, pri čemer prevladuje osebje IT in vodstvo IT v podjetjih. V materialih konference je bilo razdeljenih 500 vprašalnikov. Vrnjenih sem dobil 30 anketnih listov.

Konferenca o neprekinjenem poslovanju se je odvijala v sredini aprila 2006 v Ljubljani. Na njej je sodelovalo 65 udeležencev iz slovenskih podjetij, predvsem iz finančnih institucij, poleg tega pa še iz večjih podjetij in javne uprave. Dobil sem 50 izpolnjenih anketnih listov. Na tem dogodku je bil odziv udeležencev odličen, kar je verjetno povezano s tematiko in interesom udeležencev na tem področju.

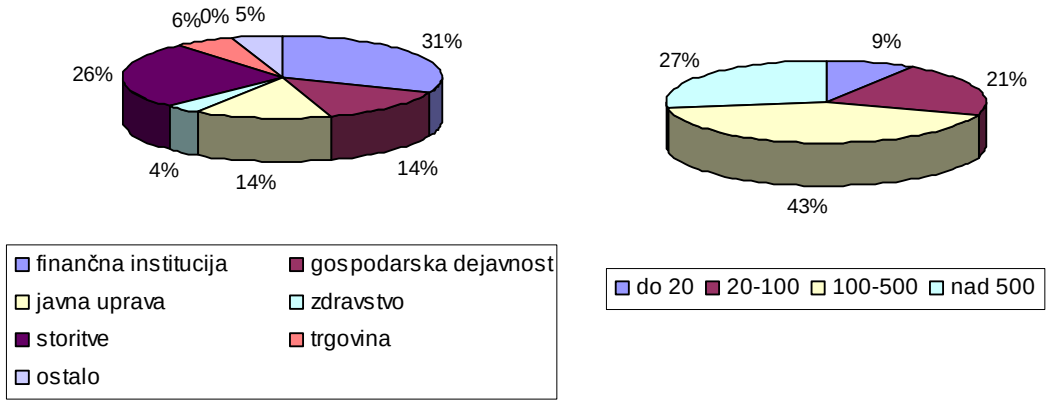
4.4 Udeleženci ankete

V anketi je bilo pridobljenih 80 odgovorov na vprašalnike.

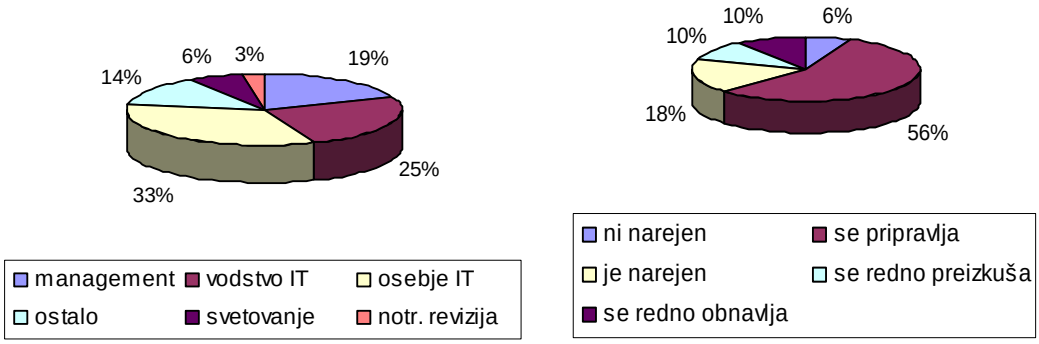
Prevladujejo štiri panoge podjetij (Slika 8): finančna industrija, storitve, javna uprava in gospodarska dejavnost. Te štiri dejavnosti, predvsem prva, so tudi najdejavnejše na področju izvajanja neprekinjenega poslovanja.

Večino odgovorov na vprašalnik (70%) sem dobil iz srednjih in velikih slovenskih podjetij z več kot 100 zaposlenih, kar ustreza začetnim pričakovanjem.

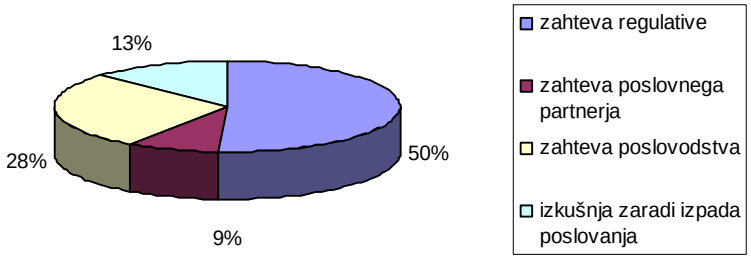
Največji del odgovorov (Slika 9) sem dobil od pričakovanih treh glavnih akterjev pri vpeljavi neprekinjenega poslovanja: managementa (1/5), vodstva IT (1/4) in osebja IT (1/3). To razmerje primerno odseva ustreznost odgovorov, saj nobena od ključnih skupin pri ocenjevanju ni izostala.



Slika 8: Struktura odgovorov glede na panogo in velikost podjetja (lasten vir).



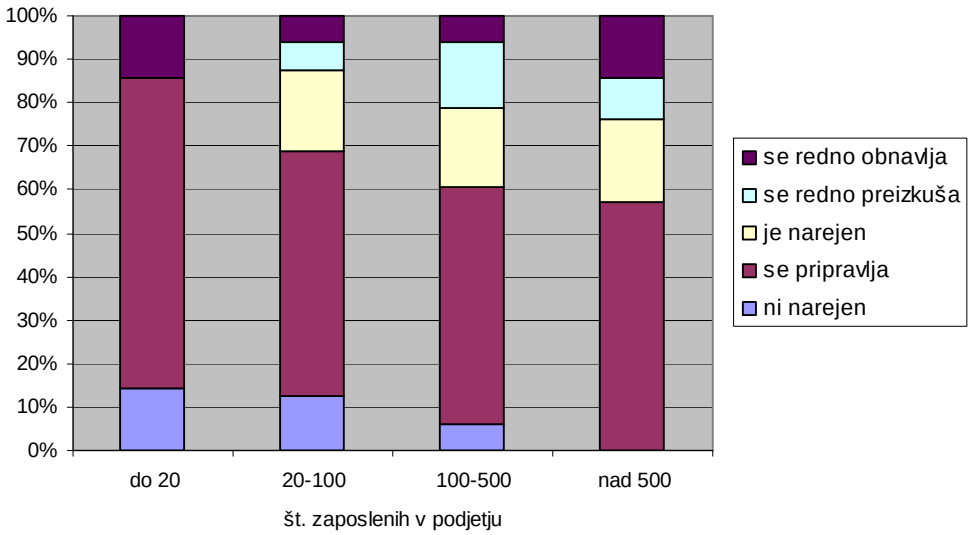
Slika 9: Struktura odgovorov glede na položaj v podjetju in stanje pripravljenosti načrta obnove poslovanja v podjetju (lasten vir).



Slika 10: Razlog za uvedbo načrta neprekinjenega poslovanja v podjetju (lasten vir).

