UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

Metode razvoja visoko razpoložljivih informacijskih sistemov

Ljubljana, december, 2006 Peter Cvar

IZJAVA

Študent Peter Cvar izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Mira Gradišarja in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 18.12.2006

Podpis: _____

Kazalo:

Kazalo slik:

Kazalo tabel:

1. Uvod

1.1. Opredelitev problema

Živimo v informacijski dobi. To je čas, v katerem informacijska tehnologija nima več statusne vrednosti, temveč predstavlja tako posamezniku kot podjetjem osnovo, brez katere je praktično nemogoče uspešno funkcionirati. Mnoga podjetja so z informacijsko tehnologijo neločljivo povezana in si ne morejo predstavljati svojega obstoja in delovanja brez nje. Nihče se več ne sprašuje ali so vlaganja v informatizacijo smiselna. Namesto tega se postavlja vprašanje, kako jo čim bolje izkoristiti, približati poslovanju in jo narediti učinkovitejšo, zanesljivejšo in razpoložljivejšo (Khosrow, 2005, str. 1317). Usodnega 11. septembra 2001 je z grozljivim napadom na ameriški Svetovni trgovinski center pojem razpoložljivosti dobil povsem nove razsežnosti. Poleg vseh grozot terorističnega napada je dogodek razkril tudi situacijo, o kateri se ni na veliko pisalo v medijih, je pa povzročila nemalo skrbi med strokovnjaki informacijske tehnologije. V do tal uničenih stavbah je imelo informacijske sistemske prostore kar nekaj podjetij in mnoga izmed njih po tragediji niso uspela obnoviti svojih virov (Jolly, 2003, str. 13).
Teroristični napad na ameriška nebotičnika je bil skrajno dejanje, ki ga v Sloveniji (morda naivno) res ne pričakujemo, vendar lahko do izpada delovanja informacijskega sistema privedejo tudi za naše okolje veliko bolj običajni dogodki. Do izpada lahko pride zaradi poplav, potresov, požarov, človeških napak, izpusta vode iz napeljave, okvar strojne in programske opreme (Bakshi, 2006, str. 471). Prekinitve v delovanju informacijske opreme so lahko načrtovane ali nenačrtovane. Načrtovane prekinitve so posledica vzdrževalnih dogodkov, med katere spadajo nadgradnje, popravki in arhiviranje. Do nenačrtovanih prekinitev pa pride zaradi napak v strojni ali programski opremi (Vargas, 2000, str. 2). Vsak izpad delovanja predstavlja za podjetje visoke stroške, ki so tako direktno merljivega kot tudi nemerljivega značaja. Med direktno nemerljive vrednosti spada izguba ugleda podjetja in zmanjšanje zaupanja pri strankah. Predvsem slednje je izredno težko povrniti, ko je enkrat omajano (Toigo, 1996, str. 107).
Zaradi vsega naštetega se pojavlja potreba po izgradnji visoko razpoložljivega informacijskega sistema, ki čas nedelovanja zaradi izpada zmanjša na najnižjo možno vrednost.
Investicije v informacijske sisteme, ki zagotavljajo visoko razpoložljivost, so zelo visoke, zato mora vsako podjetje oceniti svoje maksimalne in minimalne potrebe razpoložljivosti in na njihovi osnovi izbrati strategijo, ki še izpolnjuje njihove zahteve.
Izdelati je treba temeljito analizo obstoječe situacije, v kateri se identificira kritične komponente in resurse, brez katerih poslovanje ni mogoče (Maiwald, Sieglein, 2002, str. 180). Potrebno je izdelati okrevalni načrt, ki ga lahko podjetje izdela samo ali pa njegovo izdelavo zaupa zunanjim strokovnjakom. V načrtu so zajeti vsi potrebni podatki in postopki, ki jih je v primeru nesreče potrebno izpeljati (Baschab, Piot, 2003, str. 162).
V Sloveniji so na področju zagotavljanja visoke razpoložljivosti delovanja informacijskega sistema največ storila finančna podjetja. V to so jih vodili sklepi Banke Slovenije, objavljeni v Uradnem listu št. 52/2000. V skladu s sklepi so vse banke in hranilnice dolžne upoštevati standard ISO/IEC 17799. S tem standardom so podjetja dolžna ščititi svoje poslovanje pred izpadom, ki je posledica napak in nesreč.
V zadnjem času se vse več slovenskih podjetij odloča za izgradnjo rezervnega informacijskega centra. Glede na to, da se njegova prava vrednost pokaže šele v primeru izpada primarnega centra, je potrebno vložiti precej truda in angažirati najvišje vodstvo podjetja, ki mora izvedbo neomajno podpirati, sicer se lahko zgodi, da projekt, ki ne kaže takojšnih rezultatov, kmalu zvodeni (Gallagher, 2003, str. 55).

Obstajajo številni pristopi in metode uvajanja sistemov visoke razpoložljivosti. Izbira ustrezne metode je odločilnega pomena za uspeh projekta.

1.2. Namen in cilj magistrskega dela

Z magistrskim delom želim predstaviti razloge, ki vodijo v izgradnjo informacijskega sistema z visoko razpoložljivostjo delovanja. Pri tem se bom opiral tako na priporočila krovnih institucij in standardov, kot tudi na razloge, ki izhajajo iz samega poslovanja podjetja.

Namen magistrskega dela je predstaviti teoretične osnove in različne metode razvoja visoko razpoložljivih informacijskih sistemov, jih med seboj primerjati in podati ugotovitve.

Glede na to, da v Sloveniji ne obstaja literatura, ki bi se nanašala na omenjeno problematiko, sem se namenil prikazati praktični primer izdelave načrta za neprekinjeno poslovanje, ki lahko služi kot model vsem podjetjem, ki se v vode visoke razpoložljivosti in neprekinjenosti poslovanja šele podajajo in taka podjetja so pri nas v večini.

Končni cilj magistrskega dela je funkcionalni načrt neprekinjenega poslovanja za konkretno podjetje.

1.3. Metode dela

Pri izdelavi magistrske naloge bom uporabil znanje, pridobljeno med študijem, ki ga bom dopolnil z večletnimi lastnimi izkušnjami na izbrani tematiki.

V prvem delu bom uporabil deskriptivno metodo na osnovi lastnih izkušenj ter člankov in literature tujega in domačega porekla. Pomagal si bom z internimi viri podjetij in principalov. Uporabil bom tudi analitični pristop, ki bo temeljil na osnovi poizvedovalne raziskave. Z metodo primerjalne analize bom primerjal temeljne metode za izgradnjo visoko razpoložljivega informacijskega sistema.

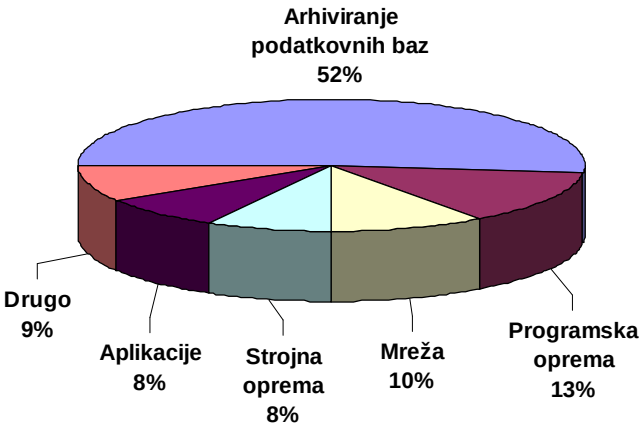
V drugem delu se bom posvetil konkretnemu primeru. Z empiričnim pristopom bom teoretični prikaz iz prvega dela dopolnil s praktičnim primerom.

2. Vzroki za izpad poslovanja

Zaradi tesne povezanosti informacijskega sistema z glavno dejavnostjo podjetja predstavlja izpad delovanja informacijskega sistema največkrat tudi izpad primarne funkcionalnosti podjetja, zato ga je praktično nemogoče ločiti in obravnavati samostojno. Nesreča, ki ogrozi delovanje informacijskega sistema, direktno ali indirektno ogroža celotno poslovanje podjetja.
Za potrebe tega magistrskega dela je nesreča definirana kot vsaka nenačrtovana prekinitev delovanja informacijskega sistema ali njegovega bistvenega dela za čas, ki je daljši od za podjetje še sprejemljivega (Toigo, 1996, str. 1).
Z vidika informacijske tehnologije se prekinitve delijo na nenačrtovane in načrtovane prekinitve oz. nesreče (Brooks, 2002, str. 5). Po raziskavi podjetja IBM je 90 odstotkov vseh prekinitev načrtovanih (slika 1). Razlog načrtovanih prekinitev so razne podporne,

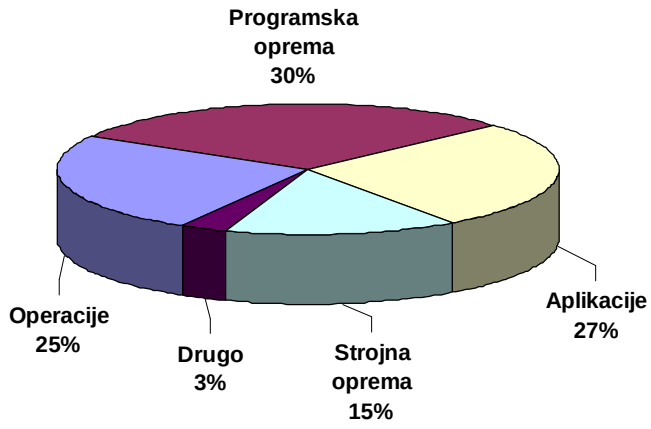
preventivne in vzdrževalne dejavnosti, med katere spada arhiviranje podatkovnih baz, vzdrževanje računalniških mrež, aplikacij ter strojne in programske opreme.
Nenačrtovane prekinitve zavzemajo približno 10 odstotkov vseh prekinitev (slika 2). Vzroki nenačrtovanih prekinitev so najpogosteje programske in aplikativne narave. Sledijo prekinitve, ki jih s svojimi namernimi ali nenamernimi posegi povzroči človek, in okvare na strojni opremi. Najmanjši, vendar najbolj uničujoč del prekinitev predstavljajo druge nesreče, med katere spadajo potresi, poplave, požari, zmrzal, snežni meteži, viharji, orkani in druge katastrofe.

Slika 1: **Načrtovane prekinitve v delovanju IT**



Vir: Brooks, 2002, str. 5

Slika 2: **Nenačrtovane prekinitve v delovanju IT**



Vir: Brooks, 2002, str. 5

3. Statistična dejstva in raziskave

Nekaj različnih statistični podatkov in dejstev, ki govorijo v prid izvedbe visoko razpoložljivega informacijskega sistema in ustreznega okrevalnega načrta (Moskal, 2006):

- Samo v letu 2004 se je zgodilo 68 katastrofalnih nesreč (FEMA, 2005).
- Avgusta 2003 je severno vzhodni del Združenih držav Amerike ostal brez elektrike. Brez energije in komunikacij se je znašlo 50 milijonov ljudi. Ekonomski strošek je znašal med 7 in 10 milijardami ameriških dolarjev (ICF Consulting, 2004).
- Samo nekaj minut po tem, ko je 11. septembra, 2001 prvi avion zadel nebotičnik v New Yorku, je več kot 200 podjetij razglasilo katastrofo in začelo izvajati svoje okrevalne načrte (Gartner, 2003).
- Dve od petih podjetij, ki doživijo katastrofalno nesrečo, propadeta v roku petih let (Gartner, 2004).
- Skoraj polovica podjetij, ki izgubijo podatke v nesreči, poslovanja ne uspe obnoviti. 90 odstotkov jih propade v roku dveh let (Univerza v Teksasu, Center za raziskovanje informacijskih sistemov, 2004).
- 43 odstotkov podjetij, ki doživijo katastrofalno nesrečo, poslovanja nikoli ne obnovijo in 29 odstotkov jih propade v roku dveh let (McGladrey in Pullen, 2004).
- 80 odstotkov podjetij brez okrevalnega načrta je v primeru katastrofalnih poplav ali požara prisiljeno zaključiti s poslovanjem v roku 12 mesecev (Londonska zbornica za trgovino in industrijo, 2003).
- Od 850 vzorčnih srednje-velikih in velikih globalnih podjetij jih je imelo 60 odstotkov nenačrtovane izpade, ki so trajali od ene ure do enega dneva (Veritas, 2003).

Rezultati ankete, ki jo londonski pooblaščeni inštitut za upravljanje (Chartered Management Institute) že od leta 1999 izvaja vsako leto med 440 naključno izbranimi vodilnimi kadri, kažejo na to, da smatra večina anketiranih za največjo grožnjo svojega podjetja prav izpad delovanja informacijskega sistema (tabela 1).

Tabela 1: **Seznam groženj, ki lahko vplivajo na poslovanje podjetja.**

N=440	1999 (%)	2001 (%)	2002 (%)	2003 (%)	2004 (%)	2005 (%)
Izpad IT	78	82	46	58	60	70
Izpad telekomunikacij	-	-	-	-	62	64
Požar	45	62	32	51	53	56
Izguba znanja	37	59	43	51	48	56
Izguba ljudi	-	-	-	54	48	55
Izguba prostorov	33	55	32	54	51	53
Terorizem	22	30	23	47	48	53
Izguba ugleda	41	50	40	46	48	48
Slaba reklama	34	43	37	45	46	44
Zdravje zaposlenih	22	30	22	35	34	35
Okoliški pripetljaji	20	19	19	26	23	35
Izguba dobaviteljev	-	-	25	34	32	35
Poplava ali vihar	18	29	9	24	25	29
Varnost produktov	19	21	22	25	26	27
Vojaški konflikti	-	-	-	16	24	27
Protesti	7	14	9	14	27	20

Vir: Business Continuity Management, 2005, str. 2

Na vprašanje katera vrsta prekinitve je bila v preteklem letu najbolj pogosta se je večina anketiranih ponovno izrekla za izpad informacijskega sistema (tabela 2).

Tabela 2: **Seznam groženj, ki so v preteklem letu vplivale na poslovanje podjetja.**

N=440	1999 (%)	2002 (%)	2003 (%)	2004 (%)	2005 (%)
Izpad IT	6	19	24	25	41
Izguba ljudi	-	-	26	20	28
Izpad telekomunikacij	-	-	-	23	25
Izguba znanja	1	33	16	14	20
Poplava ali vihar	4	18	15	10	18
Zdravje zaposlenih	0	13	9	8	19
Slaba reklama	2	24	17	16	17
Izguba prostorov	2	5	5	6	11
Izguba ugleda	1	15	7	8	11
Izguba dobaviteljev	-	19	11	12	10
Okoliški pripetljaji	2	9	5	4	7
Varnost produktov	1	11	6	4	6
Protesti	1	10	7	7	6
Požar	2	6	5	5	5
Vojaški konflikti	-	-	2	5	4
Terorizem	1	2	1	1	2

Vir: Business Continuity Management, 2005, str. 3

3.1. Analiza stanja v Sloveniji

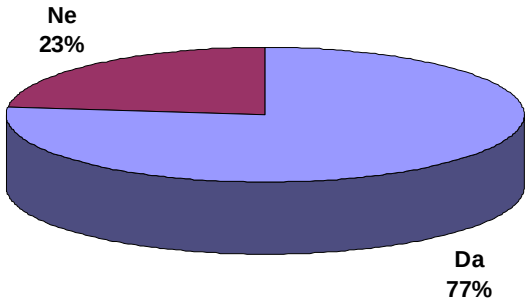
Tudi v Sloveniji smo priča različnim nesrečam, katastrofam in informacijskim izpadom. Spomnimo se le požarov v tovarnah kot so Gorenje, Steklarna Rogaška Slatina in Color Medvode. V začetku letošnjega leta je prišlo zaradi računalniške napake do enodnevnega izpada poslovanja v eni večjih slovenskih bank. Novica je bila objavljena v vseh medijih. Zadnji večji primer je bil večurni izpad delovanja vseh bankomatov v državi.

Da bi ugotovil stanje na področju razpoložljivosti informacijskih sistemov v slovenskih podjetjih, sem v prvi polovici meseca novembra, 2006 opravil anonimno poizvedovalno anketo. Izdelal sem spletno anketno aplikacijo (http://www.anketa.gallart.net) in k sodelovanju povabil predstavnike informacijskih oddelkov iz pomembnejših srednje velikih in velikih slovenskih podjetij. Na vabilo se je odzvalo 68 predstavnikov vodilnih slovenskih podjetij, ki poslujejo na različnih področjih. Imena vseh podjetij, ki so sodelovala v raziskavi, se nahajajo na spletnem naslovu http://www.anketa.gallart.net/ rezultati.htm.

Zastavljena vprašanja in rezultati poizvedovalne ankete:

1. »*Ali je v vašem podjetju v preteklosti že kdaj prišlo do okvare ali izpada bistvenega dela informacijskega sistema in je zato trpelo poslovanje podjetja?*«

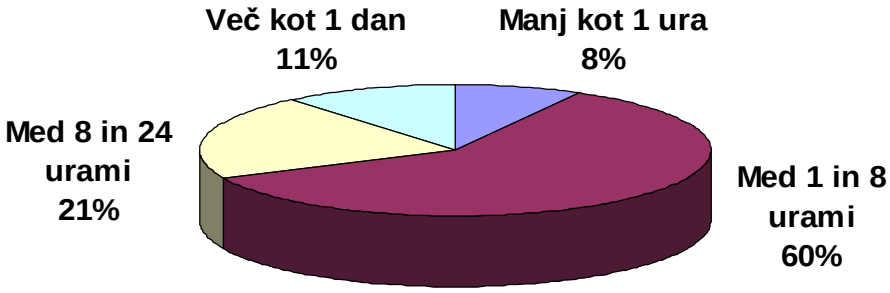
Slika 3: **Delež slovenskih podjetij, ki so se že srečala z izpadom IT**



Vir: Lasten

2. »*Če je odgovor na prejšnje vprašanje DA: kako dolgo je trajal najdaljši izpad?*«

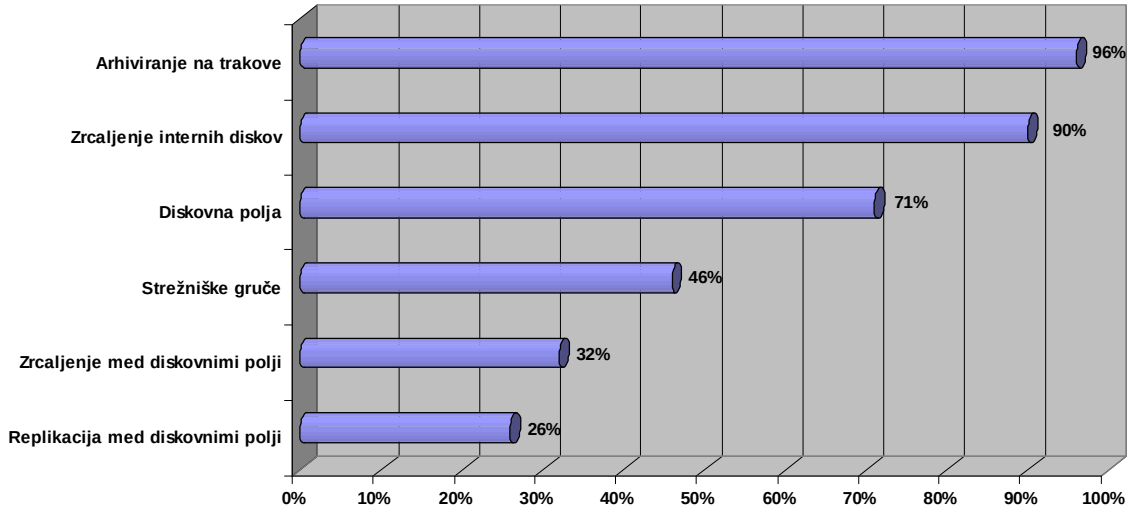
Slika 4: **Trajanje izpada IT v slovenskih podjetjih**



Vir: Lasten

3. *»Kakšne postopke v podjetju uporabljate za varovanje in shranjevanje podatkov?«*

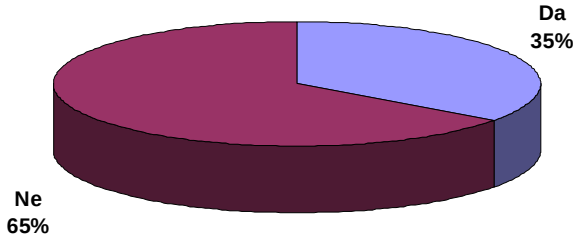
Slika 5: **Postopki za varovanje in shranjevanje podatkov v slovenskih podjetjih**



Vir: Lasten

4. *»Ali ima vaše podjetje rezervno lokacijo, na kateri je mogoče vzpostaviti funkcionalnost informacijskega sistema, če pride do izpada delovanja le-tega na primarni lokaciji?«*

