UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

# DIPLOMSKO DELO

## NEPREKINJENO POSLOVANJE Z VIDIKA POSLOVNE INFORMATIKE

Ljubljana, september 2005 SAMO DRNOVŠEK

IZJAVA

Študent **Samo Drnovšek** izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom **dr. Aleša Groznika** in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 14.09.2005 Podpis_____

# KAZALO VSEBINE

# KAZALO SLIK



# KAZALO TABEL

# 1 UVOD

Večina sodobnih organizacij je odvisnih od tehnologije in avtomatiziranih sistemov. Tudi nekajdnevni izpad takšnih sistemov lahko povzroči velike finančne izgube ter ogrozi preživetje organizacije. Uspešno neprekinjeno delovanje organizacije je odvisno od vedenja vodstva o morebitnih katastrofalnih posledicah nezgod, njihove zmožnosti, za izdelavo plana, ki bo zagotovil minimalen vpliv takšnih nezgod na kritične poslovne funkcije organizacije, ter njihove sposobnosti, da hitro in uspešno ponovno vzpostavijo delovanje v primeru nezgode. Neprekinjenost poslovanja je temeljna zahteva informacijsko podprtih poslovnih sistemov in procesov, v katerega ne vključujemo le informacijsko tehnološki segment, ampak celoten del poslovnega okolja, v katerem se informacije obravnavajo. Motnje iz okolice v različnih stopnjah ogrožajo (poslovne) rezultate poslovanja na vseh segmentih obravnavanja podatkov, zato je potreba poslovne funkcije, da ugotovi težo posameznih poslovnih procesov, možne grožnje in vpliv na izvajanje ter na tej osnovi določi sredstva in postopke, s katerimi zagotavlja sprejemljiv nivo poslovanja. Pri tem določi tudi zahtevan nivo storitev (oziroma kriterije) za vse tiste dejavnosti, ki podpirajo poslovne procese.

Neprekinjenost poslovanja organizacije je moč zagotoviti na različne načine, na primer s podvojenimi zmogljivostmi, podvojenim obravnavanjem podatkov, podvojenimi komunikacijami in podvojenim hranjenjem podatkov. Glede na ocenjena tveganja pri poslovanju se organizacija lahko odloči za cenejšo možnost zagotavljanja neprekinjenega poslovanja, to je za načrte izvajanja poslovnih procesov v primeru nedelovanja dela ali celote informacijske tehnologije oziroma nerazpoložljivosti komunikacij. Pripravljeni načrti se morajo preizkušati in vzdrževati glede na spremembe v informacijski ureditvi in na podlagi na novo prepoznanih poslovnih tveganj.

## 1.1 Namen in cilji diplomske naloge

Informacije v organizaciji pomenijo premoženje (za mnoge celo najpomembnejše), ki ima prav tako kot druge vrste premoženja, svojo vrednost in ga je treba na primeren način varovati in to ne glede na obliko ali način shranjevanja. Ustrezno varovanje ščiti informacije in podporne sisteme pred širokim spektrom groženj ter nevarnosti z namenom, da se zagotovi nemoten potek poslovanja, da se minimizira škoda ob morebitni uresničitvi katere od groženj ter da se na drugi strani omogoči največji izkoristek investicij v informacijsko tehnologijo in uspešna izraba poslovnih priložnosti. Učinkovita uporaba informacijske tehnologije lahko pomembno spremeni organizacijo in njene poslovne postopke ter poveča konkurenčnost. Vse to lahko v določeni meri omogoča zagotavljanje neprekinjenega poslovanja, ki združuje številne aktivnosti, katerih namen temelji predvsem na zagotavljanju neprekinjenosti poslovanja in okrevanju kritičnih poslovnih procesov v primeru nepredvidljivih dogodkov in katastrof. Namen diplomskega dela je dati tej problematiki

ustrezen poudarek ter s tem prikazati pomen in vsebino zagotavljanja ter načrtovanja neprekinjenega poslovanja.

V diplomskem delu se bom v največji meri dotaknil aktivnosti in procesov, ki so namenjeni zagotavljanju neprekinjene informacijske podpore poslovanju in poslovnim procesom ter funkcijam. Tako bom na tej osnovi poskušal v nadaljevanju doseči zastavljene cilje diplomskega dela:

- Iz različnih dostopnih metodologij zagotavljanja delovanja informacijskega sistema, ki jih je mogoče zaslediti v literaturi, izluščiti najpomembnejše značilnosti in jih povezati v smiselno celoto, ki bi lahko služila kot referenca pri reševanju tega problema.
- Predstaviti praktičen pristop k vzpostavitvi neprekinjenega poslovanja.
- Izpostaviti probleme, s katerimi se organizacije in informatiki srečujejo pri vzpostavitvi ter izvajanju procesa neprekinjenega poslovanja.
- Na podlagi opredeljenih problemov predlagati določene praktične rešitve.

# 2 ZAGOTAVLJANJE POSLOVANJA GOSPODARSKIH SUBJEKTOV IN NEPROFITNIH ORGANIZACIJ

Poslovni informacijski sistemi so v današnjem času postali temelj, na katerih sloni in deluje celotno poslovanje ter delovanje večine poslovnih procesov in funkcij v organizaciji. Za poslovni uspeh organizacije (podjetja, institucije javnega sektorja itd.) je danes eden bistvenih pogojev uspešno upravljanje informacij in informacijske tehnologije. Informacije lahko nastopajo v različnih oblikah. Lahko so napisane ali natisnjene, shranjene v elektronski obliki, se pošiljajo po pošti ali elektronskih kanalih, so prikazane na vizualnih sredstvih ali so preprosto izgovorjene. Skokovita rast in ponudba informacijskih rešitev, ki so namenjene upravljanju odnosov s strankami, upravljanju preskrbovalnih verig, vedno večja uporaba različnih e-storitev, jasno nakazujejo da bo v prihodnje uspešno poslovanje organizacije temeljilo na učinkoviti informacijsko telekomunikacijski (ITkT) podpori. Obenem pa ta podpora vedno bolj tanjša mejo med pridobitnimi in nepridobitnimi organizacijami ter med veliki, srednjimi in malimi podjetji. V globalnem svetu so vedno bolj začrtane smernice poslovanja tako imenovanih virtualnih organizacijah, ki v celoti slonijo na ITkT podpori. Vendar pa z naraščanjem pomena informacijskih sistemov, narašča tudi obseg potencialne škode, ki jo utrpijo organizacije ob prekinitvi njihovega delovanja. Vsak izpad informacijske podpore hkrati pomeni tudi izpad dohodka, v nekaterih primerih, če izpad traja predolgo, ali če se nekateri ključni podatki trajno izgubijo, pa tudi grožnjo za obstoj same organizacije (Verton, 2002b).

## 2.1 Poslovne zahteve 21. stoletja

V konkurenčnem poslovnem okolju so informacije vedno bolj izpostavljene raznim oblikam odtujitve in izgube, ki so lahko interne, zunanje, po nesreči ali namerne. Z današnjimi

novimi tehnologijami shranjevanja, prenosa in pregledovanja informacij in podatkov se povečujejo tveganja za občutljive informacije. Zato se povečujejo tudi zahteve podjetij za zaščito zaupnosti, celovitosti in razpoložljivosti informacij. Z odtujitvijo informacij lahko nastane velika poslovna škoda.

Kadar imamo opraviti z zaupnimi ali občutljivimi informacijami, v papirnati ali elektronski obliki, tako že stopamo na področje informacijske varnosti. Vzroki za to, da se morate ukvarjati z varovanjem in zaščito informacijskega premoženja, so lahko različni:

- pravni normativi;
- zakonodaja;
- dobra poslovna politika podjetja in upravljanje s tveganji;
- zahteve podjetij, s katerimi poslujete;
- večja izpostavljenost možnosti odtujitve informacij.

Vsaka zaščita in vsako varovanje informacijskega premoženja zahtevata določene postopke in navodila, ki so združeni v varnostni politiki. Cilj varnostne politike je zgraditi celovit varnostni sistem, ki združuje in usklajuje vse obstoječe ter na novo razvite varnostne in zaščitne aktivnosti in mehanizme, zato da se:

- zavaruje informacijsko premoženje podjetja;
- zagotovi nemoteno poslovanje;
- zmanjša poslovna škoda z zmanjšanjem vpliva varnostnih dogodkov;
- zagotovi nemoten pretok informacij in sredstev, obenem pa zagotovi njihova zaščita;
- zavaruje informacijsko premoženje tretjih oseb, do katerega ima podjetje dostop;
- Vzpostavi varnostna kultura v podjetju.

## 2.2 Identifikacija in obvladovanje tveganj

Tveganje je možnost, da se nek problem pojavi v prihodnosti. Tveganje še ne pomeni dejanskega obstoja nekega problema. Zaradi kompleksnosti in naše nezmožnosti obvladovanja vseh podrobnosti, vedno obstaja možnost, da se zgodi kaj nepredvidenega. Tveganje je dejstvo, ki spremlja vsako dejavnost. Za obstoj tveganja sta potrebna dva pogoja:

P - verjetnost za nastop nekega pojava

L - škodljivost tega pojava.

Kako pomembno je tveganje in s kakšno resnostjo ga je potrebno obravnavati, nam pove kritičnost tveganja. Kritičnost tveganja (E) je odvisna od verjetnosti (P) in škodljivosti (L). Izrazimo jo kot produkt verjetnosti in škodljivosti: E = P*L (Hunton, 2004, str. 52).

Pogosto se zgodi, da se tveganja ne zavedamo. Če je razlog temu nepomembnost tveganja, to ni zaskrbljujoče. Drugače pa je v primeru, kadar se ne zavedamo kritičnega tveganja, kajti

kritična tveganja je potrebno upoštevati, ugotoviti njihove dejavnike, nadzorovati njihov razvoj in po potrebi ukrepati, da preprečimo njihovo uresničitev.

Tveganje samo po sebi še ne prinaša škode. Škoda se pojavi šele takrat, ko se tveganje uresniči. Največji stroški so običajno povezani z odpravo posledic nastale škode. Izkaže se, da je najbolj racionalno vlagati napore in sredstva v dejavnosti za ugotavljanje tveganj in preprečevanje njihovega razvoja. Na tej ugotovitvi sloni metoda upravljanja tveganj.

Ker so tveganja pri poslovanju nenehno prisotna, mora podjetje vzpostaviti ustrezne kontrolne procese in postopke. Tveganja lahko obravnavamo z vidikov priložnosti (povezava tveganja in možnosti za povečanje donosa), negotovosti (razhajanje med pričakovanimi in dejanskimi rezultati) in nevarnosti (možnost pojava dogodka z negativnimi posledicami za podjetje). Naloga managementa organizacije je, da na podlagi ugotovitve poslovnih ciljev in strategij podjetja ter analize in ocene posameznih tveganj določi sprejemljiv nivo tveganja in ustrezne ukrepe za obvladovanje le-teh. Pri tem je pomembno vedeti, da je lahko sprejemanje premajhnega tveganja z vidika priložnosti ali pretirano upravljanje nevarnosti enako neuspešno kot dopuščanje prevelikega nenadzorovanega tveganja. Zato je treba vzpostaviti procese proaktivnega ocenjevanja tveganj in dobro premišljenega upravljanja z njimi, da se v podjetju pridobijo razumna zagotovila glede doseganja kontrolnih ciljev (Vozlič, 2003, str. 1).

Informacije ne glede na pojavno obliko, predstavljajo pomembno premoženje podjetja, ki ima svojo vrednost in zato zahteva ustrezno pozornost. Za zagotavljanje uspešnosti poslovnih procesov je treba obvladovati pretok informacij znotraj organizacije in v izmenjavi z zunanjim okoljem. Informacijski sistem v organizaciji v tem kontekstu pomeni celotno okolje, v katerem se pojavljajo informacije, zato ga ne smemo zamenjevati zgolj z računalniškim sistemom v ožjem smislu, saj ta pomeni samo tehnično infrastrukturo informacijskega sistema. Pristop k obvladovanju informacijskih tveganj mora biti zato veliko širši in se ne sme omejiti samo na tehnični vidik. Lahko rečemo, da je danes informacijska tehnologija ključna komponenta poslovnih procesov. Vedno večja uporaba informacijske tehnologije na drugi strani zahteva vedno večje investicije, povečuje se tveganje za neuspeh projektov in posledično zavest, da je treba stvar ustrezno upravljati in nadzorovati (Vozlič, 2002, str. 2). Tako lahko rečemo, da obvladovanje poslovnega tveganja v informacijskem sistemu v podjetju in zagotovitev ustrezne varnosti informacijskega premoženja, zahtevata jasne smernice in podporo vodstva podjetja, zagotovitev potrebnih finančnih in drugih sredstev, ustrezno okolje v podjetju za promocijo in izvajanje dobre informacijske varnostne politike na vseh nivojih podjetja in zagotovitev potrebnih človeških virov.

# 3 ZAGOTAVLJANJE NEPREKINJENEGA POSLOVANJA

## 3.1 Ozadje zagotavljanja neprekinjenega poslovanja

Neprekinjeno poslovanje je v sodobnem času izziv, s katerim se soočajo gospodarski subjekti in neprofitne organizacije, kot so organizacije javne uprave. Vsaka organizacija se mora zavedati posledic nepričakovanih zastojev informacijskega sistema, ki jih lahko prinesejo izredne okoliščine. Po nastopu nepričakovanega uničujočega dogodka se mora v najkrajšem času zagotoviti normalno delovanje. Potreba po hitrem okrevanju in vzpostavitvi poslovanja v prvotno stanje zahteva vnaprejšnje planiranje in pripravo. Pri tem potrebujemo izdelan načrt neprekinjenega poslovanja (angl. Business Continuity Plan - BCP). S pomočjo načrta neprekinjenega poslovanja organizacija ostaja pripravljena na nepričakovane dogodke in njihove negativne posledice. Ustrezen načrt organizaciji zagotavlja, da lahko nevarnost prepozna pred njenim nastopom ter se nanjo pravočasno in ustrezno odzove.

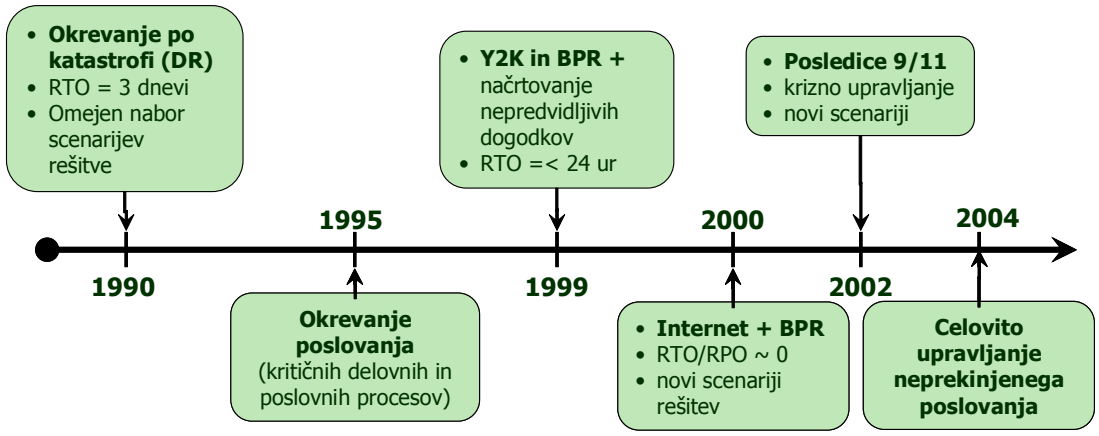
Iz teh predpostavk izhaja ugotovitev, da je treba pripravo organizacije na nepredvidene dogodke, ki lahko ogrozijo njeno poslovanje, začeti pri načrtu zagotavljanja delovanja njenega poslovnega informacijskega sistema. Prvi razlog za to je v že prej navedeni čedalje tesnejši povezanosti večine funkcij poslovnega sistema skozi poslovni informacijski sistem, zaradi česar lahko z opazovanjem delovanja posameznih njegovih delov opazujemo tudi delovanje posameznih funkcijskih enot poslovnega sistema. Drugi razlog pa je v tem, da poslovni informacijski in telekomunikacijski sistem zaradi svoje fizične razprostranjenosti, tehnološke zapletenosti in čedalje tesnejše navezave z okoljem ter s tem čedalje večje odprtosti pomeni enega najbolj ranljivih delov poslovnega sistema.

## 3.2 Razvoj neprekinjenega poslovanja

Zgodovina neprekinjenega poslovanja sega v začetek sedemdesetih let prejšnjega stoletja, ko so se začele razvijati prve aktivnosti na področju načrtovanja okrevanja po katastrofah. Povečevanje obsega informacijskih sistemov, vključevanje le-teh v poslovne procese in eksponentno naraščanje količine podatkov so pripeljali do novih tveganj, s katerimi so se soočile takratne gospodarske družbe. To tveganje je vodilo k izvajanju različnih novih aktivnosti, predvsem izdelavi varnostnih kopij, omejevanju dostopa do podatkov, zagotavljanju fizične varnosti, rezervne elektroenergetske zmogljivosti itd. Takratne zmogljivosti so zagotavljale še sprejemljiv čas izpada informacijskega sistema do nekaj dni. Vzrok je bil predvsem v nerazviti tehnologiji in ekstremno visokih stroških rezervne lokacije, ki bi bila v pripravljenosti za vključitev v sistem v primeru katastrofe. Izdelava načrtov okrevanja po katastrofi je bila tedaj omejena predvsem na finančne organizacije (banke, zavarovalnice, itd.), katerih občutljivost na nepredvidene izpade je bila ogromna, kar je vzpodbujalo investicije v primerne in zadovoljive sistemske zmogljivosti na primarni lokaciji ter hkrati vzpostavitev varnih rezervnih lokacij, ki so omogočale vključitev v sistem v najkrajšem možnem (Gallagher, 2003, str. 6).

V osemdesetih letih so se pojavili prvi premiki h komercializaciji okrevalnih postopkov, ki so zagotavljali primerne sistemske vire in zmogljivosti, da so gospodarski subjekti skrb za okrevanje po nepredvidenih dogodkih in katastrofah, oddajale v zunanje izvajanje. Ključni problem, ki se je pojavljal v tistem času, je bila 100% usmerjenost na okrevanje in ponovno vzpostavitev zgolj informacijske tehnologije. Cilj vseh okrevalnih načrtov je bil preprečiti oziroma vsaj minimizirati vplive nepredvidenih dogodkov na poslovanje gospodarskih subjektov (Gallagher, 2003, str. 7). Pri tem so bile vse aktivnosti in procesi usmerjeni v ponovno vzpostavitev različnih informacijskih sistemov, popolnoma pa so zanemarili dejstvo, da je v primeru katastrofe potrebno zagotoviti tudi ostalo infrastrukturo, ki bi omogočalo kar se da hitro vzpostavitev kritičnih sistemov. To je bil ključni povod, da se je v devetdesetih letih proces okrevanja po nepredvidenih dogodkih razširil na načrtovanje neprekinjenega poslovanja. Ta premik je zagotavljal velike spremembe pri skrajševanju sprejemljivega časa okrevanja, ki se je štel v urah in ne več v dnevih, obenem pa je načrt neprekinjenega poslovanja poleg informacijske tehnologije vključeval vse vidike organizacij poslovanja.

**Slika 1:** Razvoj procesa neprekinjenega poslovanja skozi zgodovino




- *RTO - trenutek, ko so aplikacije funkcionalne v takšni meri, da lahko ponovno vzpostavimo transakcije.*
- *Y2K - problem milenijskega hrošča*
- *BPR - prenova poslovnih procesov*
- *RPO - točka v procesu okrevanja, v kateri lahko začnemo s ponovnim priklicom konsistentnih podatkov.*
- *9/11 - Teroristični napad na stavbi WTC v New York-u*

*Vir: Claunch, 2004, str. 4.*

Zadnje desetletje sta na področju zagotavljanja neprekinjenega poslovanja zaznamovala predvsem dva dogodka:

1. Problem »milenijskega hrošča« (Y2K), ki je pravzaprav prvi večji dejavnik, ki je vzpodbudil širši obseg gospodarskih subjektov po celem svetu k razmišljanju in načrtovanju neprekinjenega poslovanja. K temu so v prvi meri pripomogla naslednja dejstva:
   - povečana zavest o problematiki potencialne zaustavitve poslovanja;
   - zavedanje in spoznanje ranljivosti kritičnih procesov;

- negotovost in nemoč, s katero so se soočali vsi, tako informatiki kot tudi managerji in širša strokovna javnost, ki bi jo lahko povzročil »milenijski hrošč« (popoln mrk vseh na informacijski tehnologiji temelječih sistemov);
- večina organizacij se je prvič soočila z dejstvom, da je celotno poslovanje odvisno od majhnega računalniškega čipa.

2. Teroristični napadi na stavbi Svetovnega trgovinskega centra v New Yorku (»9/11«), ko je management neprekinjenega poslovanja dobil nove razsežnosti in nov pomen. Večina vrhovnih managerjev večine gospodarskih subjektov po celem svetu se je seznanila z nemočjo v primeru nepričakovanih in katastrofalnih dogodkov.

## 3.3 Pomen neprekinjenega poslovanja

Tragični dogodki 11. septembra 2001, ko sta bila uničena dvojčka Svetovnega trgovinskega centra v New Yorku, so imeli poleg drugih daljnosežnih posledic tudi eno, o kateri se v širši javnosti manj govori, zato pa toliko več v strokovni javnosti, še zlasti med strokovnjaki. Ti dogodki so namreč drastično pokazali, kako pomembne so podrobne predhodne priprave na možno katastrofo, ki vsem organizacijam, tako javnega kot zasebnega sektorja, omogoča, ob uničenju takih razsežnosti, kakršnemu smo bili priča, hitro ponovno vzpostavitev ključnih poslovnih funkcij in kritičnih aplikacij. To pa lahko v nadaljevanju prevesi jeziček na tehtnici med obstankom in propadom podjetja. Sam koncept načrtovanja neprekinjenega poslovanja je bil znan in upoštevan že prej, dejansko pa šele resnične katastrofe postavijo v središče pozornosti predhodne priprave na katastrofo in s tem poudarijo resnično pomembnost. Kar nekaj podjetij je imelo v podrtih stavbah Svetovnega trgovinskega centra v New Yorku svoje glavne informacijske centre in so se ob njihovem popolnem uničenju morala spoprijeti s težkim izzivom, kako v najkrajšem možnem času spet vzpostaviti sisteme informacijske podpore in nadaljevati poslovanje. Nekaj je bilo takih, ki so bila dobro pripravljena in so to lahko storila v razmeroma kratkem času, veliko več pa jih je ugotovilo, da načrtov za take primere nimajo. Marsikatero je zaradi nezmožnosti, da bi hitro nadaljevalo s poslovanjem, tudi propadlo. Podjetja se morajo zavedati posledic nepričakovanih zastojev informacijskega sistema, ki jih lahko povzročijo izredne okoliščine. V najkrajšem možnem času morajo zagotoviti normalno delovanje po nepričakovanem uničujočem dogodku. Potreba po hitrem restavriranju poslovanja zahteva vnaprejšnje planiranje in pripravo, ki se odražata skozi management neprekinjenega poslovanja.

Ustrezno načrtovanje, kako ravnati ob morebitni veliki katastrofi in uničenju, presega področje informatike. Je pa zaradi vse pomembnejše vloge te podporne poslovne funkcije in vse večjega opiranja celotnega poslovanja nanjo eno od osrednjih področij, za katera je treba načrtovati ukrepe za zmanjšanje tveganj izpadov večjih razsežnosti. Zmotno bi bilo misliti, da pod pojem katastrofa sodijo le dogodki takih razsežnosti, ki smo jim bili priča septembra leta 2001.

Kaj pravzaprav je katastrofa?

Katastrofa je prekinitev temeljnega oskrbovanja z informacijami oziroma ključnih in bistvenih poslovnih funkcij za nesprejemljivo obdobje. Kar je katastrofa za eno družbo, ni nujno, da je katastrofa tudi za drugo družbo. Na osnovi finančnega učinka je treba oceniti, kaj je za družbo nesprejemljiva prekinitev.

Katastrofe so opredeljene tudi glede na čas. Pomembno je, kdaj pride do prekinitve in koliko časa traja. Zaradi prekinitve pomembnejšega obdelovanja (na primer mesečnega ali letnega) ima družba večje težave kot zaradi prekinitve krajših obdelav.

Katastrofa je lahko v informatiki marsikaj. Najpogostejše situacije, v katerih so podjetja razglasila stanje katastrofe, so po svoji naravi precej različne. Med temi so v ospredju predvsem izpadi električne energije, sledijo napake v strojni opremi, požari, poplave, potresi, vremenski ekstremi (hurikani, snežna in običajna neurja), napake v programski opremi, bombni napadi in izpadi komunikacijskih povezav. Statistika zadnjih let pa pravi, da lahko med vzroke katastrofe uvrstimo tudi napade virusov in hekerjev ter škodo, ki jo povzročijo nezadovoljni zdajšnji ali nekdanji uslužbenci podjetja.