V večini primerov (skoraj 2/3) načrt neprekinjenega poslovanja še ni pripravljen. Pri preostalih prevladujejo podjetja, ki načrt naredila, vendar ga še niso preizkusila. V 10% primerov podjetja načrt redno preizkušajo in v prav toliko preostalih odstotkih podjetja poleg tega načrt tudi redno obnavljajo.

Pri polovici vprašanih je glavni razlog za uvedbo načrta neprekinjenega poslovanja (Slika 10) zahteva regulative. V dobri četrtini primerov je ta razlog zahteva



Slika 11: Nivo uvedbe plana neprekinjenega poslovanja glede na velikost podjetja (lasten vir).

poslovodstva. Zahteva poslovnega partnerja po uvedbi neprekinjenega poslovanja običajno velja za podjetja, ki poslovno sodelujejo s podjetji z vpeljanim upravljanjem neprekinjenega poslovanja. Po rezultatih sodeč je v Sloveniji takega sodelovanja še relativno malo (9%). Podobno malo je tudi vpeljave neprekinjenega poslovanja zaradi preteklih izkušen izpada (13%).

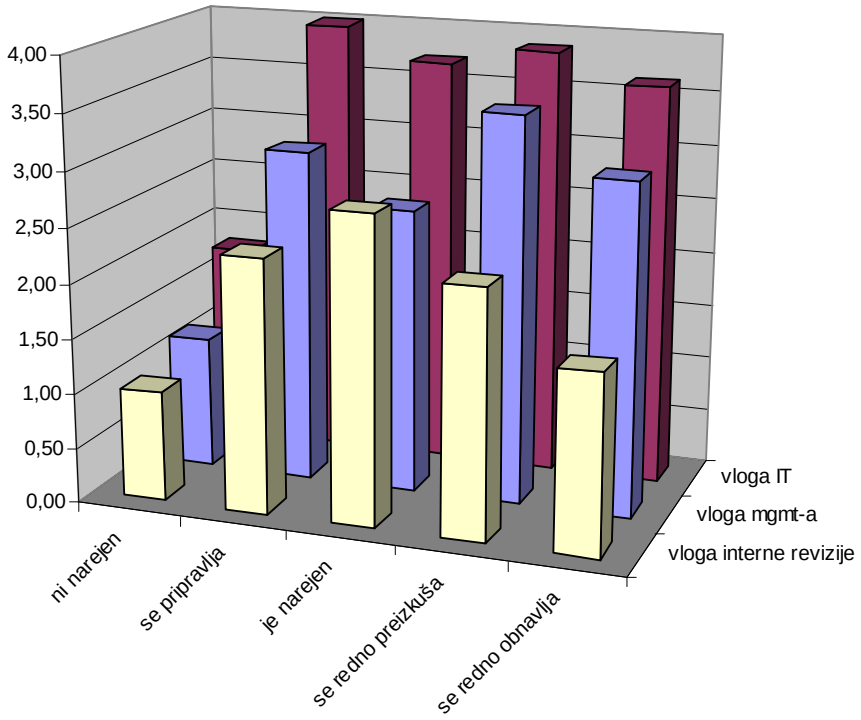
4.5 Stopnja vpeljave neprekinjenega poslovanja

Če pogledamo, katere organizacije imajo vpeljan načrt neprekinjenega poslovanja, se po pričakovanjih izkaže (Slika 11), da so to večja podjetja z več kot 100 zaposlenimi.

Pri polovici vprašanih je glavni razlog za uvedbo načrta neprekinjenega poslovanja zahteva regulative. V dobri četrtini primerov je vzrok zahteva managementa in le v dobrih desetih odstotkih je to izkušnja zaradi izpada poslovanja ali zahteva poslovnega partnerja.

Precej slabo pa je stanje pri testiranju in rednem pregledu načrta neprekinjenega poslovanja. V obeh primerih ena tretjina sploh še ni izvedla testiranja oz. pregledala načrta in naslednja tretjina to opravlja le občasno. Preostale organizacije testiranje in pregled načrta izvajajo vsaj enkrat letno.

Zanimiva je tudi primerjava vloge posameznih ključnih udeležencev (Slika 12). Vidimo, da je vloga notranje revizije ob vpeljavi načrta neprekinjenega poslovanja pomembna, nato pa se njena vloga po mnenju udeležencev ankete manjša. Na



Slika 12: Vloga posameznih funkcij pri vpeljavi plana neprekinjenega poslovanja (lasten vir).

drugi strani vidimo stalno visoko vlogo oddelka informacijske tehnologije, ki se ji pri vpeljanih načrtih neprekinjenega poslovanja približa vloga managementa.

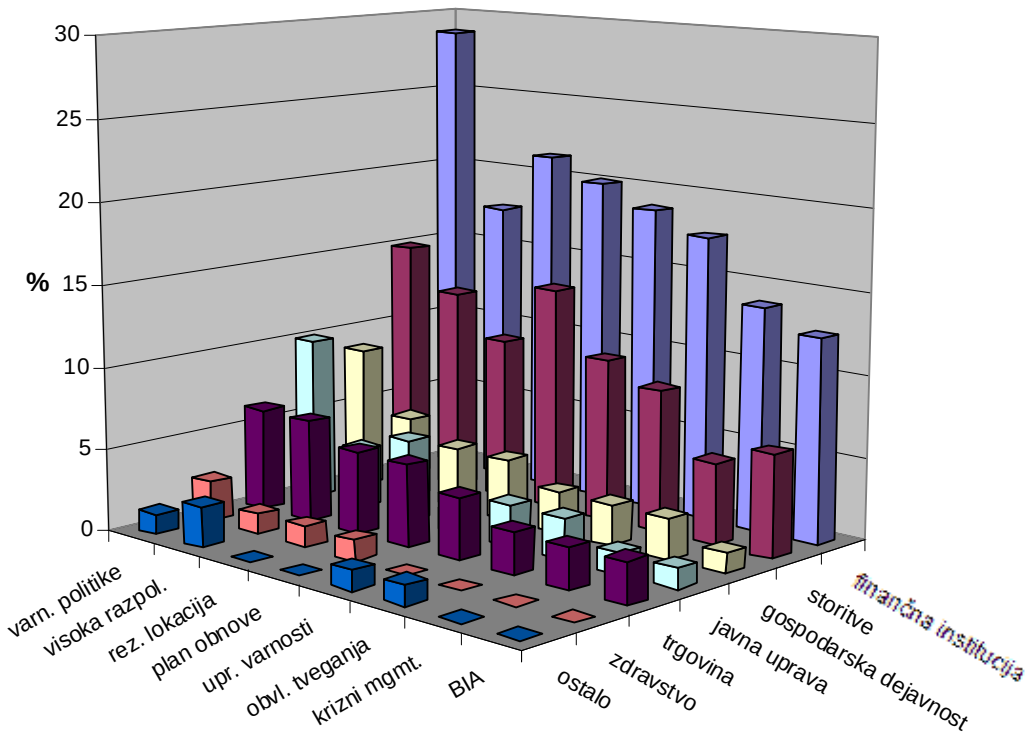
Tukaj je pomembno opozoriti, da žal praksa kaže na pristop k uvajanju neprekinjenega poslovanja, ki ga avtorji v strokovni literaturi izrecno odsvetujejo. Gre za veliko možnost problemov pri uvajanju in upravljanju načrta neprekinjenega poslovanja, če vloga managementa ni ključna tako v fazi uvedbe kot kasneje v fazi upravljanja neprekinjenega poslovanja.