Slika 6: **Delež slovenskih podjetij, ki imajo rezervno lokacijo za IT**

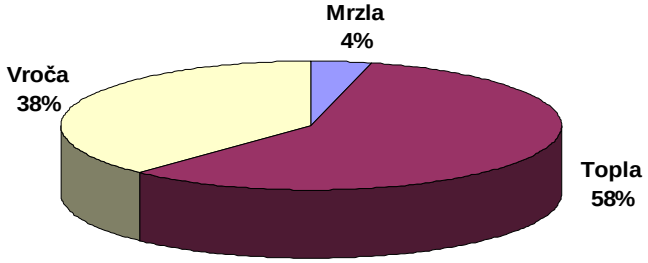


Vir: Lasten

5. *»Če je odgovor na prejšnje vprašanje DA: kakšnega tipa je rezervna lokacija?«*

- *Mrzla lokacija ni opremljena. Pridobitev, namestitev in priprava strojne in programske informacijske opreme lahko traja več tednov.*
- *Topla lokacija ima nekaj najpotrebnejše strojne in, programske opreme že nameščene. Pridobitev in namestitev manjkajoče opreme lahko traja nekaj dni do dveh tednov.*
- *Vroča lokacija je v celoti opremljena in pripravljena za uporabo. Tako lokacijo je mogoče aktivirati v nekaj urah.*

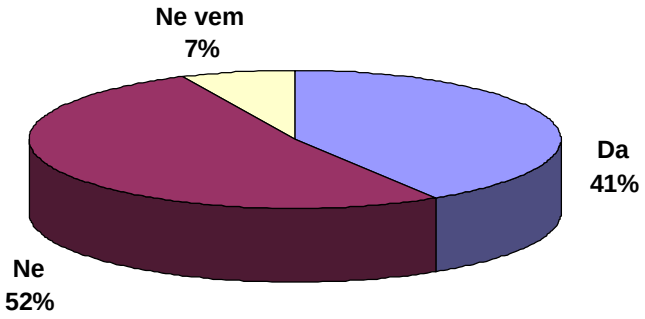
Slika 7: **Tip rezerve lokacije za IT**



Vir: Lasten

6. *»Ali ima vaše podjetje izdelan dokument oz. načrt neprekinjenega poslovanja, ki eksplicitno navaja postopke ravnanja v primeru izpada delovanja informacijskega sistema?«*

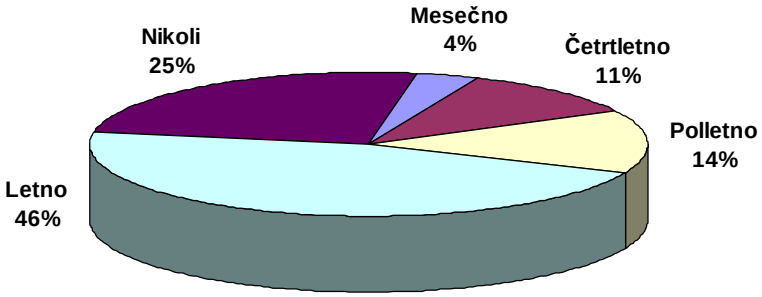
Slika 8: **Delež slovenskih podjetij z izdelanim NNP**



Vir: Lasten

7. *»Če je odgovor na prejšnje vprašanje DA: kako pogosto kontrolirate ali preizkušate načrt neprekinjenega poslovanja?«*

Slika 9: **Pogostost preizkušanja NNP v slovenskih podjetjih**



Vir: Lasten

Iz rezultatov je razvidno, da sta se dve tretjini slovenskih podjetij, ki so sodelovala v raziskavi, v preteklosti že srečali z večjimi okvarami informacijskih sistemov, ki so bistveno vplivale na poslovanje podjetja (slika 3). V 60 odstotkih so bili izpadi zaradi okvar daljši od ene ure in krajši od osem ur (slika 4). Rezultati so pokazali, da skoraj vsa podjetja uporabljajo vsaj najosnovnejše oblike varovanja podatkov (slika 5). Rezervno lokacijo za informacijski sistem ima približno tretjina anketiranih podjetij (slika 6). Najpogostejša je t.i. topla rezervna lokacija, ki ima nekaj najosnovnejše strojne, programske in komunikacijske opreme že nameščene (slika 7). Pridobitev in namestitev manjkajoče opreme pa lahko traja nekaj dni do dveh tednov. Manj kot polovica podjetij ima izdelan načrt neprekinjenega poslovanja z definiranimi postopki ravnanja v primeru izpada delovanja informacijskega sistema (slika 8). Načrt najpogosteje preizkušajo enkrat letno. Četrtina anketiranih podjetij načrta neprekinjenega poslovanja ni še nikoli preizkusila (slika 9).

4. Posledice izpada delovanja

Vodstvo podjetja se pogosto srečuje z vprašanjem smiselnosti v vlaganje oz. vpeljavo visoko razpoložljivega informacijskega sistema in okrevalnega načrta. Zagovorniki ideje velikokrat smatrajo za najprimernejši način predstavitev problema s stroškovnega vidika.

Stroški, ki nastanejo zaradi izpada delovanja informacijskega sistema in s tem povezanega poslovanja podjetja, se delijo na neposredne in posredne (Hines, 2002, str. 179).

4.1. Neposredni stroški

Neposredni stroški so predstavljeni kot stroški, ki jih ima podjetje zaradi nezmožnosti opravljanja svoje primarne dejavnosti in se razlikujejo od podjetja do podjetja. V podjetju, ki se ukvarja z razvojem računalniških programov, so stroški predvsem plače visoko kvalificiranih zaposlenih programerjev. V primeru izpada informacijskega sistema lahko ostanejo programerji brez dela. V kolikor gre za veliko podjetje, lahko plače, ki jih podjetje plačuje brezdelnim delavcem, predstavljajo precejšen strošek. Če je izpad daljši in če so roki za dokončanje posameznega projekta vnaprej določeni, je potrebno zamudo nadoknaditi z dragimi nadurami. Ravnokar opisan primer izpada informacijskega sistema v programerskem podjetju pa je neprimerljiv z izpadom dejavnosti v borznem okolju. Borzni agenti lahko opravijo v enem samem dnevu več milijonskih poslov. V borznem okolju vsaka ura nedelovanja predstavlja ogromno izgubo. Posli, ki so bili zaradi nedelovanja prezrti, so lahko za vedno izgubljeni.
Stroški, ki jih imajo ameriška podjetja z vsako uro nedelovanja, so predstavljeni v tabeli 3. Stroški se s časom seveda spreminjajo, glavno vrednost raziskave pa predstavlja primerjava med različnimi panogami (Marcus, Stern, 2003, str. 35).

Tabela 3: **Stroški zaradi enournega nedelovanja posameznih dejavnosti v ZDA**

Dejavnost	Neposredni stroški zaradi enournega nedelovanja
Posredništvo, borza	$ 6,48 milijonov
Energija	$ 2,8 milijona
Kreditne kartice	$ 2,5 milijona
Telekomunikacije	$ 2 milijona
Finance	$ 1,5 milijona
Proizvodnja	$ 1,6 milijona
Finančne ustanove	$ 1,4 milijona
Trgovina	$ 1,1 milijona
Farmacija	$ 1 milijon
Kemija	$ 704.000
Zdravstvo	$ 636.000
Mediji	$ 340.000
Letalske rezervacije	$ 90.000

Vir: Marcus, Stern, 2003, str. 35

4.2. Posredni stroški

Čeravno so neposredni stroški najhitreje vidni, imajo podjetja zaradi izpada delovanja opraviti tudi s tako imenovanimi posrednimi stroški, ki so veliko težje merljivi in dolgotrajnejši (Marcus, Stern, 2003, str. 36).

Nezadovoljstvo strank
Kot primer si lahko ogledamo podjetje, ki se ukvarja s kataloško prodajo. V primeru izpada informacijskega sistema podjetje ne more izpolnjevati naročil. Ko stranka pokliče, jo uslužbenci obvestijo, da imajo težave z informacijskim sistemom in da naj poskusi kasneje.

Ker je v navadi ljudi, da ko si enkrat določeno stvar zaželijo jo hočejo tudi čimprej dobiti, stranka pokliče drugo podjetje z enako dejavnostjo. V kolikor je bila stranka s storitvijo drugega podjetja zadovoljna, se bo najverjetneje tudi v bodoče posluževala storitev tega podjetja in hkrati obveščala vse svoje znance o njihovi solidnosti. Izguba za prvo podjetje je tako večkratna.
Zlato pravilo trgovanja pravi, da je desetkrat težje pridobiti novo stranko kot zadržati obstoječo.

Slaba reklama
Nemalokrat se zgodi, da mediji izpad poslovanja podjetja zaradi želje po senzaciji povzdignejo v nebo, kar lahko močno omaja ugled podjetja. Ko je ugled podjetja načet, je uporabnike izredno težko prepričati v nasprotno.

Vrednost delnic
V medijih omajanemu ugledu podjetja navadno sledi upad vrednosti delnic.

Pogodbene obveznosti
Podjetje, predvsem pa njegovo vodstvo sta odgovorna in dolžna svojim strankam in poslovnim partnerjem zagotavljati dogovorjene usluge. V primeru izpada poslovanja se lahko podjetje sooči s tožbami, ki jih proti njemu vložijo stranke in poslovni partnerji zaradi neizpolnjenih obveznosti.
V primeru nesreče je lahko vodstvo podjetja odgovorno tudi delničarjem oz. lastnikom podjetja, ker ni poskrbelo in storilo vsega, kar bi bilo možno za premostitev izpada poslovanja ob nesreči.

Morala zaposlenih
Slaba reklama, upad vrednosti delnic in kazenske tožbe lahko zelo negativno vplivajo na moralo zaposlenih. Lahko se zgodi, da začnejo ključni zaposleni zapuščati podjetje, ostali pa se delu ne posvečajo tako zavzeto kot prej.

Ugled podjetja
Ko se razve, da so ključni zaposleni nezadovoljni in da zapuščajo podjetje, se ugled podjetja dodatno poslabša. Slabe novice zmanjšujejo ugled podjetja, nizek ugled pa še dodatno poslabša razmere znotraj podjetja.

Ostali posredni stroški
Med posredne stroške spadajo tudi zamude pri poslovnem obračunavanju, stroški zaradi izgubljenih poslovnim priložnostim, kazni zaradi neoddanih davčnih in drugih poročil, stroški zaradi neizterjanih dolgov, idr.

5. Razlogi za vpeljavo visoko razpoložljivega IS

Poleg v predhodnem poglavju opisanih negativnih posledic, ki jim je vzrok izpad delovanja informacijskega sistema in posledično s tem povezanega poslovanja podjetja, vplivajo na razvoj visoko razpoložljivega informacijskega sistema tudi drugi bolj pozitivni dejavniki (Toigo, 1996, str. 7).

Konkurenčna prednost
Informacijski sistem z visoko razpoložljivostjo delovanja je za podjetje dobra reklama, ki jo lahko marketing predstavi kot veliko zavezanost podjetja k neprekinjenemu

zagotavljanju svojih uslug. To velja še posebej za domača podjetja, ki delujejo na tujih trgih, kjer veljajo precej strožja pravila kot pri nas. Domača podjetja, ki upoštevajo pravila in zakonodajo naprednejših držav, imajo pri poslovanju v teh državah veliko prednost pred podjetji, ki teh pravil ne zadovoljujejo.

Zmanjševanje stroškov zavarovanja
Vpeljava sistema z visoko razpoložljivostjo delovanja lahko zmanjša stroške poslovanja na dva načina (Toigo, 1996 str. 7):

- Temeljita analiza tveganj, do katere pride med pripravo načrta, optimizira in zmanjša potreben obseg zavarovanj pri zavarovalnici. Brez temeljite analize tveganj se običajno zavarovanja sklepa v »paketu«, kar končne stroške močno poveča. S podatki, pridobljenimi v analizi, pa se lahko osredotoči samo na točno določena in za dano situacijo relevantna področja zavarovanj.
- Drugi način zmanjševanja stroškov zavarovanja predstavlja poudarek na preventivnem preprečevanju nesreč. Analiza tveganj in fizična namestitev proti-vlomnih in požarnih detektorjev ter sistema za avtomatično gašenje požara vpliva na zmanjšanje zavarovalnin.

Izraba rezerve lokacije
Med normalnim delovanjem informacijskega sistema je mogoče rezervno lokacijo občasno uporabljati v izobraževalne in testne namene. Tipičen primer je namestitev programskih popravkov, ki se pred namestitvijo v primarno produkcijsko okolje najprej preizkusijo na rezervni lokaciji. V kolikor se podjetje odloči, da bo rezervno lokacijo uporabljalo tudi v testne namene, je to potrebno posebej specificirati in upoštevati med izdelavo postopkovnih načrtov.

6. Zakonodaja

V zadnjih letih prihaja v senci velikih katastrof (11. september, 2001, cunami, 2004) do izraza vse več standardov, priporočil in zakonov, ki se ukvarjajo tudi s tematiko neprekinjenega poslovanja in okrevalnih načrtov ter posredno ali neposredno spodbujajo podjetja v razvoj načrta za neprekinjeno poslovanje, ki temelji na visoko razpoložljivem informacijskem sistemu.
Skladnost s temi zakoni, standardi in priporočili je postalo glavno vodilo osebju, ki se z omenjeno tematiko ukvarja (Toigo, 1996, str. 165).

V Združenih državah Amerike je 30. julija 2002 stopil v veljavo Sarbanes-Oxley zakon imenovan tudi SOx ali SarbOx. Zakon, ki vsebuje 11 poglavij in na novo določa odgovornost vodilnih pri vodenju podjetja, se v sekciji 404 posredno dotika tudi neprekinjenega poslovanja podjetja (Knowledge Leader, 2006).
V Evropi je veliko bolj znan bančni sporazum Basel II, sprejet v januarju 2001, ki ne obvezuje samo svojih članic (skupina G-10), ampak vpliva tudi na vse druge finančne institucije, ki poslujejo z njimi. Dogovor Basel II predpisuje bančnim ustanovam izvedbo okrevalnega načrta, ki zagotavlja neprekinjenost poslovanja (BIS, 2006).

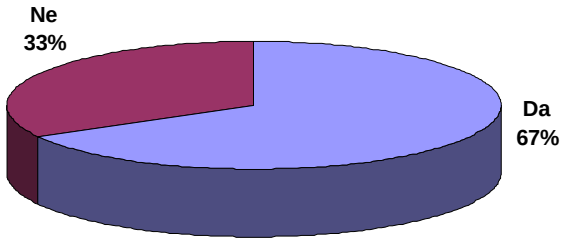
V Sloveniji je Banka Slovenije že leta 2004 izdala sklep o določitvi pogojev, ki jih mora izpolnjevati banka oziroma hranilnica za opravljanje bančnih oziroma drugih finančnih storitev. Uradni list RS, št. 38/06, določa, da mora banka v svojem poslovanju upoštevati slovenska standarda SIST BS 7799-2:2003 in SIST ISO/IEC 17799:2003, ki med drugim predpisuje izvedbo okrevalnega načrta in neprekinjenega poslovanja. Finančne in državne

ustanove ter vedno večje število podjetij v Sloveniji so že pričeli z uvajanjem standarda ISO/IEC 17799.

Iz rezultatov poizvedovalne ankete, ki sem jo opravil med vodilnimi slovenskimi podjetji, je razvidno, da slovenska finančna podjetja, glede na ostale panoge, veliko več vlagajo v razpoložljivost informacijskih sistemov. V anketi sem zajel večino slovenskih bank, zavarovalnic in hranilnic. Ko sem rezultate sortiral po panogah in se osredotočil samo na finančna podjetja, so rezultati pokazali, da ima kar dve tretjini slovenskih finančnih podjetij pripravljeno rezervno lokacijo, na kateri je mogoče vzpostaviti funkcionalnost informacijskega sistema (slika 10). Več kot devetdeset odstotkov slovenskih finančnih podjetij ima izdelan dokument, ki navaja postopke ravnanja v pimeru izpada delovanja informacijskega sistema (slika 11).

1. *»Ali ima vaše podjetje rezervno lokacijo, na kateri je mogoče vzpostaviti funkcionalnost informacijskega sistema, če pride do izpada delovanja le-tega na primarni lokaciji?«*

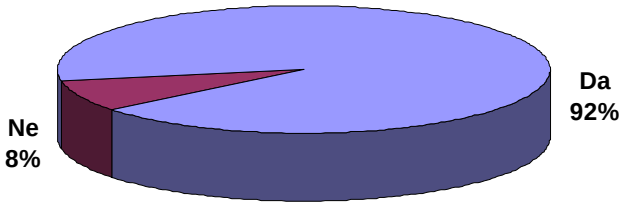
Slika 10: **Delež slovenskih finančnih podjetij, ki ima rezervno lokacijo za IT**



Vir: Lasten

2. *»Ali ima vaše podjetje izdelan dokument oz. načrt neprekinjenega poslovanja, ki eksplicitno navaja postopke ravnanja v primeru izpada delovanja informacijskega sistema?«*

Slika 11: **Delež slovenskih finančnih podjetij z izdelanim NNP**



Vir: Lasten

V nadaljevanju sledi še nekaj ameriških zakonov, ki podjetjem predpisujejo izvedbo načrta za neprekinjeno poslovanje (Sollicito, 2005).

- Zakon za odgovornost in prenosljivost zdravstvenega zavarovanja (Health Insurance Portability and Accountability Act - HIPAA) iz leta 1996, ki predpisuje, da lahko uporabniki kar se da enostavno prehajajo med zdravstvenimi zavarovalnicami, predpisuje tudi, da morajo imeti zavarovalnice izdelan načrt neprekinjenega poslovanja.
- Gramm-Leach-Bliley zakon (Gramm-Leach-Bliley Act - GLBA) iz leta 1999 določa, da morajo imeti vse finančne institucije shranjene podatke na varnem mestu tudi v primeru katastrofe.
- Federalni zakon za informacijsko varnost in upravljanje (Federal Information Security Management Act - FISMA) iz leta 2002 se nanaša na varnost vladne računalniške in mrežne opreme ter opreme vseh povezanih organizacij. Zakon predpisuje dosegljivost v primeru nesreče.
- Zakon za poklicno varnost in zdravje (Occupational Safety and Health Act - OSH) iz leta 1970 narekuje, da so podjetja in ustanove pripravljene na nevarnost (OSH, 2006).
- Zakon o razpoložljivosti vloženih sredstev (Expedited Funds Availability - EFA) iz leta 1989 predpisuje, da imajo pooblaščene federalne finančne ustanove izdelan načrt za neprekinjeno poslovanje (EFA, 2006).

V Angliji so leta 2004 predstavili civilno pobudo (Civil Contingencies Bill), ki poziva vlado in lokalno upravo, da izpeljejo postopke za neprekinjeno poslovanje (Civil Contingencies Bill, 2006). Pričakovano je, da naj bi imela ta pobuda verižno reakcijo, ki bi se odrazila tudi v poslovnem svetu. Skupaj s priporočili, standardi in direktivami naj bi pobuda nadomestila potrebo po uradnem zakonu kot je Sarbanes-Oxley.

Smoter predstavljenih zakonov in predpisov z vidika neprekinjenega poslovanja je v vseh primerih enak: podjetje mora zagotoviti, da so kritični podatki in računalniški sistemi vsak trenutek dosegljivi, kar velja tudi za primer nesreče.

7. Kontrolna ogrodja, priporočila in standardi

Najvišja vodstva podjetij se vse bolj zavedajo pomena, ki ga ima lahko informacijska tehnologija pri poslovnem uspehu podjetja. Želijo si razumeti funkcioniranje te tehnologije in njen prispevek pri doseganju konkurenčnih prednosti poslovanja, zato se pri uvajanju in optimizaciji poslužujejo uporabe preizkušenih kontrolnih ogrodij, priporočil in standardov. Z njihovo pomočjo je mogoče doseči boljšo izkoriščenost in transparentnost informacijskih sistemov. Uporabljajo se zaradi racionaliziranja stroškov za informacijske sisteme, zaradi potrebe po zadostitvi zakonov kot sta Sarbanes-Oxley in Basel II, z namenom zmanjševanja tveganja in varnostnih pomanjkljivosti informacijskih sistemov, zaradi zahtev po nadzoru kritičnih aktivnosti in z namenom večanja produktivnosti in manjšanja poslovnih tveganj. Njihova uporaba zmanjšuje potrebo po angažiranju tehnoloških ekspertov. Odpravljajo potrebo po ponovnem izumljanju že izumljenega in povečujejo zaupanje s strani vodstva, partnerjev in uporabnikov.
V nadaljevanju so opisana kontrolna ogrodja, priporočila in standardi, ki predpisujejo izgradnjo visoko razpoložljivih informacijskih sistemov in načrta za neprekinjeno poslovanje. Izpostavljeni so deli, ki se nanašajo na izvedbo visoke razpoložljivosti oz. neprekinjenosti poslovanja.
Vsa opisana ogrodja, priporočila in standardi predstavljajo temelje za vpeljavo visoko razpoložljivega informacijskega sistema. Na teh temeljih slonijo vse priznane metodologije načrtovanj neprekinjenega poslovanja.