Večina strokovnjakov iz prakse se strinja, da ni nekega vseobsegajočega modela za načrtovanje za primer katastrof, ki bi bil uporaben za vse vrste in velikosti organizacij, saj je oblika in vsebina takih načrtov odvisna od velikosti ter vrste organizacije. Vseeno pa je moč najti nekaj vodil, ki so splošna in jih lahko priporočimo vsakomur.

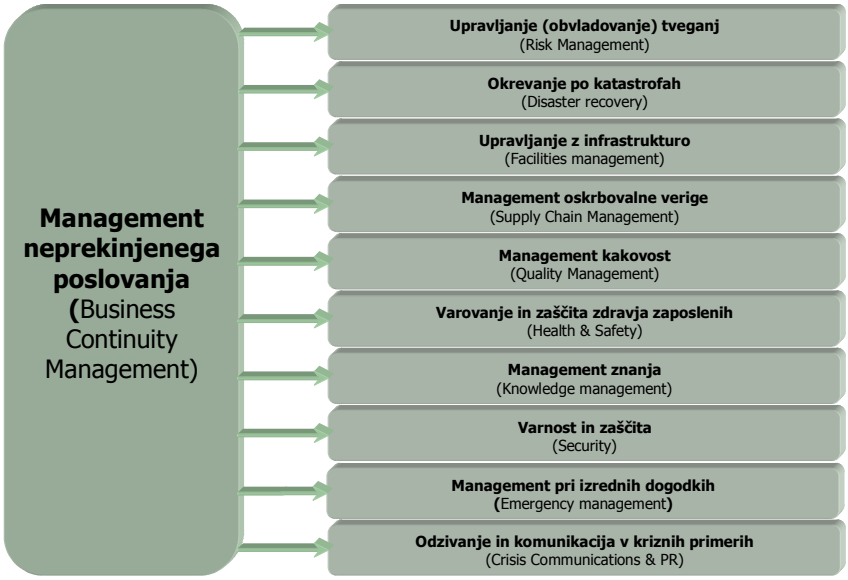
Najpomembneje se je zavedati, da se problemi, tudi tisti najhujši, dogajajo. Seveda ne gre vedno zgolj za sesutje poslovne stavbe ali uničenje take stavbe v požaru; lahko gre le za okvaro diska v pomembnem strežniku ali pa pušča streha in voda zalije računalniško opremo. Ne glede na stopnjo resnosti in obsežnosti težav je treba o vseh možnostih razmisliti, jih načrtovati, uvajati rešitve in – kar je najpomembnejše, a tudi najpogosteje zanemarjeno – rešitve neprestano preverjati v praksi in jih dopolnjevati (Šalehar, 2004). Osnovni pristop je pravzaprav dokaj enostaven: začeti je treba pri osnovah, kot so dobro fizično varovanje, varnostno kopiranje podatkov, dosledno izvajanje vsakdanjih postopkov upravljanja in nadzorovanja informacijskega sistema. Šele potem lahko začnemo razmišljati o pripravah na take dogodke, kot sta močan potres ali obsežen požar.

## 3.4 Management neprekinjenega poslovanja

Skozi razvoj neprekinjenega poslovanja se je vsebina tega pojma neprestano spreminjala. V prejšnjih poglavjih sem izpostavil razvoj od okrevanja po katastrofah (angl. Disaster Recovery) do načrtovanja neprekinjenega poslovanja. V zadnjem času pa se je o neprekinjenem poslovanju pričelo govoriti kot o procesu in ne zgolj načrtovanju. Govoriti se je začelo o managementu neprekinjenega poslovanja (angl. Business Continuity Management), ki vključuje tudi načrtovanje neprekinjenega poslovanja. Vzrok temu je dejstvo, da je načrtovanje neprekinjenega poslovanja zgolj proces, ki ima definiran začetek in konec, medtem ko je management neprekinjenega poslovanja dinamičen, proaktiven in

ciklični proces, ki mora nenehno zagotavljati nemoteno poslovanje vseh posameznih enot organizacije, tudi v primeru nepredvidenih dogodkov in katastrof večjih razsežnosti (Smith, 2003). Kljub vsemu je ob navedenem potrebno poudariti, da management neprekinjenega poslovanja ni le sopomenka za okrevanje po katastrofi. Management neprekinjenega poslovanja je več kot le okrevanje po katastrofi. Tu gre za nabor poslovno orientiranih procesov, ki združujejo širok nabor različnih managerskih disciplin (Lam, 2002, str.23). Prav v povezavi s tem se pojavlja ključni dejavnik neuspešnosti vzpostavitve celovitega zagotavljanja neprekinjenega poslovanja. Management neprekinjenega poslovanja je celostni postopek vodenja, ki identificira možne posledice, ki grozijo organizaciji, ter podaja okvir za vzpostavitev odpornosti in sposobnosti uspešnega odziva, ki varuje interese deležnikov, ugled, znamko ter aktivnosti, ki prinašajo vrednost (Smith, 2003, str 27-28). Managament neprekinjenega poslovanja je namenska poslovna in poslovodna dejavnost organizacije, ki združuje širok spekter poslovnih in upravljavskih disciplin, tako v javnem kot v zasebnem sektorju, vključno z upravljanjem krize, upravljanje tveganj in obnove tehnologije po nesreči. Management neprekinjenega poslovanja je dejavnost, ki je neposredno povezana z vodenjem organizacije in vzpostavlja temelj za dobro upravljanje (Gallagher, 2003, str. 28).

**Slika 2:** Management neprekinjenega poslovanja




*Vir: Smith, 2003, str. 28.*

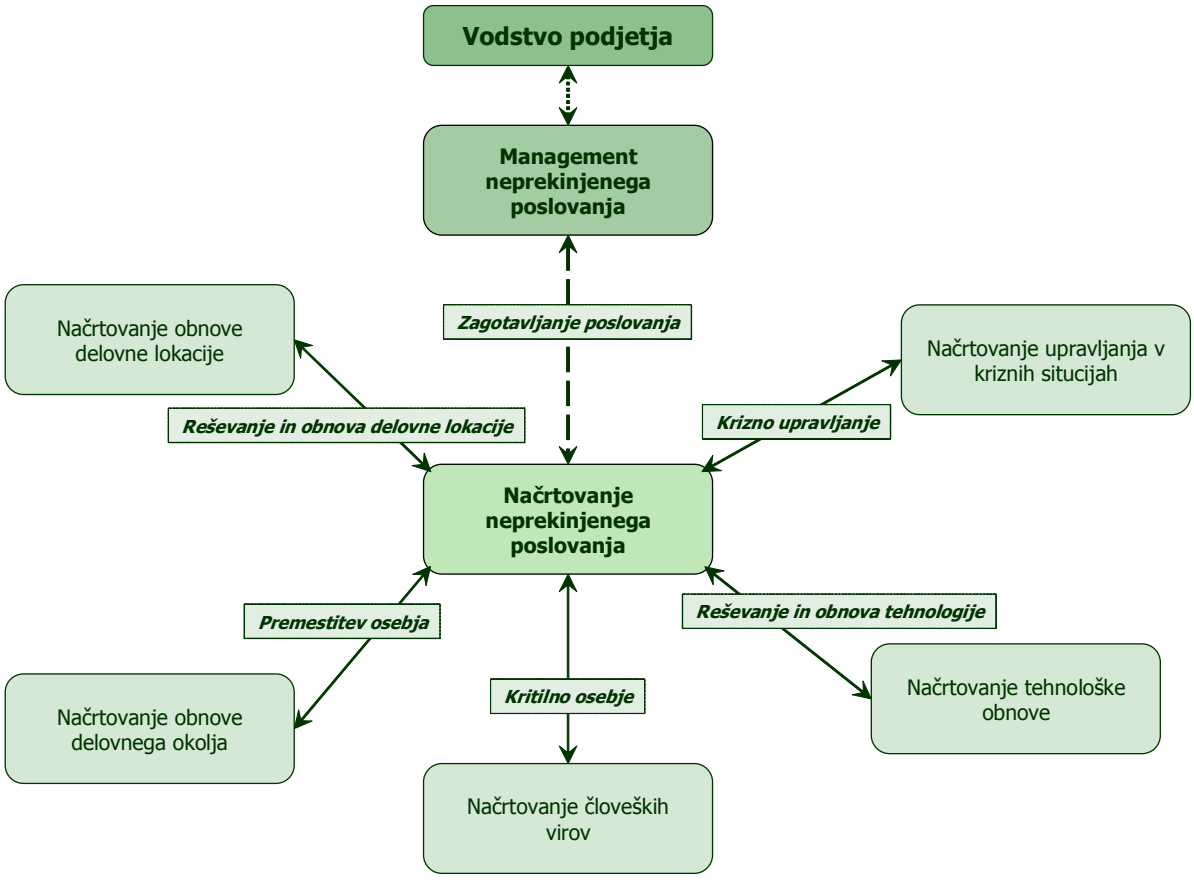
Za razvoj in vzdrževanje neprekinjenega poslovanja v organizaciji naj bi bil potreben upravni postopek, ki naj združuje elemente upravljanja neprekinjenega poslovanja, med katerimi so ključni predvsem:

- razumevanje nevarnosti, s katerimi se sooča organizacije z vidika verjetnosti in posledic;
- opredelitev ključnih poslovnih procesov in njihova razvrstitev po pomembnosti;
- razumevanje vpliva, ki ga imajo različne motnje na poslovanje, kjer je pomembno, da se poišče rešitve, ki bodo razrešile manjše incidente in resne incidente, kateri lahko ogrozijo obstoj organizacije;

- postavitev poslovnih ciljev, ki jih imajo zmogljivosti za obdelavo podatkov;
- pridobitev ustreznega zavarovanja, ki je lahko del procesa neprekinjenega poslovanja;
- oblikovanje in dokumentiranje strategije za neprekinjeno poslovanje, ki je v skladu z dogovorjenimi poslovnimi cilji;
- oblikovanje in dokumentiranje načrtov za neprekinjeno poslovanje, ki je v skladu z dogovorjenimi strategijami;
- redno preverjanje in dopolnjevanje sprejetih načrtov in postopkov;
- zagotovili, da je upravljanje neprekinjenega poslovanja postalo del postopkov in strukture organizacije.

Management neprekinjenega poslovanja tvori strateški in akcijski okvir za dejavno povečanje odpornosti podjetja za motnje, prekinitve ali izgube pri dobavi svojih izdelkov in storitev. To naj ne bi bil zgolj reakcijski ukrep. Management neprekinjenega poslovanja zahteva podrobno in natančno načrtovanje na različnih področjih organizacije (Publicly Available Specification 56, 2002, str. 26).

**Slika 3:** Odnosi znotraj managementa neprekinjenega poslovanja

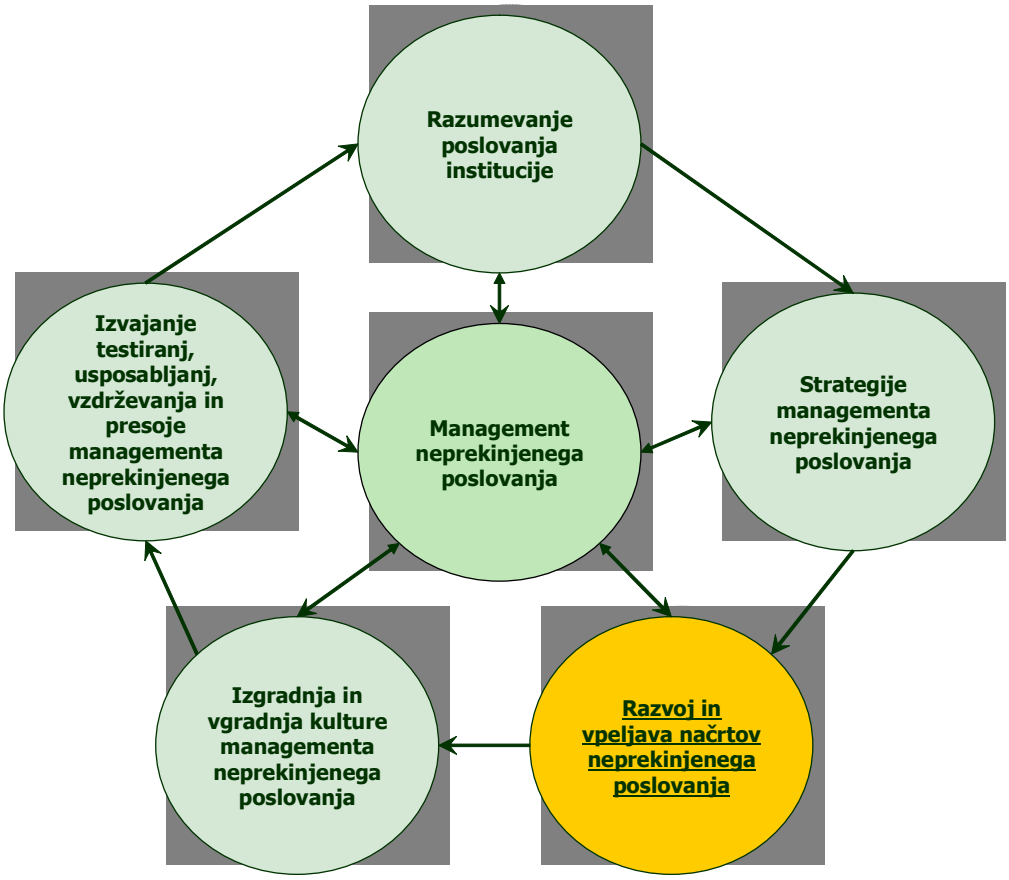



*Vir: Publicly Available Specification 56, 2002, str. 26.*

Pri vzpostavitvi managementa neprekinjenega poslovanje je potreben celovit pristop. Organizacije morajo pri vpeljavi managementa neprekinjenega poslovanja zagotoviti, da bo le-ta ustrezal poslovnemu okolju, poslovnim zahtevam in kritičnosti njihovih poslovnih dejavnosti ter bo tako odražal njihovo individualno kulturo in poslovno okolje.

Management neprekinjenega poslovanja lahko opredelimo s šestimi stopnjami življenjskega cikla in postopka managementa neprekinjenega poslovanja, kjer gre za neprekinjen ciklični proces.

**Slika 4:** Življenjski cikel managementa neprekinjenega poslovanja




*Vir: Smith, 2002, str. 46.*

### 3.4.1 Management neprekinjenega poslovanja

Organizacija potrebuje jasno začrtan in dokumentiran proces upravljanja neprekinjenega poslovanja, da lahko uspešno izmeri, nadzoruje, presoja in zagotavlja program le-tega neprekinjenega poslovanja. Vloge odgovornosti in pristojnosti morajo biti jasno opredeljene v okviru tega programa in znotraj organizacije.

Za podporo in management neprekinjenega poslovanja je potrebno pri tem vključiti številne strokovnjake z različnih področij (informacijska tehnologija, varovanje IT, varnost pri delu, krizni management, PR, fizična in požarna varnost, itd.). Količina potrebnih sredstev za investicije v management neprekinjenega poslovanja je odvisna od velikosti in raznolikosti organizacije.

Namen managamenta neprekinjenega poslovanja je zagotoviti trajno upravljanje, koordiniranje in vodenje kot zagotovilo, da se dejavnosti zagotavljanja neprekinjenega poslovanja izvajajo in vpeljujejo na dogovorjen način, ki omogoča dosego ciljev, zastavljenih v okviru zagotavljanja neprekinjenega poslovanja.

V fazi nastajanja programa managementa neprekinjenega poslovanja organizacije je pomembno oblikovati in načrtovati program tako, da se proces in struktura managementa v celoti vgradita v procese ter postopke organizacije. Ta proces mora vključevati zgodnjo določitev jasno opredeljenih in dokumentiranih vlog, odgovornosti in pristojnosti znotraj programa managementa neprekinjenega poslovanja, pri čemer mora biti usmerjen v naslednje dejavnike:

- da so vloge, odgovornosti in pristojnosti pravilno razumljene ter dodeljene pravim osebam na pravih položajih znotraj organizacije in imajo moč in avtoriteto za uresničitev in implementacijo ideje o zagotavljanju neprekinjenega poslovanja;
- da je postopek zagotavljanja neprekinjenega poslovanja usklajen v vsej instituciji;
- da celotni vrhovni in srednji management organizacije priznajo management neprekinjenega poslovanja kot poglavitno disciplino upravljanja, ki se izvaja, ker dodaja vrednost instituciji;
- da se management neprekinjenega poslovanja promovira, sporoča in razlaga ljudem, ki so vpleteni v ta proces tako, da so cilji in zahteve jasne, utemeljene ter da posamezniki poznajo svoje odgovornosti.

### 3.4.2 Razumevanje poslovanja organizacije

Organizacija, ki želi vzpostaviti celovit program managementa neprekinjenega poslovanja, si mora najprej postaviti pet ključnih vprašanj. Ta vprašanja so:

1. Kateri so ključni poslovni cilji organizacije?
2. Kateri proizvodi, storitve ali predmeti dobave so potrebni, da organizacija doseže te cilje?
3. Kdaj mora organizacija doseči poslovne cilje?
4. Kdo mora sodelovati (notranji in zunanji sodelavci), da se dosežejo poslovni cilji organizacije?
5. Kako namerava organizacija doseči zastavljene poslovne cilje?

Na podlagi odgovorov na ta vprašanja lahko nato določimo ključne strateške cilje, vrednote in dejavnosti organizacije ter omogočimo vzpostavitev kritičnih ciljnih poslovnih procesov in funkcij.

Prepoznavanje kritičnih poslovnih funkcij igra bistveno vlogo pri omogočanju, da management neprekinjenega poslovanja pripomore k doseganju poslovnih ciljev. Organizacija mora v okviru tega opredeliti tudi prepoznavanje pridruženih dejavnikov, tako notranjih kot zunanjih, ki podpirajo ali priskrbijo vhodne podatke tem kritičnim poslovnim procesom, obenem pa opredeli tudi posamezne odpovedne točke.

Obstajata dve sredstvi, s katerimi je mogoče to razumeti in tako opredeliti poslovne zahteve:

- Analiza tveganj, katere namen je prepoznati, opredeliti in vrednotiti tveganja, s katerimi se sooča organizacija v odnosu do njenih kritičnih poslovnih procesov z namenom, da se vzpostavi sprejemljiv nivo tveganja in načrt za obravnavo teh tveganj.

- Analiza vpliva na poslovanje, kjer je glavni namen prepoznati poslovne posledice (z vidika izgube, prekinitve ali motenj), če kritični poslovni procesi ne morejo nadaljevati z delom, in določiti časovni rok, v katerem je potrebno obnoviti kritične poslovne procese in njihove pridružene dejavnosti na določeno raven funkcionalnosti in delovanja.

Oba procesa sta natančneje opredeljena v nadaljevanju diplomske naloge v okviru poglavja, ki se dotika predvsem načrtovanja neprekinjenega poslovanja (Poglavji 5.1.1 Vzpostavitev projekta in 5.1.2 Analiza vpliva na poslovanje).

### 3.4.3 Definiranje strategij managementa neprekinjenega poslovanja

V kontekstu managementa neprekinjenega poslovanja zadeva strategija, določevanje in izbor alternativnih delovnih metod in lokacij, ki se jih uporabi po incidentu za vzdrževanje kritičnih poslovnih procesov organizacije, na sprejemljivo nizki ravni. Izkušnje in dobra praksa so že večkrat jasno pokazale, da zgodnja zagotovitev organizacijske strategije managementa neprekinjenega poslovanja zagotavlja, da so dejavnosti le-tega usklajene s strategijo organizacije in jo podpirajo. Pri tem je smiselno upoštevati oziroma uporabljati tri ravni strateškega načrtovanja managementa neprekinjenega poslovanja:

- Organizacijska (splošna) strategija, katere namen je nuditi jasno opredeljeno in dokumentirano politiko, okvir ter operativno usmeritev, ki zagotovi odpornost in neprekinjenost delovanja kritičnih poslovnih procesov organizacije. Organizacijska strategija naj v svojem okviru navaja specifična področja strategij na procesni ravni ter strategij za obnovo sredstev, da omogoči gladek prehod iz ene strategije na drugo in pripomore k razvoju teh strategij.
- Strategija na procesni ravni, ki je dokumentiran okvir, ki se osredotoči na odpornost in visoko zanesljivost kritičnih poslovnih procesov organizacije tako z organizacijske kot industrijske politike. V tem okviru je mogoče razviti strategijo managementa neprekinjenega poslovanja, sredstev za obnovo, načrtovanja neprekinjenega poslovanja in posledično zmožnost.
- Strategija za obnovo sredstev, katere namen je v okviru načrta neprekinjenega poslovanja priskrbeti vnaprej določeno raven sredstev, ki omogočajo vpeljavo organizacijske strategije in strategije na procesni ravni.

### 3.4.4 Razvoj in vpeljava načrtov neprekinjenega poslovanja

Razvoj načrtov neprekinjenega poslovanja ne pomeni zaključka procesa managementa neprekinjenega poslovanja, temveč predstavlja mejnik. Načrt ne predstavlja zmožnosti managementa, temveč je to pristop k vzpostavitvi uspešne zmožnosti.

Namen načrta neprekinjenega poslovanja je nuditi uspešen, ustrezen, vnaprej določen in dokumentiran okvir in proces za odzivanje na incidente, ki vplivajo na kritične poslovne procese organizacije. Vsebina in raven podrobnosti v vsakem sestavnem delu načrta neprekinjenega poslovanja sta odvisna od narave, obsega in kompleksnosti organizacije.

Sam proces razvoja in vpeljava načrtov neprekinjenega poslovanja je natančneje predstavljen v osrednjem delu diplomske naloge v nadaljevanju (Poglavje 5 Praktični pristop k vpeljavi neprekinjenega poslovanja in izkušnje).

### 3.4.5 Izgradnja in vgraditev kulture managementa neprekinjenega poslovanja

Management neprekinjenega poslovanja naj kot rezultat vgradnje njegove kulture postane sestavni del strateškega in vsakdanjega operativnega upravljanja. Ustvarjanje in vgrajevanje kulture managementa neprekinjenega poslovanja v instituciji je lahko dolgotrajen proces in se lahko sooča z različnimi odpori, ki se jih ne sme podcenjevati. Uspeh organizacije je na prvem mestu odvisen od:

- managementa neprekinjenega poslovanja kot sestavnega dela strateške in vsakdanje upravljalne etike organizacije;
- izobraževanja, zavedanja in sodelovanja kot elementa spremembe kulture;
- priprave in izvajanja programa za ustvarjanje korporacijske zavedanosti ter izboljšavo sposobnosti, znanja in izkušenj, potrebnih za vpeljevanje, vzdrževanje, upravljanje in izvajanje managementa neprekinjenega poslovanja;
- izjave o viziji in vidne dejavne podpore izvršnega, višjega ter srednjega vodstva organizacije;
- lastništva managementa neprekinjenega poslovanja, saj naj bodo lastniki različni deli organizacije - od koder izvira in kjer se nahaja operativno tveganje;
- zavezanosti k rednemu vzdrževanju in pregledovanju politike, strategij, okvirja, načrtov ter rešitev managementa neprekinjenega poslovanja organizacije;
- spoštovanja in priznavanja pomena, ki ga ima management neprekinjenega poslovanja za organizacijo, in vlog, ki jih imajo posamezniki v njegovem okviru;
- obveščanja deležnikov in tretje stranke, od katerih je odvisen.

Če organizacija sprejme te pristope, morajo imeti vsi, ki so povezani z organizacijo, zaupanje v njeno zmožnost upravljanja med incidenti, s čimer se bo začelo vgrajevanje uspešne kulture managementa neprekinjenega poslovanja.

### 3.4.6 Izvajanje testiranja, usposabljanj vzdrževanja in presoje managementa neprekinjenega poslovanja.

V preteklosti, se je izvedbi testiranj na področju informacijskih sistemov dajalo prevelik poudarek. Danes to velja za preozek pristop pri izvedbi in implementaciji managementa neprekinjenega poslovanja. Ključni elementi so ljudje in njihove sposobnosti, znanje, upravljanje ter sprejemanje odločitev. Potreba po ponavljanju vlog je sedaj v celoti priznana kot ključni element testiranja in usposabljanja organizacije.

Poleg testiranj in usposabljanj je eden ključnih elementov v okviru managementa neprekinjenega poslovanja tudi vzdrževanje. Večina organizacij obstaja v dinamičnem okolju in je podvržena spremembam osebja, procesov, dobaviteljev, trga, tveganj, okolja geografskih dejavnikov in poslovnih strategij. Za zagotovilo, da bo management neprekinjenega poslovanja še naprej odseval naravo, obseg in kompleksnost organizacije, ki

jo podpira, ga je potrebno aktivno vzdrževati. Namen vzdrževanja managementa neprekinjenega poslovanja je zagotoviti, da ostane organizacija sposobna in zmožna uspešno, primerno ter aktualno zagotavljali neprekinjeno poslovanje in izpolnjevanje poslovnih zahtev.