4.6 Rezultati ankete

4.6.1 Vpeljani elementi neprekinjenega poslovanja

Pogled na vpeljane elemente neprekinjenega poslovanja (Slika 13) glede na panogo kaže veliko izstopanje finančnih institucij, kjer so vsi elementi precej enakomerno zastopani. Solidno je tudi stanje v storitveni dejavnosti, kjer pa že vidimo slabšo zastopanost kompleksnejših elementov (analiza vpliva kriznega dogodka – BIA, krizni management). Slabše stanje je v preostalih obravnavanih panogah (gospodarstvo, javna uprava in trgovina), kjer je do neke mere prisotna le vpeljava varnostnih politik.

Izrazito slabo pa je stanje v zdravstvu, kjer tako rekoč ni vpeljanih elementov neprekinjenega poslovanja. Kritični poslovni procesi zdravstva imajo tudi na

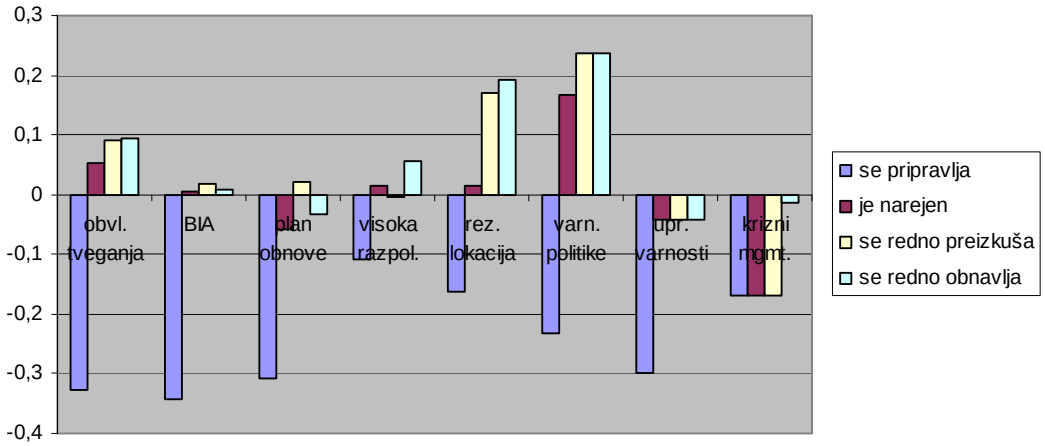


Slika 13: Elementi neprekinjenega poslovanja po panogah (lasten vir).

nivoju celotne družbe posebno vlogo (npr. reševanje življenj), zato bi pričakoval podobno vlogo neprekinjenega poslovanja, kot npr. v finančnih institucijah. Razlogov za tako stanje je lahko več: morda informatika v zdravstvu ne igra zadosti pomembne vloge v ključnih procesih, morda so ključni procesi zadosti dobro pokriti z ročnimi/alternativnimi postopki, morda pa le zakonodajalec ni opravil svoje vloge z uvedbo ustrezne regulative.

V ZDA, npr., velja za zdravstvene organizacije, zaposlene v zdravstvu in zdravstvene zavarovalnice zakon HIPAA. Sestavljen je iz dveh delov in v drugem delu je pet pravil, ki preprečujejo prevaro in zlorabo v zdravstvu. S tematiko neprekinjenega poslovanja se ukvarja varnostno pravilo, ki zahteva vzpostavitev načrta aktivnosti za nepredvidene situacije. Ta obsega tudi pripravo varnostnih kopij podatkov in izdelavo procedur za obnovo v primeru katastrofe, kar posledično vodi do uvajanja neprekinjenega poslovanja v zdravstvo v ZDA.

V panogah, kjer do uvajanja neprekinjenega poslovanja prihaja predvsem zaradi zahteve managementa, vidim večjo naklonjenost rešitvam visoke razpoložljivosti (nasproti rezervni lokaciji), kar je verjetno povezano z nižjimi stroški take rešitve in manjšim pritiskom regulative in zakonodaje.



Slika 14: Odvisnost med stanjem plana obnove in posameznimi elementi (lasten vir).

4.6.2 Stopnja vpeljave elementov neprekinjenega poslovanja

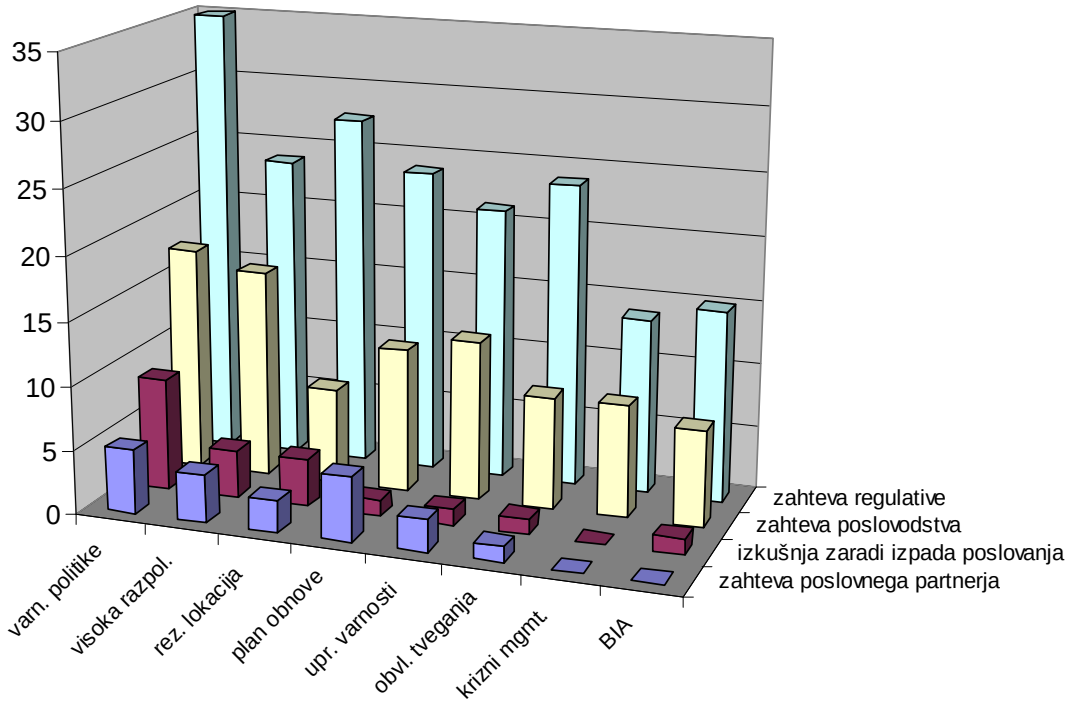
Tretji vpogled v rezultate ankete prikazuje odvisnost med stopnjo vpeljave neprekinjenega poslovanja in vpeljanimi elementi neprekinjenega poslovanja.