7.1. COBIT 4.0

Kontrolno ogrodje za informacijsko in z njo povezano tehnologijo (Control Objectives for Information and related Technology – COBIT) je ogrodje za informacijsko varnost, ki sta ga leta 1992 izdelala združenje za nadzor in kontrolo informacijskih sistemov (Information Systems Audit and Control Association - ISACA) in vladni inštitut za IT (IT Governance Institute - ITGI). COBIT je sklop navodil namenjen vodstvu, revizorjem in uporabnikom informacijske tehnologije z namenom maksimiziranja uporabnosti informacijske tehnologije v podjetju (COBIT, 2006).

Priročnik COBIT je bil prvič izdan leta 1996, druga izdaja je izšla leta 1998, leta 2000 je sledila tretja izdaja, danes pa se predstavlja v četrti različici, ki je izšla v decembru leta 2005. Ponuja uporabne rešitve kontrolnega modela s podporo poslovnim procesom podjetja. COBIT je orodje lastnikov poslovnih procesov za določanje odgovornosti. Temelji na predpostavki, da procesi informacijske tehnologije izrabljajo vire (aplikacije, informacije, infrastrukturo, ljudi) za zagotovitev informacij, ki jih podjetje potrebuje za doseganje svojih ciljev. Procesni model COBIT se deli na področja planiranja in

organizacije, nabave in izvedbe, dobave in podpore ter kontrole in vrednotenja (Allemon, 2005, str. 14). Področja vsebujejo 34 procesov z 215 kontrolami (Bakshi, 2006, str. 34).
Vsakemu procesu odgovarja kontrolni cilj na višjem nivoju. Smatra se, da je kontrolni sistem primeren za okolje informacijske tehnologije takrat, ko so doseženi kontrolni cilji na najvišjem nivoju. Pri doseganju teh ciljev se upoštevajo poslovne zahteve za učinkovitost, uspešnost, zaupnost, celovitost, razpoložljivost, skladnost in zanesljivost.
COBIT dobro zagotavlja kontrole IT, ima pa omejitve v zvezi z varnostjo. Njegova slabost je, da ne pove, kako kaj narediti (Hoekstra, Conradie, 2002, str. 22).
COBIT predpisuje uporabo načrta za neprekinjeno poslovanje. V zvezi z obravnavano visoko razpoložljivostjo pride najbolj do izraza informacijski kriterij razpoložljivosti. S tem kriterijem v celoti sovpadajo 4 kontrolni cilji oz. procesi. Procesi, ki v celoti sovpadajo, so: ocena tveganja IT, upravljanje sprememb, zagotovitev neprekinjenega poslovanja in upravljanje okolja (tabela 4). Kot je razvidno iz tabele 4, več procesov delno sovpada z informacijskim kriterijem razpoložljivosti.

Tabela 4: **Kontrolni cilji modela COBIT**

			Informacijski kriteriji							Viri IT			
Področja		**Procesi**	**uspešnost**	**učinkovitost**	**zaupnost**	**celovitost**	**razpoložljivost**	**skladnost**	**zanesljivost**	**aplikacije**	**informacije**	**infrastruktura**	**ljudje**
Planiranje in organizacija	PO1	Določanje strateškega plana IT	P	S						X	X	X	X
	PO2	Določanje informacijske arhitekture	S	P	S	P				X	X		
	PO3	Določanje tehnoloških smernic	P	P						X		X	
	PO4	Določitev procesov IT, organizacije in povez.	P	P									X
	PO5	Upravljanje investicij IT	P	P					S	X		X	X
	PO6	Predstavitev ciljev in usmeritev vodstva	P					S			X		X
	PO7	Ravnanje s človeškimi viri	P	P									X
	PO8	Upravljanje kakovosti	P	P		S			S	X	X	X	X
	PO9	Ocena tveganja IT	S	S	P	P	P	S	S	X	X	X	X
	PO10	Upravljanje projektov	P	P						X		X	X
Nabava in izvedba	AI1	Prepoznavanje avtomatiziranih rešitev	P	S						X		X	
	AI2	Nabava in vz. aplikativne programske opreme	P	P		S			S	X			
	AI3	Nabava in vzdrževanje tehnološke infrastruk.	S	P		S	S					X	
	AI4	Razvoj in uporaba postopkov	P	P		S	S	S	S	X		X	X
	AI5	Pridobitev IT virov	S	P				S		X	X	X	X
	AI6	Upravljanje sprememb	P	P		P	P		S	X	X	X	X
	AI7	Postavitev in določitev rešitev in sprememb	P	S		S	S			X	X	X	X
Dobava in podpora	DS1	Opredelitev in upravljanje nivoja storitev	P	P	S	S	S	S	S	X	X	X	X
	DS2	Upravljanje storitev zunanjih izvajalcev	P	P	S	S	S	S	S	X	X	X	X
	DS3	Upravljanje zmogljivosti in kapacitet	P	P			S			X		X	
	DS4	Zagotovitev neprekinjenega poslovanja	P	S			P			X	X	X	X
	DS5	Zagotovitev varnosti sistema			P	P	S	S	S	X	X	X	X
	DS6	Določitev in razporejanje stroškov		P					P	X	X	X	X
	DS7	Izobraževanje in usposabljanje uporabnikov	P	S									X
	DS8	Pomoč in svetovanje	P	P						X			X
	DS9	Upravljanje konfiguracij	P	S			S		S	X	X	X	
	DS10	Upravljanje s težavami	P	P			S			X	X	X	X
	DS11	Upravljanje podatkov				P			P		X		
	DS12	Upravljanje okolja				P	P					X	
	DS13	Upravljanje operacij	P	P		S	S			X	X	X	X
Kontrola in vrednotenje	ME1	Nadzor in ocena učinkovitosti IT	P	P	S	S	S	S	S	X	X	X	X
	ME2	Nadzor in ocena notranjih kontrol	P	P	S	S	S	S	S	X	X	X	X
	ME3	Zagotovitev zakonskih skladnosti						P	S	X	X	X	X
	ME4	Zagotovitev nadzora IT	P	P	S	S	S	S	S	X	X	X	X

P – primarno (proces popolnoma sovpada z informacijskim kriterijem)
S – sekundarno (proces delno vpliva na informacijski kriterij)
X – možna uporaba

Vir: Allemon, 2005, str. 175

Struktura procesov, ki v celoti sovpadajo z informacijskim kriterijem razpoložljivosti (PO9 – ocena tveganja, AI6 – upravljanje sprememb, DS4 – zagotovitev neprekinjenega poslovanja, DS12 – upravljanje okolja):

- PO9 - kontrola nad procesom »ocena tveganja« obravnava IT tveganja in vplive na proces poslovanja.
    - PO9.1 – povezava poslovnega in IT tveganja
    - PO9.2 – uvedba konteksta tveganja
    - PO9.3 – identifikacija dogodkov
    - PO9.4 – analiza tveganja
    - PO9.5 – odgovor na tveganje
    - PO9.6 – vzdrževanje in nadzor načrta za odgovor na tveganje
- AI6 - kontrola nad IT procesom »upravljanje sprememb« obravnava vse spremembe (nepredvideni posegi in popravki) nad aplikacijami in infrastrukturo v produkcijskem okolju, ki morajo biti formalno predpisani in kontrolirani.
    - AI6.1 – določitev standardov in procedur pri vpeljavi sprememb
    - AI6.2 - ocena vpliva sprememb, določitev prioritet in odobritev
    - AI6.3 – nepričakovane spremembe
    - AI6.4 – sledenje in obveščanje o statusu sprememb
    - AI6.5 – dokumentiranje zaključka sprememb
- DS4 - kontrola procesa »zagotovitev neprekinjenega poslovanja« obravnava neprekinjeno IT poslovanje.
    - DS4.1 – okvir neprekinjenega delovanja IT
    - DS4.2 – načrt neprekinjenega delovanja IT
    - DS4.3 – opredelitev kritičnih komponent IT
    - DS4.4 - vzdrževanje načrta neprekinjenosti delovanja IT
    - DS4.5 – testiranje načrta za neprekinjeno delovanje IT
    - DS4.6 - usposabljanje v skladu z načrtom za neprekinjeno delovanje IT
    - DS4.7 – distribucija načrta za neprekinjeno delovanje IT
    - DS4.8 – okrevanje in ponovna vzpostavitev IT
    - DS4.9 – rezervna lokacija
    - DS4.10 – izdelava poročila po obnovitvi funkcij IT
- DS12 - upravljanje okolja zagotavlja primerno okolje za zaščito ljudi in tehnoloških naprav pred nevarnostmi.
    - DS12.1 – izbira prostorov
    - DS12.2 – določitev varnostnih mer
    - DS12.3 – avtorizacija dostopa
    - DS12.4 – zaščita pred vplivi okolja
    - DS12.5 – upravljanje s prostori

7.2. ITIL 2.0

Literaturo o infrastrukturi informacijske tehnologije (Information Technology Infrastructure Library – ITIL) je leta 1980 na pobudo angleške vlade izdala centralna agencija za računalništvo in telekomunikacije (Central Computer and Telecommunication Agency – CCTA). ITIL je bil odgovor na vse večjo odvisnost od informacijske tehnologije in spoznanje, da prihaja brez standardnih postopkov, tako pri vladnih agencijah kot tudi v privatnem sektorju do vse pogostejših napak in nepotrebnih stroškov. Priporočila so objavljena v seriji knjig, od katerih vsaka pokriva svoje področje upravljanja informacijske

tehnologije. Leta 2001 se je CCTA združila v vladno trgovinsko zbornico (Office of Government Commerce - OGC). Decembra 2005 je OGC objavil novico, da pripravljajo tretjo, osveženo verzijo ITIL priporočil, ki naj bi izšla konec leta 2006. Mnoga podjetja se poslužujejo ITIL priporočil, ki vsebujejo močne smernice za razvoj procesa neprekinjenega poslovanja. ITIL je procesno naravnana metodologija, ki zagotavlja integracijo procesov IT z ostalimi procesi podjetja (Hoekstra, Conradie, 2002, str. 22).

ITIL procesi pokrivajo področji zagotavljanja in vzdrževanja storitev IT na način, ki omogoča hiter, pregleden in nadzorovan razvoj informacijske tehnologije, s tem pa je zagotovljeno ustrezno okolje, ki prinaša zmanjšanje števila prekinitev delovanja informacijske tehnologije. Na ta način je zagotovljena razpoložljivost IT podpore za ostala ključna področja delovanja podjetja (Pušnik, 2005, str. 271).

V ITIL verziji 2 so IT priporočila zajeta v osmih knjigah, ki jim je bila pred kratkim dodana še deveta, s priporočili za manjše informacijske enote.

Osrednji področji ITIL procesov sta (Rudd, 2004, str. 10):
- Zagotavljanje storitev
    - Upravljanje ravni storitev
    - Upravljanje zmogljivosti
    - Upravljanje neprekinjenosti storitev IT
    - Upravljanje razpoložljivosti
    - Upravljanje financ
- Podpora storitvam
    - Podpora uporabnikom
    - Upravljanje konfiguracij
    - Upravljanje incidentov
    - Upravljanje problemov
    - Upravljanje sprememb
    - Upravljanje verzij

Poleg njiju ITIL pokriva še pet drugih področij:
- Upravljanje aplikacij
- Upravljanje infrastrukture
- Upravljanje varnosti
- Upravljanje storitev
- Upravljanje poslovnega vidika

ITIL področje, ki se najbolj neposredno nanaša na neprekinjenost delovanja IT, je področje zagotavljanja storitev s procesoma za upravljanje neprekinjenosti storitev IT in za upravljanje razpoložljivosti.

a) Upravljanje neprekinjenosti storitev informacijske tehnologije je namenjeno zmanjševanju tveganj, ponovni vzpostavitvi delovanja storitev informacijske tehnologije v primeru nesreče ter njeno vključitev v strategije za zagotavljanje neprekinjenega poslovanja podjetja. Postopek obsega analiziranje poslovnega učinka in tveganja, možnosti za ugotavljanje neprekinjenosti delovanja, pripravo metodologije za zagotavljanje neprekinjenosti in izvedbo, testiranje, vzdrževanje in posodabljanje metodologije.

   Glavne naloge procesa za upravljanje neprekinjenosti storitev IT:
   - Priprava strategije

- Upravljanje in zmanjševanje tveganj
- Zniževanje zavarovalnin
- Skladnost z zakonodajo
- Večanje ugleda podjetja
- Povrnitev v funkcionalno stanje po izpadu

Proces upravljanja neprekinjenosti storitev IT tesno sodeluje s procesi za upravljanje ravni storitev, zmogljivosti, razpoložljivosti, konfiguracij, incidentov in sprememb.

b) Upravljanje razpoložljivosti je proces, ki se ukvarja z načrtovanjem, uvajanjem in optimizacijo razpoložljivosti IT za zadostitev poslovnih zahtev. Potrebno je ugotoviti ustrezen nivo razpoložljivosti in ga uskladiti z zmožnostmi informacijske tehnologije. Proces se ukvarja z analizo možnih okvar in jih skuša na ta način preprečiti.

Glavne naloge procesa za upravljanje razpoložljivosti:
- Razpoložljivost je določena s pogodbami o zagotovitvi storitvenega nivoja
- Zmanjševanje pogostosti in časa trajanja izpadov IT

Proces upravljanja razpoložljivosti je močno povezan s procesom za upravljanje zmogljivosti in s procesom za upravljanje problemov.

7.3. ISO/IEC 17799:2005

Danes mednarodno veljavni standard se je prvič pojavil leta 1995 kot angleški standard BS 7799. V letu 1999 se je standard razdelil v dva dela in postal bolj usmerjen v mednarodno okolje.
Mednarodna organizacija za standardizacijo (International Organization for Standardization - ISO) in Mednarodna komisija za elektrotehniko (International Electrotechnical Commission - IEC) tvorita specializiran sistem za mednarodno standardizacijo. ISO/IEC je leta 2000 skoraj v celoti povzela smernice standarda BS 7799 in izdala prvi standard za varovanje informacij z imenom ISO/IEC 17799:2000. V juliju leta 2005 so naredili zadnjo revizijo standarda in ga poimenovali ISO/IEC 17799:2005 (Guldentops, 2005, str. 15).

V oktobru istega leta je izšel tudi standard ISO/IEC 27001:2005, ki daje navodila, kako uporabljati standard ISO/IEC 17799:2005. ISO/IEC 27001:2005 je mednarodno priznan standard, namenjen vodstvenemu osebju in predstavlja model za učinkovit sistem upravljanja varovanja informacij, skrajšano SUVI (Information security management system – ISMS). Uporablja procesni pristop z naslednjimi fazami:
- Načrtuj (določi se področje, politika, ocena tveganje, načrt obravnave tveganja, izjava o primernosti)
- Stori (upravljanje s tveganji, izvedba kontrol, izobraževanje in ozaveščanje zaposlenih, odkrivanje varnostnih incidentov)
- Preveri (pregled upravljanja, notranja revizija, vodstveni pregledi, analiza trendov)
- Ukrepaj (izboljšave, sankcioniranje, preventiva in korektiva)

ISO/IEC 17799 je najmočnejši v varnosti IT, je pa nekoliko omejen s procesnega vidika. Njegova slabost je, da ne pove, kako se kaj naredi (Hoekstra, Conradie, 2002, str. 22).

Standard ISO/IEC 17799, katerega upoštevanje zahteva tudi Banka Slovenije, predpisuje izvedbo okrevalnega načrta in neprekinjenega poslovanja.

Standard ISO/IEC 17799:2005 obsega 11 temeljnih varnostnih kontrolnih področij, ki skupaj vsebujejo 39 varnostnih kategorij in eno uvodno področje z oceno tveganj in groženj (Information technology, 2005, str. 4). Varnostna kontrolna področja so:

- Varnostna politika (usmerjanje in podpora varovanja informacij s strani vodstva podjetja)
- Organiziranost varovanja informacij (upravljanje varovanja informacij podjetja)
- Upravljanje sredstev (določitev odgovornosti, klasifikacija informacij)
- Varovanje človeških virov (izobraževanje in obrazložitev varnostnih vidikov pred nastopom dela in med aktivnim delom ter določitev postopkov ob prenehanju dela)
- Fizična zaščita in zaščita okolja (zaščita pred škodo v poslovnih prostorih in informacijah in pred nepooblaščenim dostopom)
- Upravljanje s komunikacijami in s produkcijo (zagotavljanje funkcioniranja zmogljivosti za obdelavo informacij)
- Nadzor dostopa (avtorizacija, odgovornost, nadzor dostopa do informacij in virov IT)
- Razvoj in vzdrževanje informacijskih sistemov (zagotavljanje varnosti IT, preprečevanje napak in izgube informacij v aplikacijah, šifriranje)
- Upravljanje informacijskih varnostnih incidentov (poročanje o dogodkih informacijske varnosti in o pomanjkljivostih, upravljanje incidentov informacijske varnosti in izboljšave)
- Upravljanje neprekinjenega poslovanja (zagotavljanje neprekinjenega poslovanja in zaščita kritičnih procesov pred okvarami in nesrečami v informacijski tehnologiji)
- Združljivost (revizija in združljivost z zakoni, standardi in varnostno politiko)

Kontrolno področje za upravljanje neprekinjenega poslovanja predvideva vzpostavitev upravljalnega procesa, z namenom minimiziranja posledic za podjetje in obnovitev po izpadu delovanja informacijske tehnologije na še sprejemljiv nivo, s kombinacijo preventivnih in obnovitvenih kontrol (Information technology, 2005, str. 95). Do izpada delovanja informacijske tehnologije lahko pride zaradi nesreč, katastrof, okvar na opremi in zaradi namernih posegov. Opredelijo se kritični poslovni procesi in integrirajo informacijsko varnostne zahteve po neprekinjenem poslovanju z drugimi zahtevami neprekinjenega delovanja (osebje, materiali, transport, oprema, prostori).
Posledice nesreč, varnostnih napak, izpada storitvenosti in razpoložljivost so teme, s katerimi se ukvarja analiza vpliva na poslovanje. Načrt neprekinjenega poslovanja mora biti razvit za zagotovitev čimprejšnje operativnosti bistvenih operacij. Proces upravljanja neprekinjenega poslovanja mora vsebovati kontrole, s pomočjo katerih se lahko identificirajo in zmanjšajo tveganja.
Kontrolni postopki področja za upravljanje neprekinjenega poslovanja so:

- Vključitev informacijske varnosti v upravljalni postopek neprekinjenega poslovanja.
- Neprekinjeno poslovanje in ocena tveganja.
- Izdelava načrtov za neprekinjeno poslovanje.
- Okvir za načrtovanje neprekinjenega poslovanja.
- Preverjanje, vzdrževanje in ponovno ocenjevanje načrtov za neprekinjeno poslovanje.

7.4. NFPA 1600

Nacionalno protipožarno združenje (National Fire Protection Association – NFPA) je mednarodna neprofitna organizacija, ki je bila ustanovljena leta 1896 z namenom zmanjšanja globalnih tegob vezanih na požarno problematiko. Združenje povezuje več kot 60000 posameznikov iz celega sveta in več kot 80 nacionalnih organizacij (NFPA 1600,

2006). Leta 1991 je NFPA svet za standarde ustanovil odbor za upravljanje z nesrečami, katerega naloga je bila razviti dokument s priporočljivimi aktivnostmi v slučaju nesreče. Delo je bilo zaključeno in uradno potrjeno leta 1995. Leta 2000 je dokument z imenom NFPA 1600 postal uradni standard in bil s področja upravljanja z nesrečami nadgrajen na področje upravljanja nepričakovanih situacij in na področje upravljanja neprekinjenega poslovanja. Standard je potrdil ameriški nacionalni inštitut za standardizacijo (American National Standards Institute – ANSI). Potrdila ga je tudi ameriška federalna agencija za upravljanje z nevarnostmi (Federal Emergency Management Agency – FEMA). Trenutno veljavna verzija standarda NFPA 1600 je bila objavljena aprila 2004.
Naloga standarda NFPA 1600 je zagotoviti kriterije za oceno nepričakovane situacije, nesreče in zmožnosti neprekinjenosti poslovanja. Zagotavlja tudi smernice za pripravo, lajšanje in okrevanje po nepričakovani situaciji oz. nesreči.