Proces presoje managementa neprekinjenega poslovanja igra ključno vlogo pri zagotavljanju, da so sposobnosti in zmožnosti slednjega robustne, uspešne in ustrezajo svojemu namenu. Namen presoje managementa neprekinjenega poslovanja je preiskati obstoječe sposobnosti in zmožnosti le-tega, preveriti združljivost z vnaprej določenimi standardi in kriteriji ter izdati poročilo o presoji, ki natančno poda ugotovitve, sklepe in priporočila. Presoja ima pet ključnih funkcij (Publicly Available Specification 56, 2002, str.67):

- neodvisno preveri združljivost s politikami, strategijami in okvirji managementa neprekinjenega poslovanja ter s smernicami dobre prakse ali s standardi, ki jih je sprejela organizacija;
- neodvisno pregleda rešitve managementa neprekinjenega poslovanja organizacije;
- neodvisno pregleda rešitve in potrdi načrt neprekinjenega poslovanja organizacije ter postopke za upravljanje kriznih situacij;
- neodvisno preveri in potrdi, da organizacija izvaja ključne programe testiranja, usposabljanja ter vzdrževanja v skladu s pomembnimi programi, procesi in okvirjem managementa neprekinjenega poslovanja organizacije;
- osvetli ključne pomembne pomanjkljivosti ter zagotovi njihovo odpravo.

# 4 NAČRTOVANJE NEPREKINJENEGA POSLOVANJA

## 4.1 Potreba po izdelavi načrta neprekinjenega poslovanja

Potreba po vzpostavljanju mehanizmov in infrastrukture, s katerimi bi zagotovil normalno delovanje po nepričakovanem uničujočem dogodku, v sprejemljivem času zahteva vnaprejšnje planiranje in pripravo, ki se odražata skozi izdelan načrt neprekinjenega poslovanja ter vzpostavljeno ustrezno infrastrukturo.

Organizacije se morajo zavedati posledic nepričakovanih zastojev informacijskega sistema, ki jih lahko povzročijo izredne okoliščine, kot so: naravne nesreče, požari, večji izpadi električne energije ali katastrofalne napake. Ena izmed temeljnih vlog pri zagotavljanju neprekinjenega poslovanja je zagotavljanje normalnega delovanja po nepričakovanem uničujočem dogodku v najkrajšem času. Podjetja namreč ne morejo delovati brez kritičnih sistemov (finančni sistem, varnostni mehanizmi, itd). Posledice morebitnih prekinitev v delovanju ključnih informacijskih sistemov imajo lahko znaten vpliv tako na delovanje podjetja samega kot na poslovne odnose in poslovanje z drugimi subjekti. Pri tem se morajo posamezna podjetja na področju ključnih informacijskih sistemov zavedati ključne vloge pri zagotavljanju varovanja in zaščite podatkov ter nemotenega delovanja.

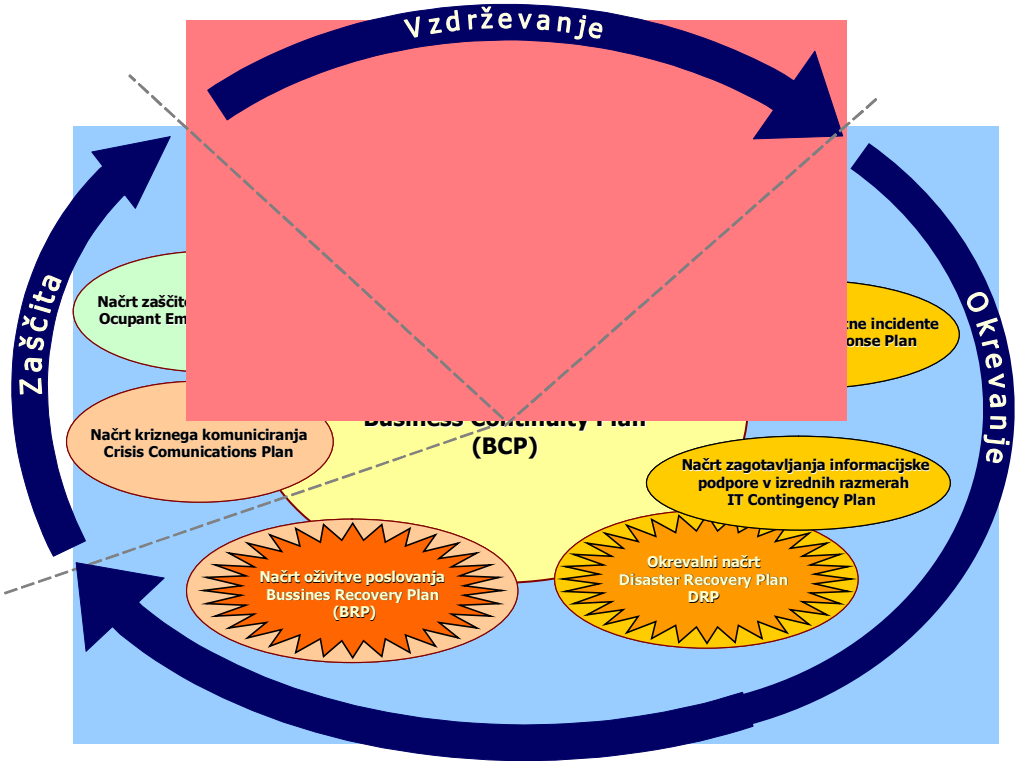
Zagotavljanje neprekinjenega poslovanja zahteva vso potrebno infrastrukturo, kadre in vzpostavljene logistične procese. Poleg tega to pomeni, da upravljamo s 30 do 50% višjimi zahtevami po razpoložljivih resursih. Ostrejše zahteve kot postavimo za sposobnost zagotavljanja neprekinjenega poslovanja oziroma čas okrevanja od uničujočega dogodka, več sredstev je potrebno vložiti.

## 4.2 Načrt neprekinjenega poslovanja

Standardna definicija Načrta neprekinjenega poslovanja ne obstaja. V literaturi s tega področja je mogoče najti različne opredelitve in povezave s sorodnimi pojmi. Načrt neprekinjenega poslovanja (angl. Business Continuity Plan) se osredotoča na vzpostavitev vitalnih poslovnih funkcij po morebitni prekinitvi poslovanja zaradi pojava nepredvidljivih dogodkov ter katastrof manjših in večjih razsežnosti. Lahko je prilagojen posameznemu poslovnemu procesu, lahko pa zadeva vse temeljne in vitalne poslovne procese. Usmerjen je v zagotavljanje neprekinjenega izvajanja poslovnih procesov (Šalehar, 2004). Informacijska tehnologija je v okviru načrta neprekinjenega poslovanja obravnavana kot podpora izvajanju poslovnih procesov. Pojem načrt neprekinjenega poslovanja pogosto srečamo v povezavi s pojmi:

- načrt zagotavljanja informacijske podpore v izrednih razmerah (IT Contingency Planning oz. Continuity of Support Plan);
- okrevalni načrt (Disaster Recovery Planning);
- načrt odziva na varnostne incidente (Cyber Incident Response Plan);
- načrt oživitve poslovanja (Business Recovery Plan);
- načrt komuniciranja v izrednih razmerah (Crisis Comunication Plan);
- načrt zaščite življenj in lastnine (Occupant Emergency Plan);
- načrt zagotavljanja strateške podpore v izrednih razmerah (Continuity of Operations Plan).

**Slika 5:** Povezava načrta neprekinjenega poslovanja z drugimi načrti



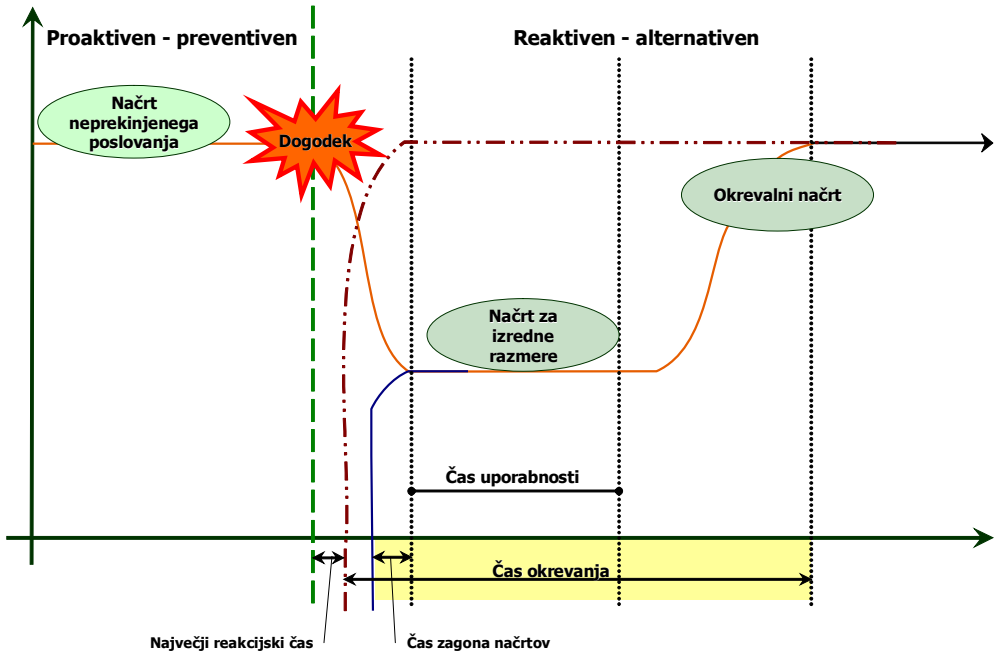

*Vir: Swanson, Wohl, 2002, str. 11*

### 4.2.1 Definicija načrta (načrtovanja) neprekinjenega poslovanja

Načrt neprekinjenega poslovanje je metodologija in praksa, ki organizacijam omogoča pripravo ter hitrejši odziv na spremembe v poslovnem okolju. Zajema procese razvijanja ukrepov in postopkov, ki omogočajo odgovor na uničujoči dogodek, zagotovijo nadaljnje delovanje poslovnih funkcij ter v določenem času ponovno vzpostavijo normalno delovanje (Barnes, 2003). Po drugi strani pa je vloga načrta neprekinjenega poslovanja predvsem preventivna, saj se običajno v okviru njegove priprave vzpostavi sisteme in sproži preventivne ukrepe, ki preprečujejo pojav prekinitve v poslovanju. Poleg tega preventivno vlogo načrtu postavlja že sam postopek planiranja, ki preko opredelitve tveganj povečuje zavedanje o nastopu možnih prekinitev in načrtovanje ukrepov za zmanjšanje verjetnosti nastopa le-teh. Vključuje razvoj in implementacijo postopkov, ki jih je po implementaciji potrebno neprestano vzdrževati in prilagajati. Z načrtom neprekinjenega poslovanja se določi postopke, ukrepe in delovanje storitev, ki jih nudi organizacija v času od začetka katastrofe do popolne vzpostavitve poslovanja, ko se okrevanje konča (Smith, 2003). Načrt neprekinjenega poslovanja vsebuje informacije o kontaktih v nujnih primerih, strategije za zmanjšanje škode, postopke, ki se morajo izvršiti, in komunikacijske procese, ki morajo biti izpolnjeni kot odgovor na uničujoč dogodek. Imeti prepoznavno strukturo, vključno z oceno tveganja uničujočega dogodka, ki zajema vse ključne poslovne aktivnosti, pokriva in dokumentira strategije za restavriranje celotnega področja poslovnih procesov, vključno z informacijsko tehnologijo, komunikacijami, poslovnimi informacijami, podporo uporabnikom, odnosi z javnostjo itd (MetaGroup, 2004, str. 13).

Načrt neprekinjenega poslovanja se osredotoča na vzpostavitev vitalnih poslovnih funkcij po morebitni prekinitvi poslovanja zaradi pojava nepredvidljivih dogodkov ter katastrof manjših in večjih razsežnosti. Lahko je prilagojen posameznemu poslovnemu procesu, lahko pa zadeva vse temeljne in vitalne poslovne procese. Usmerjen je v zagotavljanje neprekinjenega izvajanja poslovnih procesov. Informacijska tehnologija je v okviru načrta neprekinjenega poslovanja obravnavana kot podpora izvajanju poslovnih procesov. V kontekstu časovne razmejitve lahko načrt neprekinjenega poslovanja razumemo kot ločen načrt, ki mu sledita načrt za izredne razmere ter okrevalni načrt. V vsakem primeru pa bi morala biti načrt za izredne razmere in okrevalni načrt podrejena načrtu neprekinjenega poslovanja (Šalehar, 2004).

**Slika 6:** Časovna razmejitev načrta neprekinjenega poslovanja




*Vir: Težak, 2002, str. 15.*

Na podlagi zgornje slike lahko ugotovimo, da je načrt neprekinjenega poslovanja širok pojem in v prvi vrsti izhaja iz kriznega managementa. Ta ugotovitev sloni na dejstvu, da je krizni management najpomembnejši v trenutku, ko se pojavi nepričakovan dogodek, ki lahko prepreči ustaljen način poslovanja. Ustrezni način vodenja v kriznih trenutkih je tisti, ki lahko zagotovi, da bodo zaposleni, stranke, partnerji, investitorji in splošna javnost ohranili zaupanje v delovanje in nadaljnji obstoj prizadete organizacije. Načrt je oblikovan po principih kriznega menedžmenta in pokriva vse štiri kritične komponente, ki jih ponazarja spodnja tabela.

**Tabela 1:** Kritične komponente načrta neprekinjenega poslovanja

| | Okrevanje po nesreči | Okrevanje poslovanja | Nadaljevanje poslovanja | Obvladovanje tveganja |
|---|---|---|---|---|
| **Cilj** | Kritične aplikacije | Kritični poslovni procesi | Poslovno okolje | Zunanji dogodek |
| **Problem** | Izpad lokacije ali komponente | Izpad lokacije | Izpad aplikacije | Zunanji dogodek, ki vpliva na poslovanje |
| **Izdelek** | Načrt okrevanja po nesreči | Načrt okrevanja poslovanja | Načrt alternativnih načinov poslovanja | Analiza možnega tveganja za poslovanje |
| **Primer dogodka** | Potres; poškodba osrednje informacijske infrastrukture | Izpad napajanja za celotno lokacijo | Izpad aplikacije plačilnega prometa | Izpad pomembne dobave zaradi težav dobavitelja |
| **Primer možne rešitve** | Podvojena informacijska infrastruktura | Oddaljeni osrednji informacijski center | Ročna obdelava postopkov | Zaloga kritičnih surovin in/ali nadomestni dobavitelji |

*Vir: Claunch, 2004, str. 3*

### 4.2.2 Namen in cilji načrta neprekinjenega poslovanja

Namen načrta neprekinjenega poslovanja je ugotavljanje ter zmanjševanje nevarnosti za nemoteno poslovanje gospodarskih subjektov ter subjektov javnega sektorja ter hitra obnovitev pomembnih poslovnih procesov po nesrečah. Načrt neprekinjenega poslovanja mora zajemati celotno poslovanje družbe in ne le obnovitev informacijske podpore poslovanju (Andolšek, 2001). Hkrati s tem se v okviru načrta neprekinjenega poslovanja izvede tudi ocenitev tveganj in opis možnih izgub za družbo v primerih posameznih vrst nesreč, pri čemer je treba upoštevati območje, na katerih se izvajajo pomembne poslovne funkcije subjekta. Namen izdelave tega načrta je tudi opredelitev postopkov za kontrolirano obnovitev ključnih poslovnih funkcij po nesrečah.

Standard BS ISO/IEC 17799: 2000 določa, naj načrtovanje neprekinjenega poslovanja zajema ukrepe za ugotavljanje in zmanjševanje nevarnosti, omejuje posledice v primeru uresničitve grožnje in zagotavlja hitro vzpostavitev pomembnih dejavnosti

V načrtu neprekinjenega poslovanja je potrebno opredeliti ključne in bistvene poslovne funkcije, ki morajo biti zavarovane pred večjimi nesrečami in katastrofami. Stopnja pomembnosti poslovnih funkcij se določi na podlagi analize tveganj, ta pa obsega po prednosti razvrščene ključne sisteme v skladu s časovno občutljivostjo, pomembnostjo in nujnostjo potrebe po nadaljevanju poslovanja, ki sledi nesreči.

Hitra obnovitev ključnih poslovnih funkcij preprečuje, da bi imele prekinitve katastrofalne posledice za poslovanje. Zato družbe načrtujejo obnovo poslovnih funkcij po katastrofi na nadomestni lokaciji in kasneje vzpostavitev te funkcije na osnovni lokaciji. Načrt neprekinjenega poslovanja zajema med drugim načrte arhiviranja, načrte ukrepanja takoj po nesreči in načrte obnavljanja (načrt obnavljanja računalniških sistemov, načrt obnavljanja komunikacijske infrastrukture, uporabniški načrt obnavljanja). Namen načrtovanja obnove

po katastrofi ni obnova celotne organizacijske strukture, ampak le pokritje ključnih funkcionalnih zahtev, dokler kriza ne mine.

### 4.2.3 Okvir za načrtovanje neprekinjenega poslovanja

Potrebno bi bilo zagotoviti in vzdrževati enoten okvir načrtovanja neprekinjenega poslovanja v katerikoli instituciji, pa naj si gre za zasebni ali javni sektor. Tako lahko zagotovimo, da so vsi načrti med seboj usklajeni. V vsakem načrtu neprekinjenega poslovanja naj bi bili jasno določeni pogoji za njegovo delovanje kot tudi posamezniki, ki so odgovorni za izvajanje vseh delov načrta. Ko se opredelijo nove zahteve, bi bilo potrebno dodati ustaljene ukrepe za ravnanje v sili (na primer planiranje evakuacije ali drugi obstoječi rezervni ukrepi).

Okvirni načrt neprekinjenega poslovanja naj upošteva naslednje (BS 17799: 2000, 2001):

- pogoje za sprožitev načrta, ki določajo postopke, ki jih je potrebno izvesti pred sprožitvijo vsakega načrta;
- ukrepe v sili, kjer so opisana dejanja, ki jih je potrebno izvesti po nesreči, katere je ogrozila poslovne operacije in/ali človeška življenja. Sem spadajo tudi dogovori glede upravljanja stikov z javnostjo in učinkovite povezave z organi v primeru nesreče (policija, gasilci, krajevna oblast, civilna zaščita in drugi);
- rezervne postopke, kjer je opisano, kaj je potrebno storiti, da se ključne poslovne dejavnosti ali podporne storitve začasno preselijo v druge prostore, in se v zahtevanem času ponovno vzpostavijo poslovni procesi;
- obnovitvene postopke, kjer je opisano, kaj je potrebno storiti, da se ponovno začne normalno poslovati;
- urnik vzdrževanja, kjer je natančno določeno, kako in kdaj se izvaja preverjanje načrta in njegov postopek;
- ozaveščanje in izobraževanje, kjer so opredeljeni postopki na način, da omogoča razumevanje procesa neprekinjenega poslovanja ter zagotavlja, da bo ta proces še naprej učinkovito potekal;
- odgovornost posameznikov, kjer je določeno, kdo je odgovoren za izvajanje posameznih delov načrta. Po potrebi naj se imenuje tudi nadomestna oseba za prevzem odgovornosti;
- vsak načrt neprekinjenega poslovanja, naj bi imel točno določenega lastnika. Za ukrepe v sili, rezervne načrte in za obnovitvene načrte naj bi bil odgovoren lastnik ustreznih poslovnih virov ali vpletenih procesov.

### 4.2.4 Ključni dejavniki uspešnosti načrta neprekinjenega poslovanja

Ne glede na obliko in obseg načrta neprekinjenega poslovanja ter načrtovanih postopkov je zanimivo, da se njihova učinkovitost v različnih organizacijah lahko zelo razlikuje. Številni strokovnjaki so si različni pri določanju ključnih dejavnikov uspešnosti načrta neprekinjenega poslovanja. Gartner je v raziskavah prišel do naslednjih najpomembnejših kritičnih dejavnikov uspešnosti načrtov neprekinjenega poslovanja (Neil, 2001):

- Odnos višjega menedžmenta do problematike in njegova pripravljenost za vsestransko podporo izvajanja potrebnih ukrepov za zagotavljanje neprekinjenega poslovanja. Pomanjkanje interesa navadno privede do odtegovanja sredstev in ljudi s področja, kar privede do nepopolnih in zato tudi neučinkovitih rešitev.
- Preprostost načrta, saj je zaradi časovne stiske in drugih pritiskov pri definiranih postopkih možnost neuspeha pri zapletenih in obsežnih načrtih večja kakor pri preprostejših.
- Trajno vzdrževanje, ki izvira iz dejstva, da izvajanje ukrepov zagotavljanja neprekinjenega poslovanja ni enkratna naloga, pač pa mora postati stalnica pri oblikovanju informacijskega sistema pa tudi pri načrtovanju razvoja na drugih področjih delovanja organizacije.
- Načrtovanje neprekinjenega poslovanja mora biti stalna naloga osebe ali posebne skupine, ki nosi odgovornost za vzdrževanje ukrepov in ima za to tudi vsa potrebna pooblastila.
- V načrtu neprekinjenega poslovanja morajo biti različne aplikacije smiselno razdeljene glede na njihovo kritičnost za delovanje organizacije. Kategorizacijo kritičnosti je treba stalno spremljati in jo prilagajati spremembam v poslovanju.

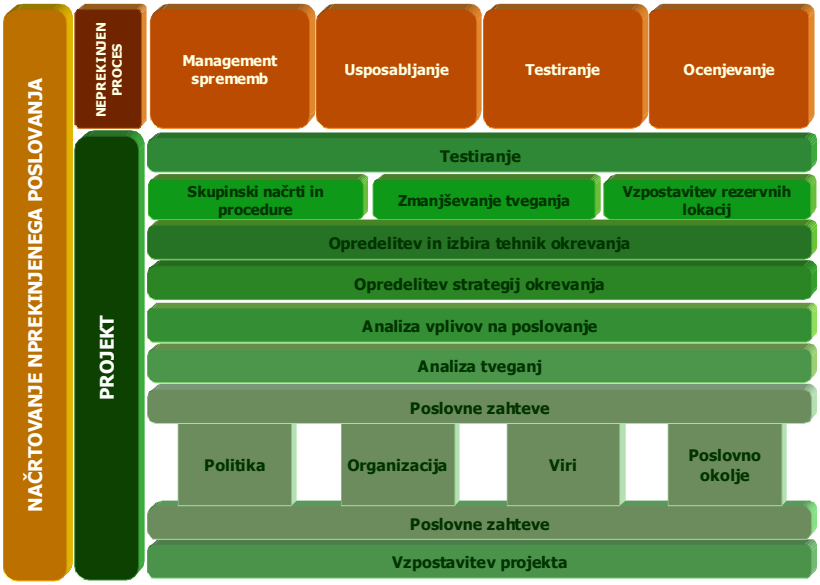
# 5 PRAKTIČNI PRISTOP K VPELJAVI NEPREKINJENEGA POSLOVANJA IN IZKUŠNJE

Postopki zagotavljanja neprekinjenega poslovanja se odražajo v postopkih zagotavljanja neprekinjene informacijske podpore gospodarskih in negospodarskih subjektov, pri čemer morajo biti zapisani v formalni ter strukturirani obliki. Načrt neprekinjenega poslovanja mora vključevati postopke, ki bodo preprečevali prekinitve poslovanja, postopke za izredne razmere v času prekinitev, postopke okrevanja in vzpostavljanja normalnega poslovanja gospodarske družbe oziroma organizacije javnega sektorja po prekinitvi ter postopke usklajevanja projektov razvoja novih informacijskih sistemov z izdelanim načrtom. Iz načrta morajo biti jasno razvidne vloge, odgovornosti, naloge ter nosilci vlog. Nosilci vlog, ki so zadolženi za izvajanje postopkov, morajo biti v postopku izdelave načrta ustrezno usposobljeni za izvajanje postopkov. V času izdelave načrta je potrebno vzpostaviti vso potrebno infrastrukturo, ki bo omogočala izvedbo postopkov in s tem doseganje postavljenih ciljev, doseganja določene stopnje razpoložljivosti, varnosti in zaupnosti. Pri izdelavi načrta je potrebno upoštevati namembnost posameznih načrtov in vsebino posameznih dokumentov glede na potrebe ter stadij izvedbe načrta. Načrt vsebinsko pokriva tri različna časovna obdobja: čas pred nesrečo, med nesrečo in po nesreči. V času pred nesrečo se osredotočimo predvsem na obstoječe stanje, ranljivosti, ki obstajajo, ter načine, s katerimi zmanjšamo tveganja do najmanjše možne mere. V času med nesrečo je glavni cilj zagotavljati neprekinjeno poslovanje in vplive uničujočih dogodkov s ustrezno zaščito in vpeljavo postopkov zmanjšati na najmanjšo možno škodo, ki jo uničujoči dogodki lahko povzročijo. Po nesreči se ukvarjamo predvsem z obnovo sistema in vzpostavitvijo le-tega v prvotno stanje. Pri preverjanju celovitosti nam lahko pomaga miselni diagram, kateri

opozarja na ključne elemente, ki jih moramo upoštevati pri pripravi in izvedbi načrta neprekinjenega poslovanja.