Opazimo (Slika 14), da organizacije v okviru neprekinjenega poslovanja vpeljejo predvsem varnostne politike. Pri organizacijah, ki načrt neprekinjenega poslovanja tudi preizkušajo in/ali obnavljajo, so dodatno večkrat vpeljani še rezervna lokacija in obvladovanje tveganja.

Organizacije, ki se pripravljajo na vpeljavo neprekinjenega poslovanja, imajo negativno odvisnost za vse elemente, iz česar lahko sklepamo, da običajno nimajo vpeljanega še nobenega elementa neprekinjenega poslovanja. Morda je potrebno oznako »se pripravlja« razumeti bolj v smislu želje oz. nekakšnega srednjeročnega cilja, kot pa da se projekt vpeljave neprekinjenega poslovanja že izvaja.

4.6.3 Zunanji faktorji vpeljave

Če pogledamo odvisnost vpeljave posameznih elementov neprekinjenega poslovanja glede na razlog vpeljave, vidimo (Slika 15), da je zahteva regulative ali zakonodaje najmočnejši faktor za vpeljavo načrta neprekinjenega poslovanja. Najmočnejši trije elementi so varnostne politike, rezervna lokacija in obvladovanje tveganja, kar je verjetno posledica močne zastopanosti finančne industrije v tej skupini in vpliv dogovora Basel II. Basel II predstavlja priporočila bančnih nadzornikov in centralnih bank iz 13 držav, ki sestavljajo Baselski odbor za nadzor bančništva. Njihov cilj je poenotenje upravljanja s tveganji v bankah in poenotenju pristopa med državami. V okviru upravljanja operativnega tveganja morajo finančne institucije zagotavljati tudi neprekinjeno poslovanje in s tem implementacijo elementov neprekinjenega poslovanja.



Slika 15: Vpliv spodbujevalcev neprekinjenega poslovanja na vpeljavo elementov neprekinjenega poslovanja (lasten vir).

Naslednja pomembna ugotovitev je povezana z nizko oceno managementa kot spodbujevalca vpeljave neprekinjenega poslovanja. Če se spomnimo citata ekonomista Peter F. Druckerja iz uvoda, je za glavno nalogo organizacije postavil preživetje in vodilni princip poslovne ekonomije izogibanje izgubi. Način zagotavljanja preživetja je preprečevanje izpada poslovanja, kar se v organizacijah izvaja v okviru procesa upravljanja neprekinjenega poslovanja. Iz tega bi pričakoval bistveno večjo podporo, sodelovanje in zahtevo managementa po vpeljavi neprekinjenega poslovanja v organizacijo. Žal pa kaže, da je v Sloveniji povsem drugače. Postavlja se vprašanje, če se management zares zaveda tveganj, ki jim je izpostavljena njihova organizacija?

4.7 Sorodne analize

Na temo neprekinjenega poslovanja je bilo v svetu narejenih precej analiz, medtem ko so le-te v Sloveniji še redkost. V tem poglavju bom predstavil izsledke ene slovenske in treh tujih analiz neprekinjenega poslovanja podjetij. Tuje analize kažejo na vse večjo težo programu neprekinjenega poslovanja, ki mu jo posvečajo v podjetjih. Glavna motivacija so zakonodaja, regulativa, zahteve strank ter zahteva po operativni odpornosti poslovanja. Analize kažejo tudi na naraščajoče zavedanje in sodelovanje managementa v tem programu, kar je najbrž posledica nekaterih odmevnih računovodskih škandalov (npr. Enron) in posledično strožje regulative (npr. Sarbens-Oxley).

4.7.1 Graselli

Graselli je v letošnjem letu opravil raziskavo zmogljivostno zrelostne ocene programa upravljanja neprekinjenega poslovanja (Graselli, 2006), v kateri je na podlagi ankete izvedel oceno zrelosti programa upravljanja neprekinjenega poslovanja slovenskih podjetij. V analizi je uporabil model, ki izhaja iz Cobita (poglavje 2.4.6). Analizo in rezultate je razdelil na 5 področij, pri čemer je vsako področje ocenjeval z oceno od 0 do 5:

1. *Odnos zaposlenih* do programa neprekinjenega poslovanja – stopnja zrelosti 2,5. Nekaj vodij kritičnih poslovnih procesov v organizaciji je prepričanih, da je upravljanje neprekinjenega poslovanja strateškega pomena za organizacijo. Večina v organizaciji meni, da bo organizacija utrpela poslovno škodo, če ne bo imela izdelanega načrta za ukrepanje v primeru incidenta. Odgovorni za upravljanje neprekinjenega poslovanja o programu občasno poroča vodstvu organizacije. Večina zaposlenih je bila obveščena, da potekajo aktivnosti, povezane s programom neprekinjenega poslovanja.

2. *Razširjenost in zrelost* programa neprekinjenega poslovanja – stopnja zrelosti 2,3. Obstaja nekaj krovnih dokumentov s področja neprekinjenega poslovanja. Za večino ključnih poslovnih procesov so definirani in dokumentirani postopki ukrepanja v primeru nesreče. Postopki in dokumenti so bili izdelani na podlagi preteklih izkušenj in raznih člankov in publikacij. Praviloma obstajajo okrevalni načrti za posamezne vire, pogosto srečamo načrt ukrepanja v krizni situaciji.

3. *Nadomestljivost in usposobljenost* zaposlenih za delo v primeru krize – stopnja zrelosti 2,5. Povprečna organizacija, sodelujoča v anketi ima okoli tisoč zaposlenih, s programom neprekinjenega poslovanja pa se v njej z vsaj tretjinskim delovnim časom ukvarjajo štirje zaposleni. Če bi bilo v primeru nesreče odsotno večje število zaposlenih, bi se s tem ukvarjali takrat; nekateri lastniki poslovnih procesov so določili enega ali več namestnikov za delavce na ključnih mestih. Izobraževanje za program neprekinjenega poslovanja se izvaja občasno, novo zaposlene delavce pa pogosto izobrazijo sodelavci na neformalen način.

4. *Določitev odgovornosti* in prenosa pooblastil za ukrepanje v primeru krize – stopnja zrelosti 3,1. V povprečni organizaciji, sodelujoči v anketi, so za ukrepanje v primeru incidenta določene dolžnosti in odgovornost, določeni so lastniki poslovnih procesov, ki pa dostikrat nimajo dovolj pooblastil, da bi lahko učinkovito izvajali zadolžitve.

5. *Spremljanje izvajanja* in izboljševanja programa upravljanja neprekinjenega poslovanja – stopnja zrelosti 3,1. Posamezniki spremljajo določene kazalce, povezane s programom neprekinjenega poslovanja. Deloma se spreminjajo stroški, ki se nanašajo na program. Odstopanja od politik, prakse in postopkov neprekinjenega poslovanja občasno javijo posamezniki, v polovici primerov se ne zgodi nič, v drugi polovici pa se pomanjkljivosti odpravijo do naslednjega pregleda.