Dokument NFPA 1600 vsebuje pet poglavij. Prva tri poglavja obravnavajo administrativne detajle in tehnične definicije (NFPA 1600 Standard, 2004, str. 4):

- Administracija
- Reference
- Definicije

Četrto in peto poglavje pa vsebujeta zahteve NFPA 1600:

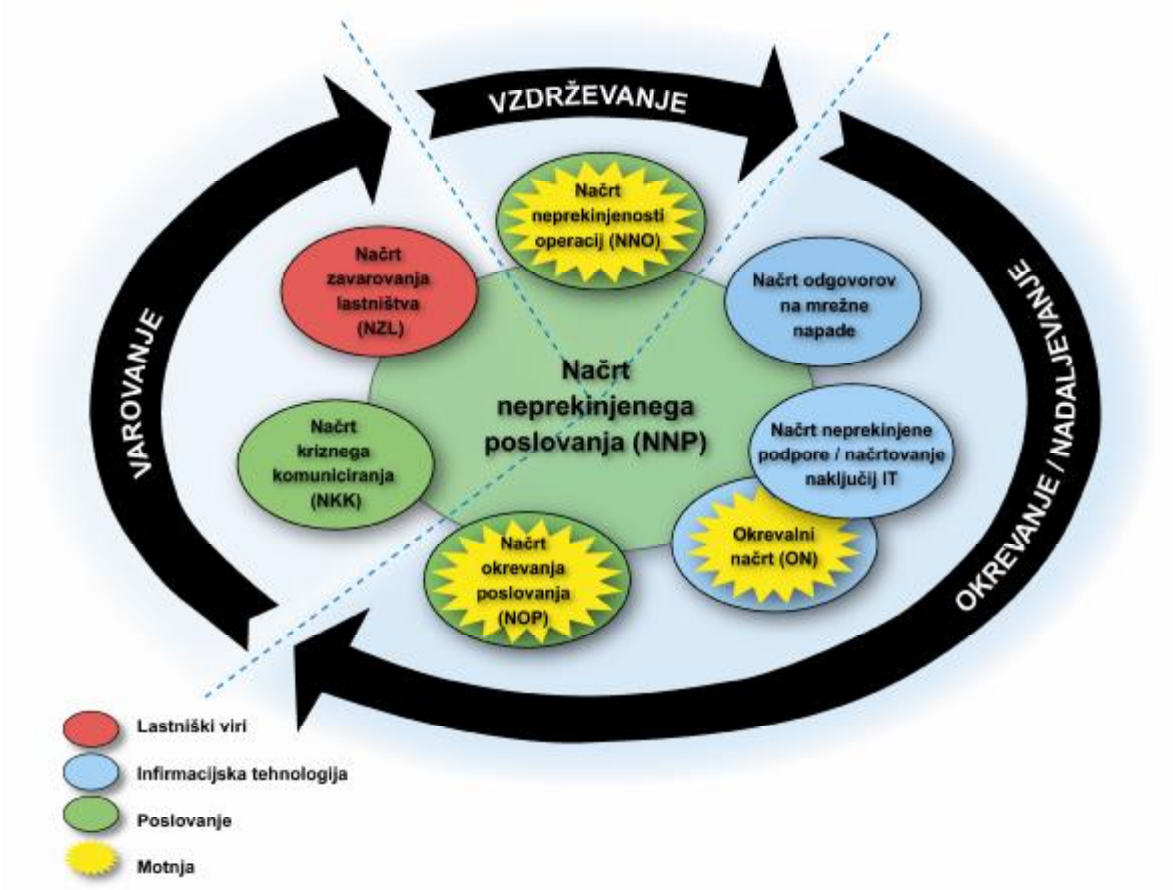
- Upravljanje programa
    - Dokumentiranje programa
    - Določitev koordinatorja programa
    - Ustanovitev svetovalnega odbora
    - Vrednotenje programa
- Elementi programa
    - Razvoj programa za upravljanje nesreč in nevarnosti
    - Spoštovanje zakonodaje
    - Identifikacija nevarnosti, analiza vplivov, ocena tveganja
    - Razvoj strategije za zmanjševanje tveganja
    - Upravljanje resursov
    - Dogovori o vzajemni pomoči
    - Priprava načrta programa
    - Razvoj koordinacije incidentov in kontrolnih sposobnosti
    - Komunikacije in opozorila
    - Uvedba operativnih procedur
    - Izgradnja logističnih zmožnosti
    - Omogočiti šolanje
    - Izboljšave programa
    - Vpeljava kriznega komuniciranja
    - Upravljanje finančnih procedur

8. Vrste načrtovanj

Načrtovanje možnih naključij v delovanju informacijske tehnologije obravnava različne aktivnosti, ki jim je skupen cilj zagotoviti delovanje ali obnovitev kritičnih komponent informacijske tehnologije v slučaju izpada. Načrtovanje naključij na področju informacijske tehnologije je del širšega spektra za zagotavljanje pripravljenosti na težave, ki vključuje organizacijske in poslovne procese kontinuitete in obnovitve. Z vnaprejšnjim načrtovanjem podjetje pripravi ustrezne odgovore na možne težave v informacijski tehnologiji, v poslovnih procesih in opremi. Za vsa kritična področja podjetja se izdela

načrte aktivnosti v primeru nesreče, ki eksplicitno navajajo postopke ravnanja v kriznih situacijah. Načrti za posamezna področja so lahko ločeni in nepovezani, vendar je v tem primeru potrebna izredna koordinacija, da ne pride do kontradikcij, prekrivanj in podvajanj. Veliko pregledneje in enostavneje je vključiti posamezne načrte v enovit, krovni načrt poslovanja za celotno podjetje. Struktura krovnega načrta omogoča enostavno dodajanje in integracijo novih sklopov.
Področje načrtovanja neprekinjenosti sestavljajo trije sklopi, ki vključujejo načrte za posamezna področja in povezovalni načrt neprekinjenega poslovanja za celotno podjetje (slika 12). Prvi sklop predstavlja varovanje, ki predvideva postopke komuniciranja v primeru nesreče in prvi odgovor na krizno situacijo. Drugi sklop, vzdrževanje, zagotavlja neprekinjenost poslovanja po nesreči. Tretji sklop vključuje postopke za nadaljevanje in okrevanje informacijske tehnologije in poslovanja po zaznani motnji.

Slika 12: **Medsebojen odnos načrtov neprekinjenosti**



Vir: Swanson, 2002, str. 11

V nadaljevanju podajam obrazložitve posameznih oblik načrtovanj (Swanson, 2002, str. 7), ki jih je mogoče obravnavati ločeno ali pa kot prepletene dele načrta za neprekinjeno poslovanje.

8.1. Načrt neprekinjenega poslovanja

Načrt neprekinjenega poslovanja, krajše NNP (Business Continuity Plan – BCP), je osredotočen na ohranjanje poslovnih funkcij podjetja med in po izpadu. Primer poslovne funkcije je lahko proces izplačevanja plač ali pa uporabniški informacijski proces. NNP je lahko oblikovan samo za posamezen poslovni proces, lahko pa pokriva vse ključne

poslovne procese. Okrevalni načrt (Disaster Recovery Plan), načrt nadaljevanja poslovanja (Business Resumption Plan) in načrt zavarovanja lastništva (Occupan Emergency Plan) so lahko del NNP. Odgovornosti in prioritete, določene znotraj NNP, morajo biti usklajene s tistimi v načrtu neprekinjenosti operacij (Continuity of Operations).

8.2. Načrt kriznega komuniciranja

Načrt kriznega komuniciranja, krajše NKK (Crisis Communications Plan). Podjetja morajo pripraviti notranje in zunanje postopke komuniciranja pred pojavom nesreče. Načrt kriznega komuniciranja pogosto pripravijo organizacije za stike z javnostjo. Procedure načrta morajo biti usklajene z vsemi drugimi načrti, da v javnost zagotovo pridejo samo potrjene in odobrene izjave. Načrt je ponavadi dodatek načrta za neprekinjeno poslovanje. NKK opredeli posameznike, ki so avtorizirani za dajanje izjav v zvezi z nesrečo. V načrt so vključene tudi predloge za komunikacijo z mediji.

8.3. Načrt zavarovanja lastništva

Načrt zavarovanja lastništva, krajše NZL (Occupant Emergency Plan - OEP), omogoča odgovor na situacije (požar, poplava, kriminal, itd.), v katerih je ogroženo zdravje in varnost osebja, okolje in lastništvo. Načrt zavarovanja lastništva je lahko del načrta za neprekinjeno poslovanje, vendar se izvaja ločeno.

8.4. Načrt neprekinjenosti operacij

Načrt neprekinjenosti operacij, krajše NNO (Continuity Of Operations Plan – COOP) je usmerjen v restavriranje glavnih funkcij podjetja na rezervni lokaciji in izvajanje teh funkcij v obdobju, ki ni daljše od 30 dni. Načrt neprekinjenosti operacij pokriva najvišji nivo podjetja (vodstvo), zato je razvit in izvajan neodvisno od načrta neprekinjenega poslovanja. Za načrt neprekinjenosti operacij ni obvezno vključevanje operacij informacijske tehnologije, lahko pa dodatno vključuje načrt neprekinjenega poslovanja, načrt okrevanja poslovanja in okrevalni načrt.

8.5. Načrt odgovorov na mrežne napade

Načrt odgovorov na mrežne napade (Cyber Incident Response Plan) vsebuje postopke razreševanja mrežnih napadov na informacijske sisteme podjetja. Postopki pomagajo varnostnemu osebju identificirati, blažiti in odpravljati zlonamerne računalniške incidente, ki se kažejo kot neavtoriziran dostop do sistemov in podatkov, kot tudi neavtorizirane spremembe na podatkih in sistemski strojni ter programski opremi. Načrt je lahko kot dodatek vključen v načrt neprekinjenega poslovanja podjetja.

8.6. Načrt neprekinjene podpore/načrtovanje naključij IT

Načrt neprekinjene podpore/načrtovanje naključij IT (Continuity of Support Plan/IT Contingency Plan). Načrt neprekinjene podpore se uvede za glavne podporne sisteme, načrt naključij IT pa za glavne aplikacije. Ker naj bi bil načrt uveden za vse pomembnejše podporne sisteme in aplikacije, je lahko več načrtov znotraj načrta neprekinjenega poslovanja podjetja.

8.7. Okrevalni načrt

Okrevalni načrt, krajše ON (Disaster Recovery Plan – DRP), se nanaša na velike nesreče in katastrofe, ki onemogočijo delovanje informacijske tehnologije za daljše obdobje. ON predvideva po nesreči ponovno vzpostavitev delovanja informacijske tehnologije na drugi, t.i. rezervni lokaciji. ON lahko prekriva dele načrta za neprekinjeno podporo in načrtovanje naključij, vendar je bolj ozko usmerjen in se ne ukvarja z manjšimi težavami, ki ne zahtevajo preklopa na drugo lokacijo. ON je lahko del načrta za neprekinjeno poslovanje.

8.8. Načrt okrevanja poslovanja

Načrt okrevanja poslovanja, krajše NOP (Business Recovery Plan – BRP), se lahko imenuje tudi načrt nadaljevanja poslovanja (Business Resumption Plan). Načrt pokriva področje restavriranja poslovnih procesov po izpadu. Za razliko od načrta za neprekinjeno poslovanje se ne ukvarja s procedurami za zagotovitev delovanja kritičnih poslovnih procesov med izpadom. Razvoj načrta za okrevanje poslovanja mora biti koordiniran z okrevalnim načrtom in načrtom neprekinjenega poslovanja. NOP je lahko del načrta za neprekinjeno poslovanje.

8.9. Primerjava načrtov

V primerjalni tabeli 5 so navedeni posamezni načrti in področja, ki jih pokrivajo.

Tabela 5: **Primerjava načrtov neprekinjenosti**

Načrt	Namen	Področje
Načrt neprekinjenega poslovanja	Zagotavlja postopke za vzdrževanje bistvenih poslovnih operacij med okrevanjem zaradi izpada	Poslovni procesi, IT pokriva kot podporo poslovnim procesom
Načrt okrevanja poslovanja	Zagotavlja postopke za okrevanje poslovnih operacij takoj po izpadu	Poslovni procesi, slabo usmerjen v IT, pokriva ga samo kot podporo poslovnim procesom
Načrt neprekinjenosti operacij	Zagotavlja postopke za vzpostavitev strateških poslovnih funkcij na rezervni lokaciji, za dobo do 30 dni	Pokriva vodstveni del podjetja, ni usmerjen v IT
Načrt neprekinjene podpore/načrtovanje naključij IT	Zagotavlja postopke za okrevanje pomembnih aplikacij in sistemov	Pokriva prekinitve v delovanju sistemov IT
Načrt kriznega komuniciranja	Zagotavlja postopke za posredovanje informacij osebju in javnosti	Pokriva področje komuniciranja, ni usmerjen v IT
Načrt odgovorov na mrežne napade	Zagotavlja strategije za odkrivanje in odgovarjanje na mrežne napade	Pokriva področje varnosti IT
Okrevalni načrt	Zagotavlja postopke za okrevanje po nesreči na rezervni lokaciji	Usmerjen v večje prekinitve delovanja IT
Načrt zavarovanja lastništva	Zagotavlja postopke za zmanjševanje poškodb in varovanje lastnine	Pokriva področje lastnine in osebja, ni usmerjen v IT

Vir: Swanson, 2002, str. 10

Načrti, ki se neposredno nanašajo na področje informacijske tehnologije, so lahko hkrati tudi sestavni del načrta neprekinjenega poslovanja podjetja. Načrt neprekinjenega poslovanja je krovni načrt, v katerega so kot sestavni deli vključeni drugi načrti. Napačna je predstava, da je potrebno znotraj podjetja obe področji obravnavati ločeno. Ločena obravnava lahko pripelje do velikih neskladij in nepovezanosti. Tudi če se podjetje odloči samo za izdelavo okrevalnega načrta, je le tega potrebno obravnavati po postopkih krovnega, celovitega načrta. Na ta način je možno v bodoče zelo enostavno dograjevati nove sestavne dele. V nadaljevanju magistrskega dela bom obravnaval načrtovanje neprekinjenega poslovanja podjetja s poudarkom na informacijski tehnologiji.

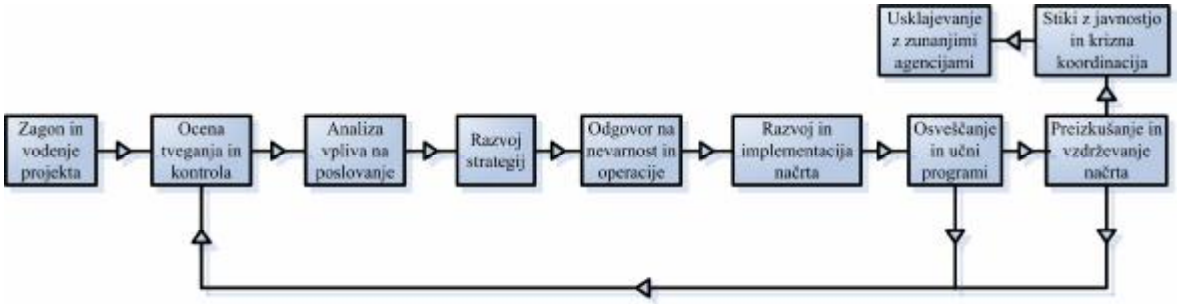
9. Metodologije

Metodologij, ki opisujejo proces načrtovanja neprekinjenosti poslovanja, je veliko in bi jih bilo praktično nemogoče vse zajeti. Zaradi njihove velike prilagodljivosti potrebam podjetja se nenehno pojavljajo nove metode, ki pa jim je vsem skupno, da skušajo v kar največji meri zadovoljiti zakonske predpise, priporočila in standarde, opisane v predhodnih poglavjih. Metodologije so rezultat raziskav in dolgoletnih izkušenj organizacij in posameznikov, strokovnjakov s področja načrtovanja neprekinjenosti poslovanja.
Sledi prikaz nekaterih najpogosteje uporabljenih metod načrtovanja neprekinjenosti poslovanja. Metodologije so zaradi lažjega razločevanja poimenovane po avtorjih.

9.1. DRII

Mednarodni inštitut za okrevanje po nesreči (Disaster Recovery Institute International – DRII) je bil ustanovljen leta 1988. Glavni cilj inštituta je bil razviti skupek znanj, potrebnih za načrtovanje naključij in poslovnih tveganj, ter izobraziti in certificirati kvalificirane posameznike z vsaj minimalnim sprejemljivim nivojem merljivega znanja in promovirati kredibilnost in profesionalnost certificiranih posameznikov. Danes je inštitut ena vodilnih ustanov za izobraževanja in certificiranja s področja načrtovanja neprekinjenega delovanja in upravljanja. Leta 1997 je inštitut objavil skupek znanj, imenovan Profesionalne prakse za načrtovalce neprekinjenosti poslovanja (Professional Practices for Business Continuity Planners, 2003, str. 1), ki se v industriji uporablja kot standard najboljših praks. DRII predvideva 10 področij oz. korakov razvoja neprekinjenega poslovanja (slika 13).

Slika 13: **Koraki razvoja neprekinjenega poslovanja po metodologiji DRII**



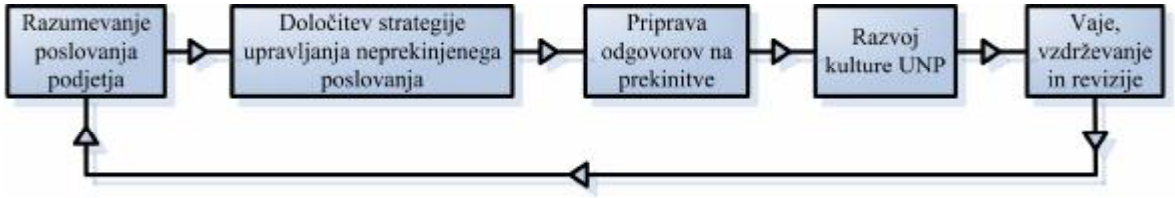
Vir: Professional Practices for Business Continuity Planners, 2003, str. 1

1. Zagon in vodenje projekta
2. Ocena tveganja in kontrola
3. Analiza vpliva na poslovanje
4. Razvoj strategij neprekinjenosti poslovanja
5. Odgovor na nevarnost in operacije
6. Razvoj načrtov za neprekinjeno poslovanja
7. Osveščanje in učni programi
8. Preizkušanje in vzdrževanje načrtov za neprekinjeno poslovanje
9. Stiki z javnostjo in krizna koordinacija
10. Usklajevanje z zunanjimi agencijami

9.2. BCI

Inštitut za neprekinjenost poslovanja (Business Continuity Institute – BCI) govori o življenjskem ciklu upravljanja neprekinjenosti poslovanja (UNP), ki je sestavljen iz petih, med seboj povezanih sklopov (Wright, 2005, str. 8). Za učinkovito neprekinjenost poslovanja mora podjetje izpeljati predpisane postopke iz vseh petih sklopov (slika 14).

Slika 14: **Koraki razvoja neprekinjenega poslovanja po metodologiji BCI**



Vir: Wright, 2005, str. 8

1. Razumevanje poslovanja podjetja
- Razumevanje strategije, okolja in poslovanja podjetja je predpogoj za določitev pravega programa neprekinjenosti poslovanja.
- Analiza vpliva na poslovanje, identificira, kvantificira in kvalificira poslovne izgube zaradi izpada.
- Ocena tveganja raziskuje verjetnost in vpliv različnih groženj, ki lahko povzročijo prekinitev poslovanja.

2. Določitev strategije upravljanja neprekinjenega poslovanja
- Določitev celotne strategije upravljanja neprekinjenega poslovanja omogoča jasno opredelitev in dokumentiranje politike, okvira in operativnih smernic za zagotovitev nepretrganosti poslovanja.
- Določitev strategije posameznih procesov omogoča izdelavo navodil za ponovno vzpostavitev delovanja enega ali več poslovno kritičnih procesov in aktivnosti.
- Določitev strategije virov koordinira in zagotavlja vire znotraj načrta neprekinjenega poslovanja, ki omogočajo izgradnjo celotne strategije podjetja in strategije posameznih procesov.

3. Priprava odgovorov na prekinitve
- Načrt kriznega upravljanja definira postopek odločanja vodstva v kriznih situacijah. Do izraza pride predvsem takrat, ko krizna situacija ni v popolnosti pokrita v načrtu neprekinjenega poslovanja (npr, sovražni prevzem). Načrt kriznega upravljanja se nahaja na t.i. strateškem nivoju podjetja.

- Načrt neprekinjenega poslovanja obravnava poslovne prekinitve in izgube od prvega odgovora do točke, v kateri so ponovno vzpostavljene normalne poslovne operacije. Vsebuje procedure za zagotovitev okrevanja. Načrt je pozicioniran na taktični nivo podjetja.
- Načrt nadaljevanja dela poslovnih enot je namenjen operativnim oddelkom in vsebuje postopke za nadaljevanje poslovnih funkcij. Pokriva operativni nivo podjetja.

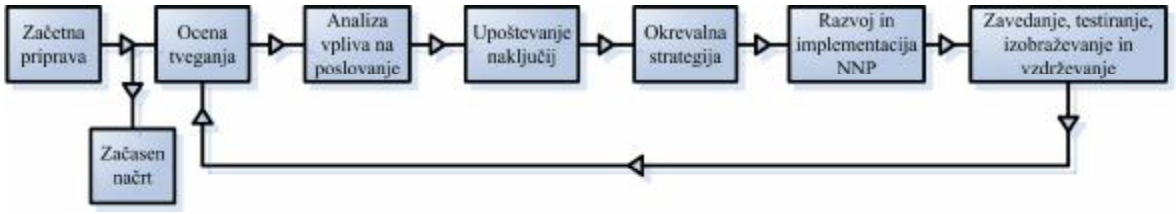
4. Razvoj kulture UNP
- Zagotovitev zavesti je postopek za ugotavljanje trenutnega in želenega nivoja zavedanja o upravljanju neprekinjenega poslovanja. Definira katerim področjem se je treba posvetiti in kako čim učinkoviteje doseči večjo raven zavedanja med zaposlenimi.
- Razvoj kulture vsebuje aktivnosti za definiranje informacij in sporočil s področja upravljanja neprekinjenosti poslovanja, ki jih mora osvojiti osebje. Vsebuje tudi načine, kako ta poročila uspešno posredovati osebju.
- Spremljanje kulture UNP in potrebnih znanj zagotavlja učinkovitost UNP.