Proces načrtovanja neprekinjenega poslovanja je pravzaprav razdeljen v dva ločena dela, kjer gre pri prvem za projekt razvoja načrta neprekinjenega poslovanja. Drugi del je neprekinjen proces, ki ga je potrebno neprestano izvajati, kjer eno pomembnejših vlog igra management sprememb (angl. Change Management), katerega naloga je neprestano spremljanje poslovanje organizacije in spreminjanje okolja, v katerem se organizacija nahaja. Posledično vse to pomeni spreminjanje poslovnih zahtev organizacije, kar kasneje rezultira v določenih spremembah z vidika tveganj, vplivov na poslovanje in tako na sam načrt neprekinjenega poslovanja. Strukturo načrtovanja neprekinjenega poslovanja prikazuje spodnja slika.

**Slika 7:** Struktura načrtovanja neprekinjenega poslovanja




*Vir: Claunch; 2004, str. 5*

## 5.1 Praktični pristop k načrtovanju neprekinjenega poslovanja

Načrt je potrebno redno letno testirati in ga usklajevati z novimi zahtevami ter na novo zaznanimi tveganji. V grobem si koraki izdelave načrta sledijo v naslednjem vrstnem redu:

- vzpostavitev projekta,
- izdelava analize vpliva poslovanja,
- opredelitev preventivnih in korektivnih ukrepov na podlagi analize tveganja,
- izdelava načrta neprekinjenega poslovanja,
- testiranje načrta neprekinjenega poslovanja in usposabljanje,
- skrbništvo in vzdrževanje načrta neprekinjenega poslovanja,

### 5.1.1 Vzpostavitev projekta

Pri vzpostavitvi projekta načrtovanja neprekinjenega poslovanja se je potrebno najprej seznaniti z okoljem organizacije, v kateri pripravljamo načrt neprekinjenega poslovanja. To omogoča projektni skupini:

- izpopolnjevanje namena projekta in programa dela;
- razvoj časovnega okvira projekta in
- identificiranje vseh dejavnikov, ki vplivajo na predajo rezultatov projekta in končni uspeh projekta.

Vse uvodne aktivnosti v okviru vzpostavitve projekta so temelj za nadaljnje aktivnosti, ki so povezane predvsem z zbiranjem podatkov in poslovnih zahtev in izdelavo analize tveganj, saj vse to predstavlja temelj vzpostavitve projekta

Pridobitev podpore vodstva

Poglavitni problem v zvezi z načrtovanjem ukrepov za nemoteno poslovanje ob razdejanjih in katastrofah s stališča najvišjega vodstva v posameznih organizacijah, bodisi zasebnega oziroma javnega sektorja, je v tem, da so vsa sredstva vložena v to, pravzaprav mrtva sredstva. Investirati je namreč treba v prostore, informacijsko infrastrukturo, komunikacijske povezave, ljudi, potem pa vse to samo čaka, da se bo kaj zgodilo. Razumljivo je, da je to za vsako organizacijo znaten strošek, v katerega je najvišji management navadno precej težko prepričati. Zato je velik del energije in časa pri pripravi načrtov neprekinjenega poslovanja informacijske podpore največkrat treba vložiti prav v prepričevanje vodstva, zakaj so vsi ti ukrepi potrebni in kako pomagajo pri zaščiti poslovanja. Eden od načinov, ki po zagotavljanju tistih, ki so se s tem že srečali, daje dobre rezultat, je primerjava z običajnim zavarovanjem stavb in opreme, saj gre tu v resnici za isti koncept. Podobno kakor pri zavarovanju plačamo zgolj za to, da nam bodo povrnili škodo, če bi se zgodilo kaj nepredvidenega, si namreč tudi s pripravo načrtov in ukrepov za neprekinjeno delovanje informacijskega sistema krijemo hrbet ob morebitnih večjih katastrofah.

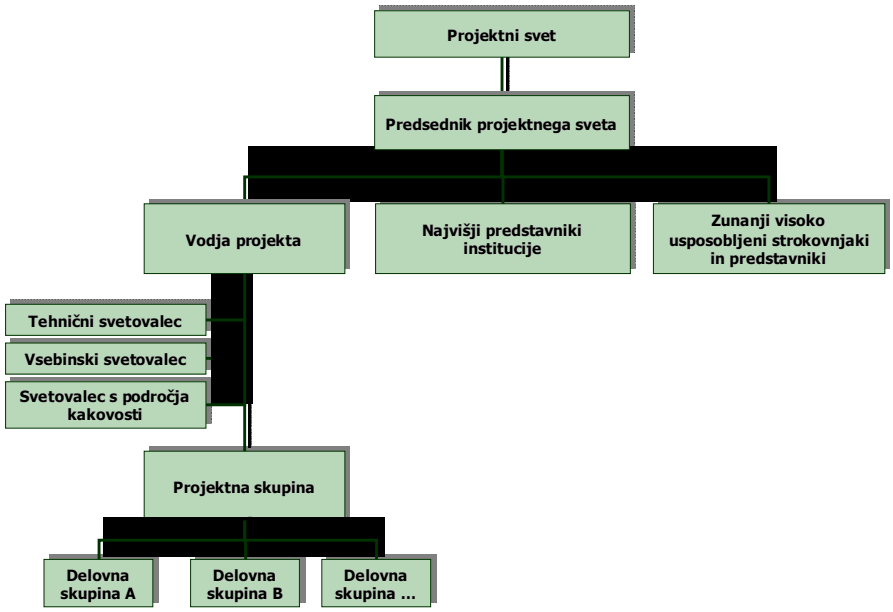
Vgraditev pravil projektnega managemnta

V okviru te faze se oblikuje projektni svet, ki je v celoti odgovoren za dodeljevanje navodil in smernic članom projektne skupine. Projektni svet sprejema tudi vse odločitve, ki vodijo do končnega uspeha načrtovanega okrevanja, in imenuje projektno skupino. Vodja projekta, v sodelovanju s projektnim svetom, opredeli podroben načrt dela in načrt intervjujev, ki so potrebni za izdelavo analize vpliva poslovanja organizacije. Ključne in pomembnejše aktivnosti, ki se izvajajo v okviru te faze, so predvsem:

- potrditev investicijske in projektne dokumentacije projekta;
- imenovanje članov projektnega sveta in projektne skupine;
- vzpostavitveni sestanek projektne skupine;
- opredelitev podrobnega načrta dela;

- opredelitev načrta intervjujev, ki so potrebni za izdelavo analize vpliva poslovanja organizacije;
- izdelava politike, ki podpira programe okrevanja;
- izdelava programa za usposabljanje zaposlenih, ki bodo sodelovali pri projektu;
- objava politike neprekinjenega poslovanja;
- izdelava programa usposabljanja članov projektne skupine;
- vzpostavitev sistema obvladovanja projekta in projektne dokumentacije.

**Slika 8:** Organizacijske strukture za projekt izdelave načrta neprekinjenega poslovanja




*(Vir: Interna gradiva proučevane institucije)*

Zbiranje podatkov

Pred samim začetkom zbiranja podatkov je treba identificirati najpomembnejše stranke, ki so zainteresirane, da organizacija posluje v okviru pričakovanj (Malik, 2001):

- poslovni partnerji, ki želijo nemoteno poslovati z organizacijo;
- zaposleni, ki jih zanima njihova usoda v zvezi z zaposlitvijo in varnostjo v organizaciji in
- investitorji, ki potrebujejo zagotovila, da so njihove investicije v organizaciji varne.

Nekateri avtorji (Noakes-Fry, Diamond, 2003) k tem trem dodajajo še zakonodajalce, ki terjajo, da je zakonskim zahtevam, ne glede na okoliščine, zadoščeno, in zavarovalnice, ki pričakujejo, da se vodi ustrezna skrb za zavarovane entitete.

Zbiranje podatkov o poslovanju, informacijski podpori in varnostni situaciji v organizaciji ter podatki o grožnjah, ki pretijo delovanju informacijskega sistema, je pravzaprav temelj celotnemu načrtovanju neprekinjenega poslovanja, kajti tako lahko pridemo do osnovnega poznavanja organizacije, v kateri načrtujemo neprekinjeno poslovanje. Količina in obseg podatkov, ki jih je treba zbrati, je odvisna predvsem od obsega, ki ga želi organizacija zajeti s programom uvajanja pogojev za nadaljevanje poslovanja.

Zbrane informacije se uporabljajo za analiziranje tveganj in ugotavljanje stroškov, povezanih s prekinitvijo posameznih poslovnih funkcij. Večino potrebnih podatkov je mogoče pridobiti v organizaciji sami, in sicer od pristojnih oddelkov ali služb. Podatke o poslovnih procesih je najbolje zbrati v posameznih oddelkih organizacije z uporabo vprašalnikov in z osebnimi pogovori. Ključne kategorije podatkov, ki jih je potrebno v tej fazi zbrati, so (Rihar, 2003, str. 11):

- podatki o poslovnih procesih v organizaciji (pomen posameznih poslovnih procesov, medsebojna odvisnost poslovnih procesov, odvisnost od zunanjih partnerjev);
- zakonske in pogodbene zahteve (zakonodaja, pogodbe z zunanjimi partnerji);
- podatki o informacijski podpori poslovnim procesom (aplikacije, podatki, strojna oprema, povezave z okoljem, zunanji ponudniki informacijskih storitev);
- podatki o infrastrukturi (zgradbe, telekomunikacijske povezave, energetska oskrba, prometne povezave);
- podatki o zaposlenih (ključne osebe, možnost dostopa do različnih lokacij);
- varnostni podatki (varnostni elementi infrastrukture, zaščita informacijskega sistema, varnostni standardi v organizaciji);
- podatki o nevarnostih (zunanje nevarnosti, notranje nevarnosti).

Pri tem je potrebno zagotoviti jasen opis podatkov in zapisov poslovnih funkcij za potrebe in zahteve arhiviranja. Na tej osnovi je potrebno oceniti zunanji vpliv stroškov in izgub v primeru izpada informacijskega sistema, v primeru katastrofe oziroma drugih nepredvidenih dogodkov. Poleg tega je potrebno izvesti ocene stopnje pomembnosti poslovnih funkcij in povezanih tehnologij ter obenem ugotoviti odvisnosti med posameznimi funkcijami in drugimi sredstvi. Podobno velja za organizacijske enote, kjer morajo vodje le teh opisati postopke oziroma procese za izvajanje poslovnih funkcij v svojih organizacijskih enotah, ki morajo biti med seboj usklajeni. Vse v tej fazi pridobljene informacije so osnova za:

- ocenjevanje možnih izgub;
- upravičevanje stroškov, povezanih s preprečevanjem katastrof;
- ugotavljanje podatkov, ki jih je treba arhivirati;
- oblikovanje strategij za obnovo poslovnih funkcij.

Analiza tveganj

Analiza tveganja (angl. Risk Analysis) pomeni prvo in najpomembnejšo fazo pri uvajanju pogojev za zagotavljanje delovanja poslovnega informacijskega sistema organizacije in s tem njenega poslovanja. Namen te faze je razumeti nevarnosti, katerim je delovanje informacijskega sistema in s tem poslovanje organizacije izpostavljeno, saj je le tako mogoče izbrati najbolj ustrezno metodo zagotavljanja poslovanja in pridobiti za to nalogo ustrezno podporo vodstva organizacije (Federal Financial Institutions Examination Council, 2003, str. 12). Cilj analize tveganja je poiskati povezave med poslovanjem organizacije in njegovo izpostavljenostjo različnim tveganjem, ki mu pretijo.

Proces analize tveganj zagotavlja temelje celotnemu procesu načrtovanja neprekinjenega poslovanja. Pri vsakem varovanju in zaščiti podatkov se moramo zavedati, kaj varujemo, pred čim in zakaj. Pri načrtovanju neprekinjenega poslovanja se pogosto zanemarja faza analize, saj je to na prvi pogled odvečno dodatno delo, ki nas časovno in predmetno oddaljuje od samega rezultata – načrta za neprekinjeno poslovanje. Vendar pa nam ravno kakovostna ter pravilna analiza stanja lahko omogoči prihranek in učinkovit izkoristek časa (Barnes, 2001, str.57-59).

Pri izdelavi analize tveganj so zaradi različnega obsega opazovanja in različnih poudarkov razlike med metodologijami precejšnje. Tako različni avtorji, katerih delo obsega identifikacije in izvedbe analize tveganj, različno identificirajo splošne dejavnosti, procese in aktivnosti, ki jih je potrebno izvajati v okviru te faze. Med deli in prispevki različnih avtorjev, ki sem jih pregledal, sem se pri pripravi tega izdelka oprl predvsem na delitev, ki jo predvideva Levitt (1997), ki to fazo imenuje upravljanje tveganja in jo opredeljuje s štirimi koraki, ki pravzaprav vsebujejo celoten koncept zagotavljanja poslovanja:

- identifikacija groženj;
- ugotavljanje verjetnosti pojavljanja nepredvidenih dogodkov in njihovega vpliva na poslovanje;
- zmanjševanje tveganja;
- vzpostavitev pogojev za nadaljnje poslovanje.

Pri tem lahko trdimo, da je prvi korak izredno pomemben za nadaljevanje analize, saj s tem, identificiramo nevarnosti, ki lahko kadarkoli in nepričakovano ogrozijo poslovanje organizacije, oziroma predstavljajo grožnje oziroma potencialne vire prekinitve poslovanja oziroma izpad informacijske podpore poslovnim procesom. Na tej osnovi pa lahko ugotovimo in ocenimo verjetnost pojavljanja teh nepredvidenih dogodkov. To pa je podlaga za pripravo učinkovitih mehanizmov in ukrepov za čim učinkovitejše zmanjšanje negativnih vplivov v primeru nepredvidenih dogodkov in katastrof, ter obenem zmanjševanje tveganja pojava nevarnosti oziroma grožnje.

Kljub precejšnjim razlikam v podrobnostih si je večina avtorjev enotnih glede pomena, ki ga ima ta faza v procesu zagotavljanja delovanja poslovnega informacijskega sistema. Izsledki te faze najpomembneje vplivajo na način in obseg reševanja te problematike v organizaciji, ne glede na to, ali je višji management, zaradi zakonskih obveznosti ali drugih razlogov, že sprejel načelno odločitev o izvedbi programa uvajanja rešitev, ali pa je morebitni sprejem take odločitve odvisen od izsledkov te analize (Rihar, 2003, str. 10). V drugem primeru imajo prav ugotovitve analize tveganja ključni vpliv za doseganje podpore v vodstvu organizacije in s tem na odločitev o uvajanju pogojev za zagotavljanje poslovanja. Zato mora biti ta faza izvedena izjemno skrbno in racionalno, a brez nepotrebnega pretiravanja.

Nevarnosti, ki pretijo delovanju informacijskega sistema in poslovanju organizacije, so zelo različne, tako po načinu nastanka kot po obsegu in verjetnosti pojavljanja. Seznam potencialnih nevarnosti je odvisen od države in lokacije (ali lokacij), na kateri se organizacija nahaja, od vrste dejavnosti in načina organiziranosti, zato ni mogoče uporabljati splošnega, temveč si mora vsaka organizacija sestaviti svoj posebni seznam

nevarnosti in groženj. Nevarnosti je mogoče razdeliti tudi glede na izvor, to je na notranje in zunanje. Taka razdelitev je nekoliko preglednejša, saj je preprečevanje nevarnosti v vsakem primeru različno, poleg tega so notranje nevarnosti navadno precej bolj specifične za posamezno organizacijo kakor zunanje.

**Slika 9:** Tveganja in nevarnosti, katerim so izpostavljene organizacije


*Vir: Breunhoelder, 2002*

Vendar pa nepričakovani dogodki niso edini vzrok za izpad informacijske podpore. Zelo pomemben in večkrat prezrt razlog za izpad so tudi zaustavitve zaradi rednega vzdrževanja, obnavljanja, razširitve ali prenove strojnega oziroma programskega dela informacijskega sistema. Čedalje večji del tovrstnih posegov je sicer mogoče opraviti na delujočem sistemu, vendar se prav vsem zaustavitvam nikoli ne bo mogoče izogniti. Ker vzdrževalni posegi navadno povzročijo relativno dolge izpade, ki lahko trajajo tudi 24 ur ali dlje, je treba v analizi tveganja upoštevati tudi te, čeprav so ti izpadi načrtovani in jih v tem pogledu ni mogoče opredeliti kot dejavnike tveganja. Na obseg tovrstnih posegov vpliva izbira tehnološke platforme in strukture informacijskega sistema, kar je treba upoštevati že pri načrtovanju njegovega razvoja ali prenove. Poleg tega pa je treba pri uvajanju pogojev za zagotavljanje delovanja informacijskega sistema iskati take rešitve, ki bodo uspešno nadomestile informacijsko podporo tudi ob načrtovanih izpadih.

### 5.1.2 Analiza vpliva na poslovanje

Analiza vpliva na poslovanje (angl. Business Impact Analysis) skupaj z analizo tveganja predstavlja ključni korak v procesu načrtovanja neprekinjenega poslovanja. Pri analizi tveganj gre tako za ocenjevanje obstoječe fizične in okoljske varnosti ter nadzora, kakor tudi oceno njihove primernosti glede na potencialna tveganja v organizaciji. Analiza vpliva na poslovanje pa vključuje identifikacijo ključnih poslovnih funkcij v organizaciji ter opredelitev vpliva izpada teh funkcij, ki presega najvišji spremenljivi čas izpada (Swanson, Wohl, 2002).

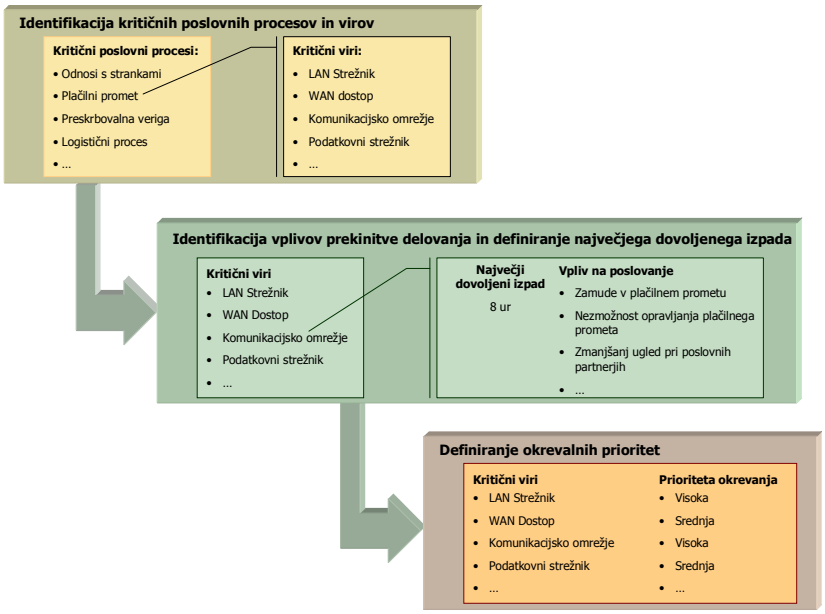
Smisel analize vpliva na poslovanje je predvsem v tem, da se evidentirajo in ocenijo vse ali vsaj večina posledic izpada posameznega poslovnega procesa. Ker gre za oceno, pri analizi nima smisla pretiravati z natančnostjo merjenja stroškov, saj bi bilo to predrago in bi trajalo predlogo časa, poleg tega pa vseh posledic niti ni mogoče natančno cenovno ovrednotiti in je zato marsikdaj treba upoštevati tudi vrednostne ocene. Analiza mora biti dovolj pregledna, preprosta in razumljiva, da jo je mogoče pozneje brez težav dopolnjevati s poslovnimi, organizacijskimi ali tehničnimi spremembami, ki nastanejo v organizaciji. V nekaterih primerih je dobro pripraviti tudi preprost pregled izsledkov analize vpliva na poslovanje, kar je mogoče izvesti na več načinov, pri čemer je pomembno predvsem to, da je pregled preprost, a dovolj popoln, da daje višjemu managementu podlago za sprejemanje odločitev o uvajanju pogojev za zagotavljanje delovanja poslovnega informacijskega sistema. Analiza vplivov na poslovanje omogoča projektni skupini, ki se ukvarja z načrtovanjem neprekinjenega poslovanja, da v celoti podrobno opiše vse sistemske zahteve in procese, ki jih predvideva informacijska podpora poslovanja. Poleg vsega navedenega je namen analize tudi izpostaviti soodvisnost specifičnih sistemskih komponent s kritičnimi poslovnimi procesi, ter na tej osnovi določiti posledice prekinitve delovanja informacijske podpore poslovanju (Barnes, 2001, str. 67).

Na podlagi analize se za posamezne dele informacijskega sistema določita ciljna točka restavriranja podatkov (Recovery Point Objective - RPO) in ciljni čas vzpostavitve delovanja (Recovery Time Objective - RTO). Ciljni čas vzpostavitve delovanja sistema je najdaljše trajanje izpada sistema, ki ga organizacija še lahko dopusti, ne da bi resneje ogrozila svoje poslovanje. Ciljna točka restavriranja podatkov je najbolj oddaljena točka v preteklosti, do katere je še dopustno restavrirati podatke, tako da ponazarja največjo količino podatkov, ki jih organizacija še lahko izgubi brez resnejših posledic. Oba cilja pomenita temeljno merilo za izbiro vrste in obsega ukrepov, ki jih je treba uvesti za zagotavljanje delovanja poslovnega informacijskega sistema organizacije.

Določitev vitalnih poslovnih procesov, aplikacij in podatkovnih virov

Analiza vpliva na poslovanje predvideva, da je posamezne poslovne procese zaradi lažje analize smotrno razvrstiti po stopnji njihove kritičnosti na več skupin. Tako se razdelijo tudi njihove podporne aplikacije, s tem pa tudi poslovni informacijski sistem na več delov, ki zahtevajo različno obravnavo glede na zahtevano stopnjo zagotavljanja delovanja.

**Slika 10:** Primer postopka določitve kritičnih poslovnih procesov za BIA




*Vir: Swanson, Wohl, str. 16*

Razvrstitev je uporabna tudi za določanje potrebnega dogovora o ravni storitev v primeru, da je poslovni proces deloma ali v celoti prepuščen zunanjemu izvajalcu. V spodnji tabeli (Tabela 2) so prikazane štiri kategorije, kot jih je opredelil Gartner, z zelo natančno določenimi pripadajočimi potrebnimi ravnmi storitev in primeri poslovnih procesov, ki sodijo v posamezno kategorijo.

**Tabela 2:** Razvrstitev poslovnih procesov po kritičnosti

| Kategorija | Primer poslovnih procesov | Potrebna raven storitve |
|---|---|---|
| **1.** | Odnosi s strankami / poslovnimi partnerji<br>Procesi, kritični za pridobivanje dohodka | • Delovanje 24x7<br>• 99,9% razpoložljivost (sprejemljivi izpadi < 45 min/mesec)<br>• RTO < 2 uri; RPO = 0 |
| **2.** | Manj kritični procesi za pridobivanje dohodka,<br>Preskrbovalna veriga | • Delovanje 24x7<br>• 99,5% razpoložljivost (sprejemljivi izpadi < 3,5 ure/mesec)<br>• RTO 8-12 ur; RPO 4 ure |
| **3.** | Organizacijsko pisarniško poslovanje | • Delovanje 18x7<br>• 99% razpoložljivost (sprejemljivi izpadi < 5,5 ure/mesec<br>• RTO 3 dni, RPO 1 dan |
| **4.** | Oddelčni procesi | • Delovanje 24x6<br>• 98% razpoložljivost (sprejemljivi izpadi < 13,5 ure/mesec)<br>• RTO 5 dni; RPO 1 dan |

*Vir: Claunch, 2004, str. 2*

Poslovne funkcije lahko razvrstimo glede na časovno občutljivost in glede na potrebnost za nadaljevanje poslovanja. Na tej osnovi lahko uporabimo razdelitev, ki temelji na razvrščanju elementov poslovnega informacijskega sistema in podpira navedene poslovne funkcije (Toigo, 2000, str. 46-48):

- Kritične poslovne funkcije; to so tiste, katerih prekinitev lahko organizaciji povzroči nepopravljive posledice že v zelo kratkem času. Takih procesov organizacija ne more izvajati, če nima na razpolago popolnih nadomestnih zmogljivosti.
- Vitalne poslovne funkcije; to so tiste, katerih prekinitev lahko organizacija za krajši čas, na primer 48 ur, dopusti pod pogojem, da se potem v popolnosti obnovijo. Teh funkcij ni mogoče izvajati na alternativen način, ali pa je to mogoče le zelo kratek čas in z velikimi stroški. Če v dveh do petih dneh podpora teh funkcij ni v celoti vzpostavljena, ima njihova prekinitev za organizacijo podobne posledice, kakršne veljajo za kritične procese.
- Občutljive poslovne funkcije; to so tiste funkcije, ki jih je mogoče dlje časa ob sprejemljivih stroških izvajati tudi na alternativen način, vendar pa je treba po prehodu na normalno poslovanje podatke in postopke v celoti restavrirati.
- Nekritične poslovne funkcije; to so tiste, ki jih lahko organizacija brez posebne škode pogreši tudi dlje časa in ne zahtevajo restavriranja ali pa je to relativno poceni.