Povprečna ocena zrelosti, ki jo je Graselli dobil za analiziranih 34 organizacij je bila 2,4, kar je primerljivo s podatki v okviru storitve Cobit online. V njej je zajetih 163 organizacij s celega sveta in njihova povprečna ocena je 2,1. Pri omenjeni analizi je potrebno upoštevati, da je vzorec podjetij zelo majhen in obsega predvsem velika podjetja s povprečno tisoč zaposlenimi.

Graselli je svojo analizo izvajal na podlagi rezultatov, ki jih je dobil na Konferenci o neprekinjenem poslovanju, kjer sem tudi jaz dobil del rezultat za mojo analizo. Zato lahko sklepam, da je večina udeležencev njegove ankete iz finančne in storitvene industrije ter javne uprave. Prav tako so bili to udeleženci iz organizacij, kjer je zavedanje o pomenu neprekinjenega poslovanja nadpovprečno visoko.

4.7.2 EnvoyWorldWide

EnvoyWorldWide je leta 2005 izvedel (EnvoyWorldWide, 2005) raziskavo in analizo trendov neprekinjenega poslovanja in upravljanja tveganj med člani raznih organizacij in združenj za neprekinjeno poslovanje v ZDA. Raziskava je zajela 145 podjetij.

Med obravnavanimi podjetji je v skupini za neprekinjeno poslovanje v 93% zastopan oddelek informacijske tehnologije, v 78% management in v 67% oddelek upravljanja s tveganji.

66% vprašanih je opazilo povečan interes njihovih strank za načrt neprekinjenega poslovanja podjetja, podoben odstotek (68%) pa je zahteve po tem načrtu opazil kot zahtevo pri povpraševanju strank.

Visok delež, 78% vprašanih, je odgovoril, da državni zakoni neposredno vplivajo na neprekinjeno poslovanje. 81% podjetij vprašanih je podvrženo Sarbanes-Oxley in 47% HIPAA zahtevam.

Odgovornost za usklajenost načrta neprekinjenega poslovanja z zahtevami regulative je pri več kot polovici vprašanih (58%) odgovornost skupine za neprekinjeno poslovanje in le v 15% odgovornost pravnega svetovalca.

Zelo visok odstotek vprašanih (87%) razume načrt za komunikacijo kot eno ključnih komponent načrta neprekinjenega poslovanja, kamor sodi načrt komunikacije z zaposlenimi, strankami, dobavitelji, regulatorji in mediji.

Čeprav je rezultate te raziskave težko direktno primerjati z mojo raziskavo, pa vseeno kaže nekatere trende, ki se bodo s časom verjetno pokazali tudi v Sloveniji. Najprej bi poudaril visok odstotek treh četrtin podjetij, kjer je načrt neprekinjenega poslovanja močno povezan z zahtevami zakonodaje in regulative. Drug močan razlog, ki ga pri nas še ne vidimo, je zahteva strank. Poudaril bi še nov element načrta, ki je pri anketiranih podjetjih že našel svoje mesto, in sicer načrt komuniciranja v primeru krize.

4.7.3 CPM in Deloitte & Touche

Skupina CPM in Deloitte & Touche LLP (CPM and Deloitte & Touche, 2006) sta v letu 2005 izvedli šesto zaporedno raziskavo o neprekinjenem poslovanju podjetij, ki je pokazala, da funkcija neprekinjenega poslovanja igra močno vlogo pri upravljanju operativnega tveganja. Izvršni management podjetij v glavnem skrbi za usklajenost z zakonodajo in regulativo ter za izvajanje operativne odpornosti poslovanja kot odziv na širok sklop dogodkov, ki bi lahko prekinili poslovanje.

Zanimivo je, da predstavlja operativna odpornost poslovanja s 33% močnejše gonilo programa neprekinjenega poslovanja kakor usklajenost z regulativo z 19% ali odgovornosti izvršnega managementa za upravljanje tveganja z 20%. Ostali razlogi so bistveno manjši (pod 10%).

Pri oceni stanja programa neprekinjenega poslovanja so analizirana podjetja v boljšem položaju kot analizirani vzorec v moji raziskavi:

- 6% nima načrta neprekinjenega poslovanja,
- 11% izdeluje načrt neprekinjenega poslovanja,
- 14% ima izdelan načrt neprekinjenega poslovanja za omejeno število poslovnih funkcij,
- 28% ima izdelan načrt neprekinjenega poslovanja za kritične poslovne funkcije,
- 42% ima izdelan načrt neprekinjenega poslovanja za vse poslovne funkcije.

V primerjavi z mojo raziskavo je v tej raziskavi veliko večji delež podjetij že izdelan načrt neprekinjenega poslovanja za podjetje vsaj za nekatere poslovne funkcije.

Zahteve poslovodstva glede časa obnove (RTO) za kritične poslovne funkcije so:

- Brez tolerance izpada pri 12% vprašanih,
- Manj kot 2 uri pri 16% vprašanih,

- Do 8 ur pri 19% vprašanih
- Do 24 ur pri 27% vprašanih,
- Do 3 dni pri 18% vprašanih,
- Do 5 dni pri 6% vprašanih in
- Več kot 5 dni pri 2% vprašanih.

Podatkov o času obnove v svoji raziskavi nisem zajel, vendar bi iz izkušenj ocenil, da imajo anketirana podjetja v obravnavani analizi zahteve po krajših časih obnove, kot je običajno v slovenskih podjetjih.

4.7.4 CSO

Revija CSO je v februarju in marcu 2005 izvedla spletno anketo o neprekinjenem poslovanju (CSO, 2005) med 158 varnostnimi strokovnjaki. Ugotovili so, da ima velika večina anketiranih podjetij (93%) načrt neprekinjenega poslovanja, vendar pa ga je v praksi preizkusila le dobra tretjina (37%). Polovica (46%) vprašanih pravi, da njihovo podjetje nima konsistentnega načina informiranja zaposlenih o načrtu.

V skoraj vseh primerih (97%) obsega načrt neprekinjenega poslovanja obnovo informacijskega sistema, medtem ko v 80% obsega neprekinjeno delovanje in obnovo poslovnih procesov. Postopki za preselitev delovnih mest so vpeljani v 60% vprašanih podjetij.

Večina podjetij (73%) preverja in obnavlja načrt neprekinjenega poslovanja vsaj enkrat letno. Večina podjetij ima redno posodobljene kontaktne informacije o svojih zaposlenih, prav tako so večinoma (84–91%) v stiku z managementom v primeru krize. Postopki za vzpostavitev komunikacije do delničarjev in javnosti so slabše definirani (40–58%).

5. Zaključek

V magistrski nalogi sem obravnaval tematiko neprekinjenega poslovanja v slovenskih podjetjih. Prikazal sem cilje, namen in vsebino programa neprekinjenega poslovanja v podjetju. Znotraj te teme sem posebej obravnaval vlogo informatike ter njen pomen pri vpeljavi in upravljanju programa neprekinjenega poslovanja v podjetju. Namen dela je bil tudi pokazati pomembnost vzpostavitve in izvajanja programa neprekinjenega poslovanja podjetja ter opozoriti na nujnost aktivnega sodelovanja managementa in informatike pri upravljanju tega programa.