5. Vaje, vzdrževanje in revizije
- Vaje potrjujejo zanesljivost postopkov neprekinjenosti poslovanja.
- Vzdrževanje se uporablja za korekcijo vseh sprememb, ki se pojavljajo v poslovnem okolju (spremembe zaposlenih, opreme, procesov, trgov, tveganj, lokacij in strategij).
- Revizije zagotavljajo, da ima podjetje učinkovito zmožnost neprekinjenosti poslovanja.

9.3. PACE

Angleška vladna agencija za upravljanje javnega premoženja (Property Advisers to the Civil Estate – PACE) priporoča pri izgradnji načrta neprekinjenosti poslovanja uporabo 8 korakov (Business Continuity Planning Guide, 1998, str. 32), ki jih prikazuje slika 15.

Slika 15: **Koraki razvoja neprekinjenega poslovanja po metodologiji PACE**



Vir: Business Continuity Planning Guide, 1998, str. 34

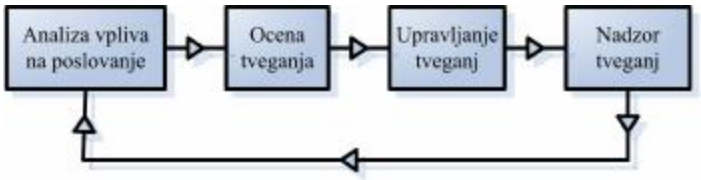
1. Začetna priprava od vodstva podjetja pričakuje pobudo za razvoj projekta načrtovanja neprekinjenosti poslovanja. Določitev lastnika, odgovornosti in področje projekta. Imenovanje upravljavca neprekinjenosti poslovanja, ki organizira in nadzoruje pripravljalna dela.
2. Začasen načrt se izdela kot poenostavljen, zasilni načrt, dokler ni dokončan pravi načrt neprekinjenega poslovanja.
3. Ocena tveganja identificira tveganja in stroškovno ovrednoti ukrepe za preprečitev. Ocena tveganja zmanjšuje verjetnost nastanka in moč nesreče.
4. Analiza vpliva na poslovanje identificira bistvene operacije in vpliv njihovega izpada ter največji sprejemljiv čas izpada.
5. Upoštevanje naključij se ukvarja z različnimi možnostmi za zamenjavo ali nadomestitev izpada originalnega vira z možnimi alternativami iz okolja.
6. Okrevalna strategija identificira in primerja različne okrevalne možnosti z namenom določitve najbolj učinkovite in stroškovno ustrezne.

7. Razvoj načrta neprekinjenega poslovanja.
8. Zavedanje, testiranje, izobraževanje in vzdrževanje načrta neprekinjenega poslovanja je ključnega pomena za zagotovitev ustreznosti in učinkovitosti.

9.4. FFIEC

Ameriški federalni svet za preučevanje finančnih ustanov (Federal Financial Institutions Examination Council – FFIEC) spodbuja finančne institucije, da se poslužujejo procesno orientiranega pristopa načrtovanja neprekinjenega poslovanja (Business Continuity Planning, 2003, str. 5). Priporočene korake prikazuje slika 16.

Slika 16: **Koraki razvoja neprekinjenega poslovanja po metodologiji FFIEC**



Vir: Business Continuity Planning, 2003, str. 5

1. Analiza vpliva na poslovanje je prvi korak, ki vključuje identifikacijo potencialnih nekontroliranih dogodkov na poslovne procese in uporabnike. Analiza pokriva vse poslovne oddelke in funkcije. Ukvarja se z analizo najdaljšega še sprejemljivega časa prekinitve in s še sprejemljivimi nivoji podatkovnih, operativnih in finančnih izgub.
2. Ocena tveganja je drugi korak in vključuje sestavo seznama potencialnih poslovnih prekinitev glede na pomembnost in verjetnost pojava. Vključuje tudi analizo groženj glede na moč udara na samo institucijo, stranke in finančni trg.
3. Upravljanje tveganj predvideva izdelavo načrta neprekinjenega poslovanja, ki dokumentira strategije in procedure za ohranitev, nadaljevanje in okrevanje kritičnih poslovnih funkcij in procesov.
4. Nadzor tveganj je zadnji korak v načrtovanju neprekinjenosti poslovanja. Nadzor tveganj skozi testiranja, revizije in posodobitve ohranja načrt vitalen.

9.5. NIST

Ameriški nacionalni inštitut za standardizacijo in tehnologijo (National Institute of Standards and Technology – NIST) priporoča pri načrtovanju neprekinjenega delovanja informacijskih sistemov uporabo sedmih korakov (Swanson, 2002, str. 14). Korake načrtovanja prikazuje slika 17.

Slika 17: **Koraki razvoja neprekinjenega poslovanja po metodologiji NIST**

Vir: Swanson, 2002, str. 14

1. Določitev politike načrtovanj. Formalna politika podjetja ali oddelka omogoča avtoriteto in smernice za razvoj učinkovitega načrta.
2. Analiza vpliva na poslovanje pomaga identificirati kritične informacijske sisteme in komponente.
3. Določitev preventivnih kontrol povečuje sistemsko razpoložljivost in zmanjšuje stroške.
4. Razvoj okrevalne strategije omogoča hitro in učinkovito okrevanje sistema po prekinitvi.
5. Razvoj načrta neprekinjenega delovanja vsebuje detajlne procedure za vzpostavitev delovanja prizadetega sistema.
6. Testiranje načrta, izobraževanje in vaje izboljšujejo učinkovitost načrta in celovito pripravljenost podjetja.
7. Vzdrževanje načrta oz. dopolnitve se izvedejo, ko nastopijo spremembe, ki jih je treba v načrtu dokumentirati.

9.6. ASIS

Mednarodna organizacija za svetovalce s področja varnosti, ASIS International, predlaga pri načrtovanju neprekinjenega poslovanja uporabo petih sklopov (Ahrens, 2005, str. 10), ki jih prikazuje slika 18.

Slika 18: **Koraki razvoja neprekinjenega poslovanja po metodologiji ASIS**

Vir: Ahrens, 2005, str. 10

1. Pripravljenost določa pripravljalne korake za zagotovitev ustrezne podlage za izgradnjo načrta neprekinjenega poslovanja.
- Določitev odgovornosti
- Ocena tveganja
- Analiza vpliva na poslovanje
- Določitev strateških načrtov
- Razvoj skupine za odgovore in krizno upravljanje

2. Preventivnost omogoča podjetju izogibanje, preprečevanje in zmanjševanje kriznih situacij.
- Skladnost s politiko podjetja
- Strategije blažitev
- Izogibanje, opozorila in odkrivanje

3. Odgovor na krizne situacije.
- Prepoznava potencialnih kriz
- Opozorila skupinam
- Ocena situacije
- Razglasitev krize
- Izvedba načrta
- Komunikacija

- Upravljanje z viri

4. Okrevanje določa procedure za ponovno vzpostavitev delovanja kritičnih procesov v primeru izpada.

- Ocena udarca in škode
- Nadaljevanje kritičnih in drugih procesov
- Vrnitev na normalne operacije

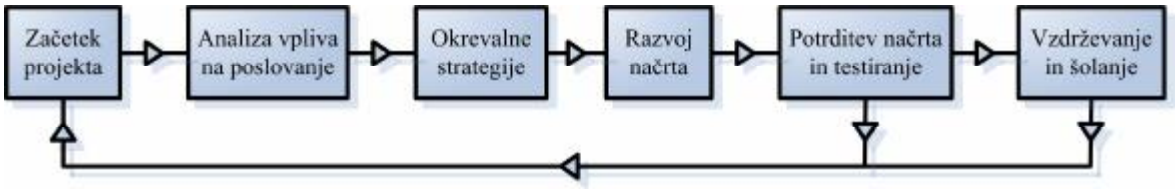
5. Izobraževanje, testiranje in vzdrževanje načrta neprekinjenega poslovanja.

- Šolanje in vaje
- Testiranje načrta neprekinjenega poslovanja

9.7. TDIR

Ministrstvo za informacijske vire v Ameriški zvezni državi Teksas (Texas Department of Information Resouces - TDIR) priporoča uporabo 6 korakov (Jamar, 2004, str. 57). Predstavlja jih slika 19.

Slika 19: **Koraki razvoja neprekinjenega poslovanja po metodologiji TDIR**



Vir: Jamar, 2004, str. 57

1. Začetek projekta

- Identifikacija uporabniških in poslovnih potreb
- Identifikacija zunanjih zahtev (vlada, industrija, zakonodaja)
- Ocena tveganja
- Pridobitev podpore s strani vodstva
- Izvedba projektnega načrtovanja in kontrole procesov

2. Analiza vpliva na poslovanje

- Določitev kriterijev kritičnosti
- Identifikacija vitalnih poslovnih procesov, aplikacij, podatkov in opreme
- Stroškovna ocena nesreče glede na poslovne procese
- Identifikacija medsebojnih odvisnosti
- Definiranje okrevalnega časa

3. Okrevalne strategije

- Definiranje procesov in procesnih alternativ
- Določitev komunikacijskih alternativ
- Določitev alternativnih okrevalnih strategij
- Formulacija strategij glede na stroške in tveganje
- Pregled strategij z okrevalnimi skupinami, upravo in uporabniki

4. Razvoj načrta

- Določitev okrevalnih skupin, vodstev, vlog in odgovornosti
- Objava in aktiviranje procedur načrta
- Določitev procedur v primeru nesreče
- Razvoj detajlnih okrevalnih procedur
- Določitev načina distribucije načrta in kontrolnih procedur

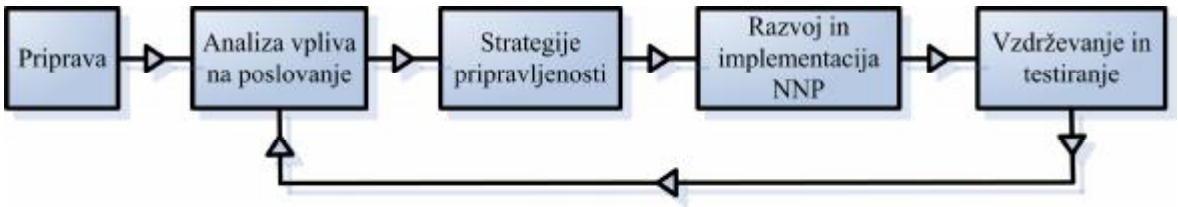
5. Potrditev načrta in testiranje
- Določitev načina testiranj načrtov
- Razvoj simulacij
- Izvedba testov
- Vrednotenje rezultatov testiranj
- Izvedba izboljšav na osnovi rezultatov testiranj

6. Vzdrževanje in šolanje
- Razvoj procesa vzdrževanja
- Revizija informacij
- Po potrebi razviti revidiran načrt neprekinjenosti poslovanja
- Razvoj korporacijskega programa zavedanja
- Razvoj specifičnih programov šolanj

9.8. Williamson

John Williamson, avtor knjige Načrtovanje neprekinjenega poslovanja za vodstvo in informatike (Business Continuity Planning, A Primer for Management and IT Personnel) navaja v procesu načrtovanja neprekinjenega poslovanja 5 korakov (Williamson, 2002, str. 3). Korake načrtovanja prikazuje slika 20.

Slika 20: **Koraki razvoja neprekinjenega poslovanja po metodologiji Williamson**



Vir: Williamson, 2002, str. 3

1. Priprava vsebuje pripravljalne aktivnosti kot so uvodni sestanek z vodstvom podjetja, prezentacije, sestava vprašalnikov, itd.
2. Analiza vpliva na poslovanje ugotavlja finančno izpostavljenost in operativne udarce izpada delovanja.
3. Strategije pripravljenosti na nesrečo definirajo in stroškovno ocenijo alternative nadaljevanja poslovanja.
4. Razvoj načrta neprekinjenega poslovanja.
5. Vzdrževanje in testiranje načrta.

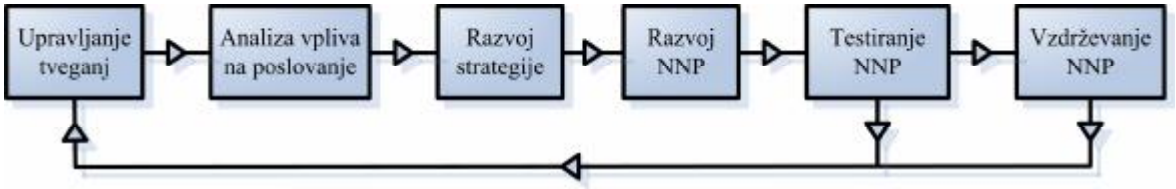
9.9. Syed

Akhtar in Afsar Syed, avtorja knjige Metodologija načrtovanja neprekinjenosti poslovanja (Business Continuity Planning Methodology), razdelita načrtovanje neprekinjenosti poslovanja na upravljalno in procesno področje (Syed, 2004, str. 9).

Procesni del načrtovanja neprekinjenega poslovanja je sestavljen iz šestih stopenj (slika 21):
1. Upravljanje tveganj opredeljuje grožnje, obstoječe pomanjkljivosti, potencialne nesreče in identificira kontrole potrebne za preprečevanje in zmanjševanje izpadov.

2. Analiza vpliva na poslovanje identificira kritične procese in analizira vplive na poslovanje v primeru prekinitve teh procesov zaradi nesreče.
3. Razvoj strategije neprekinjenega poslovanja določa zahteve in išče možnosti okrevanj kritičnih procesov in virov v slučaju izpada zaradi nesreče.
4. Razvoj načrta neprekinjenega poslovanja se ukvarja z zagotavljanjem neprekinjenosti poslovanja. Temelji na rezultatih predhodnih korakov.
5. Testiranje načrta neprekinjenega poslovanja zagotavlja veljavnost, obstojnost in popolnost načrta.
6. Vzdrževanje načrta neprekinjenega poslovanja omogoča stalno funkcionalnost načrta.

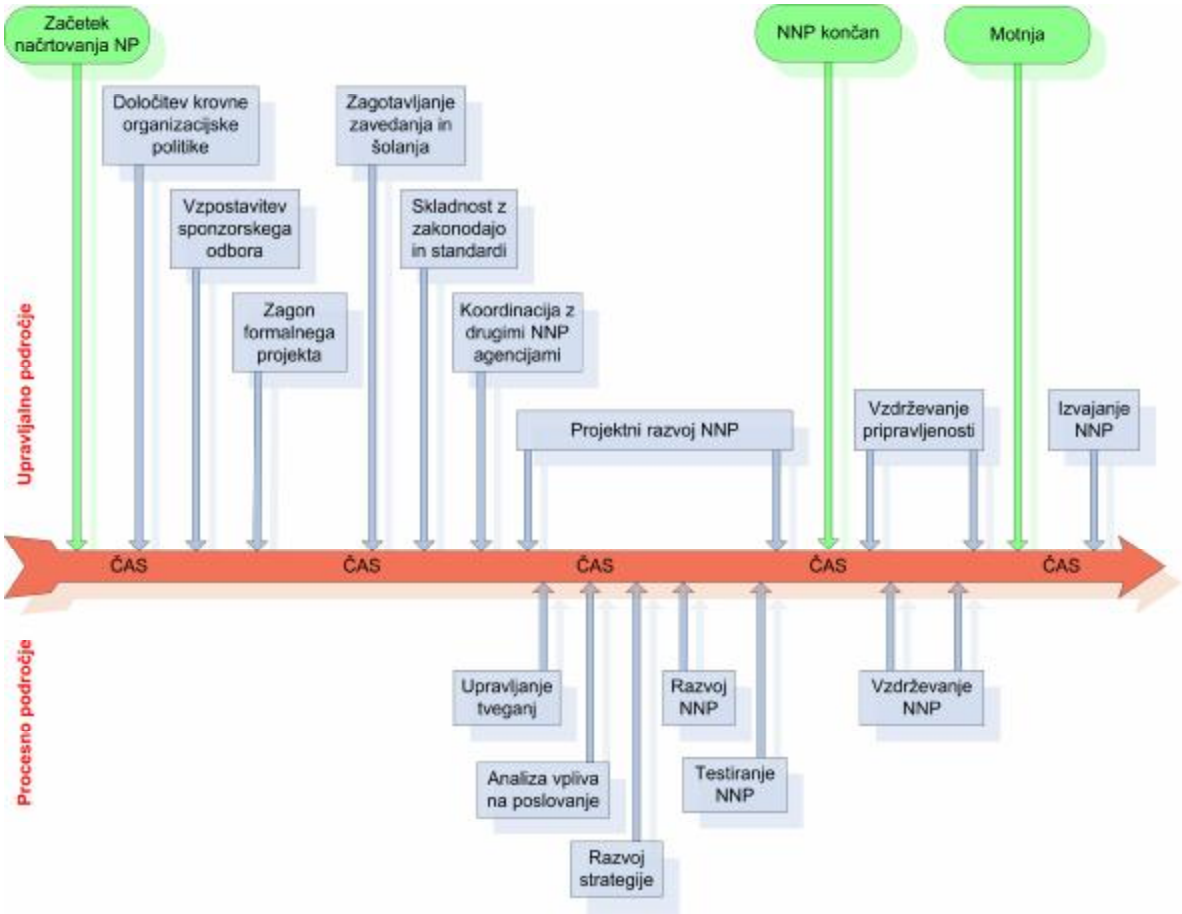
Slika 21: **Koraki razvoja neprekinjenega poslovanja po metodologiji Syed**



Vir: Syed, 2004, str. 11

Upravljalni del načrtovanja neprekinjenega poslovanja se posveča upravljalnim in organizacijskim komponentam NNP (slika 22).

Slika 22: **Celostno načrtovanje neprekinjenosti poslovanja po metodologiji Syed**



Vir: Syed, 2004, str. 9

Bistvene komponente upravljalnega dela so:

- Določitev krovne politike neprekinjenosti poslovanja, ki tako vodstvu kot tudi osebju posameznih poslovnih enot delegira obveznost do zagotovitve delovanja kritičnih funkcij in procesov v slučaju prekinitve delovanja.
- Vzpostavitev t.i. sponzorskega odbora s člani iz najvišjega vodstva podjetja. Odbor definira področje delovanja NNP, vzpodbuja razvoj, nadzoruje status in napredek ter zagotavlja finančno podporo.
- Zagon formalnega projekta za razvoj načrta neprekinjenega poslovanja.
- Potrebno je zagotoviti, da je osebje, ki je vključeno v razvoj in izvedbo NNP, ustrezno izšolano. Na nivoju celotnega podjetja je treba zagotoviti dovolj visoko stopnjo zavedanja o NNP in vpeljati izobraževalne programe.
- Zagotoviti je treba, da so aktivnosti NNP v skladu z zakonodajo in standardi.
- Aktivnosti NNP se koordinirajo z drugimi ustreznimi agencijami za NNP in z lokalno oblastjo.
- Zagotoviti je treba, da je NNP ves čas v pripravljenosti.

V primeru nesreče je treba izvesti NNP.

9.10. Primerjava metodologij

Cilj vseh predstavljenih načrtovanj neprekinjenega poslovanja je zagotoviti učinkovite postopke za nadaljevanje poslovanja v slučaju nesreče.
Iz prikazov posameznih metodologij sledi, da je ključnih aktivnosti, ki se pojavljajo pri večini avtorjev, šest. Bistvene aktivnosti procesa načrtovanja so ocena tveganja, analiza vpliva na poslovanje, določitev strategije, razvoj načrta za neprekinjeno poslovanje, testiranje in vzdrževanje. Večina avtorjev gradi na teh osnovnih aktivnostih, ki jih po svoje prilagaja, umešča v proces in združuje z novimi, dodatnimi aktivnostmi oz. koraki.

- DRII predlaga uporabo prej navedenih aktivnosti, ki jim doda uvodni korak za zagon projekta in poglavja za hitri odgovor na nevarnost, za krizno koordinacijo in stike z javnostjo ter usklajevanje z zunanjimi agencijami.
- BCI ključne aktivnosti združi v sklope. Razvoj načrta za neprekinjeno poslovanje predvidi v sklopu odgovorov na prekinitve, kjer se nahajata še načrt za krizno upravljanje in načrt nadaljevanja dela. Dodan je tudi sklop za razvoj kulture upravljanja neprekinjenega poslovanja.
- PACE začne proces načrtovanja s pobudo vodstva. Predvideva izgradnjo začasnega načrta in nadomestitev izpada originalnih virov z alternativami iz okolja.
- FFIEC združi izdelavo strategije in načrta za neprekinjeno poslovanje v upravljanje tveganj. Nadzor tveganj pa vključuje tako testiranje kot tudi vzdrževanje načrta.
- NIST najprej določi politiko načrtovanja. Namesto ocene tveganja išče preventivne kontrole.
- ASIS podobno kot BCI posamezne aktivnosti združi v pet glavnih sklopov. Ključne aktivnosti vključi v sklope za pripravljenost, okrevanje in vzdrževanje. Doda še sklopa z aktivnostmi za zmanjševanje kriznih situacij in odgovor nanje.
- TDIR predlaga šest korakov, ki vsebujejo vse ključne aktivnosti.
- Williamson začne proces načrtovanja s pripravljalnimi aktivnostmi, prezre pa aktivnosti za oceno tveganja.
- Syed razdeli proces načrtovanje na upravljalno in procesno področje. Upravljalno področje vključuje vse pripravljalne in podporne aktivnosti projektiranja, ki so jih nekateri avtorji dodali v sam proces načrtovanja neprekinjenega poslovanja. Procesno področje pa vsebuje samo bistvene aktivnosti za načrtovanja neprekinjenega poslovanja.