Določitev stroškov povzročene škode zaradi prekinitve delovanja

Stroški ki nastanejo zaradi prekinitve delovanja so različni. Tu mislim predvsem na dve delitvi stroškov. Prva delitve stroškov je glede na ročnost:

- Kratkoročni stroški, ki nastanejo takoj ob prekinitvi delovanja informacijske podpore in jih je relativno lahko oceniti.
- Dolgoročni stroški, ki nastanejo kot sekundarna posledica prekinitve (stroški povrnitve ugleda pri kupcih in poslovnih partnerjih, stroški izgube vrednosti blagovne znamke itd.) in se navadno pojavijo šele ob daljši prekinitvi.

Druga delitev nastalih stroškov je glede na vpliv na poslovanje organizacije. Ta delitev predvideva:

- Neposredne stroške, ki jih je mogoče tako kot kratkoročne relativno natančno oceniti s finančnimi kazalci. Ti stroški lahko naraščajo sorazmerno s trajanjem prekinitve, pogosto pa je njihova rast tudi skokovita ali celo eksponentna.
- Posredne stroške, ki so dokaj težko merljivi in včasih tudi manj pomembni. Pri institucijah javnega sektorja predvsem državne uprave ti stroški lahko izhajajo iz prekinitve katerega od ključnih poslovnih procesov. Posledica je padec ravni podpore občanov, s tem pa tudi padec njihove pravne in druge varnosti (varnost osebnih podatkov in podobno), kar pa je lahko težko merljiva kategorija. Poleg tega so posredni stroški prekinitve delovanja na ravni državne uprave lahko kritični za delovanje in obstoj države (primer so policija, vojska, carina in druge institucije).

### 5.1.3 Tehnike okrevanja

Ključne aktivnosti v okviru definiranja tehnik okrevanja so:

- opredelitev strategije neprekinjenega poslovanja;

- opredelitev preventivnih in korektivnih ukrepov;
- določitev postopkov izdelave varnostnih kopij;
- določitev postopkov restavriranja iz varnostnih kopij in
- vzpostavitev rezervne lokacije;

Strategija neprekinjenega poslovanja

Na podlagi analize tveganja in analize vpliva na poslovanje oblikujemo ustrezno strategijo neprekinjenega poslovanja. Strategija neprekinjenega poslovanja vključuje vse elemente v povezavi z izvedbo neprekinjenega poslovanja (način izvedbe – npr. najem lokacije, kakšne vrste partnerstva se bo sklenilo, za kakšne vrste rezervno lokacijo bo šlo - hladno, vročo ali razžarjeno, opredeli se tudi katere nivoje katastrof se bo obvladovalo). To pa pomeni, da načrt neprekinjenega poslovanja vsebuje skupek strategij, ki pokrivajo različna področja:

- Preventiva; osrednji namen preventivnih ukrepov in aktivnosti je minimiziranje pojava nepredvidljivih dogodkov oziroma minimiziranje škode v primeru le-teh.
- Odzivanje na nepredvidene dogodke in katastrofe; osrednji namen je definiranje postopkov odzivanja v primeru izrednih dogodkov. To v prvi vrsti predvideva zaustavitev nevarnosti in širjenja tveganj ter škode, obenem pa je potrebno oceniti škodo, ki je nastala ob nepredvidenem dogodku. O vsem tem je potrebno vzpostaviti učinkovite komunikacijske kanale, ki bodo omogočali poročanje vsem pristojnim organom in širši javnosti o posledicah katastrofe.
- Ponovna vzpostavitev poslovanja; v tej strategiji je potrebno opredeliti postopke čim hitrejše vzpostavitve delovanja kritičnih poslovnih procesov.
- Okrevanje po katastrofi; v okviru te strategije je potrebno opredeliti postopke okrevanja manj kritičnih poslovnih procesov. Poleg vseh potrebnih dejavnikov, morajo ti postopki vključevati tudi možnost selitve in okrevanja na rezervni lokaciji
- Obnova poslovanja; strategija obnove poslovanja predvideva predvsem postopke vzpostavitve normalnega poslovanja organizacije na primarni lokaciji. Rezultat je ponovno vzpostavljeno celotno poslovanje in delovanje organizacije.

Opredelitev preventivnih ukrepov

Preventivno delovanje zajema zelo širok spekter dejavnosti, ki jih v večjem ali manjšem obsegu za zaščito svojih informacijskih sistemov izvajajo vse organizacije. Preventivna dejavnost je pomembna predvsem zato, ker je preprečevanje izrednih dogodkov cenejše, kakor odpravljanje njihovih posledic. Prav zato je treba v postopku uvajanja pogojev za zagotavljanje delovanja informacijskega sistema evidentirati vse preventivne dejavnosti, ki jih organizacija že izvaja, ovrednotiti njihov učinek in v skladu z ugotovitvami analize tveganja po potrebi predlagati njihovo spremembo ali dopolnitev.

- pri definiranju preventivnih ukrepov v okviru preventivnih dejavnosti je potrebno izhajat iz tistih, ki so skupni vsem IT sistemom, kjer le-ti predstavljajo osnovo za pripravo nabora vseh potrebnih preventivnih ukrepov:

- dovolj pogosta izdelava varnostnih kopij in shranjevanje podatkov, aplikacij in operacijskih sistemov na varnih alternativnih mestih, ki jih izredni dogodki ne morejo doseči;
- redundanca kritičnih sistemskih komponent ali zmožnosti;
- dokumentacija sistemske konfiguracije in zahtev;
- interoperabilnost med sistemskimi komponentami ter med primarno in alternativno opremo in
- primerno velik in ustrezno konfiguriran sistem menedžmenta in nadzora okolja;

V okvir preventivne dejavnosti organizacije v širšem pomenu seveda sodijo prav vse dejavnosti, ki so namenjene uvajanju pogojev za zagotavljanje neprekinjenega delovanja informacijskega sistema. S stališča zaščite informacijskega sistema organizacije lahko tako opredeljene preventivne dejavnosti razdelimo v dva sklopa (Rihar, 2003, str. 26):

- Preventivne dejavnosti, ki so namenjene fizični zaščiti kritičnih infrastruktur, kot so: objekti, prostori, napeljave ali naprave. Obseg in vrsto teh preventivnih dejavnosti v organizaciji največkrat določajo zakonske obveznosti ali splošna varnostna politika organizacije, odvisne pa so tudi od okoliščin, v katerih organizacija deluje. Fizična zaščita je pomemben varnostni preventivni element za zagotavljanje delovanja informacijskega sistema in jo je v tem pomenu treba upoštevati pri izdelavi analize tveganja.
- Drugi sklop preventivnih dejavnosti je vezan neposredno na informacijski sistem organizacije in ga tvorijo postopki, ki so namenjeni njegovi logični zaščiti pred vdori. Ta del preventivnih dejavnosti je odvisen predvsem od varnostne politike in kulture organizacije ter postaja z vedno tesnejšim informacijskim povezovanjem organizacij z okolico vse pomembnejši. Logično zaščito sestavljajo vse dejavnosti, ki so namenjene zaščiti informacijskega in telekomunikacijskega sistema organizacije pred nepooblaščenimi dostopi ter računalniškimi vdori. Za zaščito informacijskega sistema pred nepooblaščenimi dostopi sta pomembna predvsem dva varnostna elementa in sicer: nadzor vstopa v sistem in varovanje komunikacijskih poti, po katerih potujejo podatki.

Potrebne preventivne ukrepe med drugim omogoča analiza tveganj, v okviru katere se identificira vsa tveganja, ki vplivajo na delovanje informacijske podpore in samo poslovanje organizacije. Vzpostavljeni preventivni ukrepi povečajo sposobnost zagotavljanja neprekinjene informacijske podpore storitvam organizacije. Na tej osnovi je potrebno v prvi fazi določiti ključne aktivnosti, ki se bodo izvajale v okviru definiranja potrebnih preventivnih ukrepov:

- izdelava metodologije popisa postopkov neprekinjenega poslovanja;
- izdelava seznama preventivnih ukrepov;
- opredelitev povezav med preventivnimi ukrepi in tveganji z oceno zmanjšanja tveganj;
- opis preventivnih postopkov ter sistemov in opreme, vključno s postopki njihove uporabe in vzdrževanja;

- opredelitev vlog in odgovornosti;

Navedene aktivnosti nakazujejo smernice, katerih se je potrebno držati pri opredelitvi preventivnih ukrepov.

Eden izmed rezultatov aktivnosti preventivne dejavnosti je definiran nabor preventivnih ukrepov, ki omogočajo minimiziranje verjetnosti pojava nepredvidenega dogodka oziroma minimizirajo vplive in škodo v primeru prekinitve delovanja. Preventivne ukrepe je mogoče ločiti na preventivne postopke ter preventivne sisteme in opremo.

1. Preventivni postopki vključujejo:
   - postopke vzdrževanja strojne in programske opreme,
   - postopke vzdrževanja infrastrukturne opreme,
   - postopke varovanja fizičnega dostopa do sistema,
   - postopke preverjanja zaposlenih in zunanjih izvajalcev,
   - postopke zgodnjega odkrivanja nastopa naravnih nesreč, ki utegnejo vplivati na poslovanje,
   - postopke sklepanja dogovorov z dobavitelji o posebnih pogojih dobave itd.
2. Preventivni sistemi in oprema za zagotavljanje neprekinjenega poslovanja obravnavane organizacije vključujejo:
   - UPS,
   - generatorje električne energije,
   - klimatske naprave, protipožarne sisteme,
   - sisteme zaznavanja vdora vode,
   - opremo za zaščito strojne opreme pred vdorom vode,
   - protipožarne in vodoodporne omarice za hrambo elektronskim medijev in dokumentacije,
   - sistem za izredno ustavitev sistema,
   - arhiv na rezervni lokaciji,
   - rezervno lokacijo (hladna, topla, vroča, mobilna in razžarjena lokacija),
   - sisteme izdelave varnostnih kopij,
   - podvojene kapacitete itd.

Med preventivne ukrepe spadajo tudi redno izdelovanje varnostnih kopij, ki predstavljajo osnovni pripomoček za izvedbo okrevanja po katastrofi. Ko definiramo postopke za obnovo storitev, hkrati opredelimo tudi vso potrebno infrastrukturo. Nadalje je potrebno določiti samo še katere so zahteve glede rezervne lokacije, kar predstavlja osnovo za investicijsko dokumentacijo in načrt nabav.

Vse opredeljene preventivne postopke ter sisteme in opremo za preprečevanja prekinitev poslovanja organizacije je potrebno dokumentirati. Zaposleni in zunanji izvajalci morajo biti z njimi seznanjeni in usposobljeni za njihovo uporabo. Zaradi enotnega zajema podatkov je potrebno predhodno opredeliti metodologijo popisa preventivnih ukrepov in vseh ostalih postopkov neprekinjenega poslovanja. Le-ti morajo biti enotno popisani in vključeni v

izdelani načrt neprekinjenega poslovanja. Metodologijo je smiselno opredeliti v enem koraku v začetni fazi izdelave načrta neprekinjenega poslovanja (Toigo, 2000, str. 75).

Pomembna prvina preventivnega delovanja je tudi skrb za delavce, ki so tako ali drugače povezani z delovanjem informacijskega sistema, kamor sodijo izobraževanje, varnostno osveščanje in nadzor zaposlenih. Izobraževanje zaposlenih je zelo pomembno zaradi hitrih tehnoloških sprememb na informacijskem in telekomunikacijskem področju, in to tudi tedaj, ko je oskrbovanje informacijskega sistema prepuščeno zunanji organizaciji. Varnostno osveščanje in nadzor pa pripomoreta k spoštovanju in ustreznem uresničevanju sprejetih varnostnih standardov v organizaciji. Pogosto se namreč dogaja, da je razkorak med sprejeto in dejansko uresničevano varnostno politiko dokaj velik.

Opredelitev postopkov usklajevanja projektov razvoja informacijskih sistemov z načrtom neprekinjenega poslovanja organizacije

Organizacija mora v fazi načrtovanja razvoja informacijskih sistemov, ki gostujejo oziroma bodo gostovali na infrastrukturi organizacije, sodelovati z razvijalci in lastniki sistema. Pred razvojem in implementacijo sistema morajo organizacija in razvijalci ter lastniki sistema doseči dogovor o tehnoloških in varnostnih vidikih informacijskega sistema. Novi sistemi in popravki obstoječih sistemov nikakor ne smejo ogrožati varnosti poslovanja organizacije. Po drugi strani pa mora organizacija izpolnjevati zahteve po neprekinjenem poslovanju, ki jih postavljajo uporabniki storitev oziroma lastniki gostujočih informacijskih sistemov. Spremenjenim in poostrenim zahtevam se mora prilagajati tudi načrt neprekinjenega poslovanja. V ta namen je potrebno opredeliti postopke usklajevanja projektov razvoja informacijskih sistemov z izdelanim načrtom neprekinjenega poslovanja.

Določitev okrevalnih postopkov

Pomembna sestavina načrta neprekinjenega poslovanja je opredelitev vseh postopkov izdelave varnostnih kopij ter postopkov obnovitve poslovanja in okrevanja iz varnostnih kopij. Pri opredeljevanju okrevalnih postopkov je potrebno zajeti vse postopke za izvajanje ključnih poslovnih funkcij ob nastanku nesreče ali katastrofe na osnovni ali nadomestni lokaciji. Pri manjši nesreči (delna odpoved informacijskega sistema) se postopki obnavljanja nanašajo na vzpostavitev tega sistema na osnovni lokaciji. Pri katastrofi (na primer potresu, poplavi, požaru) je treba poslovanje ključnih in bistvenih poslovnih funkcij prenesti na nadomestno lokacijo. Za primere, ko v nobeni obliki ni možno vzpostaviti delovanja informacijskega sistema, je potrebno predvideti in opredeliti vse ročne postopke (Andolšek, 2001). Te opredelitve morajo vsebovati podrobne postopke za vzpostavitev prvotnega stanja IT sistema ali sistemskih komponent. Okrevalni postopki morajo biti dokumentirani, korak za korakom v obliki kontrolnega seznama postopkov. V izogib težavam ali zmedi v izrednih situacijah ne sme biti prezrt ali zanemarjen nobeden izmed korakov v okrevalnem postopku. Kontrolni seznam se uporablja za dokumentiranje zaporednih okrevalnih postopkov ter za iskanje in odstranjevanje težav, ki nastanejo kot posledica nepravilnega okrevanja sistema.

V okviru opredelitve okrevalnih postopkov je potrebno opredeliti:

- postopek notranjega in zunanjega obveščanja poslovnih partnerjev, ki so kakorkoli povezani s sistemom;
- postopek oskrbe z nujnimi delovnimi sredstvi;
- postopek nabave nadomestne opreme;
- postopek pridobivanja in nameščanja nujnih komponent strojne opreme;
- postopek vzpostavitve kritičnih operacijskih sistemov in programske opreme;
- postopek vzpostavitve sistemskih podatkov;
- postopek testiranja sistemskih funkcionalnosti, vključno z varnostno kontrolo;
- postopek povezave sistema na omrežje ali drugi zunanji sistem;

Osrednji in najpomembnejši del okrevalnih postopkov je, ne glede na izbiro metodologije, namenjen obravnavi postopkov ponovne vzpostavitve delovanja informacijskega sistema organizacije. Pri tem je treba nameniti pozornost trem glavnim elementom sistema: podatkovni infrastrukturi, računalniški infrastrukturi in telekomunikacijski infrastrukturi (Federal Financial Institutions Examination Council, 2003, str. E-1 do E-8).

### *Podatki*

Obstaja mnogo različnih načinov varovanja podatkov. Ti so odvisni od velikosti organizacije, količine podatkov, tehnološke platforme informacijskega sistema, splošne varnostne politike v organizaciji ipd. Na splošno pa se različne metode varovanja podatkov med sabo razlikujejo v treh temeljnih karakteristikah, in sicer: glede na vrsto nevarnosti, pred katerimi ščitijo podatke, na obseg varovanih podatkov in na hitrost obnovitve varovanih podatkov.

1. Hranjenje na redundantnih tipih podatkovnih nosilcev, ki je namenjeno predvsem zaščiti pred strojnimi okvarami posameznega diskovnega pogona, ne more zagotoviti varovanja podatkov ob okvari ali uničenju celotnega diskovnega sistema. Nekoliko boljšo zaščito zato daje redno kopiranje podatkov na trakove ali drug diskovni sistem ter vodenje dnevnika sprememb na operativnih podatkih. Poglavitni namen rednega kopiranja je predvsem možnost hitrega restavriranja podatkov ob okvari podatkovnega nosilca, na katerem se podatki nahajajo, zato morajo biti kopije in dnevniki blizu ter hitro na razpolago.
2. Kopiranje na trakove in odvažanje trakov na varno lokacijo, ki je najstarejša in najcenejša tehnika, ki se še vedno najpogosteje uporablja. Ažurnost podatkov je odvisna od pogostnosti kopiranja in odvažanja trakov, ki se odvija v najboljšem primeru enkrat na dan, navadno pa še redkeje. Dobra stran tega načina je nizka cena, slabi strani pa sta predvsem možnost napak zaradi ročnega posredovanja in dolgotrajno restavriranje podatkov. Zaradi hitre rasti količine podatkov se v organizacijah, ki poslujejo v režimu 24*7, lahko pojavita tudi problema določanja točke konsistentnosti in pomanjkanja časa za kopiranje podatkov.
3. Kopiranje na oddaljeni tračni sistem, ki dražji od prejšnjega, saj zahteva vzdrževanje dveh tračnih sistemov, oddaljene lokacije in telekomunikacijske povezave med njima. Zagotavlja pa precej večjo ažurnost podatkov, saj je mogoče kopirati podatke

pogosteje, lahko se kopirajo dnevniki sprememb in delajo inkrementalne kopije, poleg tega je zaradi avtomatizacije postopka možnost napak bistveno manjša. Še vedno pa ostaja problem dolgotrajnega restavriranja podatkov s trakov.

4. Kopiranje podatkov na oddaljeni diskovni sistem je najdražji način kopiranja podatkov. Terja vzdrževanje dveh diskovnih sistemov in precej zmogljivo medsebojno povezavo. Podatki se lahko kopirajo sinhrono – spreminjajo se sočasno na obeh diskovnih sistemih, ali asinhrono – podatki na oddaljenem diskovnem sistemu se spreminjajo z zamudo, ki navadno traja od nekaj sekund do nekaj minut. Ker se podatki na oddaljeni lokaciji nahajajo v izvorni obliki, so po potrebi lahko takoj na razpolago in jih ni treba posebej restavrirati.

*Strojna in programska oprema*

Restavriranje strojne opreme pomeni ponovno vzpostavitev procesorskih zmogljivosti, s katerimi je mogoče izvajati operacije, ki zagotavljajo informacijsko podporo delovanju poslovnega sistema. Obstaja mnogo načinov vzpostavitve nadomestnih procesorskih zmogljivosti, ki se med sabo tehnološko in finančno lahko zelo razlikujejo, zato je prav izbira načina restavriranja strojne opreme najpomembnejša odločitev, ki jo je treba sprejeti pri uvajanju rešitev za zagotovitev poslovanja. Od te izbire je v marsičem odvisna tudi izbira tehnologije restavriranja podatkov in telekomunikacijskih povezav. Najprej se je namreč treba odločiti o tem, kateri so tisti ključni poslovni procesi, ki jim je treba zagotoviti informacijsko podporo. Odgovor na to vprašanje izhaja predvsem iz ugotovitev analize vpliva na poslovanje. V tej fazi pa je treba ugotoviti, katere so tiste procesorske zmogljivosti, ki zagotavljajo informacijsko podporo najbolj kritičnim poslovnim procesom.

To je mogoče v tehničnem pogledu narediti na več načinov, bodisi z vzpostavitvijo redundantnih strojnih zmogljivosti bodisi z alternativnimi rešitvami, vendar delujejo z drugačno konfiguracijo strojne opreme. V vsakem primeru pa je treba vzpostaviti tako imenovano minimalno sprejemljivo strojno konfiguracijo, ki je sposobna zagotavljati informacijsko podporo najnujnejšim poslovnim procesom. V nadaljevanju so navedene glavne značilnosti, prednosti in slabosti petih različnih metod, ki jih uporabljajo organizacije za restavriranje centralnega računalniškega sistema (Federal Financial Institutions Examination Council, 2003, str. E-1 – E-8; Swanson, Wohl, 2002, str. 51-61; Barnes 2003, str. 93-96).

1. Mrzla/ hladna rezervna lokacija; ponuja le okolje z napajanjem, urejenimi podi in osnovnimi instalacijami ter morda zahteva tedne za vzpostavitev poslovanja. Hladna lokacija nima nobene opreme, pripravljena jo je le sprejeti za vzpostavitev delovanja. Je sicer najcenejša možnost med rezervnimi lokacijami, zahteva pa največ časa za postavitev okolja, v katerem organizacija lahko začne delovati po katastrofi.
2. Topla rezervna lokacija; te so delno urejene z nekaj osnovne računalniške opreme, ki ni razpoložljiva v trenutku. Računalniška oprema na tej lokaciji ni podvojena, kajti opremljanje s podvojeno opremo je zelo drago, tako da s toplo lokacijo posedujemo le lokacijo in določen del osnovne informacijske ter komunikacijske infrastrukture, ki ni razpoložljiva v trenutku. Topla lokacija ponuja predvsem razpoložljivost za

daljše obdobje (ni za nekajurno nadomestitev) in je navadno v izključni uporabi ene organizacije. Posebno je primerna takrat, ko organizacija uporablja neobičajne sisteme, ker jih lahko v primeru nesreče prenese na toplo lokacijo. Letnega testiranja, ki je mogoče pri vroči lokaciji, navadno ni mogoče doseči in tako organizacija ne more biti povsem prepričana v čas vzpostavitve delovanja na topli rezervni lokaciji. Podatki pridejo v tak center prek varnostnih kopij. Zagon take lokacije traja kar nekaj časa, saj je treba zagnati sisteme, naložiti podatke ter po potrebi tudi ustrezno konfigurirati računalnike in programe.

3. Vroča rezervna lokacija; je rezervna lokacija, ki je popolnoma opremljena in pripravljena za delovanje v zelo kratkem času, na primer v nekaj urah. Vsa aparaturna in sistemska programska oprema mora biti v celoti kompatibilna s podatki na rezervni kopiji, saj tem zagotovimo sinhroniziranost obeh okolij, omogoča takojšen prevzem delovanja s strani rezervnega centra To možnost uporabljajo organizacije, ki morajo delovati z najmanjšimi možnimi izpadi. Organizacija ima izključne pravice do vroče lokacije in jo tudi edina uporablja. Vroča lokacija lahko pokriva dolgoročne ali kratkoročne izpade normalnega poslovanja. Najmanj enkrat letno jo je potrebno preizkušati, če zadovoljuje vse potrebe. To je najdražja možnost dislociranih rezervnih lokacij, ki lahko povzroča težave, če organizacija uporablja neobičajne sisteme ali naprave.
4. Razžarjena rezervna lokacija; lokacija, na kateri ne samo, da so računalniki stalno pripravljeni za prevzem obdelav in so podatki na obeh lokacijah sinhronizirani, temveč poleg tega rezervna lokacija tudi neprestano nadzoruje primarno in brž, ko opazi, da je njeno delovanje ogroženo, prevzame njeno vlogo. To je edina res odporna rešitev, proti težavam, saj sama poskrbi za nemoten prenos nalog. Pravzaprav v teh primerih največkrat ni dejanske podrejenosti ene lokacije drugi, temveč sta obe enakovredni in služita druga drugi kot rezerva. S posebnimi tehnikami se zagotavlja, da ne pride do neregularnih položajev, v katerih bi se funkcije prenesle napačno. Za zdaj zaradi zelo visokih stroškov tak način uporabljajo le tiste organizacije, ki se ukvarjajo s poslovnimi področji, kjer praktično ne sme priti do izpada, kot so: avtorizacije kreditnih kartic in bančništvo. Vendar pa se v zadnjem času zaradi padanja cen strojne opreme in telekomunikacijskih povezav za take rešitve odloča čedalje več organizacij tudi z drugih področij.

Navedene možnosti vzpostavitve rezervne lokacije so tem dražje, čim bolj zapletene so, kar pa je spet odvisno od zahtevane razpoložljivosti ter obsega razpoložljivih finančnih sredstev. Za katero rešitev se bo organizacija odločila, je odvisno predvsem od tega, koliko časa si lahko privošči biti brez ustrezne informacijske podpore, pa tudi od tega, katera tveganja želi s tako rešitvijo pokrivati. Pogosto se podjetja, da bi znižala stroške, odločajo za medsebojno zagotavljanje zmogljivosti. Pogoj za tako rešitev je, da imajo vsi pogodbeni partnerji združljivo strojno in programsko opremo, saj se v nasprotnem primeru taka rešitev precej zaplete. Podjetja, ki si ponujajo tako pomoč, morajo imeti dovolj presežnih zmogljivosti, da lahko gostijo dve okolji.