Analiza stanja neprekinjenega poslovanja v slovenskih podjetjih je pokazala, da je najpomembnejši razlog za vpeljavo programa neprekinjenega poslovanja regulativa. Posledica tega je, da je program najmočneje prisoten v finančni industriji, predvsem zaradi dogovora Basel II. Stanje, kot ga kaže analiza, je dobro v storitvah in slabše v gospodarstvu in javni upravi. Zelo slabo pa je stanje neprekinjenega poslovanja v zdravstvu, kjer bi glede na posebno vlogo zdravstva v družbi, pričakoval bistveno boljše rezultate.

Med vpeljanimi elementi neprekinjenega poslovanja zasledimo pri podjetjih na začetku uvajanja predvsem varnostne politike, visoko razpoložljivost ali rezervno lokacijo in upravljanje tveganj. Pri podjetjih in organizacijah, v katerih je program neprekinjenega poslovanja že dalj časa vpeljan (predvsem v finančni industriji), so dobro zastopani tudi drugi elementi neprekinjenega poslovanja.

Na začetku naloge sem postavil dve tezi, ki sem jih v nadaljevanju poskušal potrditi. Prva teza je bila, da je sodelovanje managementa v programu neprekinjenega poslovanja podjetja bistveno in da presega vlogo informatike v tem procesu. Analiza literature, anketa med slovenskimi podjetji in tuje analize – vse kažejo na odločujočo vlogo managementa. Obenem kažejo tudi na pogosto stanje tudi v slovenskem prostoru, ko je informatiki prepuščena iniciativa, izvedba in upravljanje tega programa brez podpore in udeležbe managementa. Ta pristop kaže na prenizko stopnjo zavedanja managementa o pomenu neprekinjenega poslovanja za podjetje. Kaže tudi na pogled managementa, da je neprekinjeno poslovanje, če je že potrebno, bolj problem in naloga informatikov.

Druga postavljena teza je bila, da je glavni razlog za vpeljavo neprekinjenega poslovanja v slovenska podjetja zunanji faktor, in sicer zakonodaja in regulativa na eni strani ter zahteve partnerjev na razvitih trgih na drugi strani. Rezultati analize so pokazali, da je v Sloveniji glavni razlog za vpeljavo programa neprekinjenega poslovanja regulativa in zakonodaja, medtem ko zahteve partnerjev z razvitih trgov niso pomemben razlog. Dodatno so tuje analize pokazale, da je pomemben dodaten faktor za uvedbo neprekinjenega poslovanja na razvitih trgih še zahteva kupcev in zahteva po operativni odpornosti poslovanja in razpoložljivosti, ki jih v raziskavi v Sloveniji nisem zaznal.

V magistrskem delu sem prikazal vlogo in pomen neprekinjenega poslovanja podjetja kot potrebnega elementa poslovanja v sodobnem podjetju. Zanje je vse bolj pomembno, da je njihovo poslovanje pripravljeno na dinamično prilagajanje nepredvidenim situacijam na trgu, v zakonodaji, motnjam iz okolja. Zato morajo preko začetnega projekta in nadaljnjega programa neprekinjenega poslovanja z močno podporo managementa ta pristop prenesti v strategijo in kulturo podjetja. V izvedeni anketi sem poskušal ugotoviti trenutno stanje slovenskih podjetij na tem področju in narediti primerjavo s tujimi raziskavami. Vrednost izvedene ankete se bo bistveno povečala, če se bosta anketa in analiza periodično ponavljali.

S tem bi lahko bolje opazovali trende in razvoj na tem področju skozi časovno obdobje. Izvedena anketa je imela določene omejitve, ki bi se jih v prihodnjih raziskavah lahko rešilo:

- Zajeti širši krog anketiranih podjetij,
- Natančnejša razvrstitev področja delovanja podjetja,
- Dodatni oz. novi razlogi za uvedbo programa neprekinjenega poslovanja: zahteva strank, zahteva po operativni odličnosti,
- Zajeti še dodatne elemente neprekinjenega poslovanja podjetij: načrt komuniciranja, učinkovitost testiranja,...

Ne glede na te možne popravke pa sem mnenja, da sta anketa in analiza zadovoljivo pokazali glavne značilnosti stanja neprekinjenega poslovanja v slovenskih podjetjih in znotraj tega pokazali vlogo informatike. Z nadaljnjimi raziskavami bi bilo mogoče ocenjevati tudi trende razvoja tega področja in eventualno približevanje načina upravljanja neprekinjenega poslovanja v slovenskih podjetij s pristopi podjetij na razvitih trgih.

6. Literatura in viri

6.1 Literatura

[1] Adams Tony: Satisfaction Varies With Experience in Outsourced Business Continuity and Disaster Recovery Services – User Wants and Needs. Gartner, junij 2003. 18 str.

[2] Adler Steven: You can't protect data if you don't know what it is worth. IBM SecureWorld 2005, november 2005.

[3] Andolšek Irena: Namen načrta neprekinjenega poslovanja. Revizor, oktober 2001. 13 str.

[4] Božič Julij: Ugotavljanje pripravljenosti bank na Basel II z uporabo IBM metode samoocenitve. Diplomsko delo. Ljubljana: Ekonomska fakulteta, september 2005. 53 str. [URL: http://www.cek.ef.uni-lj.si/u_diplome/bozic2072.pdf], 22.6.2006.

[5] Claunch Carl: Management Update: Best Practices in Business Continuity and Disaster Recovery. Gartner Research, marec 2004. 13 str.

[6] Cocchiara Richard: Beyond disaster recovery: Becoming a resilient business. IBM, oktober, 2005. [URL:http://www-1.ibm.com/services/us/bcrs/pdf/wp_becoming-a-resilient-business.pdf], 28.5.2006.

[7] CPM and Deloitte & Touche: Business Continuity Survey. Januar, 2006, 24 str. [URL: http://www.deloitte.com/dtt/cda/doc/content/us_assur_2005vBCM SURVEY REPORT.pdf], 17.6.2006.

[8] Croy Michael: The Business Value of Data. Forsythe, 2004. [URL: http://www.forsythe.com/Forsythe/itriskman/bc&dr/thebusinessvalueofdata.jsp;jsessionid=6D5594DE63E8C261556F3DE70D6C960B], 3.9.2006.

[9] CSO: Business Continuity survey. [URL: http://www.csoonline.com/csoresearch/report85.html], 17.6.2006.

[10] Denscombe Martyn: The Good Research Guide for small-scale social research projects, Second Edition. Open University Press, 2003. 310 str.

[11] Drnovšek Samo: Neprekinjeno poslovanje z vidika poslovne informatike. Diplomsko delo. Ljubljana: Ekonomska fakulteta, september 2005. 64 str. [URL: http://www.cek.ef.uni-lj.si/u_diplome/drnovsek2043.pdf], 7.6.2006.

[12] Drucker Peter F.: Technology, Management, and Society. New York: Harper and Row Publishers, 1972.

[13] Fulmer Kenneth L.: Business Continuity Planning: A Step-by-Step Guide with Planning Forms, Third Edition. Rothstein Associates, 2005. 190 str. [URL: http://www.books24x7.com/book/id_8575/toc.asp], 11.6.2006.