Zaradi smiselne in predvsem pregledne ločitve projektnega in procesnega dela, bom v nadaljevanju obdelal vseh šest ključnih aktivnosti procesnega načrtovanja neprekinjenega poslovanja po metodologiji Syed in teorijo podkrepil s praktičnimi primeri.
Bistvene aktivnosti pri načrtovanju neprekinjenega poslovanja po metodologiji Syed si sledijo v naslednjem zaporedju (Syed, 2004, str. 11):

- Upravljanje tveganj
- Analiza vpliva na poslovanje
- Razvoj strategije neprekinjenega poslovanja
- Načrt neprekinjenega poslovanja
- Testiranje načrta neprekinjenega poslovanja
- Vzdrževanje načrta neprekinjenega poslovanja

10. Upravljanje tveganj

Podjetje se sooča z mnogimi dejavniki tveganja, ki ogrožajo učinkovitost poslovanja in lahko pripeljejo tudi do katastrofalnih posledic za podjetje. Na podjetje prežijo napake v informacijski tehnologiji, okvare naprav, potresi, poplave, požari in druge nevšečnosti, katerih posledice so lahko katastrofalne za poslovanje podjetja. Posledice se kažejo kot neoperativnost informacijskih sistemov in opreme, poškodbe zgradb ter kot ogroženost zdravja in človeških življenj. Vsa tveganja je praktično nemogoče odpraviti, jih je pa možno zmanjšati na neko sprejemljivo raven (Hiles, 2002, str. 21).
Ogrodje upravljanja s tveganji omogoča dosego tega cilja. Razdeljeno je na sedem faz:

- Ocena tveganja
- Ocena kontrolnih možnosti
- Ocena kontrolnih stroškov in učinkovitosti
- Poročanje
- Izbira kontrolnih možnosti
- Implementacija kontrol
- Nadzor tveganj

10.1. Ocena tveganja

Ocena tveganja je proces, ki je sestavljen iz 6 korakov, v katerih se vsako tveganje opredeli z vidika grožnje in posledic, kot rezultat izvršene grožnje. Vsaka grožnja se nadalje členi na verjetnost pojava, kategorijo, vir in opis grožnje.
V procesu se za končno določitev vrednosti tveganja uporablja kvantitativna metoda PLI (pričakovan letni izpad) ali kvalitativna metoda PLV (pričakovan letni vpliv), ki jo je treba izbrati pred začetkom samega procesa.

Identifikacija virov

Prvi korak procesa ocene tveganj je identifikacija potencialnih virov groženj. Viri se delijo glede na nastanek, na naravne tehnične in človeške vire.
Med naravne vire groženj spadajo poplave, požari, potresi, orkani, vročinski udari, viharji, epidemije, idr.
Med tehnične vire groženj spadajo izpadi električne energije, okvare strežnikov in posameznih računalniških strojnih komponent, programske napake, mrežne okvare, telefonske komunikacijske prekinitve, okvare prezračevalnih naprav, idr.

Med človeške vire groženj spadajo vandalizem, terorizem, računalniški vdori in virusi, nesreče pri delu, vojaški udar, idr.
V tabeli 6 je kot vir grožnje predstavljena prekinitve električnega voda, ki spada med tehnične vire groženj.

Tabela 6: **Identifikacija potencialnega vira grožnje**

Tveganje
Grožnja
Kategorija: tehnična
Vir grožnje: prekinitev električnega voda

Vir: Lasten

Določitev dogodkov

Naslednji korak je opis grožnje oz. določitev dogodkov, ki sledijo v predhodnem koraku, identificiranemu viru grožnje.
V predstavljenem primeru pride zaradi prekinitve električnega voda do izpada električne energije (tabela 7).

Tabela 7: **Opis potencialne grožnje**

Tveganje	
Grožnja	
Kategorija: tehnična	
Vir grožnje: prekinitev el. voda	**Opis grožnje:** izpad elektrike

Vir: Lasten

Določitev posledic

V tretjem koraku se določi posledice groženj, opredeljenih v predhodnih dveh korakih. V tem koraku se določi tudi kritične dele premoženja (poslovni procesi, informacije, viri), ki jih podjetje potrebuje za normalno poslovanje.
Za vsako grožnjo se izbere del, ki ga lahko grožnja prizadene. Sledi določitev posledic (tabela 8).

Tabela 8: **Določitev posledic potencialne grožnje**

Tveganje		
Grožnja		**Posledice**
Kategorija: tehnična		Izpad delovanja informacijskega sistema.
Vir grožnje: prekinitev el. voda	**Opis grožnje:** izpad elektrike	

Vir: Lasten

Ocena verjetnosti

V četrtem koraku se oceni verjetnost grožnje. Ocena je, da pride do izpada elektrike zaradi prekinitve električnega voda enkrat v desetih letih. Letni pojav grožnje (LPG) je torej 1/10. Obstaja 10 odstotna verjetnost, da bo prišlo do izpada elektrike zaradi prekinitve električnega voda (tabela 9).

Tabela 9: **Ocena verjetnosti grožnje**

<table>
<tr><th colspan="3">Tveganje</th></tr>
<tr><th colspan="2">Grožnja</th><th>Posledice</th></tr>
<tr><td colspan="2">Kategorija: tehnična</td><td rowspan="3">Izpad delovanja informacijskega sistema.</td></tr>
<tr><td colspan="2">Verjetnost:
10 odstotna verjetnost, da bo do izpada elektrike prišlo zaradi prekinitve el. voda

1/10 (do izpada elektrike zaradi prekinitve el. voda pride enkrat na deset let) Letni pojav grožnje (LPG)</td></tr>
<tr><td>Vir grožnje: prekinitev el. voda</td><td>Opis grožnje: izpad elektrike</td></tr>
</table>

Vir: Lasten

Merjenje posledic

Peti korak meri posledice grožnje. Meri se pričakovani enkratni izpad (PEI) ali pričakovani enkratni vpliv (PEV). PEI kvantitativno meri delež skupne vrednosti kritičnega dela premoženja in virov, ki so izpostavljeni tveganju. PEV kvalitativno meri izpostavljenost kritičnih delov premoženja posledicam grožnje.

- Pričakovani enkratni izpad (PEI) je produkt vrednosti potencialnega zmanjšanja premoženja (VPZP) in faktorja izpostavljenosti (FI). VPZP meri potencialni finančni izpad v primeru, da je celotno premoženje podvrženo grožnji. Faktor izpostavljenosti (FI) predstavlja odstotek VPZP, ki je izpostavljen enkratnemu pojavu grožnje.

  V primeru izpada delovanja celotnega informacijskega sistema je strošek izpada ocenjen na 10 milijonov evrov (VPZP). Faktor izpostavljenosti je 10 odstotkov VPZP (tabela 10).

  PEI = VPZP * FI = 10.000.000 EUR * 10/100 = 1.000.000 EUR

- PEV je predstavljen z vrednostmi od 1 do 100. Vrednost 1 predstavlja najmanjši vpliv, vrednost 100 pa največjega.

  V primeru izpada delovanja informacijskega sistema zaradi izpada elektrike je PEV zaradi visokega vpliva ocenjen z vrednostjo 80 (tabela 10).

Tabela 10: **Merjenje posledic grožnje**

<table>
<tr><th colspan="3">Tveganje</th></tr>
<tr><th colspan="2">Grožnja</th><th>Posledice</th></tr>
<tr><td colspan="2">Kategorija:
tehnična</td><td rowspan="3">Izpad delovanja informacijskega sistema.

Kvantitativno je predviden izpad dohodka 1 milijon EUR.
Pričakovani enkratni izpad (PEI)

Kvalitativno je predviden vpliv na poslovanje visok, oz. 80.
Pričakovani enkratni vpliv (PEV)</td></tr>
<tr><td colspan="2">Verjetnost:
10 odstotna verjetnost

Letni pojav grožnje (LPG) je 1/10</td></tr>
<tr><td>Vir rožnje:
prekinitev el. voda</td><td>Opis grožnje:
izpad elektrike</td></tr>
</table>

Vir: Lasten

Določitev vrednosti tveganj

V zadnjem koraku se določi vrednost tveganj. Uporabi se lahko kvantitativno metodo pričakovanega letnega izpada (PLI) ali kvalitativno metodo pričakovanega letnega vpliva (PLV).
Kvantitativno metriko se uporablja za merjenje numeričnih vrednosti tveganj (npr. 100.000 EUR letnega tveganja zaradi grožnje izpada elektrike). Kvalitativna metrika pa uporablja vrednosti nizek, srednji in visok nivo tveganja.

- Pri uporabi kvantitativne metode merjenja tveganj se upošteva predviden izpad dohodka in verjetnost, da do tega izpada pride. Pri predvidenem milijonskem izpadu dohodka in 10 odstotnem tveganju znaša vrednost tveganja 100.000 EUR. Posledica in vrednost tveganja sta izraženi kvantitativno. Pomanjkljivost kvantitativne metode je, da zahteva veliko časa in truda. Pri kvantitativni metodi je tudi obrazložitev rezultatov veliko zahtevnejša.
- Kvalitativna metoda je za uporabo enostavnejša in razumljivejša. Tako posledica kot vrednost tveganja sta izražena kvalitativno. Pri visokem vplivu na poslovanje je ob 10 odstotni verjetnosti vrednost tveganja ocenjena kot nizka. Največja pomanjkljivost metode je, da so ocene tveganja rezultat subjektivnih presoj in kot take neponovljive.

- PLI ugotavlja vrednosti tveganj na osnovi verjetnosti letnega pojava grožnje (LPG) in na osnovi posledic pričakovanega enkratnega izpada (PEI).

  Do izpada elektrike zaradi prekinitve električnega voda pride enkrat v desetih letih. Letni pojav grožnje (LPG) je torej 1/10. Vrednost tveganja oz. pričakovani letni izpad (PLI) je produkt pričakovanega enkratnega izpada in letnega pojava grožnje (tabela 11).

  PLI = PEI * LPG = 1.000.000 EUR * 1/10 = 100.000 EUR

- PLV ugotavlja vrednosti tveganj na osnovi verjetnosti letnega pojava grožnje (LPG) in na osnovi posledic pričakovanega enkratnega vpliva (PEV) grožnje. Do izpada elektrike zaradi prekinitve električnega voda pride enkrat v desetih letih. Letni pojav grožnje (LPG) je torej 1/10.

  PLV = PEV * LPG = 80 * 1/10 = 8

Vrednost tveganja je visoka če je PLV vrednost med 67 in 100. Če je PLV med 34 in 66 je vrednost tveganja srednja. Če PLV med 1 in 33 je vrednost tveganja nizka.

V opisanem primeru predstavlja izpad elektrike zaradi prekinitve električnega voda nizko tveganje za podjetje (tabela 11).

Tabela 11: **Določitev vrednosti tveganja**

<table>
<tr><th colspan="3">Tveganje</th><td rowspan="2">Kvantitativno:
pričakovani letni izpad (PLI)

Vrednost tveganja:
100.000 EUR</td><td rowspan="2">Kvalitativno:
pričakovani letni vpliv (PLV)

Vrednost tveganja:
nizka</td></tr>
<tr><th colspan="2">Grožnja</th><th>Posledice</th></tr>
<tr><td colspan="2">Kategorija: tehnična</td><td rowspan="2">Izpad delovanja informacijskega sistema.

Kvantitativno je predviden izpad dohodka 1 milijon EUR
Pričakovani enkratni izpad (PEI)

Kvalitativno je predviden vpliv na poslovanje visok, oz. 80.
Pričakovani enkratni vpliv (PEV)</td></tr>
<tr><td colspan="2">Verjetnost:
10 odstotna verjetnost

Letni pojav grožnje (LPG) je 1/10</td></tr>
<tr><td>Vir grožnje:
prekinitev el. voda</td><td>Opis grožnje:
izpad elektrike</td><td></td><td></td><td></td></tr>
</table>

Vir: Lasten

10.1. Kontrolne možnosti

Kontrolne možnosti tveganj se delijo na štiri kategorije:

- Sprejemanje tveganj ne predvideva nobenih akcij. Uporabi se, kadar so vse druge možnosti izredno drage ali pa je tveganje nepomembno.
- Izogibanje tveganjem je najbolj zaželena kontrolna možnost, ki pa je pogosto neizvedljiva ali stroškovno neupravičena.
- Zmanjševanje tveganj je druga najbolj zaželena možnost. V prvem koraku je treba določiti še sprejemljiv nivo tveganja, v drugem koraku pa se razišče kontrolne možnosti, ki zmanjšujejo tveganje na določen sprejemljiv nivo.
- Prenos tveganj na drugo organizacijo (npr. zavarovalnico ali zunanjega izvajalca). Prenos tveganj je mogoče kombinirati tudi z zmanjševanjem tveganj.

V tabeli 12 so navedene kontrolne možnosti za primer izpada električne energije. Predlagane so tri kontrolne možnosti. Prva kontrolna možnost predstavlja izogibanje, druga zmanjševanje in tretja prenos tveganja.

Tabela 12: **Določitev in opredelitev kontrolnih možnosti**

	Kontrolna možnost	Kategorija
1.	Priklop računalniškega sistema na dva ločena in neodvisna vira napajanja z električno energijo	Izogibanje tveganju
2.	Uporaba naprav za neprekinjeno napajanje (UPS)	Zmanjševanje tveganja
3.	Zavarovanje škode pri zavarovalnici	Prenos tveganja

Vir: Lasten

10.2. Ocena kontrolnih stroškov in učinkovitosti

Naloga tretje faze je oceniti stroške in učinkovitost kontrolnih možnosti iz druge faze. Najprej se izvede ocena stroškov izvedbe kontrolne možnosti, sledi ocena učinkovitosti, na koncu pa se izvede stroškovno efektivna primerjava (tabela 13).

1. Kontrolni stroški se nanašajo na zahtevano opremo, material, transport, storitve, dajatve, zavarovanja, najemnino in vzdrževanje.
2. Za oceno učinkovitosti kontrolne možnosti je treba najprej določiti vrednost tveganja brez kontrol.
   *Pri pričakovanem enkratnem izpadu (PEI) 1 milijon EUR in verjetnosti letnega pojava grožnje (LPG) 1/10, je pričakovani letni izpad (PLI) enak 100.000 EUR (PLI = PEI * LPG)*
   Nova vrednost tveganja PLI je rezultat združitve ocene tveganja iz prve faze in posameznih kontrolnih možnosti.
   *V primeru dveh ločenih virov napajanja pride do izpada električne energije na vsakih 100 let. PLI = 1.000.000 EUR * 1/100 = 10.000 EUR. Stroški tveganja so se zmanjšali za 90.000 EUR (100.000 EUR – 10.000 EUR) na 10.000 EUR.*
   *V primeru naprav za neprekinjeno napajanje pride do izpada enkrat na 20 let. PLI = 1.000.000 EUR * 1/20 = 50.000 EUR. Stroški tveganja so se zmanjšali za 50.000 EUR (100.000 EUR – 50.000 EUR) na 50.000 EUR.*
3. Stroškovno efektivna primerjava služi za izbiro najboljše kontrolne možnosti s primerjavo kontrolnih stroškov in zmanjšanjem tveganja. Za primerjavo se uporabljajo stroški zmanjšanja tveganja na enoto (SZTE = kontrolni stroški / zmanjšanje tveganja). SZTE pomaga izbrati najboljšo varianto kontrolne možnosti. Manjša vrednost SZTE predstavlja boljšo izbiro in pomeni nižje stroške zmanjšanja tveganja.

Tabela 13: **Ocena kontrolnih stroškov**

	Kontrolna možnost	Kategorija	Kontrolni stroški	Vrednost PLI	Zmanjšanje tveganja	SZTE
1.	Dva vira napajanja	Izogibanje	150.000 EUR	10.000 EUR	90.000 EUR	1,66 EUR
2.	UPS	Zmanjševanje	60.000 EUR	50.000 EUR	50.000 EUR	1,2 EUR
3.	Zavarovanje	Prenos	130.000 EUR za 30 let	0	100.000 EUR	1,3 EUR (30 letno obdobje)

Vir: Lasten

10.3. Poročanje

S četrto fazo se v poročilu dokumentira rezultate prvih treh faz.
Poročilo mora vsebovati identificiranje grožnje, tveganja in kritične dele, ki so izpostavljeni grožnjam. Za vsako grožnjo morajo biti definirane kontrolne možnosti in njihove kategorije. Za vsako kontrolno možnost je treba dokumentirati stroške izvedbe, efektivnost zmanjšanja tveganja, stroške zmanjšanja tveganja na enoto (SZTE) in na osnovi SZTE predlagati najboljšo kontrolno možnost.
Poročilo mora vsebovati tudi opis področja, ki ga obravnava, obrazložitev predvidevanj, definicije uporabljenih metod in vire podatkov.

10.4. Izbira kontrolnih možnosti

V predhodni fazi izdelano poročilo se predstavi vodstvu, ki se na osnovi poročila odloča za najboljše kontrolne možnosti tveganja. Proces odločanja vsebuje naslednje korake:

1. Najprej je potrebno določiti nivo sprejemljivega tveganja (ST), ki ga vodstvo dopušča.
2. Sledi izbira groženj s tveganjem znotraj nivoja sprejemljivega tveganja (ST). Za izbrane grožnje je vodstvo pripravljeno sprejeti tveganje in zanemari v poročilu predvidene kontrolne možnosti.
3. Za vsako grožnjo, ki ima vrednost tveganja višjo od ST, se izbere nabor kontrolnih možnosti, ki zmanjšujejo tveganje na sprejemljivo raven ali pa ga popolnoma odpravijo.
4. Izmed izbranih kandidatov se izbere eno, najprimernejšo kontrolno možnost. Izbira temelji na osnovi pridobljenih in v poročilu prikazanih podatkov in na objektivni odločitvi vodstva.

Rezultat je spisek sprejemljiv tveganj in kontrolnih možnosti tveganj.

10.5. Izvedba kontrol

Sledi izvedba kontrolnih izbir:

1. Najprej se izdela študijo izvedljivosti implementacije posameznih kontrolnih možnosti tveganj. Študija vsebuje podatke o tem ali je kontrolna možnost sprejemljiva z operativnega, tehničnega in ekonomskega vidika.
2. Poročilo oz. študijo izvedljivosti se predstavi vodstvu, ki potrdi ali zavrne izvedbo.
3. V kolikor vodstvo potrdi izvedbo projekta, se izvede implementacija kontrolnih možnosti tveganj.

10.6. Nadzor tveganj

Zadnja faza predstavlja nenehno spremljanje sprememb obstoječih in pojavljanje novih groženj ter ustrezno ukrepanje ob odkritju sprememb.

11. Analiza vpliva na poslovanje

Analiza vpliva na poslovanje (AVP) se ukvarja s posledicami finančnih in operativnih vplivov nepredvidenih dogodkov na poslovanje podjetja. Finančni vplivi se kažejo v denarnih prodajnih in investicijskih izgubah v ter pogodbenih kaznih. Operativni vplivi pa se nanašajo na poslovne operacije in se lahko kažejo skozi izgubo konkurenčne prednosti, v zmanjšanju zaupanja investitorjev, v slabih uporabniških storitvah, nizki morali in v zmanjšanem ugledu podjetja (Fulmer, 2000, str. 49).

Upravljanje tveganj ocenjuje grožnje in tveganja, s katerimi se sooča podjetje. Tveganja kontrolira s pomočjo kontrolnih možnosti. Zaradi visokih stroškov, truda ali neizvedljivosti se izbor kontrolnih možnosti pogosto skrči na sprejemanje in zmanjševanje tveganja. Obe omenjeni kontrolni možnosti podjetje še vedno delno ali v celoti izpostavljata tveganjem, zato mora le to izdelati načrt za soočenje s temi tveganji.
Analiza vpliva na poslovanje je vez med fazo upravljanja s tveganji in fazo razvoja načrta za neprekinjeno poslovanje. AVP identificira kritična področja poslovanja in potrebo po neprekinjenosti, ki je bistvenega pomena za načrt neprekinjenega poslovanja.

Pri analizah finančnih vplivov mora sodelovati predstavnik finančnega oddelka, ključno pa je tudi sodelovanje vodstva, ki izbere projektnega vodjo in zagotovi t.i. sponzorja. Sponzor je član najvišjega vodstva podjetja. Njegov namen je zagotoviti formalno podporo nadaljnjim aktivnostim.