Pri izbiri oddaljene lokacije je treba izhajati iz dveh izhodišč. Prvo izhodišče so splošna priporočila, ki se nanašajo na varnostne in druge značilnosti, katerim morajo ustrezati izbrana mikrolokacija ter prostori za namestitev centra, na primer potresna ogroženost, infrastrukturna opremljenost ipd. Drugo izhodišče pa sestavljajo značilnosti sekundarne lokacije v razmerju do glavne lokacije, kot sta na primer medsebojna oddaljenost ali infrastrukturna soodvisnost. Vsa splošna priporočila je seveda treba upoštevati v okviru ugotovitev analize tveganja, kjer so opredeljene povsem specifične in konkretne okoliščine ter nevarnosti, ki lahko vplivajo na delovanje informacijskega sistema posamezne organizacije (Calvert, 2001).

Pri izbiri najprimernejše metode restavriranja strojne opreme mora organizacija izhajati iz ugotovitev analiz tveganja in poslovanja. Ker pa poslovanje postaja čedalje bolj odvisno od informacijske podpore in si organizacije ne morejo več privoščiti dolgotrajnega izpada ali celo tveganja, da sistema ne bodo mogle ponovno vzpostaviti, se čedalje več organizacij odloča za prehod na eno od zadnjih dveh metod restavriranja strojne opreme. Dodatno spodbudo za ta prehod pomenijo tudi v zadnjih letih vztrajno padajoče cene strojne opreme in telekomunikacijskih povezav, zaradi česar so postale bolj kakovostne metode restavriranja cenovno mnogo bolj sprejemljive.

### *Telekomunikacijske povezave*

Za delovanje sodobnega informacijskega sistema, pa tudi nasploh za poslovanje organizacije so telekomunikacijske povezave ključnega pomena. Pod tem pojmom se skriva cela vrsta različnih komponent in tehnologij, ki sodijo na področja telekomunikacij v ožjem smislu informatike in elektronike.

Obnavljanje komunikacij zajema postopke za obnovitev prenosov podatkov in telefonskih povezav v primeru nesreč znotraj določenega obdobja ter v skladu z drugimi strategijami, ki so opredeljene v načrtu neprekinjenega poslovanja. Pri tem se ugotavljajo komunikacijske zahteve pri obnavljanju ključnih in bistvenih poslovnih funkcij, razvijejo mrežne načrte, izberejo različne opcije za preusmeritev komunikacij in strategije ter dokumentirajo stroški.

Postopki ponovne vzpostavitve različnih komponent omrežnega sistema se med sabo močno razlikujejo, a jih je za obravnavo temeljnih strategij obnove mogoče na grobo razdeliti v tri skupine (Rihar, 2003, str. 64-67; Interna gradiva proučevane institucije):

1. Restavriranje notranjega telekomunikacijskega omrežja, kamor sodijo tisti elementi telekomunikacijskega sistema, ki se nahajajo znotraj posamezne lokacije in so potrebni za notranje povezave med uporabniki, med sistemi ter med uporabniki in sistemi (lokalna računalniška omrežja, notranja telefonska vozlišča, lokalne povezave pomnilniških sistemov (SAN, NAS), stikala, lokalna ožičenja itd.);
2. Restavriranje povezovalnih komponent, kamor sodijo komponente, katerih naloga je povezati notranje uporabnike in sisteme s prostranim zunanjim omrežjem (usmerjevalniki, modemi, požarni zidovi, ISDN ali SDH adapterji, povezave do vozlišč telekomunikacijskih ponudnikov itd.). Edina metoda zagotavljanja delovanja v tem segmentu je uvajanje redundance, kar pa je lahko finančno nekoliko bolj

problematično, saj so nekatere povezovalne komponente lahko zelo drage. Redundantne komponente morajo biti konfigurirane in dimenzionirane tako, da se lahko obremenitev prenaša samodejno in za uporabnika neopazno.

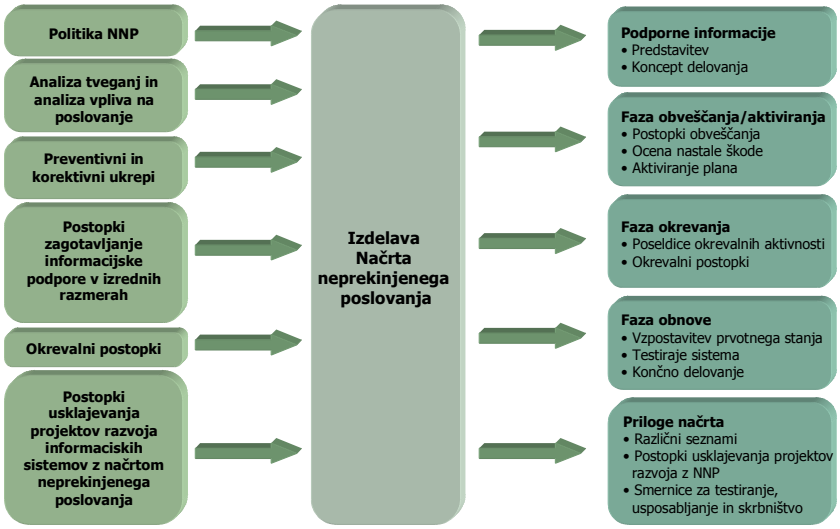
3. Restavriranje povezav v prostranem omrežju, kamor sodijo vse telekomunikacijske komponente, ki se nahajajo zunaj meja organizacije (javna ali zasebna prostrana omrežja, zunanja telekomunikacijska vozlišča, internet in drugi komunikacijski protokoli itd.). Zagotavljanje redundantnih povezav v prostranem omrežju je z vidika lastništva le-teh problematično iz dveh razlogov: rešitev s stalnim najemom nadomestnih povezav je zaradi visokih cen najema prenosnih zmogljivosti dokaj draga; drug problem pa je zagotavljanje resnične redundance v zunanjem omrežju. Tudi če povezave zagotavljata dva različna telekomunikacijska ponudnika, organizacija nima nikakršnega jamstva, da ponudnika nimata skupnih posameznih delov omrežja. Edina res zanesljiva rešitev je tako lastno omrežje, česar pa si večina organizacij ne more privoščiti.

Pri opredeljevanju postopkov okrevanja morajo biti predvideni tudi postopki vračanja na normalno delovanje, na kar se prepogosto pozablja. Ne glede na izbiro tehnologije delovanja alternativnega sistema je treba predvideti tudi postopke ponovne sinhronizacije primarnega informacijskega sistema s spremembami, ki so nastale med delovanjem na alternativnem sistemu. Pri tem je treba načrtovati postopke vračanja na normalno delovanje le za primere začasnega in delnega uničenja oziroma okvare na primarni strani, medtem ko obravnava rekonstrukcije ali nadomestitve primarne lokacije v primerih njenega trajnega in popolnega uničenja ne sodi v ta okvir.

### 5.1.4 Izdelava načrta neprekinjenega poslovanja

Ob doslednem upoštevanju navodil se pripravi načrt neprekinjenega poslovanja, ki obsega postopke zagotavljanja informacijske podpore v izrednih razmerah, okrevalne postopke in pokriva vse faze zagotavljanja neprekinjenega poslovanja. Slika 7(str. 22) prikazuje strukturo načrta neprekinjenega poslovanje z opredeljenimi vhodi in izhodi pri procesu načrtovanja.

**Slika 11:** Izdelava načrta neprekinjenega poslovanja




*Vir: Interna gradiva proučevane institucije.*

Načrt neprekinjenega poslovanja mora med drugim vključevati tudi postopke zagotavljanja informacijske podpore v izrednih razmerah, postopke vzpostavljanja normalnega poslovanja organizacije po pojavu krajših ali daljših prekinitev. Poleg klasičnih tveganj pa mora načrt predvideti tudi tveganja, ki so povezana z varnostnimi incidenti, ter postopke odziva nanje.

Skrbno izdelan načrt nam bo omogočil dosledno izvajanje postopkov v primeru nastopa uničujočega dogodka. Zavedati pa se je potrebno, da brez ustrezne priprave in treninga še tako dobro napisan načrt ne bo dosegel svojega namena.

Opredelitev postopkov zagotavljanja informacijske podpore v izrednih razmerah

Ne glede na to, ali pride do načrtovanega ali nenačrtovanega izpada informacijskega sistema, je treba v obeh primerih izvesti enake postopke za ponovno vzpostavitev delovanja. Vendar pa je razlika med primeroma v tem, da sta čas in obseg izpada pri načrtovanem izpadu izbrana, zato je vse postopke mogoče načrtovati in jih delno tudi izpeljati vnaprej, poleg tega so v tem primeru na razpolago vsi viri, ki so potrebni za vzpostavitev delovanja. Nič od tega pa navadno ne drži v drugem primeru, ko je dogajanje največkrat povsem nepredvidljivo. Zato je v organizacijskem delu načrta neprekinjenega poslovanja treba nameniti posebno pozornost prav vzpostavitvi poslovanja ob nepredvidenem izpadu, medtem ko prenos delovanja ob načrtovanih izpadih navadno sodi v opis rednih delovnih postopkov (Šalehar, 2004).

V tej fazi opredelimo nujne, takojšnje ukrepe, ki jih je potrebno uresničiti po izrednem dogodku, če ta ogroža poslovanje organizacije in človeška življenja, ter ravnanje v primeru, da se glavne poslovne dejavnosti organizacije preselijo na rezervno lokacijo (v kolikor ta obstaja).

Pri implementaciji načrta neprekinjenega poslovanja je po nastopu izrednega dogodka bistveno, ocena razsežnosti nastale škode in ugotovitev vrste škode informacijske opreme ali podatkov (poplava, ogenj in vročina, fizična poškodba in udar elektrike). Ocena

razdejanja se opravi takoj, ko dovoljujejo dane okoliščine. Prva je obveščena o nastopu izrednega dogodka skupina za neprekinjeno poslovanje organizacije Zavedati se je potrebno, da ima osebna varnost njenih članov najvišjo prioriteto. Po oceni stanja prizadetosti informacijskega sistema, skupina za neprekinjeno poslovanje aktivira postopke poslovanja organizacije v izrednih razmerah - vklopijo se rezervne sistemske komponente in po potrebi tudi delovanje sistema na rezervni lokaciji, restavrirajo se podatki iz varnostnih kopij itd. Nadalje je potrebno poiskati vzroke nastanka uničujočega dogodka, oceniti in preprečiti možnost nastanka nadaljnje škode, preveriti status infrastrukture (konstrukcijska celovitost sob z računalniki, stanje električne napeljave, telekomunikacij, ogrevanja, prezračevanja in klimatizacije), inventarja in informacijske opreme (preveriti je potrebno, ali je oprema popolnoma, delno ali ne- funkcionalna) ter sprožiti okrevalne postopke.

Člani skupine za neprekinjeno poslovanje organizacije, ki so odgovorni za poslovanje sistema v izrednih razmerah, morajo biti sposobni izpeljati postopek zagotavljanja informacijske podpore v izrednih razmerah tudi v primeru, če je načrt neprekinjenega poslovanja organizacije v papirni obliki in je v elektronski obliki uničen.

Zato je v okviru te faze potrebno opredeliti najmanj:

- postopek obveščanja o nastopu izrednega dogodka;
- postopek izvajanja nujnih ukrepov, ki sledijo nesrečam
- postopek varovanja in zaščite članov skupine za neprekinjeno poslovanje;
- postopek ocenjevanja nastale škode;
- postopek aktiviranja nadomestnega delovanja organizacije v izrednih razmerah;
- postopek iskanja vzrokov nastale škode in zaščite pred nadaljnjim uničenjem.

Ena izmed najpomembnejših nalog tega načrta je evakuacija ljudi v pravilnem vrstnem redu in zaščita njihovih življenj. Po evakuaciji zaposlenih je treba zagotoviti fizično varovanje prostorov. Osrednji namen tega načrta je preprečitev preplaha in zmede ob nastanku nesreče ali katastrofe. Pri izdelavi tega načrta lahko pomagajo tudi gasilske organizacije, inšpektorji s področja varstva pri delu in druge inštitucije.

Oblikovanje različnih skupin v okviru načrta neprekinjenega poslovanja

Organizacija mora usposobiti ljudi za izvajanje funkcij, opredeljenih v načrtu neprekinjenega poslovanja. Vse ljudi je potrebno v okviru načrta neprekinjenega poslovanja združiti v različne skupine, glede na definirane naloge, postopke, ukrepe, aktivnosti in vloge. Pri formiranju teh timov je potrebno vzpostaviti določena pravila in mehanizme delovanj, po katerih se bodo ravnali.

Pri sestavi timov je poleg značilnosti informacijskega sistema, izbrane okrevalne rešitve in morebitnih posebnih zahtev organizacije treba upoštevati tudi dejstvo, da v kritičnem trenutku vsi potrebni ljudje ne bodo na razpolago. Povsem mogoče je namreč, da bodo nekateri člani poškodovani ali nedosegljivi, da ne bodo mogli pravočasno priti na dogovorjeno lokacijo ipd. Na problem dosegljivosti članov timov je treba računati že pri izdelavi načrta neprekinjenega poslovanja, pri čemer je treba iskati rešitve v dveh smereh.

Prvič morajo biti ekipe, če je to le mogoče, sestavljene redundantno z večjim številom članov ali z nadomestnimi člani. Če v organizaciji ni na voljo dovolj ustreznih ljudi, je dobro iskati pomoč pri zunanjih izvajalcih, seveda pod pogojem, da so ti tako pomoč sposobni tudi dejansko zagotoviti. Druga pomembna ugotovitev, ki izhaja iz problema dosegljivosti ljudi in jo je treba pri izdelavi načrta neprekinjenega poslovanja nedvomno upoštevati, pa je, da mora biti načrt kar se da enostaven za izvedbo in čim bolj avtomatiziran. Tako je mogoče doseči, da bodo dejavnosti, predvidene z načrtom, izpeljane tudi tedaj, ko kateri od ključnih članov ekip ne bo mogel sodelovati pri njihovi izvedbi.

- **Vodstveni tim**; odgovoren je za sprejemanje ključnih odločitev in usklajevanje dejavnosti vseh drugih skupin. Določi, kdaj se bo začel uresničevati načrt neprekinjenega poslovanja, priskrbi ustrezna finančna sredstva, skrbi za pravne zadeve, za stike z javnostjo in mediji ter podobno.
- **Tim za arhiviranje podatkov na drugi lokaciji;** odgovoren je za prenos nosilcev podatkov z lokacije, kjer so shranjeni podatki in dokumentacija, na nadomestno lokacijo. Prav tako mora na podlagi informacij, ki prihajajo z nadomestne lokacije, nadzorovati izvajanje postopkov na lokaciji, kjer so shranjeni podatki in dokumentacija.
- **Tim za programsko opremo;** odgovoren je za namestitev in preizkušanje programske opreme, za reševanje problemov, ki se pojavijo v zvezi s programsko opremo, in za vzpostavitev delovanja na nadomestni lokaciji. Ta skupina odgovarja za nadziranje zmogljivosti in neoporečnost podatkov.
- **Tim za komunikacije;** odgovoren je za preusmeritev komunikacijskih povezav na nadomestno lokacijo in za namestitev kontrol dostopov, skratka za nadzorovanje ter vzdrževanje komunikacij.
- **Tim za varnost;** neprekinjeno nadzoruje varnost računalniški sistemov in komunikacijskih povezav ter rešuje navzkrižja, ki preprečujejo hitro vzpostavitev poslovnih funkcij, skrbi za primerno nameščanje in delovanje programskih paketov za zaščito.
- Poleg omenjeni timov delujejo še drugi, odgovorni za različna področja (nabava, logistika itd.).

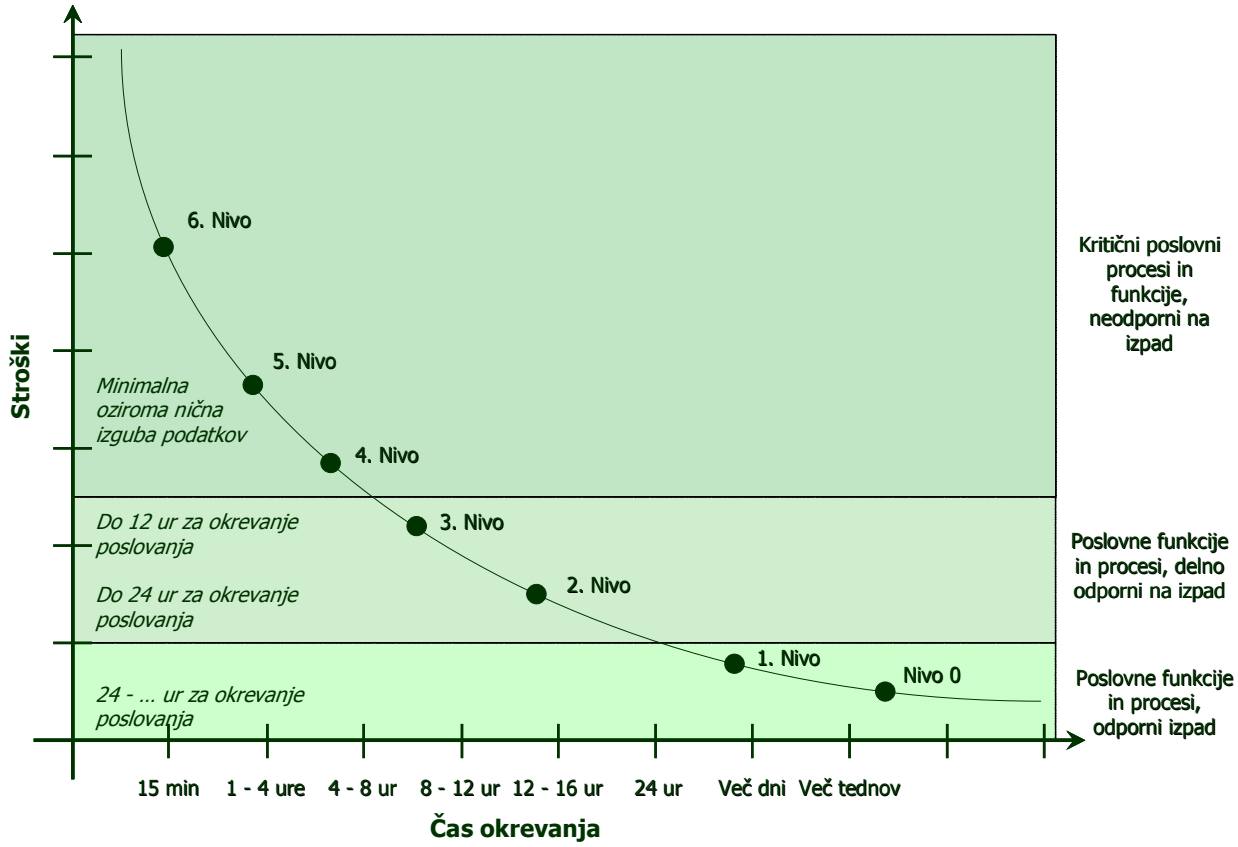
Definiranje okrevalnega načrta

Okrevalni načrt je osrednji operativni dokument, v katerem so zaobseženi cilji, ki jih želi organizacija doseči z uvajanjem pogojev za zagotavljanje delovanja svojega informacijskega sistema, ter postopki, ki jih mora izvesti za dosego teh ciljev. Načrt izhaja iz izsledkov analiz tveganja in vpliva na poslovanje, obstoječih preventivnih dejavnosti ter že uveljavljenih postopkov za zagotavljanje delovanja in odraža stopnjo pripravljenosti organizacije za reševanje te problematike.

Osrednji in najpomembnejši del okrevalnega načrta je, ne glede na izbiro metodologije, namenjen obravnavi postopkov ponovne vzpostavitve delovanja informacijskega sistema organizacije. Pri tem je treba nameniti pozornost trem glavnim elementom sistema:

podatkom, kamor sodi tudi programska oprema, strojni opremi in telekomunikacijskim povezavam. Obstaja mnogo načinov ponovnega vzpostavljanja informacijskega sistema, ki se med sabo razlikujejo po kompleksnosti, učinkovitosti in ceni. Že pri analizi vpliva na poslovanje smo opredelili dve temeljni merili, ki opisujeta zahteve, katere morajo zagotoviti okrevalni ukrepi za vzpostavitev poslovnih aplikacij, to sta ciljna točka restavriranja podatkov (RPO) in ciljni čas vzpostavitve delovanja (RTO). Za lažje razvrščanje okrevalnih postopkov glede na ti dve merili je bila leta 1992 predlagana sedemstopenjska lestvica (Warrick, Sing, 2001), ki na enostaven način ponazarja celotni možni spekter spleta okrevalnih postopkov.

**Slika 12:** Stopnje okrevanja




*Vir:Warrick, Sing, 2001, str. 24*

- Nivo 0 – ni opredeljenih okrevalnih postopkov. Organizacija nima nikakršnega okrevalnega načrta, zato so ob nesreči podatki najverjetneje izgubljeni in ni možnosti za ponovno vzpostavitev poslovanja. Tovrstna rešitev ne prinaša nikakršnih stroškov.
- 1. Nivo – kopiranje podatkov. Podatki in programska oprema se v določenih časovnih presledkih kopirajo na trakove in odvažajo na varno lokacijo. Ob nesreči je treba poiskati nadomestno lokacijo in strojno opremo, vzpostaviti telekomunikacijske povezave in sistem ter restavrirati podatke. Podatki od zadnje kopije do trenutka nesreče so izgubljeni. Stroške take rešitve tvorijo stroški kopiranja na trakove ter stroški prevoza in skladiščenja trakov na oddaljeni lokaciji.

- 2. Nivo – stopnja 1 in zagotovljena lokacija. Podoben način kopiranja kot pri stopnji 1, le da ima organizacija zagotovljeno in opremljeno nadomestno lokacijo. Čas vzpostavitve poslovanja se v primerjavi s prejšnjo stopnjo skrajša, stroški pa se povečajo za stroške vzdrževanja ali najema nadomestne lokacije.
- 3. Nivo – elektronski prenos podatkov. Podobno kot stopnja 2, le da ima organizacija na oddaljeni lokaciji na razpolago tračni sistem, na katerega kopira podatke po elektronski poti. Čas za vzpostavitev poslovanja se nekoliko skrajša, stroški pa se povečajo za ceno vzdrževanja dodatnega tračnega sistema in ceno občasnega prenosa podatkov med lokacijama.
- 4. Nivo – aktivna sekundarna lokacija. Poleg rednega kopiranja podatkov se na sekundarno lokacijo asinhrono prenašajo tudi vse vmesne spremembe podatkov. S tem načinom se količina izgubljenih podatkov bistveno zmanjša. Stroški rešitve se v primerjavi s prejšnjo stopnjo povečajo za stroške stalne telekomunikacijske povezave sistema za sprejemanje sprememb in ekvivalentnega diskovnega podsistema na sekundarni strani.
- 5. Nivo – dvofazno potrjevanje podatkov. Postavitev obeh sistemov je podobna kot pri prejšnji stopnji, le da so aplikacije prilagojene tako, da se podatki zapisujejo in potrjujejo krati na obeh straneh. Telekomunikacijske zahteve take povezave so večje kot pri asinhroni povezave, zato se pri taki rešitvi povečajo tudi telekomunikacijski stroški.
- 6. Nivo – popolna redundantna sistema. Organizacija ima na razpolago delujoč sekundarni sistem, ki vsebuje zrcalno sliko vseh podatkov in programske opreme ter je telekomunikacijsko povezano z uporabnik. Stroški se povečajo za stroške vzdrževanja delujočega sekundarnega sistema.

Osrednji del okrevalnega načrta sestavljajo opisi dejavnosti, ki jih morajo ekipe in posamezniki izvesti ob prekinitvi delovanja informacijskega sistema. Načrt mora biti kar najbolj pregleden in preprost, tako da ga je mogoče izpeljati tudi, če dokumentacije ni na razpolago. Tudi naloge, predvidene v okrevalnem načrtu, morajo biti dovolj enostavne, da jih je mogoče izvesti tudi v primeru ko ni na razpolago vseh ključnih ljudi. Člani okrevalnih timov morajo razpolagati z opomniki glede svojih nalog v okviru okrevalnega načrta, temeljne postopke pa morajo poznati na pamet. Dejavnosti okrevalnega načrta je mogoče prikazati na različne načine, med drugim tudi z diagrami dejavnosti, s katerimi je mogoče preprosto in pregledno prikazati medsebojne odnose med dejavnostmi.

Pomembnost zavarovanja

Sestavni del načrta neprekinjenega poslovanja morajo biti podatki o zavarovalnih policah in druga dokumentacija, ki jo je treba priložiti zahtevku, ki ga posredujemo zavarovalnici, za povrnitev škode. Ker zavarovanja lahko zagotovijo instituciji po nesreči oziroma katastrofi pomemben del finančnih sredstev, je treba ugotoviti, kaj je v družbi zavarovano in kaj bi še lahko bilo. Proučiti je treba, ali imajo zavarovalnice še kakšne vrste zavarovanj za posledice nesreč, ki bi pomenile nevarnost za družbo. Zavarovani naj bi bili oprema in prostori na osnovni in nadomestni lokaciji (Andolšek, 2001).