[14] Gallagher Michael: Business Continuity Management – How to Protect Your Company from Danger. FT Prentice Hall, december 2002. 168 str.

[15] Goldstein Phil, Katz Richard N., Olson Mark: Understanding the Value of IT. Educause Quarterly, št. 3, 2003. str. 14-18. [URL: http://www.educause.edu/ir/library/pdf/eqm0333.pdf], 27.11.2005.

[16] Graselli Peter: Zakaj je pomembna zmogljivostno zrelostna ocena programa UNP. Varnostni forum, maj 2006. str. 20-22.

[17] Van Grembergen Wim: The Balanced Scorecard and IT Governance. Information Systems Control Journal, 2006. [URL: http://www.itgi.org/-template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=5550], 11.6.2006.

[18] Groznik Aleš, Indihar Štemberger Mojca, Kovačič Andrej: Vloga managementa pri zagotavljanju poslovne vrednosti informatike. Ljubljana: Ekonomska fakulteta, 2005. [URL: ftp://ftp.ef.uni-lj.si/_dokumenti/predmeti/Pomeninformatike6.doc], 7.11.2005.

[19] Harris Shon: CISSP All-in-One Exam Guide, Second Edition. McGraw-Hill Osborne Media, junij 2003, 1008 str.

[20] Hiles Andrew: Business Continuity: Best Practices. Rothstein Associates, 2000. 303 str. [URL: http://www.books24x7.com/book/id_3571/toc.asp], 10.9.2006.

[21] Hiles Andrew: Business Continuity: Best Practices: World Class Business Continuity Management, 2nd Edition. Rothstein Associates 2004. 290 str. [URL: http://www.books24x7.com/toc.asp?bookid=8573], 10.9.2006.

[22] Honey Paul: Creating the Master Plan. Merrill Lynch & Co, februar 2002. [URL: http://www.sia.com/business_continuity/pdf/master_plan.pdf], 11.6.2006.

[23] Hutchinson Susan R.: Survey Research. Foundations for Research – Methods of Inquiry in Education and the Social Sciences. Mahwah, New Jersey: Lawrence Erlbaum Associates, 2004. str. 283-301.

[24] Kajić Milan: Varnostna politika in načrtovanje ukrepov za izredne razmere pri varovanju IS. Organizacija, september 1999. 6 str.

[25] Kovačič Andrej, Jaklič Jurij, Indihar Štemberger Mojca, Groznik Aleš: Prenova in informatizacija poslovanja. Ljubljana: Ekonomska fakulteta, 2004. 345 str.

[26] Krischer Josh, Scott Donna, Witty Roberta J.: Management Update: Six Myths about Business Continuity Management and Disaster Recovery. Gartner Research, marec 2005. 6 str.

[27] Krutz Ronald L., Vines Russell Dean: The CISSP Prep Guide. Willey Publishing, 2003. 944 str.

[28] Mingay Simon: Outlining the Gartner BCP Maturity Model. Gartner Research, september 2002. 4 str.

[29] Noakes-Fry Kristen, Diamond Trude: Business Continuity and Recovery Products and Services: Overview. Gartner Research, november 2004. 18 str.

[30] Noakes-Fry Kristen, Baum Christoper H., Runyon Barry: Laws Influence Business Continuity and Disaster Recovery Planning Among Industries. Gartner Research, julij 2005. 7 str.

[31] Rihar Boštjan: Uvajanje pogojev za zagotavljanje delovanja poslovnega informacijskega sistema. Magistrsko delo. Ljubljana: Ekonomska fakulteta, junij 2003. 90 str.

[32] Scott Donna: Assessing the Cost of Application Downtime. Gartner Research, maj 1998. 4 str.

[33] Scott Donna, Witty Roberta J.: Enlightening the CEO on Business Continuity Management. Gartner Research, november 2005. 6 str.

[34] Sikich Geary: Making the case for business continuity. 2004. [URL: http://www.continuitycentral.com/feature0144.htm], 3.9.2006.

[35] Šalehar-Kegl Dušan, Zupan Lucija, Černe Meta, Sotlar Mišo: Praktični pristopi k vpeljavi neprekinjenega poslovanja in izkušnje PDC. Zbornik referatov INDO 2004: posvetovanje informatikov v javni upravi, Portorož, Center za informatiko, 2004. 13 str.

[36] Tallon P.P., Kraemer K.L., Gurbaxany V.: Executives' Perceptions of teh Business Value of Information Technology: A Process-Oriented Approach. Journal of Management Information Systems, 2000, str. 145-173.

[37] Tittel Ed, Stewart James Michael, Chapple Mike: CISSP: Certified Information Systems Security Professional Study Guide, Second Edition. Sybex, 2004. 677 str. [URL: http://www.books24x7.com/book/id_9204/toc.asp], 15.7.2006.

[38] Wallace Michael, Webber Lawrence: The Disaster Recovery Handbook—A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets. Amacom, 2004. 416 str. [URL: http://www.books24x7.com/book/ id_4548/toc.asp], 11.9.2006.

[39] Warrick Cathy et al.: IBM TotalStorage Business Continuity Solution Overview. IBM Redbooks, junij 2005. 226 str.

[40] Žnidar Borut: Upravljanje tveganja. Varnostni forum, november 2005. str. 16-18.

[41] Žnidar Borut: Upravljanje neprekinjenega poslovanja v slovenskih podjetjih. Varnostni forum, julij 2006. str. 24-26.

6.2 Viri

[1] BS25999. [URL: http://www.w3j.com/xml/index.html], 5.6.2006.

[2] Business Impact Analysis. [URL: https://www-1.ibm.com/services/us/index.wss/offering/bcrs/a1000260], IBM, 30.1.2006.

[3] Business Continuity Institute. [URL: http://www.thebci.org/], 4.3.2006.

[4] Continuity Central. [URL: http://www.continuitycentral.com/], 27.2.2006.

[5] Crisis Management & Disaster Recovery. [URL:http://www.crisismanagement-disasterrecovery.com/]

[6] Disaster Recovery Institute International. [URL: http://www.drii.org/], 22.5.2006.

[7] EnvoyWorldWide: Trends in Business Continuity and Risk Management. Risk Management. Bedford, Massachusetts, junij 2005. [URL: http://www.envoyworldwide.com/news/releases/061305.shtml], 5.7.2006.

[8] Inštitut za neprekinjeno poslovanje. [URL: http://www.inp.si], 4.3.2006.

[9] ISO/IEC 17799 - Information technology — Security techniques — Code of practice for information security management, Second edition. ISO/IEC, junij 2005.

[10] PAS 56. [URL: http://www.pas56.com/], 4.6.2006.

[11] Statistični urad RS: Klasje. [URL: http://www.stat.si/klasje/klasje.asp], 18.5.2006.

[12] Statistični urad RS: Statistične informacije – Poslovni subjekti. [URL: http://www.stat.si/doc/statinf/14-SI-188-0501.pdf], 18.5.2006.

[13] Puc Katarina: Slovar informatike. [URL: http://www.islovar.org], 8.12.2005.

[14] SHARE. [URL:http://www.share.com/], 5.7.2006.