11.1. Zbiranje informacij

Analiza vpliva na poslovanje temelji na informacijah, pridobljenih od osebja podjetja. Zbiranje informacij je kompleksna naloga, zato se zbiralci poslužujejo metod, ki postopek poenostavijo. Uporabljajo vprašalnike, intervjuje in delavnice.

- Vprašalnik je sestavljen iz sklopa vprašanj, ki se pošljejo predstavnikom poslovnih enot. Vprašalnik vsebuje spremni dopis sponzorja, v katerem so navedeni razlogi za izvedbo vprašalnika oz. ankete, kontaktne informacije in časovni okvir, v katerem je treba izpolnjeni vprašalnik vrniti.
  Metoda sodelujočim dopušča, da se izpolnjevanja lotijo v času, ki jim najbolj ustreza. Pomanjkljivost metode se kaže v možnem nerazumevanju posameznih vprašanj. Pojavijo se lahko tudi zakasnitve zaradi nepravočasne vrnitve vprašalnikov.
- Z osebnim intervjujem se zbira potrebne informacije od ene ali več oseb hkrati. V osebnem soočenju je vprašanja mogoče prilagoditi posameznim intervjujancem glede na področje njihove ekspertize.
  Metoda zaradi osebnega stika zmanjšuje možnost napak zaradi nerazumevanja vprašanj. Zaradi samega načina izvajanja metoda zahteva več truda, časa in seveda stroškov za pripravo in izvedbo intervjujev.
- Delavnica omogoča skupini ljudi kolektivno sodelovanje pri zbiranju informacij. Sodelujoči diskutirajo o vprašanjih in odgovorih. Na ta način zagotovijo popolnost in zanesljivost informacij.
  Delavnica v kratkem času zagotovi veliko količino informacij. Omogoči tudi diskusije o nasprotujočih si informacijah. Največja težava, s katero se soočajo organizatorji delavnice, je zbrati vse sodelujoče ob istem času.

Na izbiro metode vplivajo stroški, učinkovitost zbiranja in kvaliteta pridobljenih informacij. Za zagotovitev najboljših rezultatov se navadno uporablja več metod hkrati. Pred izvedbo delavnice se lahko, na primer, sodelujočim pošljejo vprašalniki, ki služijo kot priprava na delavnico.

11.2. Proces analize vpliva na poslovanje

Proces analize vpliva na poslovanje je sestavljen iz posameznih korakov, ki si sledijo v zaporedju in skupaj identificirajo motnje v poslovanju ter opredeljujejo zahteve za okrevanje prekinjenih kritičnih poslovnih procesov. Proces AVP sestavlja 11 korakov:

1. Definiranje nalog, področja in domnev AVP
2. Identifikacija poslovnih funkcij in procesov
3. Ocena finančnih in operativnih vplivov
4. Identifikacija kritičnih procesov
5. Določitev NSČP in prioritet kritičnih procesov
6. Identifikacija kritičnih sistemov IT in aplikacij
7. Identifikacija drugih kritičnih virov
8. Določitev objektivnega časa okrevanja
9. Določitev objektivne točke okrevanja
10. Identifikacija zasilnih procedur
11. Izdelava povzetka AVP

Definiranje nalog, področja in domnev AVP

Prvi korak procesa AVP predstavlja osnovo za razumevanje pričakovanj vodstva v zvezi z ugotovitvami AVP. Definira tudi področje aktivnosti in oceni potrebne vire, čas in trud za izvedbo AVP.
Primarna naloga AVP je identifikacija izpadov poslovanja in opredelitev okrevalnih zahtev. AVP mora upoštevati tudi specifične naloge in pričakovanja vodstva podjetja (npr., identifikacija kritičnih področij, pomanjkljivosti obstoječih okrevalnih zmogljivosti, ocena proračuna, itd.) .
Opredelitev področja AVP usmeri delovanje v določena področja podjetja (izbere se lahko celotno podjetje ali posamezne dele, na primer, poslovne funkcije, ki uporabljajo sisteme IT).
Prvi korak AVP navaja tudi določene domneve, ki opredeljujejo možne prekinitve in zmožnosti okrevanja. Domneve predstavljajo osnovo za zbiranje informacij (npr., rezervna lokacija IT ne obstaja, prekinitev se lahko zgodi med delovnim časom, rezervnih delovnih prostorov ni, prizadeta lokacija je po izpadu nedosegljiva, itd.).

Identifikacija poslovnih funkcij in procesov

V drugem koraku AVP se, glede na opredelitev področja iz prvega koraka, izvede identifikacija poslovnih funkcij in procesov. Poslovni procesi predstavljajo naloge in aktivnosti za podporo poslovnih funkcij.

Ocena finančnih in operativnih vplivov

V tretjem koraku se izvede ocena finančnih in operativnih vplivov na podjetje v slučaju izpada poslovnih funkcij in procesov. Ocena se izvaja ločeno za finančne in operativne vplive.

Ocena finančnih vplivov

Ocena finančnih vplivov se uporablja za merjenje pomembnosti poslovnih finančnih izgub v slučaju prekinitve poslovnega procesa. Ocena se napravi za vsak poslovni proces.
Ocena finančnega izpada obravnava različne vzroke izpada dohodka in stroške, ki nastanejo zaradi prekinitve procesa. Tako se lahko npr. poleg primarnega izpada dohodka zaradi prekinitve prodajnega procesa pojavijo tudi stroški zaradi pogodbenih kazni, pride lahko do propadlih investicij in priložnosti. Pojavijo se lahko tudi dodatni stroški zaradi zaposlitve začasnih zunanjih delavcev, zaradi potovanj, nastanitve, nadur, transporta opreme IT in najemnin opreme.
Pri določitvi stopnje pomembnosti se vsak proces opredeli glede na vrednost finančnega izpada. Stopnjo pomembnosti se označuje z vrednostmi od 0 (ni vpliva) do 3 (velik vpliv).

Ocena operativnih vplivov

Ocena operativnih vplivov meri negativne vplive prekinitvenih dogodkov na različne vidike poslovnih operacij, povezanih z izgubo zaupanja investitorjev, tržnega deleža, konkurenčne prednosti, zaupanja, ugleda, morale, itd.
Ocene operativnih vplivov na posamezne procese so subjektivne ocene posameznih udeležencev AVP. Operativni vplivi se označujejo z oznakami: ni, nizek, srednji, visok, najvišji;

Identifikacija kritičnih procesov

Z identifikacijo kritičnih procesov se na osnovi ocen finančnih in operativnih vplivov določi poslovne procese, ki so nepogrešljivi za vzdrževanje poslovne kontinuitete. Proces se opredeli kot kritičen, če izpolnjuje kateregakoli od naslednjih pogojev:

- Stopnja pomembnosti finančnega vpliva je ocenjena z vrednostjo 2 ali 3.
- Vsaj tri ocene operativnih vplivov so označene z oznako »visok«.
- Vsaj dve oceni operativnih vplivov sta označeni z oznako »visok« in vsaj ena z oznako »najvišji«.
- Vsaj dve oceni operativnih vplivov sta označeni z oznako »najvišji«.

Določitev NSČP in prioritet kritičnih procesov

Identifikaciji kritičnih procesov sledi določitev njihovih največjih sprejemljivih časov prekinitev (NSČP) in določitev prioritet okrevanja.
Največji sprejemljiv čas prekinitve (NSČP) predstavlja maksimalen čas prekinitve poslovnega procesa, ki ga podjetje lahko tolerira. Po preteku tega časa dosežejo finančni in operativni vplivi nivo, ki ni več sprejemljiv. To je čas med izpadom delovanja in začetkom normalnega procesiranja.
Prioriteto okrevanja se določa glede na NSČP. Nižja vrednost NSČP predstavlja višjo prioriteto okrevanja.

Identifikacija kritičnih sistemov IT in aplikacij

Kritični informacijski sistemi in aplikacije se uporabljajo za podporo kritičnim poslovnim procesom. Najprej je treba napraviti spisek vseh sistemov in aplikacij, ki se uporabljajo pri poslovanju. Ko je spisek končan, se poveže kritične poslovne procese s kritičnimi sistemi in aplikacijami.

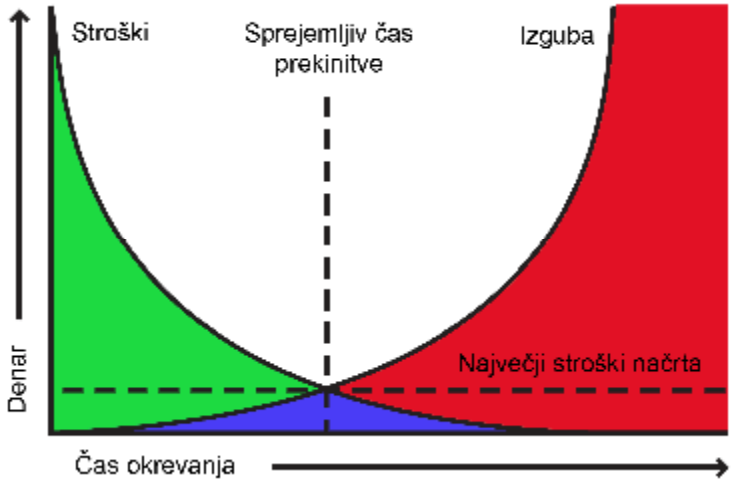
Identifikacija drugih kritičnih virov

Poleg informacijskih sistemov se v podjetju za podporo kritičnim poslovnim procesom uporablja tudi druge vire. Med kritične vire poslovnih procesov lahko spadajo pisarniška oprema in potrebščine, delovni prostor, pohištvo, varnostna oprema, komunikacijska oprema, dokumentacija, orodje, material, idr.

Določitev objektivnega časa okrevanja

Objektiven čas okrevanja (OČO) je vezan na okrevanje informacijskih in drugih virov po prekinitvi. OČO je razpoložljivi čas okrevanja prizadetih sistemov in virov (računalniški sistemi, komunikacijska oprema, prostori, itd.). To je čas med izpadom delovanja in okrevanjem sistemov in virov.
Potrebno je poiskati optimalno točko okrevanja, ki jo določajo stroški okrevanja in stroški zaradi prekinjenosti delovanja. Stroški, ki so nastali zaradi prekinitve delovanja, s časom nedelovanja rastejo, stroški povezani z izbiro okrevalne tehnologije sistemov po prekinitvi pa se s časom zmanjšujejo (Developing a Business Continuity Plan, 2003, str. 8). Kompleksnejša tehnologija omogoča hitrejše okrevanje, predstavlja pa tudi večje stroške izgradnje (slika 23).

Slika 23: **Določitev časa okrevanja**



Vir: Developing a Business Continuity Plan, 2003, str. 8

Največji sprejemljiv čas prekinitve (NSČP) je sestavljen iz vrednosti OČO in delovnega časa okrevanja (DČO). DČO je razpoložljivi čas za okrevanje sistemov in virov, povrnitev izgubljenih in ročno zbranih podatkov. To je čas od okrevanja sistemov in virov do začetka normalnega procesiranja.

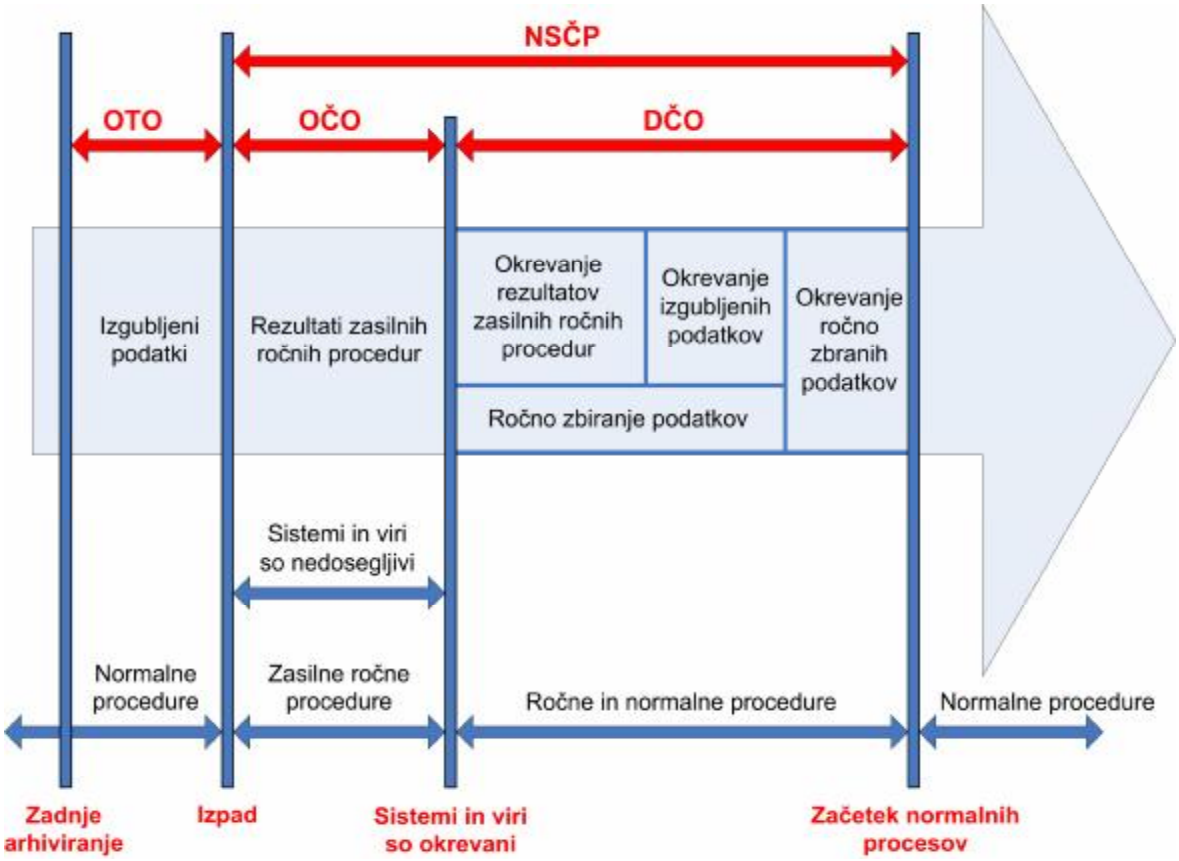
Določitev objektivne točke okrevanja

Objektivna točka okrevanja (OTO) predstavlja dopustni delež izgube podatkov poslovnega procesa, merjen z vidika časa. Gre za časovni interval od trenutka oz. točke zadnjega arhiviranja podatkov do izpada delovanja.

Vse do sedaj opisane komponente časovnih zahtev okrevanja so definirane z vidika treh dogodkov (slika 24):

- Izvedba zadnjega arhiviranja podatkov je čas pred izpadom, v katerem so bili podatki zadnjič arhivirani oz. shranjeni. Podatki, ki so bili procesirani med zadnjim arhivom in izpadom, so izgubljeni.
- Okrevanje sistemov in virov predstavlja čas, ko pride do okrevanja v normalno stanje po izpadu.
  Med okrevanjem sistemov se izvajajo zasilne ročne procedure, ki omogočijo nadaljevanje dela. Delo, procesirano s pomočjo zasilnih procedur, se kasneje vnese in procesira s pomočjo okrevanih sistemov.
- Začetek normalnega procesiranja je čas začetka izvajanja normalnih operacij na okrevanih sistemih.
  Po okrevanju sistemov in virov se vzporedno izvaja ročne in normalne procedure. Medtem ko se izgubljeni podatki in rezultati zasilnih procedur vnašajo in procesirajo s pomočjo okrevanih sistemov, se novi podatki procesirajo ročno. Po zaključenem vnosu izgubljenih podatkov in rezultatov zasilnih procedur se na sistemih začne procesiranje ročno zbranih podatkov. Ko so vsi podatki ustrezno obdelani, se začne normalno procesiranje.

Slika 24: **Časovni okvir okrevanja**



Vir: Syed, 2004, str. 67

Identifikacija zasilnih procedur

Zasilne procedure omogočajo nadaljevanje kritičnih poslovnih procesov v primeru izpada delovanja informacijskih in drugih virov. Zasilne procedure predpisujejo uporabo zasilnih metod, ki pogosto vsebuje začasne, manj učinkovite in dražje ročne operacije.

Izdelava povzetka AVP

V zadnjem koraku procesa AVP se izdela skupno poročilo z rezultati predhodnih korakov.

12. Razvoj strategije neprekinjenega poslovanja

Strategijo neprekinjenega poslovanja sestavlja sklop okrevalnih možnosti, ki jih je mogoče uporabiti, če postanejo obstoječi kritični viri nedosegljivi oz. neuporabni. Informacijski sistemi in infrastruktura, podatki in zapisi, delovni prostori in proizvodna oprema so področja, za katera je potrebno predvideti okrevalne možnosti.
Ogrodje razvoja strategije neprekinjenega poslovanja je sestavljeno iz štirih faz:

- Identifikacija okrevalnih zahtev
- Identifikacija okrevalnih možnosti
- Ocena časovne razpoložljivosti
- Ocena stroškov in sposobnosti

12.1. Identifikacija okrevalnih zahtev

Prva faza identificira okrevalne zahteve, ki jih mora upoštevati strategija neprekinjenega poslovanja. Spisek okrevalnih zahtev, ki so v glavnem pridobljene iz analize vpliva na poslovanje, določa kritične procese in vire, na katere se mora osredotočiti okrevalna strategija. Spisek opredeljuje tudi časovne zahteve (NSČP, OTO, OČO, DČO) okrevanja procesov in virov.
Identificirane okrevalne zahteve se grupira v skupine glede na področje uporabe (informacijski sistemi in infrastruktura, podatki in zapisi, delovni prostori, proizvodna oprema). Okrevalne zahteve za posamezna področja pa se delijo na kategorije:

- Področje okrevanja: delovni prostori
  Kategorije okrevalnih zahtev:
    - Rezervni delovni prostori za osebje
    - Krizni center za odločanje in upravljanje
- Področje okrevanja: proizvodna oprema
  Kategorije okrevalnih zahtev:
    - Kritična oprema in viri
    - Kritični produkti
    - Rezervni proizvodni prostori
- Področje okrevanja: informacijski sistemi in infrastruktura
  Kategorije okrevalnih zahtev:
    - Kritični sistemi IT in infrastruktura
    - Rezervna lokacija
- Področje okrevanja: podatki in zapisi
  Kategorije okrevalnih zahtev:
    - Kritični podatki in njihovo shranjevanje na drugi lokaciji
    - Kritični zapisi in njihovo shranjevanje na drugi lokaciji

12.2. Identifikacija okrevalnih možnosti

Naloga drugega koraka je predstaviti razpoložljive okrevalne možnosti glede na zahteve predhodnega koraka. Okrevalne možnosti se določijo za vsako področje.

Delovni prostori

Za področje, ki obravnava delovne prostore, se v primeru neuporabnosti le-teh predvidi možnost najema komercialne mobilne lokacije (opremljeno vozilo), najema hotelskih prostorov ali najema rezervne lokacije prostorov pri zunanjem dobavitelju. Podjetje lahko predvidi tudi uporabo rezervnih prostorov na lokaciji, ki jo ima v svoji lasti, ali pa predvidi delo od doma.
Kritične vire je v primeru izpada mogoče zagotoviti z vnaprej pripravljenimi rezervnimi kritičnimi viri, ki služijo samo za primer izpada. Drugo možnost predstavlja vnaprejšnji dogovorom z dobaviteljem o dobavi potrebnih virov v določenem času. Tretja možnost predvideva naročanje kritičnih virov pri dobaviteljih glede na potrebo, ki se pojavi po izpadu delovanja.

Proizvodna oprema

Za področje proizvodne opreme se lahko predvidi možnost pridobitve opreme in virov po izpadu glede na potrebo ali z vnaprejšnjo pripravo. Pri vnaprejšnji pripravi je mogoče z dobaviteljem skleniti pogodbo o dobavi okvarjene opreme in virov v primeru nesreče. Možno pa je kritične dele in opremo tudi vnaprej shraniti na oddaljeni rezervni lokaciji.
Za zagotovitev potrebnih materialov in produktov v primeru nesreče je možno le-te shraniti v oddaljenem skladišču. Druga možnost predvideva recipročni dogovor o pomoči s podjetji, ki se ukvarjajo s podobno dejavnostjo.
Za zagotovitev rezervnih proizvodnih prostorov lahko podjetje predvidi uporabo praznih prostorov podjetja na oddaljeni rezervni lokaciji. Prostore je mogoče najeti pri komercialnem ponudniku. Tretja možnost predvideva popravilo poškodovanih prostorov. V primeru nesreče se lahko za skupno, deljeno rabo, uporabijo tudi proizvodni prostori drugega proizvodnega področja v istem podjetju.