Upravljanje načrta neprekinjenega poslovanja

Poleg tehničnih detajlov je treba pri izdelavi načrta neprekinjenega poslovanja precejšnjo pozornost nameniti tudi organizacijskemu delu. Še tako natančno izdelani, dragi in dosledno implementirani tehnični ukrepi za zagotavljanje delovanja informacijskega sistema ne zaležejo kaj dosti, če niso primerno organizacijsko podprti. Da je načrt zasnovan organizacijsko neustrezno, se največkrat pokaže šele, ko nastane resnična potreba po uveljavitvi ukrepov – na primer zaradi nesreče – in ko je že prepozno, da bi ga kakorkoli spreminjali.

Pri izdelavi organizacijskega dela načrta neprekinjenega poslovanja je treba določiti tudi lokacijo, od koder se bodo dejavnosti prenosa informacijske podpore izvajale oziroma koordinirale. Za ta namen je najbolje izbrati sekundarno lokacijo, če je ta izbrana že vnaprej, saj je najprimerneje, da se strokovnjaki nahajajo čim bliže delujočega računalniškega centra. Poleg tega mora biti sekundarna lokacija primerno telekomunikacijsko opremljena, tako da je najlaže vzpostaviti stik z vsemi perifernimi deli organizacije in z okoljem. Pri izbiri alternativnih rešitev brez obstoječe nadomestne lokacije pa je treba vnaprej izbrati oddaljeno »štabno« lokacijo in jo primerno telekomunikacijsko opremiti.

Pri izdelavi načrta neprekinjenega poslovanja je treba imeti pred očmi dejstvo, da dogodki v nepredvidenih in kriznih situacijah ne potekajo po predvidenih načrtih, ne glede na to, kako skrbno so pripravljeni. Upoštevati je tudi treba, da strokovnjaki v organizacijah z izrednimi razmerami nimajo izkušenj, zato je, ne glede na pogostnost in resnost testiranja, dejansko ravnanje ljudi v izrednih razmerah težko predvideti. Poleg tega je treba računati tudi z dokaj realno možnostjo, da v izrednih razmerah marsikateri, tudi ključni ljudje, iz tega ali onega razloga ne bodo mogli sodelovati pri izvedbi načrta. Zaradi vsega tega mora biti načrt neprekinjenega poslovanja v tehničnem in organizacijskem smislu načrtovan čim bolj preprosto, tako da ga je mogoče po potrebi med samim izvajanjem spreminjati in prilagajati ter ga je mogoče izvesti tudi s pomanjkljivimi in strokovno nepopolnimi ekipami.

### 5.1.5 Testiranje načrta

Načrti za neprekinjeno poslovanje pogosto pri preverjanju odpovedo zaradi napačnih predpostavk, spregledov ali sprememb osebja ali opreme, zato bi jih bilo potrebno redno preverjati in testirati, s čimer zagotovimo da so posodobljeni ter učinkoviti. Testiranje je ključni element načrtovanja neprekinjenega poslovanja. Omogoča preverjanje učinkovitosti zapisanih postopkov ter zmožnosti zaposlenih in zunanjih izvajalcev za dosledno in učinkovito uporabo načrta. Splošni namen testiranja je ugotoviti, ali je mogoče z uresničevanjem načrta neprekinjenega poslovanja zagotoviti delovanje informacijskega sistema v želenem času in obsegu. Poleg tega je s testiranjem načrta (Toigo, 2000, str. 378) mogoče odkriti njegove pomanjkljivosti in jih odpraviti. V tej funkciji testiranje omogoča tudi ugotavljanje neskladnosti načrta z dejanskim stanjem informacijskega sistema. Testiranje je edini način, s katerim je mogoče ugotoviti, koliko časa je potrebno za izvedbo njegovih posameznih faz in v kolikšnem času je mogoče ponovno vzpostaviti delovanje, seveda v optimalnih razmerah. Poleg tega je med testom mogoče izmeriti tudi zmogljivosti

in učinkovitost nadomestnih zmogljivosti. Testiranje je nujno potrebno za nabiranje izkušenj. Člani timov morajo dobro poznati posamezne postopke in svoje vloge v njih, saj bodo le tako v kriznih trenutkih svoje naloge opravljali hitro in usklajeno.

V okviru testiranja mora biti preverjen in potrjen vsak najmanjši element načrta. To velja tako za postopke kot za opremo. Potrebno je preveriti sposobnost zagotavljanja informacijske podpore s pomočjo rezervne lokacije, sposobnost restavriranja podatkov iz varnostnih kopij, koordinacijo med skupinami, odgovornimi za posamezne postopke, učinkovitost sistema ob uporabi alternativnih zmogljivosti, sisteme obveščanja. Ti testi naj tudi zagotovijo, da vsi člani definiranih timov in drugi sodelujoči poznajo načrte.

Urnik preverjanja načrtov za neprekinjeno poslovanje naj določa, kako in kdaj je potrebno preveriti posamezne dele načrta. Priporoča se redno preverjanje posameznih sestavin delov načrta. Pri tem bi bilo potrebno uporabiti različne tehnike, da načrt zaživi v resničnem življenju. Te naj bodo (Smith, 2002, str. 163):

- različni scenariji (razpravljanje o različnih ukrepih za obnovo poslovanja ob primerih nepredvidenih dogodkov);
- simulacije, ki so zlasti pomembne pri usposabljanju ljudi za izpolnjevanje njihovih vlog v krizni situaciji ali po incidentu;
- preverjanje ponovnega tehničnega zagona, ki zagotavlja predvsem učinkovito obnovo informacijskega sistema;
- testiranje obnove v okviru nadomestne lokacije, ki pokriva predvsem področje upravljanja poslovnih procesov, vzporedno s potekom obnovitvenih del izven središča incidenta;
- preverjanje opreme in storitev dobavitelja, s čimer zagotovimo, da so storitve in izdelki ponudnikov opreme v skladu s pogodbenimi obveznostmi;
- ponovitev celotnega postopka, kar zagotavlja preverjanje, ali se lahko organizacija, osebje, oprema, zmogljivosti in postopki spopadejo s prekinitvami v delovanju.

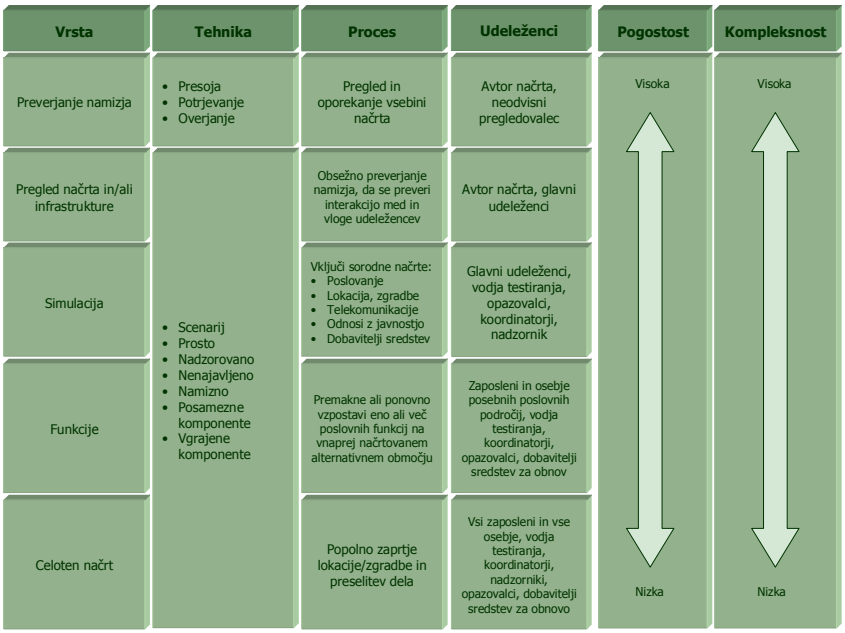
Temeljno pravilo pri izvedbi testiranja je, da to nikoli ne sme ovirati rednih delovnih postopkov in mora biti vnaprej napovedano. Testiranje igra bistveno vlogo pri dokazovanju, da strategije opredeljene v načrtu neprekinjenega poslovanja, delujejo. Čas in sredstva, ki jih iorganizacija vloži v testiranje strategij načrta neprekinjenega poslovanja, bodo organizacijo pripeljali do ustrezne sposobnosti odzivanja v primeru nepredvidljivih dogodkov, kar je bistvenega pomena v času kriz in negotovosti.

Kvalitetno testiranje načrta neprekinjenega poslovanja je odvisno od izvajajočih in realističnih scenarijev ter bodo jasno pokazale območja, ki potrebujejo izboljšave. Program testiranja se prične preprosto in se postopno stopnjuje. Raven sredstev, ki so potrebna za izvedbo testiranja in preverjanja ustreznosti načrta neprekinjenega poslovanja, se določi na podlagi ravni razvitosti avtomatiziranega poslovanja v organizaciji. Visoko avtomatizirani sistemi zahtevajo tako imenovano »visoko razpoložljivost« in bi jih bilo potrebno oblikovati tako, da testiranje poteka rutinsko, v teku običajnih operacij. Ti testi morajo biti nevidni za običajne uporabnike informacijskega sistema in ne smejo ustvarjati občutka krizne situacije. Testiranje tovrstnih sistemov lahko vključuje izklop delov opreme, da se lahko spremlja

posledice na storitvah ali s prenosom storitve na drugo lokacijo, brez ali z omejenim vplivom na delovanje. Manj napredni sistemi lahko zahtevajo več načrtovanja in preusmerjanje proizvodnih sredstev za ločeno izvajanje vaj, samostojne vzpostavitvene procese in lokacijo za obnovo. Poleg tega je potrebno pri testiranju načrta neprekinjenega poslovanja upoštevati določene zahteve in priporočila, da bi bilo le to učinkovito (Smith, 2002, str. 170 – 172):

- **Vnaprej pripravljen scenarij testa.** Vsak test mora imeti pripravljen scenarij izrednega dogodka, ki je predmet testiranja, na primer popolno uničenje osrednje lokacije, izpad prostranih povezav, uničenje pomnilniškega sistema ipd. V scenariju morajo biti opredeljene tudi morebitne privzete dodatne predpostavke, kot na primer trajanje izpada, odsotnost dela osebja ipd.
- **Jasno določeni cilji testiranja**. Cilji testiranja morajo biti določeni pred njegovim začetkom. Biti morajo jasni in merljivi, saj je le tako pozneje mogoče oceniti uspešnost testiranja, na primer čas, potreben za obveščanje in prihod izvajalcev, čas obnovitve prostranih povezav, učinkovitost nadomestnega računalniškega sistema itd.
- **Uporaba sredstev.** Pomembno je, da organizacija med testiranjem uporablja le tista sredstva, ki bodo na razpolago med dejanskim incidentom pri zagotavljanju neprekinjenega poslovanja
- **Dokumentiranje rezultatov testiranja.** Rezultati in opažanja med testiranjem morajo biti, kolikor je mogoče, natančno dokumentirani za poznejšo analizo. Dokumentirana morajo biti tudi morebitna odstopanja od načrta, do katerih je prišlo med testiranjem.
- **Rezultati testiranja.** Neuspeh, ugotovljen pri preverjanju in testiranju načrta neprekinjenega poslovanja, ni negativen rezultat. Preverjanje je namenjeno temu, da se podpira nenehno izboljševanje, tako da neuspeh velja kot pozitiven in koristen rezultat.

**Slika 13:** Postopki in vrste testiranj v okviru načrtovanja neprekinjenega poslovanja




*Vir: Smith, 2002, str. 164.*

Ključni rezultati, do katerih naj bi organizacija prišla v okviru testiranja načrta neprekinjenega poslovanja, naj vključujejo (BSI, 2002):

- prikaz sposobnosti in zmožnosti ukrepanja v primeru kriznih situacij;
- preverjanje ali so definirane strategije, postopki in ukrepi v okviru načrta neprekinjenega poslovanja, dejansko uporabni, uspešno posodobljeni, dopolnjeni in ali ustrezajo svojemu namenu;
- testiranje tehničnih, logističnih, administrativnih in drugih sistemov načrta neprekinjenega poslovanja;
- testiranje organizacije in infrastrukture v okviru načrta neprekinjenega poslovanja vključno z vodstvenimi centri, nadomestno lokacijo, delovnimi področji, obnovo tehnologije in telekomunikacijskih sredstev, razpoložljivostjo osebja in drugih;
- preverjanje, da načrt neprekinjenega poslovanja vključuje v kritične ciljne aktivnosti organizacije;
- povečano zavedanje pomena načrtovanja neprekinjenega poslovanja;
- prepoznavanje pomanjkljivosti in potrebnih izboljšav načrta neprekinjenega poslovanja itd.

Pri pogostosti testiranja načrta neprekinjenega poslovanja ni posebnega pravila. Potrebno je le upoštevati, da bi morala biti testiranja tako pogosta, da ohranja stik s spremembami v informacijskem sistemu in se vzdržuje poznavanje in znanje veščin pri izvajalcih v okviru nepredvidenih dogodkov. Tako lahko rečemo, da je pogostnost testiranja odvisna od hitrosti spreminjanja informacijskega sistema organizacije in od želene ravni poznavanja ravnanja v primeru nesreče, katastrofe ali drugega nepredvidenega dogodka. Potrebe po testiranju se med organizacijami lahko močno razlikujejo, po izkušnjah pa bi moral biti popolni test izveden najmanj enkrat na leto, delni pa glede na potrebe pogosteje. Pri tem je treba

upoštevati, da je vsak prenos delovanja na alternativni sistem v primeru načrtovanega izpada glavnega sistema zaradi vzdrževanja ali popravila lahko tudi odličen test, če je tak prenos narejen v skladu s prej navedenimi zahtevami za testiranje.

### 5.1.6 Skrbništvo načrta

Načrt neprekinjenega poslovanja je osrednja točka vsakršne strategije za zagotavljanje delovanja informacijskega sistema in izraža pripravljenost organizacije za reševanje problema izpada informacijske podpore ter njeno pripravljenost na posledice, ki jih tak izpad pomeni za njeno poslovanje. Dobro izdelan načrt pomeni vrh prizadevanja različnih strokovnjakov z različnih področij in organizaciji zagotavlja jamstvo za preživetje kriznih situacij. Ne glede na ves vloženi trud pri oblikovanju načrta in implementaciji tehničnih rešitev, ki jih načrt predvideva, pa delo na načrtu neprekinjenega poslovanja z njegovo formalno izdelavo nikakor ni končano.

Usposabljanje zaposlenih

Po končani izdelavi načrta neprekinjenega poslovanja je najprej treba usposobiti vse tiste, ki bodo sodelovali pri izvajanju predvidenih postopkov. Usposabljanje skupine za neprekinjeno poslovanje organizacije dopolnjuje testiranje načrta. To velja ne glede na to, ali so načrt sestavili v sami organizaciji ali pa so ga naredili zunanji strokovnjaki. V zadnjem primeru sta predaja znanja in skrbništva nad načrtom tako ali tako sestavni del same izdelave načrta, vendar je usposabljanje potrebno tudi v primeru, ko je bil načrt izdelan z lastnim znanjem. Pri implementaciji zagotavljanja neprekinjenega poslovanja bodo namreč zagotovo sodelovali tudi ljudje, ki pri izdelavi načrta niso sodelovali ali pa je bilo njihovo sodelovanje minimalno.

Namen usposabljanja je predvsem seznaniti vse tiste, ki bodo sodelovali pri vzpostavljanju nadomestnih informacijskih in telekomunikacijskih rešitev, z njihovimi vlogami pri teh postopkih. Usposabljanje naj bi potekalo najmanj enkrat letno in ločeno za posamezne okrevalne time ter time, odgovorne za načrt neprekinjenega poslovanja. Usmerjeno naj bi bilo predvsem na posamezne dejavnosti, ki morajo biti opravljene v okviru nalog posamezne ekipe, poleg tega pa mora biti vsaj v obrisih prikazan tudi grobi obris vseh dejavnosti v okviru načrta. Vodjem posameznih ekip mora biti predstavljena predvsem splošna slika dogajanja in nalog pri koordinaciji dejavnosti med ekipami. Oblikovati je potrebno tudi programe usposabljanja novih članov skupine za neprekinjeno poslovanje organizacije. Predavanja morajo biti dobro pripravljena in dokumentirana, saj jih bo treba pozneje še večkrat ponavljati za sodelavce, ki se bodo ekipam pridružili pozneje, bodisi zaradi zamenjave osebja bodisi zaradi razširitve nalog. Za posamezne naloge je treba usposobiti tudi nadomestne člane ekip, ki lahko priskočijo na pomoč ob morebitni odsotnosti svojih sodelavcev. Ključni cilj, ki ga je potrebno doseči pri izvedbi usposabljanja, je, da so zaposleni in zunanji izvajalci usposobljeni tako, da ob morebitni prekinitvi poslovanja sistema organizacije ne potrebujejo pisnih navodil.

Vzdrževanje in skrbništvo načrta neprekinjenega poslovanja

Sprotno vzdrževanje in dopolnjevanje načrta je ključni dejavnik uspešnosti zagotavljanja neprekinjenega poslovanja organizacije, izvedenih akcij v času prekinitev ter obnove sistema. Načrt mora odsevati spremembe dejavnikov, ki vplivajo na načrt in spremembe na strani uporabnikov. Informacijski sistemi, poslovanje in organizacija so pogosto izpostavljeni spremembam zaradi spreminjajočih se potreb v poslovanju, tehnoloških nadgradenj ali novih notranjih in zunanjih politik. Zato je nujno, da se načrt neprekinjenega poslovanja redno pregleduje in dopolnjuje in tako zagotavlja, da se nove informacije dokumentirajo, obstoječe informacije pa pregledajo in popravijo, če je to potrebno. Plan je potrebno natančno in celovito pregledati vsaj enkrat letno oziroma vedno, ko se zgodi sprememba kateregakoli elementa plana, saj le-ta zahteva dokumentiranje sprememb in verifikacijo obstoječih postopkov sistema organizacije. S tem zagotovimo nenehno učinkovitost teh načrtov. Ker plan vsebuje potencialno občutljive operativne in osebne informacije, mora biti njegova distribucija nadzorovana.

Načinov ugotavljanja potrebe po spremembah v načrtu neprekinjenega poslovanja je več. Prvi in najprimernejši način je postopek spremljanja sprememb (angl. Change Management) v informacijskem sistemu Spremljanje sprememb je v informacijskem sistemu v kombinaciji s testiranjem načrta najprimernejši, na žalost pa tudi najtežji način ugotavljanja potrebe po spremembah v načrtu neprekinjenega poslovanja. Problem tega postopka je v tem, da se informacijski sistem organizacije navadno spreminja tako hitro, da je brez skrbne organizacije nemogoče slediti spremembam. Postopek je mogoče olajšati tako, da se jasno opredelijo področja, kjer bo zagotovo prihajalo do sprememb in jih je zato treba spremljati. Potrebe po popravkih načrta se lahko pokažejo tudi pri testiranju, kjer ugotavljajo pomanjkljivosti, ki nastanejo kot posledica sprememb v sistemu. Tretji način, ki je manj primeren in vsem organizacijam niti ni na voljo, pa so zahteve po spremembah, ki jih zaradi opaženih pomanjkljivosti zahtevajo nadzorne organizacije po opravljenem pregledu načrta. Obstaja seveda še četrti način, to je odkrivanje pomanjkljivosti pri dejanskem uresničevanju načrta, ki pa je iz razumljivih razlogov povsem nezaželen in je tu naveden bolj v svarilo (Andolšek, 2001).

Vsaka sprememba v planu temelji na analizah testnih rezultatov. Situacije, ki lahko zahtevajo dopolnitev načrtov, so: nakup nove opreme ali nadgradnja operacijskega sistema in spremembe.

Spreminjanje podatkov je stalnica v informacijskih sistemih. Pri tem sta pomembni predvsem dve vrsti podatkovnih sprememb: naraščanje količine podatkov in s tem povezano tudi morebitno spreminjanje strojne opreme ter staranje oziroma arhiviranje podatkov, kar navadno pomeni prenos podatkov na drugačen pomnilniški medij. Staranje podatkov v veliki večini primerov pomeni prenos podatkov na drug pomnilniški medij, pri čemer gre navadno za prenos s hitrih diskov na trakove ali počasne diskovne medije. Pri tem nastane težava, saj se spremembe na hitrih diskovnih medijih prenašajo posamezno, za vsako datoteko posebej, medtem ko se spremembe na počasnih medijih navadno prenašajo agregatno, tako da se hkrati menja vsebina celotnega medijskega nosilca.

Sprememba programske in strojne opreme je navadno v dokaj tesni zvezi tudi s spremembo podatkov. Korenitejša sprememba obstoječih, predvsem pa uvajanje novih programskih rešitev, navadno prinašata tudi spremembe pri strojni opremi, ki jih je treba upoštevati. Sprememba strojne opreme v vsakem primeru prinaša tudi potrebo po spremembi načrta neprekinjenega poslovanja. Glede na to, da se strojna oprema najpogosteje spreminja na ravni končnih uporabnikov (delovne postaje, lokalni strežniki ipd.), je dobro poskrbeti, da je ta del načrta zasnovan bolj splošno, tako da ga je mogoče lažje spreminjati. Pogosto prinaša sprememba strojne opreme na lokalni ravni tudi spremembo operacijskega sistema, kar je prav tako treba upoštevati.

Ostale spremembe, se dotikajo predvsem organizacijskih postopkov načrta neprekinjenega poslovanja. Tu gre predvsem za spremembe osebja, naslovov ali telefonskih številk, poslovnih strategij, prostorov, naprav in virov, zakonodaje, pogodbenih partnerjev, dobaviteljev in ključnih strank, procesov (sprejete novih ali opustitev starih), tveganj (operativnih in finančnih) itd.

Plan mora odsevati spoznanja in priporočila katere ugotavljamo v postopku testiranja. Priporočljivo je, da se varnostna kopija plana hrani na varnem alternativnem mestu, ki je zavarovano pred požarom in poplavo oziroma in ga katastrofalni dogodek ne doseže. V okviru skrbništva načrta neprekinjenega poslovanja bi bilo potrebno določiti osebe, ki so odgovorne za redno pregledovanje načrta neprekinjenega poslovanja. Najprimerneje je, da je to oseba, ki je pomembno sodelovala pri načrtovanja neprekinjenega poslovanja. Njegov položaj je sicer odvisen od organizacijske strukture v organizaciji, vendar mora biti dovolj visok, da ima dober pregled nad dogajanjem v celotnem informacijskem in telekomunikacijskem sistemu organizacije. Ključne naloge te osebe so:

- spremljanje sprememb v informacijskem sistemu organizacije;
- prilagajanje načrta neprekinjenega poslovanja;
- priprava, izvedba in analiza testiranja načrta;
- koordiniranje načrtovanega ali izrednega vzpostavljanja delovanja na alternativnem informacijskem sistemu.

## 5.2 Problematika načrtovanja neprekinjenega poslovanja

Pomen zagotavljanja neprekinjenega poslovanja in s tem tudi načrtovanja le-tega se razvija šele v zadnjih dveh desetletjih. Kot sem izpostavil že v enem izmed uvodnih poglavij (Poglavje 3.2 Razvoj neprekinjenega poslovanja), se proces zagotavljanja neprekinjenega poslovanja razvija predvsem iz okrevanja delovanja kritičnih poslovnih procesov in sistemov. Tega so se v preteklosti posluževale predvsem banke in druge finančne organizacije, v katerih je bilo potrebno minimizirati vplive izpada informacijske podpore poslovnim procesom. Sam proces okrevanja poslovanja se je v zadnjem času preusmeril na širši spekter in sicer na načrtovanje neprekinjenega poslovanja, ki poleg okrevanja informacijske podpore poslovnim procesom predvideva tudi okrevanje in nadaljevanje poslovanja.

Problemi s katerimi se srečujejo pobudniki in zagovorniki načrtovanja neprekinjenega poslovanja, se v okviru institucij, pa naj si gre za javni ali zasebni okvir, izvirajo predvsem iz pomanjkanja znanja, izkušenj in argumentov, zakaj je potrebno vgraditi sistem zagotavljanja neprekinjenega poslovanja v posamezne organizacije. Dejstvo je da se tako managerji v gospodarskih subjektih kot predstavniki države v ključnih organizacijah javnega sektorja zavedajo posledic izpada informacijske podpore kritičnim poslovnim procesom, vendar večina med njimi še vedno meni, da so tovrstne aktivnosti zanemarljive in predvsem pomenijo neracionalno trošenje finančnih sredstev.

Vendar pa strokovnjaki s področja zagotavljanja neprekinjenega poslovanja ugotavljajo, da sta se v zadnjih letih zgodila dva pomembna mejnika, ki so pomembno pripomogla k dejstvu, da zagotavljanje neprekinjenega poslovanja in zanemarljivo. Ta mejnika sta predvsem pojav »milenijskega hrošča – Y2K« in teroristični napadi v New Yorku septembra 2001. Predvsem slednji je pustil močan pečat, kajti v tej katastrofi je veliko institucij izgubilo vse svoje imetje in po njej praktično niso imele možnosti in virov, da bi nadaljevale s poslovanjem.