[15] Survive. [URL: http://www.survive.com/default.cfm], 4.3.2006.

[16] Wikipedia, the free encyclopedia. [URL: http://en.wikipedia.org/], 5.5.2005.

7. Slovarček

Balanced Scorecard (BSC) – Celovit/uravnotežen sistem kazalnikov

British Standards Institution (BSI) – Angleški organizacija za standardizacijo

Business Continuity (BC) – Neprekinjeno poslovanje (NP)

Business Continuity Management (BCM) – Upravljanje neprekinjenega poslovanja (UNP)

Business Continuity Plan (BCP) –Načrt neprekinjenega poslovanja

Business Impact Analysis (BIA) – Analiza vpliva na poslovanje

Business recovery – Obnova poslovanja

Business resilience – Odpornost poslovanja

Business resumption – Vzdrževanje poslovanja

Business-to-business (B2B) – Elektronsko poslovanje med podjetji

Business-to-customer (B2C) – Elektronsko poslovanje med podjetji in potrošniki

Chief Information Officer (CIO) – Direktor informatike

Contingency planning – Načrtovanje odzivov in rezerve za nepredvidene dogodke

Continuity of operations plan (COOP) – Načrt neprekinjenega izvajanja operacij

Control Objectives for Information and related Technology (COBIT) – Kontrolni cilji za informacijsko in sorodno tehnologijo

Crisis management – Krizni management

Disaster Recovery (DR) – Obnova po katastrofi

Disaster Recovery Plan (DRP) – Načrt obnove po katastrofi

Due Care / Diligent – Primerna skrbnost / poslovnost; skrbnost dobrega gospodarja / trgovca

Health Insurance Portability and Accountability Act (HIPAA)

High Availability (HA) – Visoka razpoložljivost

Information and Communication Technology ICT) – Informacijska in telekomuni-kacijska tehnologija (IKT)

Information Systems Audit and Control Association (ISACA)

Information System Management System (ISMS) – Sistem nadzora informacijske varnosti

Information Technology (IT) – Informacijska tehnologija

International Electrotechnical Commission (IEC) – Mednarodna elektrotehnična komisija

International Organization for Standardization (ISO) – Mednarodna organizacija za standardizacijo

IT Governance Institute (ITGI)

IT Infrastructure Library (ITIL) – Knjižnica informacijske infrastrukture

Outsourcing – Zunanje izvajanje

PDCA cycle: Plan, Do, Check, Act – Cikel načrtovanja, izvajanja, preverjanja in ukrepanja.

Recovery Network Objective (RNO) – Ciljni čas vzpostavitve delovanja omrežja

Recovery Point Objective (RPO) – Ciljna točka obnavljanja podatkov

Recovery Time Objective (RTO) – Ciljni čas vzpostavitve delovanja informacijskega sistema

Return On Equity (ROE) – Količnik donosnosti sredstev

Return On Investment (ROI) – Donosnost investicije

Risk Analysis (RA) – Analiza tveganja

Run Time Enterprise (RTE) – Podjetja s poslovanjem v realnem času

Service level agreement (SLA) – Nivo zagotavljanja storitve

Single point of failure (SPOF) – Posamezna točka napake

Stakeholders – Zainteresirane stranke, déležniki

Total Cost of Ownership (TCO) – skupni stroški lastništva

Total Value of Ownership (TVO) – skupna vrednost lastništva

8. Priloga

8.1 Vprašalnik za anketo

IPI INŠTITUT ZA POSLOVNO INFORMATIKO

Upravljanje neprekinjenega poslovanja

UNIVERZA V LJUBLJANI EKONOMSKA FAKULTETA FACULTY OF ECONOMICS UNIVERSITY OF LJUBLJANA

*V okviru podiplomskega študija na Ekonomski fakulteti, v sodelovanju z **Inštitutom za poslovno informatiko**, izvajam anonimno anketo o upravljanju neprekinjenega poslovanja v slovenskih podjetjih. Vabim vas k sodelovanju v raziskavi, s katero želimo ugotoviti nivo in način uvajanja neprekinjenega poslovanja v Sloveniji. Rezultati ankete so zaupne narave in ne bodo uporabljeni v druge namene.*

1. Katera je glavna dejavnost podjetja, v katerem ste zaposleni (označite le eno)?

☐ finančna inštitucija (banka/zavarovalnica) ☐ gospodarska dejavnost ☐ javna uprava ☐ zdravstvo
☐ storitve ☐ trgovina ☐ telekomunikacije ☐ ostalo _____

2. Vaš položaj v podjetju (označite le eno)?

☐ management ☐ vodstvo IT ☐ osebje IT ☐ ostalo_____

3. Koliko ljudi je zaposlenih v podjetju (označite le eno)?

☐ do 20 ☐ 20–100 ☐ 100–500 ☐ nad 500

---

4. Ali ima podjetje vpeljan plan neprekinjenega poslovanja?

☐ se pripravlja ☐ je narejen ☐ se redno preizkuša ☐ se redno obnavlja

5. Katere elemente neprekinjenega poslovanja podjetja imate vpeljane?

☐ obvladovanje tveganj ☐ analiza vpliva na poslovanje ☐ plan obnove poslovanja ☐ visoka razpoložljivost
☐ rezervna lokacija ☐ varnostne politike ☐ upravljanje varnosti ☐ krizni management

6. Kaj je bil glavni razlog za vpeljavo neprekinjenega poslovanja v podjetju?

☐ zahteva regulative ☐ zahteva poslovnega partnerja ☐ zahteva poslovodstva ☐ izkušnja zaradi izpada poslovanja

7. Kakšna je bila vloga posameznih delov podjetja pri vpeljavi neprekinjenega poslovanja?

	odločilna				neaktivna
Management	5	4	3	2	1
Oddelek IT	5	4	3	2	1
Notranja revizija	5	4	3	2	1

8. Kako pogosto izvajate preizkus plana neprekinjenega poslovanja (označite le eno)?

☐ dvakrat letno ☐ letno ☐ občasno ☐ še nikoli

9. Kako pogosto izvajate pregled in obnovo plana neprekinjenega poslovanja podjetja (označite le eno)?

☐ dvakrat letno ☐ letno ☐ občasno ☐ še nikoli

---

10. Kako pogosto v podjetju zaznate motnje, ki bi lahko/so povzročile izpad poslovanja (označite le eno)?

☐ mesečno ☐ kvartalno ☐ letno ☐ še nikoli

11. Kakšno vrsto motnje poslovanja ste že zaznali?

☐ varnostni incident ☐ izpad IT opreme ☐ izpad komunikacij ☐ izpad el. energije
☐ naravna nesreča ☐ fizični vdor (vlom) ☐ človeški faktor ☐ drugo_____

Ali bi bili pripravljeni sodelovati v enournem intervjuju, v katerem bi obravnavana področja natančneje obdelali? V primeru pozitivnega odgovora vas prosimo za kontaktno informacijo:

kontakt: _____

Izpolnjene vprašalnike oddajte pri registracijski mizi.

Za vaše sodelovanje v anketi se vam najlepše zahvaljujem,

Borut Žnidar

Anketa_v5g.doc, 21.3.2006