Kljub velikemu koraku v smeri zavedanja in pomembnosti načrtovanja neprekinjenega poslovanja pa še vedno velja velika stopnja skeptičnosti v potrebi po zagotavljanju neprekinjenega poslovanja. Iz lastnih izkušenj lahko ugotovim, da je eden ključnih problemov pri vzpostavitvi sistema zagotavljanja neprekinjenega poslovanja argumentiranje potrebe po izdelavi načrta neprekinjenega poslovanja. V tem primeru nihče od še tako priznanih strokovnjakov nima dovolj močnega argumenta. Rešitev, ki se je poslužuje večina svetovalcev in strokovnjakov s tega področja, je izpostavljanje ranljivosti poslovanja institucij in posledic, ki jih lahko prinesejo nepredvideni dogodki in katastrofe. Edini dovolj močan argument je dejanski primer katastrofe, vendar tega nihče ne želi nobeni izmed institucij, kajti v tem primeru je lahko ogroženo poslovanje številnih institucij in celo normalno delovanje države. Dejstvo je, da se pri tem lahko strokovnjaki in svetovalci opirajo zgolj na katastrofe, ki so se zgodile v preteklosti in v katerih so številne organizacije doživele ogromno škodo (teroristični napadi 9/11, poplave v srednji in zahodni Evropi leta 2003, različni vojaški posegi (primer Crvene Zastave v Kragujevcu), številni potresi po svetu in vrsta drugih dogodkov).

Dvom v smiselnost vzpostavitve sistema zagotavljanja neprekinjenega poslovanja izvira predvsem iz velikega obsega potrebnih finančnih sredstev, ki jih je potrebno zagotoviti za financiranje te investicije. Največji obseg potrebnih sredstev predvideva predvsem zagotavljanje maksimalne odpornosti informacijskih sistemov, na katerih temeljijo in slonijo sodobni poslovni procesi in proti razdejanjem, ki jih povzročajo bolj ali manj nepredvidljivi dogodki in katastrofe. Tehnik, s katerimi je to moč doseči, je več. Vse obsegajo tako imenovano visoko razpoložljivost (angl. »High Availability), ki jo izdelovalci informacijske opreme dosežejo s tem, da v opremi podvajajo ključne elemente. Če eden od elementov odpove, vse njegove funkcije takoj prevzame drugi in naprava deluje naprej, kakor da se ni nič zgodilo. Rešitev ponuja združevanje v gručo, pri čemer dve ali več naprav združimo v gručo, v kateri si naprave enakovredno pomagajo in prevzemajo naloge tistih, ki

so morebitno odpovedale. Tako reševanje je zlasti pomembno pri strežnikih, ki so ena ključnih komponent informacijske infrastrukture.

Niti to pa ni dokončna rešitev. V kontekstu podjetja in njegovega poslovanja je namreč informacijska infrastruktura spet točka, na kateri lahko vse odpove. Če se na primer podre stavba, v kateri se nahaja, potem z vidika organizacije, ki je ostala brez celotne informacijske podpore, nič ne pomaga podvajanje kritičnih delov računalnikov in njihovo združevanj v gruče. Problem je torej težavnejši, saj se od zares odpornega sistema zahteva, da je sposoben zelo hitrega vnovičnega zagona aplikacij s popolnoma obnovljenimi arhiviranimi in tudi svežimi podatki. Kako dolg čas je še sprejemljiv, je odvisno predvsem od uporabnika in aplikacij, v zadnjem času pa tehnike okrevanja in skokovit razvoj informacijske in komunikacijske infrastrukture omogoča čas v okviru nekaj minut oziroma popolnoma brez kakršnega časovnega vpliva na poslovanje in delovanje računalniškega centra in aplikacij. To pa se navadno zagotavlja s podvojenim komponentami, pravzaprav kar s podvojenim informacijskim centrom, v katerem so strežniki, omrežne naprave in primerne diskovne zmogljivosti. In prav podvojen informacijski center je osrednja težava. Cena velikih informacijskih sistemov, s katerimi zagotavljajo informacijsko podporo poslovnim procesom predvsem organizacije, ki se srečujejo z ogromnim številom podatkov in procesov in njihovo poslovanje temelji na informacijski podpori (banke, zavarovalnice javne organizacije, predvsem carina in davkarija) zahtevajo ogromna finančna sredstva. Kot je bilo že v prejšnjih poglavjih omenjeno (Poglavje 5.1.4 Izdelava načrta neprekinjenega poslovanja), so sodobne in učinkovite tehnike okrevanja, ki omogočajo ponovno vzpostavitev poslovanja in okrevanja ključnih poslovnih procesov v nekaj minutah, neprimerljivo dražje. Za reševanje tega problema ni enotne in najboljše rešitve. Tu so našteti zgolj nekateri izmed možnih ukrepov, s katerimi se zmanjša obseg potrebnih investicijskih sredstev ali se razbremeni pritisk z porazdelitvijo na več obdobij.

Večfazni pristop instituciji zagotavlja postopno vzpostavitev sistema neprekinjenega poslovanja. Prva faza predvideva predvsem logične aktivnosti načrtovanja neprekinjenega poslovanja (vzpostavitev projekta, analiza tveganj in analiza vpliva na poslovanje, določitev okrevalnih postopkov, opredelitev preventivnih in korektivnih ukrepov, načrtovanje testiranj, opredelitev ekip itd.). Z drugo fazo, zagotovimo odpornost informacijskih sistemov na nepredvidene dogodke, predvsem z zagotavljanjem podvojenih zmogljivosti. V okviru te faze je predviden večstopenjski pristop, kjer je v prvem koraku predvidena vzpostavitev »hladne« rezervne lokacije z zagotovljenimi rezervnimi podatkovnimi kapacitetami ter manjšimi procesorskimi zmogljivostmi. S temi zmogljivostmi je zagotovljena vzpostavitev kritičnih procesov v roku treh dni ter njihovo obratovanje. V drugem koraku je predvidena nadgradnja, rezervne lokacije v »toplo« rezervno lokacijo, kjer bodo zagotovljene tako rezervne podatkovne kot tudi procesorske zmogljivosti. Tovrstne sistemske zmogljivosti bodo omogočale vzpostavitev kritičnih procesov v roku do treh ur. V zadnjem koraku pa je predvidena nadgradnja v »vročo« rezervno lokacijo, ki zagotavlja podvojene produkcijske in sistemske kapacitete informacijskega sistema organizacije.

**Slika 14:** Fazni pristop k načrtovanju neprekinjenega poslovanja


*Vir: Interna dokumentacija proučevane institucije*

Druga možnost prav tako izhaja iz dejstva, da so stroški zagotavljanja in vzdrževanja nadomestne lokacije relativno visoki, vendar si lahko organizacije, ki uporabljajo tak način restavriranja strojne opreme, pomagajo pri njihovem zniževanju na različne načine:

- Medsebojni dogovor. Dve organizaciji s tehnološko enakima in po velikosti podobnima informacijskima sistemoma si lahko s pogodbo ali dogovorom medsebojno odstopita del procesorskih zmogljivosti za potrebe vzpostavitve nadomestnega sistema. Ta način prinaša le stroške vzdrževanja nekoliko povečanih zmogljivosti strojne opreme v obeh organizacijah ter v primeru medsebojnega kopiranja podatkov stroške medsebojne telekomunikacijske povezave, sicer pa veljajo enake ugotovitve, kot za dogovor dveh organizacij o medsebojnem kopiranju podatkov. Pri dogovarjanju je treba paziti, da imata organizaciji, ki sklepata dogovor, svoja računalniška centra medsebojno dovolj oddaljena in ni nevarnosti, da bi ju prizadela ista nesreča.
- Skupni center za več organizacij. Več organizacij s podobno strojno opremo lahko vzpostavi, opremi in vzdržuje skupno nadomestno lokacijo, s čimer se sorazmerno zmanjšajo tudi stroški. Zmogljivost strojne opreme na nadomestni lokaciji je odvisna od dogovora, navadno pa bistveno ne presega potreb največje od pogodbenih organizacij. Dodatna prednost tega načina je, da je s skupno organizacijo ter skupnimi sredstvi in znanjem mogoče pridobiti vrhunsko nadomestno lokacijo ter jo izjemno kakovostno opremiti. Slabost tega načina je, da so sodelujoče organizacije prisiljene v sklepanje kompromisov, na primer pri nabavi nove strojne opreme, ki mora biti tipizirana in povsem združljiva z opremo na nadomestni lokaciji. Zaradi tesnega sodelovanja je navadno taka rešitev primernejša za državne in javne organizacije, kakor za poslovne organizacije.

- Zunanji ponudnik. Z zunanjim ponudnikom je mogoče skleniti dogovor o najemu rezervnih zmogljivosti, ki se lahko nahajajo na stalni lokaciji pod nadzorom ponudnika ali pa ima ponudnik na voljo mobilni center, ki ga je v dogovorjenem času sposoben pripeljati in konfigurirati v skladu z naročnikovimi zahtevami ter povezati z uporabniki. Pogodba je lahko omejena le na zagotavljanje nadomestnih zmogljivosti, lahko pa predvideva tudi dodatne storitve ponudnika, kot so: svetovanje in pomoč pri restavriranju sistema. Taka rešitev je dražja, zato pa ima organizacija več manevrskega prostora pri izbiri svoje opreme, saj se mora ponudnik v skladu s pogodbo prilagajati spremembam na strani naročnikovega informacijskega sistem. V Sloveniji take rešitve trenutno nihče ne uporablja, po svetu pa je precej razširjena.

Poleg problemov z zagotavljanjem potrebnih finančnih sredstev za vzpostavitev sistema za zagotavljanje neprekinjenega poslovanja pa se svetovalci, strokovnjaki in organizacije srečujejo še s kopico drugih težav in ovir, ki jih je potrebno rešiti ali v okviru zagotavljanja neprekinjenega poslovanja, največkrat pa jih je potrebno rešiti že pred tem. Te probleme lahko združimo v več skupin:

- V povezavi z zagotavljanjem potrebnih finančnih sredstev do težav pride še pred vzpostavitvijo sistema za zagotavljanje neprekinjenega poslovanja, kajti številne organizacije se soočajo s problematiko zagotavljanja delovanja informacijske infrastrukture na primarni lokaciji. Težave izvirajo predvsem iz tega, kako prepričati odgovorne osebe v organizaciji in managerje, da je za zagotavljanje informacijske podpore potrebno nenehno zagotavljati investicijska sredstva. Ključni problemi izhajajo iz dejstva, da je tako infrastruktura kot tudi osebje prevečkrat prekomerno obremenjeno, kar vodi k slabšanju kakovosti storitev, manjšanju razpoložljivosti virov in zagotavljanje učinkovitega sistema za upravljanje informacijske varnosti. Dejstvo je, da viri naraščajo linearno, potrebe po učinkoviti informacijski infrastrukturi in s tem sami stroški pa so eksponentnega značaja.
- Razvojni problemi, ki so posledica zapiranja posameznih institucij vase. Organizacije pri odločitvah o lastni informacijski infrastrukturi ne upoštevajo ekonomske logike niti ne opravljajo osnovnih analiz ekonomičnosti projektov. Za večje informacijske sistem velja, da jih je smiselno združevati v skupnih centrih, saj obratovalni stroški (prostori, neprekinjeno napajanje, varovanje, obnova poslovanja,...) z večanjem obsega storitev sorazmerno padajo.
- Problemi konsolidacije, kar je posledica neprimernega načrtovanja informacijskih sistemov. Veliko institucij se sooča s problemom nekonsolidiranih podatkovnih zbirk, ki po nepotrebnem uporabljajo proste sistemske kapacitete. Tako zavirajo nemoteno in neprekinjeno delovanje informacijskega sistema, s čimer pa povečujejo potrebe po nepotrebne investiranju v povečevanje sistemskih zmogljivosti.
- Ostali problemi: Rast števila uporabnikov, transakcij in storitev narašča z bistveno višjo stopnjo rasti od planirane, zato so potrebne investicije v širitev obstoječe infrastrukture. Zanemarjanje vlaganja v povečanje zmogljivosti lahko bistveno

prizadene kritične informacijske sistem in povzroči nezadovoljstvo med uporabniki storitev.

Vse to so zgolj nekateri problemi, s katerimi se soočajo organizacije pri vzpostavitvi projekta zagotavljanja neprekinjenega poslovanja. Zagotovo bi vsak, ki se je kadarkoli soočil z vpeljavo sistema neprekinjenega poslovanja v različne organizacije, dodal k temu še svoje videnje in bi tako po določenem času prišli do nekakšne celote. Na tej osnovi bi se lahko nato pripravila temeljita metodologija vzpostavitve neprekinjenega poslovanja v različnih organizacijah, kajti do sedaj enotne metodologije, ki bi se je izvajalci lahko posluževali pri vgradnji neprekinjenega poslovanja v organizacijsko strukturo organizacije ni bilo.

# 6 SKLEP

Učinkovitost in uspešnost poslovanja sodobnih organizacij sta iz leta v leto bolj odvisni od kakovostne in nemotene informacijske podpore, pri čemer postajajo razlike med pridobitnimi, nepridobitnimi, velikimi in manjšimi organizacijami čedalje manjše. Zato imajo že krajši izpadi informacijskega sistema precejšnje posledice na poslovanje, medtem ko lahko dlje trajajoči izpad ali trajna izguba podatkov postavita obstoj organizacije na kocko. V primerih, da se kaj takega zgodi v javnih institucijah, ima to lahko mnogo širše negativne posledice, ki lahko v zelo kritičnih primerih resno ogrozijo delovanje in celo obstoj države.

Izdelava načrta neprekinjenega poslovanja je ključnega pomena za nadaljevanje poslovanja organizacije po nepredvidenih dogodkih in katastrofah. Če družba nima tega načrta ali če je neustrezen, lahko pride do izgube njenega ugleda ali celo prekinitve njenega poslovanja.

Zato so v organizacijah na nekaterih področjih, kot so: bančništvo, vladne organizacije, telekomunikacije ipd., začeli poslovne informacijske sisteme obravnavati kot kritično infrastrukturo, za katero je treba tudi z zakonsko regulativo zagotoviti ustrezno preventivno delovanje, katerega namen je zagotoviti varnost podatkov in delovanje informacijskega sistema v izrednih situacijah. Vendar pa se tudi pri organizacijah, ki sicer ne sodijo v katero od kritičnih področij, vse pogosteje uveljavlja prepričanje, da je treba vzpostaviti možnosti za zagotavljanje informacijske podpore poslovanja, čeprav se problema marsikje lotevajo dokaj pomanjkljivo.

Pri zagotavljanju delovanja informacijskih sistemov se je v zadnjih desetih letih zgodil pomemben premik z razmišljanja od zgolj okrevanja sistema po nesreči proti zagotavljanju neprekinjenega poslovanja. Vzrok za to je širitev informacijske podpore na čedalje širši segment poslovanja, zaradi česar so postali informacijski sistemi tako zapleteni, da stari okrevalni postopki niso več primerni. S tem premikom se je odgovornost za uvajanje rešitev začela seliti s tehničnega na organizacijsko oziroma poslovno področje. Ker pomeni poslovni informacijski sistem bistveni povezovalni element poslovanja sodobne organizacije, je treba pripravo organizacije na nepredvidene dogodke začeti prav pri načrtu zagotavljanja delovanja njenega informacijskega sistema.

Uvedba rešitve zagotavljanja neprekinjenega poslovanja je tehnološko in procesno zahteven projekt. Poleg kadrovskih virov in finančnih sredstev zahteva tudi veliko časa, izkušenj, analiziranja, načrtovanja ter vztrajnosti.

Mnogo ljudi meni, da je načrtovanje za primer katastrofe nepotrebno, če ima organizacija sklenjene prave vrste poslovnih zavarovanj. Dejstvo je, da ima zavarovanje pomembno vlogo pri financiranju obnove in blaži nekatere stroške, ki se pojavijo pri nesreči. Lahko zamenjamo opremo, pripravimo nove prostore ali obnovimo osnovno lokacijo, obnovimo telekomunikacijsko omrežje, ne moremo pa dobiti izgubljenih podatkov. Če organizacija nima (ustreznega) načrta neprekinjenega poslovanja, mora razmisliti o tem, ali si lahko privošči prekinitev poslovanja v primeru katastrofe, ki ji onemogoči poslovanje. Zato si mora prizadevati za omejitev tveganj v primerih, ko nesreče ali katastrofe vplivajo na izvajanje ključnih poslovnih funkcij v instituciji.

Prvi korak, ki ga je treba narediti, sta analiza tveganja in analiza vpliva na poslovanje. Z njima je treba ugotoviti, kakšne nevarnosti pretijo delovanju posameznih delov informacijskega sistema in kakšne posledice ima izpad posameznega dela ter s tem posameznega poslovnega procesa na poslovanje organizacije. Ta korak je hkrati dobrodošla priložnost za pregled poslovnih procesov, oceno primernosti informacijske podpore ter pregled obstoječih zaščitnih in varnostnih mehanizmov v organizaciji. Analizi sta pomembni saj je prav od njunih izsledkov odvisno, v kakšnem obsegu, če sploh, se bodo izvajalo ukrepi za zagotavljanje delovanja informacijskega sistema v organizaciji.

Če se podatki v nesreči izgubijo, arhivirani podatki pa so neustrezni ali jih sploh ni, se delo v družbi ne more nadaljevati nemoteno. Zato je treba izdelati načrt izdelave varnostnih kopij in sproti izdelovati varnostne kopije podatkov, ki so potrebni za nemoteno poslovanje organizacije. Pri tem je treba upoštevati zakonske in druge predpise o arhiviranju podatkov. Vse druge dejavnosti, ki so sestavni del načrta neprekinjenega poslovanja, so v primerjavi z načrtom okrevanja drugotnega pomena. Če se podatki izgubijo, so izgubljeni za vedno.

Ključ do uspešnega načrta neprekinjenega poslovanja ni njegovo razvijanje, ampak sprotno vzdrževanje. Odgovornost za vzdrževanje načrta neprekinjenega poslovanja je naloga vseh, ki so odgovorni za izvajanje vsakodnevnih poslovnih procesov.

Uvajanje pogojev za zagotavljanje delovanja poslovnega informacijskega sistema nikakor ni ne lahka in ne poceni naloga. Vendar pa se je treba zavedati, da sta trajna izguba podatkov ali daljša prekinitev poslovanja zaradi izpada informacijske podpore za organizacijo lahko še neprimerno dražji, v nekaterih bolj izpostavljenih primerih pa tudi usodni.

# LITERATURA


1. Adams Tony: Satisfaction Varies With Experience in Outsourced Business Continuity and Disaster Recovery Services. B.k. : Gartner Research IPS WW-UW-0116. 19.06.2003.
2. Andolšek Irena: Namen načrta neprekinjenega poslovanja. Revizor, Ljubljana 10(2001), 11, str. 18-30.
3. Barnes C. James: A Guide to Business Continuity Planning. Chichester: John Wiley & sons Ltd, 2001. 171 str.
4. Calvert Michael: A Site Selection Checklist for Moving Your Data Center. Inside Gartner This Week, New York, 17(2001), 44, str. 9-10.
5. Calvert Michael: Disaster Recovery Needs Document Management. Inside Gartner This Week, New York, 18(2002), 7, str. 10-12.
6. Claunch C. Management Update: Best practices in Business Continuity and Disaster Recovery. B.k. : Gartner Article IGG-03172004-01, 2004.
7. Hall Mark: IT Watchfulness Rises, But Budgets Limit Change. Computerworld, Framingham, 36(2002), 37, str. 6.
8. Hoffman Thomas: Economy caps Security Spending. Computerworld, Framingham, 36(2002), 37, str. 48.
9. Hunton E. James. Core Concepts of Information Technology Auditing. New York : John Wiley & Sons, 2004, 282 str.
10. Gallagher Michael. Business Continuity Management; How to protect your company from danger. Edinbourgh : Prenctice Hall, 2003, 172 str.
11. Kajić Milan: Varnostna politika in načrtovanje ukrepov za izredne razmere pri varovanju IS. Organizacija, Kranj, 32(1999), 7, str. 397-402.
12. Kern R.F.: IBM Storage Infrastructure for Business Continuity. Arizona, IBM Systems Group, 2003. 37 str.
13. Lam Wing: Ensuring Business Continuity. IT Pro, Tokio, May/June 2002, str. 20-25.
14. Levitt Alan M.: Disaster Planning and recovery: A guide fo facility professionals. New York: John Wiley & Sons, 1997. 417 str.
15. Malik William: A process Approach to business Continuity Planning. B.k. : Gartner research COM-14-4299, 2001.
16. Neil David: Anticipate the need for Resilience: One Company That Did. B.k. : Gartner Reasearch CS-14-9815, 2001.
17. Noakes–Fry Kristen, Diamond Trude: Business Continuity Planning Software: Technology Overview. B.k. : Gartner Research DPRO-100469, 2003.
18. Rihar Boštjan: Uvajanje pogojev za zagotavljanje delovanja poslovnega informacijskega sistema. Magistrsko delo. Ljubljana : Ekonomska fakulteta Univerze v Ljubljani, 2003. 84 str.
19. Scott Donna. Enlightening the CEO on Business Continuity Planning. B.k. : Gartner Tutorial TU-07-7202, 2002.

20. Smith D.J.: Business Continuity and crisis management. Management quarterly,Worchester, The Business Continuity Institute, 2003, 18, str. 27-33.
21. Smith D.J.: Business Continuity Management: Good practise Guidlines. Worchester : The Business Continuity Institute, 2002, 287 str.
22. Swanson Marianne, Wohl Amy: Contingency Planning Guide for Information Technology systems. Washington : National Institue of Standard and Technlology (NIST), 2002, 92 str.
23. Šalehar-Kegl Dušan, Zupan Lucija: Praktični pristopi k vpeljavi neprekinjenega poslovanja in izkušnje PDC, Zbornik referatov INDO 2004: Posvetovanje informatikov v državni upravi, Portorož, Center Vlade za Informatiko, 2004. 12 str.
24. Toigo Jon William: Disaster Recovery Planning: For computer and communication resources. New York : John Wiley & Sons, 1996. 329 str.
25. Toigo Jon William: Disaster Recovery planning: strategies for protecting critical information. 2. izdaja. Upper Saddle River : Prentice Hall, 2000. 432 str.
26. Verton Dan: Disaster Recovery Planning Still Lags. Computerworld, Framingham, 36(2002a), 14, str. 8.
27. Verton Dan: Corporate America on Front Lines of War on Terror. Computerworld, Framingham, 36(2002b), 37, str.7.
28. Warrick Cathy, Sing John: A disaster Recovery Solution Selection Methodology; IBM Redpaper. NewYork, IBM Redbooks: 2001. 67 str.
29. Wheatman Vic: Afermath: Disaster Recovery. B.k : Gartner Research AV-14-5238, 2001. 28 str.
30. Witty Roberta: Best Practices in Business Continuity Planning. B.k : Gartner Reasearch AV – 14 – 5213, 2001. str. 21.
31. Witty Roberta: Gartner 360°: Securing Your future Through Business Continuity Planning. Gartner Symposium ITxpo, Orlando, 2002a.
32. Witty Roberta: Integrating BCP into the IT Project Life Cycle. B.k : Gartner Tutorial TU 13-8386, 2001b.

## VIRI

1. Best Practices: Disaster Recovery and Business Continuity Planning, Stamford, Meta Group, 2004.
2. Breunhoelder Gert: IT Business Continuity & Recovery Planning; Berlin, IBM Global services, 2002.
3. BS ISO/IEC 17799:2000 Information Technology – Code of practice for information security management, London: British standards Institution (BSI), 2001.
4. Burazer Renato, Golob Pavle: Načrt neprekinjenosti poslovanja – tehničnih vidik postavitve in preizkušanja, Čatež, september 2004.
5. Business Continuity Planning-IT examination Handbook, Washington, Federal Financial Institutions Examination Council (FFIEC), 2003.

6. Datamonitor: Business Continuity – be resilient, be reliable, be ready for anything. [URL: http://www.datamonitor.com], november 2003.
7. Eagle Rock Alliance: 2001 Cost of Downtime
[URL: http://www.contingencyplanningresearch.com], 2003.
8. Hiles Andrew: Business Impact Analysis: What's Your Downside?.
[URL: http://www.rothstein.com/articles/busimpact.html], 2002.
9. Interna gradiva proučevane institucije.
10. Lucent Technologies. Corporate Security: Business Continuity and Disaster Recovery post 9/11. [URL: http://physorg.tradepub.com/free/w_lu05/].
11. Priporočila za pripravo informacijske varnostne politike. Ljubljana: Center vlade za informatiko. [URL: http://www.gov.si/cvi], 2003.
12. Publicly Avalilable Specification (PAS) 56; Guide to Business Continuity Management, London : British standards Institution (BSI), 2002.
13. Vozlič Andrej: Pomen revizije informacijskih sistemov v gospodarskih družbah [URL:http://www.rr-co.si/slike/Pomen_revizije_IS.pdf], 2003.
14. Vozlič Andrej: Varovanje informacij
[URL:http://www.rr-co.si/slike/varovanje_informacij.pdf], 2002.
15. Težak Boris. Celovito obvladovanje tveganj Ljubljana, Slovenski inštitut za revizijo.
[URL:http://www.si-revizija.si/isaca/slo/datoteke/celovito_obvladovanje.pdf], 2002.