Informacijski sistemi in infrastruktura

Metode zagotavljanja rezervnih sistemov IT:

- Nadomestne kritične sisteme je mogoče zagotoviti z vnaprej (pred nesrečo) pripravljenimi sistemi, ki služijo samo za primer izpada. Možnost pride do izraza v okoljih, kjer se zahteva hitro okrevanje. Aktiviranje takih sistemov traja nekaj ur, največ nekaj dni.
- Druga možnost predvideva vnaprejšnji dogovor (pred nesrečo) z dobaviteljem o hitri dobavi sistemov v slučaju nesreče. Okrevanje traja ponavadi od dveh do sedem dni.
- Tretja možnost predvideva naročanje kritičnih sistemov pri dobaviteljih glede na potrebo, ki se pojavi po izpadu delovanja. Okrevanje traja več dni, tednov ali celo mesecev.

Rezervna lokacija za sisteme IT:
Na izbiro rezervne lokacije vpliva več faktorjev, ki jih je treba upoštevati pri izbiri (Marcus, 2003, str. 484). Oddaljenost med primarno in rezervno lokacijo mora biti dovolj velika, da večje naravne ali druge nesreče ne prizadenejo obeh lokacij hkrati. Rezervna lokacija mora imeti dobro prometno dostopnost in mrežno povezljivost s primarno lokacijo. Priporočljivo je, da lokaciji uporabljata ločene telekomunikacijske in energetske vire. Prednost imajo lokacije, ki so v bližini zdravstvenih ustanov, ki so grajene v skladu s potresnimi standardi, ki zagotavljajo želeno stopnjo varnosti, niso previsoke in nudijo dovolj prostora za informacijsko opremo in osebje.

Pri izbiri rezervne lokacije za informacijske sisteme se lahko podjetje glede na lastništvo odloča med različnimi možnostmi.

- Za rezervno lokacijo lahko izbere lastne prostore na oddaljeni lokaciji podjetja.
- Podjetje se lahko dogovori za skupno rabo prostorov z drugim podjetjem.
- Možno je najeti mobilno lokacijo ali najem rezervne lokacije pri komercialnem ponudniku.
- Pri komercialnih ponudnikih je mogoče najeti lastne rezervne prostore.
- Pri komercialnih ponudnikih je mogoče najeti skupne rezervne prostore.

Opremljenost rezervne lokacije za sisteme IT:
Rezervne lokacije se glede na opremljenost delijo na t.i. mrzle, tople in vroče lokacije (Maiwald, Sieglein, 2002, str. 185).

- Mrzla lokacija zahteva za pridobitev, namestitev in pripravo strojne in programske opreme dva do tri tedne.
- Topla lokacija ima nekaj najpotrebnejše strojne, programske in komunikacijske opreme že nameščene. Pridobitev in namestitev manjkajoče opreme lahko traja nekaj dni do dveh tednov.
- Vroča lokacija je v celoti opremljena in pripravljena za uporabo. Tako lokacijo je mogoče aktivirati v nekaj urah.

Podatki in zapisi

Pogostost shranjevanja kritičnih zapisov:
Kritični zapisi se lahko shranjujejo dnevno, tedensko, mesečno ali letno.

Mediji za shranjevanje kritičnih zapisov:
Zapisi se lahko shranjujejo na različne medije kot so mikrofilm, optični disk, magnetni trakovi, trdi diski, CD, DVD.

Restavriranje kritičnih zapisov:
Za restavriranje zapisov po nesreči se lahko sklene pogodba z zunanjim izvajalcem. Pogodba je lahko sklenjena vnaprej (pred nesrečo) ali po potrebi (po nesreči).

Lokacija za shranjevanje kritičnih zapisov:
Zapise je mogoče shranjevati na oddaljeni lokaciji v lasti podjetja, ali pa se sklene dogovor z zunanjim ponudnikom, ki razpolaga s posebej opremljenimi prostori za shranjevanje zapisov.

Pogostost shranjevanja kritičnih podatkov:
- Shranjevanje podatkov lahko poteka nepretrgoma (z uporabo replikacije na pomnilniško enoto oddaljene lokacije).
- Shranjevanje se lahko izvaja enkrat dnevno.
- Shranjevanje se lahko izvaja enkrat tedensko.
- Shranjevanje se lahko izvaja enkrat mesečno.

Tipi shranjevanja kritičnih podatkov:
Obstajajo trije načini shranjevanja podatkov (Wallace, 2004, str. 318).
- Shranjevanje oz. arhiviranje podatkov je lahko popolno (napravi se kompleten arhiv vseh podatkov).
- Shranjevanje podatkov je lahko inkrementalno (arhivirajo se samo podatki, ki so bili kreirani ali spremenjeni od zadnjega popolnega ali inkrementalnega arhiviranja).
- Shranjevanje podatkov je lahko diferentno (arhivirajo se samo podatki, ki so bili kreirani ali spremenjeni od zadnjega popolnega arhiviranja).

Načini varovanja kritičnih podatkov:
Glede na zahtevani objektivni čas okrevanja (OČO) in objektivno točko okrevanja (OTO) je mogoče uporabiti različne metode arhiviranja podatkov.
- Zrcaljenje podatkov med lokacijami se uporablja v okoljih, ki zahtevajo konstantno razpoložljivost podatkov (OČO=0, OTO=0).
- Globalne topologije gruč (multipliciranje strežnikov) med oddaljenimi lokacijami (Bachra, 2003, str. 7) zagotavljajo OČO manj kot 8 ur in OTO manj od 30 minut.

    - Replicirana podatkovna gruča ne uporablja skupnih diskov. Podatki se replicirajo med strežniki.
    - Globalna gruča povezuje več lokalnih gruč na oddaljenih lokacijah. Podatki se med oddaljenimi lokacijami replicirajo.
    - Gruča brez skupnih podatkov uporablja podatke samo za branje. Na vseh strežnikih so enaki podatki, ki se ne spreminjajo.
    - Kampus gruča hkrati dostopa do dveh ločenih diskovnih polj. Podatki med diskovnimi polji se zrcalijo (RAID 1).
    - Osnovna gruča povezuje več strežnikov, ki so priključeni na isto diskovno polje.
- Omrežna diskovna polja (OČO < 8 ur in OTO < 30 minut).
- Virtualizacija diskovnih polj združi več diskovnih polj v eno navidezno enoto (OČO < 8 ur in OTO < 30 minut).
- Varovanje podatkov s pomnoženo množico neodvisnih diskov (Redundant Array of Independent (Inexpensive) Disks – RAID). Obstaja več variant konfiguracije RAID (Troppens, Erkens, 2004, str. 23), ki pridejo v poštev za OČO manj kot 8 ur in OTO manj kot 30 minut.
    - RAID 0 – ne ščiti pred izgubo podatkov. Omogoča združevanje diskov.
    - RAID 1 – zrcaljenje diskov.
    - RAID 2 – podatke razdeli po diskih.
    - RAID 3 – podatke razdeli po diskih manj razdrobljeno kot RAID 2.
    - RAID 4 – podatke razprši po diskih. Na dodatnem disku ima kontrolne informacije, ki omogočajo povrnitev podatkov.
    - RAID 5 – podatke in kontrolne informacije razprši po več diskih.
    - RAID 0+1 – združi dva niza diskov RAID 0 na način RAID 1.
    - RAID 10 – združi več parov RAID 1 v niz diskov RAID 0.
- Senčenje volumnov oz. posnetki volumnov omogočajo občuten napredek pri arhiviranju in varovanju podatkov (Shapiro, 2004, str. 26). Osnovni koncept tehnologije je v kreiranju kopij volumnov v izbranem trenutku (OČO < 8 ur in OTO < 30 minut).
- Replikacija podatkov med lokacijami (Marcus, 2003, str. 435) pride v poštev za OČO manj kot 8 ur in OTO manj kot 30 minut.
    - Sinhrona replikacija poteka v realnem času in predstavlja veliko komunikacijsko obremenitev. Zahteva se sprotna potrditev o korektnosti pošiljanja za vsak poslan paket. Primerna je za manjše razdalje.
    - Pri asinhroni replikaciji se podatki zbirajo lokalno in pošiljajo, ko je mogoče. Replikacija je primerna za večje razdalje.
    - Pol-sinhrona replikacija je produkt podjetja EMC za produkte SRDF, ki ne omogočajo asinhrone replikacije.
    - Pri periodični replikaciji se podatki pošiljajo v paketu, vsi naenkrat.
- Avtomatično arhiviranje (electronic vaulting) zagotavlja OČO manj kot 72 ur in OTO manj kot 24 ur.
- Pošiljanje transakcijskih logov na rezervno lokacijo (remote journaling) zagotavlja OČO manj kot 72 ur in OTO manj kot 24 ur.
- Kadar čas okrevanja ne igra bistvenejše vloge (OČO>72h, OTO>24h), se uporabi tradicionalna metoda arhiviranja podatkov na kasete.

Lokacija za shranjevanje kritičnih podatkov:
- Podatke je mogoče shranjevati na oddaljeni lokaciji v lasti podjetja.
- Dogovor z zunanjim ponudnikom, ki razpolaga s posebej opremljenimi prostori za arhiviranje podatkov.

12.3. Ocena časovne razpoložljivosti

Namen tretje faze je ugotoviti uporabnost identificiranih okrevalnih možnosti iz predhodne faze. Naredi se ocena pričakovanega razpoložljivega časa (PRČ) virov okrevalnih možnosti. Za vsako okrevalno možnost se oceni čas, v katerem je možno zagotoviti funkcionalnost virov. PRČ se nato primerja z zahtevanimi časi okrevanja (največji sprejemljiv čas prekinitve – NSČP, objektiven čas okrevanja – OČO, objektivna točka okrevanja – OTO, delovni čas okrevanja – DČO). V kolikor PRČ zadovoljuje zahteve časov okrevanja, je okrevalna možnost uporabna.

12.4. Ocena stroškov in sposobnosti

Okrevalne možnosti, ki so ustrezne z vidika časovnih zahtev, se ocenijo in primerjajo z vidika stroškov in sposobnosti, ki jih nudijo. Izbrane rešitve postanejo del strategije neprekinjenega poslovanja.
V prvem koraku se izdela lista atributov, ki opredeljujejo sposobnosti okrevalnih možnosti. Z atributi se lahko opiše nivo truda, ki je potreben za izvedbo, kvaliteto produktov, podatkov in storitev, ki jih rešitev omogoča, zadovoljitev varovalnih zahtev, nivo kontrole, ki jo ima podjetje pri izgradnji in uporabi ter fizično in informacijsko varovanje.
V drugem koraku se vsaka okrevalna možnost oceni s stroškovnega vidika. Stroškovna ocena se pripiše atributom iz prvega koraka. Tako za stroške kot tudi za opredelitev atributov se lahko uporabi opisne vrednosti: nizek, srednji, visok;

Pri izbiri ustrezne strategije je potrebno paziti na splošna priporočila glede karakteristik in zmožnosti posameznih variant in ustreznost pogodb ter dogovorov z dobavitelji in zunanjimi izvajalci.

13. Načrt neprekinjenega poslovanja

Načrt neprekinjenega poslovanja predpisuje vnaprej pripravljene postopke, ki jih podjetje uporabi v slučaju krize in tako zmanjša vpliv na poslovanje. Naloga NNP je vzpostaviti delovanje kritičnih procesov znotraj določenega časovnega okvira.
Posamezni načrti neprekinjenega poslovanja se lahko med seboj precej razlikujejo. Odvisni so od potreb podjetja. Vsak NNP je sprejemljiv, če je aktualen, prilagodljiv in ni prezahteven za izgradnjo z vidika razpoložljivih virov. Da je NNP sprejemljiv, mora biti tudi dovolj obsežen. Pokrivati mora vse kritične procese in vsebovati vse v nadaljevanju opisane izvršilne faze načrta, ki si sledijo po prekinitvenem dogodku.
V nadaljevanju so predstavljena osnovna poglavja, ki naj bi jih vseboval načrt neprekinjenega poslovanja.

13.1. Namen in področje NNP

Namen načrta za neprekinjeno poslovanje je zmanjšati posledice motnje na sprejemljiv nivo, s pomočjo vnaprej pripravljenih okrevalnih procedur. Glavna naloga NNP je vzpostavitev delovanja kritičnih procesov, ki so bili identificirani v analizi vpliva na poslovanje.
Področje NNP določa operativna in tehnična področja znotraj in zunaj podjetja (specifične lokacije podjetja, poslovne enote, rezervne lokacije, lokacije za arhiviranje podatkov, poslovne partnerje, stranke, dobavitelje opreme, javne ustanove, idr.).

Prvo poglavje lahko vsebuje tudi informacije o največji dolžini časa, ki je predviden za okrevalne operacije, o tipu dogodkov, ki lahko povzročijo izvajanje načrta, in o področjih, ki jih načrt ne pokriva.

13.2. Definicija nesreče

Za nesrečo se šteje vsak dogodek, ki moti normalno delovanje kritičnih poslovnih procesov in zmanjšuje njihovo delovanje na nivo, ko postanejo posledični operativni in finančni vplivi na podjetje nesprejemljivi.
Definicija nesreče pomaga pri določitvi, ali se motnja lahko opredeli kot nesreča, ki zahteva uporabo procedur iz NNP, ali pa se lahko za njeno sanacijo uporabi standardne operativne postopke.
Definicija klasificira nesreče tudi z vidika pomembnosti, kar pomaga določiti pravilni odziv v krizni situaciji. Klasifikacija lahko predstavlja delitev na manjše, srednje in velike nesreče:

- Manjše nesreče se, glede na ostale tipe nesreč, pojavljajo najpogosteje. Nesreča je pogosto izolirana na manjše dele kritičnih poslovnih procesov. Poslovne enote, ki so odvisne od prizadetih kritičnih procesov, lahko določeno obdobje še vedno nadaljujejo z izvajanjem svojih osnovnih operacij. Vzrok prekinitve je pogosto okvara posamezne komponente, sistema ali servisa. Primeri manjših nesreč so lahko okvare računalniških diskov in mrežnih komponent.
- Srednje nesreče se pojavljajo manj pogosto, zato pa je njihov vpliv na delovanje veliko večji kot pri manjših nesrečah. Srednje nesreče motijo normalno delovanje posameznih, vendar ne vseh poslovnih enot. Do motenja delovanja pride zaradi večjih okvar na več sistemih in opremi. Primer nesreče srednjega tipa je vdor vode v sistemski prostor zaradi okvare na napravah za hlajenje.
- Velike nesreče se pojavljajo zelo redko, kadar pa se pojavijo, je njihov učinek katastrofalen. Velike nesreče prekinejo delovanje večine ali vseh kritičnih poslovnih procesov. Posledice se kažejo v nedelovanju ali nedosegljivosti večine ali vseh sistemov in opreme. Primer velike nesreče predstavlja nedosegljivost ali uničenje delov podjetja zaradi požara, potresa ali sabotaže.

13.3. Povzetek upravljanja s tveganji

Povzetek vsebuje bistvene informacije upravljanja s tveganji. V njem so sledeče informacije:

- Seznam groženj in tveganj.
- Seznam kritičnih delov, ki so izpostavljeni grožnjam.
- Seznam uporabljenih kontrolnih možnosti tveganj in preostalih tveganj.

13.4. Povzetek analize vpliva na poslovanje

Povzetek vključuje bistvene ugotovitve analize vpliva na poslovanje. Povzetek vsebuje seznam kritičnih procesov in njihovih zahtev za okrevanje z vidika naslednjih komponent:

- Največji sprejemljiv čas prekinitve (NSČP).
- Kritični sistemi IT in aplikacije.
- Drugi kritični sistemi.
- Objektiven čas okrevanja (OČO), objektivna točka okrevanja (OTO), delovni čas okrevanja (DČO) kritičnih aplikacij in virov.

13.5. Povzetek strategije neprekinjenega poslovanja

Povzetek predstavlja izbrane okrevalne strategije za posamezna področja in kategorije:

- Področje okrevanja: delovni prostori
  Kategorije okrevalnih zahtev:
    - Rezervni delovni prostori za osebje
    - Krizni center za odločanje in upravljanje
- Področje okrevanja: proizvodna oprema
  Kategorije okrevalnih zahtev:
    - Kritična oprema in viri
    - Kritični produkti
    - Rezervni proizvodni prostori
- Področje okrevanja: podatki in zapisi
  Kategorije okrevalnih zahtev:
    - Kritični podatki in njihovo shranjevanje na drugi lokaciji
    - Kritični zapisi in njihovo shranjevanje na drugi lokaciji
- Področje okrevanja: informacijski sistemi in infrastruktura
  Kategorije okrevalnih zahtev:
    - Kritični sistemi IT in infrastruktura
    - Rezervna lokacija

13.6. Skupine za neprekinjeno poslovanje

Poglavje definira organizacijo, vlogo in odgovornosti skupin za neprekinjeno poslovanje. Velikost in število skupin je odvisno od področja in zahtevnosti NNP. Člani skupine so izbrani na podlagi njihovega znanja in izkušenj. Ponavadi so skupine sestavljene iz ljudi, ki opravljajo enake ali podobne operacije tudi v normalnih pogojih delovanja. Če je mogoče, je vsak član hkrati tudi rezerva nekemu drugemu članu, če je ta med postopkom okrevanja nedosegljiv. Člani skupine morajo poznati tudi naloge in procedure drugih skupin. Treba je upoštevati tudi možnost, da nesreča posameznim članom skupine onemogoči udeležbo, zato skupine, če je mogoče, vključujejo tudi člane iz drugih geografskih področij, pogodbeno osebje in zunanje partnerje. Vsaka skupina ima vodjo, ki usmerja in potrjuje operacije, komunicira z drugimi vodji skupin in vodstvom podjetja.
Običajno so skupine razdeljene v tri nivoje, ki jih predstavlja krizno upravljanje, nadaljevanje poslovanja ter tehnično in operativno okrevanje.

Skupina za krizno upravljanje

Skupina za krizno upravljanje vključuje več ekip, ki jih usmerja vodja ekipe za krizno upravljanje in med seboj koordinira koordinator neprekinjenega poslovanja:

- Ekipa za krizno upravljanje (EKU) upravlja in kontrolira izvajanje načrtov neprekinjenega poslovanja, nujnega odgovora in kriznega komuniciranja. Vodja ekipe mora biti član najvišjega vodstva podjetja, ki prevzame celovito usmerjanje. Vodja ekipe za krizno upravljanje ima v svojih rokah končno odločitev in pooblastila za zagon izvajanja NNP. Preostali člani ekipe so koordinator neprekinjenega poslovanja in vodje ekip za nujen odgovor, za oceno škode, za krizno komuniciranje, za obveščanje, za logistiko in preskrbovanje virov ter za oceno tveganja. Navedeni člani vodji EKU zagotavljajo informacije o aktivnostih svojih ekip. EKU lahko vključuje tudi predstavnike iz oddelka informacijske tehnologije, kadrovske službe, pravnega oddelka, finančnega oddelka in predstavnike iz drugih relevantnih poslovnih enot.

- Koordinator neprekinjenega poslovanja (KNP) je odgovoren za celovito upravljanje izvedbenih faz (začetni odgovor in oznanilo, ocena problema in eskalacija, razglasitev nesreče, logistika, okrevanje, normalizacija). Koordinira aktivnosti in predstavlja komunikacijsko povezavo med ekipo za krizno komuniciranje in drugimi ekipami. KNP je zadolžen tudi za razvoj, testiranje in vzdrževanje načrta.
- Ekipa za oceno škode (EOŠ) je mobilizirana takoj po nastanku motnje. Zadolžena je za oceno obsega škode in potrebnega časa za okrevanje.
- Ekipa za obveščanje (EO) je odgovorna za obveščanje ekip in ljudi, ki sodelujejo pri izvajanju načrta in njegovih okrevalnih procedur.
- Ekipa za nujni odgovor (ENO) je odgovorna za zaščito življenj, lastništva in okolja takoj po nesreči. ENO pomaga pri evakuaciji, reševanju, medicinski pomoči in preprečevanju incidentov. Svoje aktivnosti usklajuje s policijo, reševalci in gasilci. ENO skuša stabilizirati situacijo. V ta namen uporablja procedure in smernice iz načrta za nujni odgovor.
- Ekipa za krizno komuniciranje (EKK) zagotavlja osebju, vodstvu, poslovnim partnerjem, strankam in javnosti konsistentne, pravočasne in točne informacije o nastali krizi. V skladu z vnaprej pripravljenimi smernicami iz načrta za krizno komuniciranje EKK zagotavlja informacije o tipu prekinitve, statusu, akcijah in predvidenem času okrevanja.
- Ekipa za logistiko in preskrbovanje virov (ELPV) je zadolžena za hitro pridobitev potrebnih virov in opreme za okrevanje. Zadolžena je tudi za mobilizacijo ljudi, virov, opreme in zalog na rezervno lokacijo.
- Upravljavec ocene tveganja (UOT) oceni in nadzira tveganja, ki so povezana z nastalo motnjo in izvajanjem NNP. Ocena vključuje tveganja, ki se nanašajo na varnost, zavarovanje, pravne obveze in zaščito.

Skupina za nadaljevanje poslovanja

Skupina za nadaljevanje poslovanja je sestavljena iz dveh ekip, katerih delovanje usklajuje koordinator neprekinjenega poslovanja:

- Ekipa za uporabniško upravljanje (EUU) celovito oceni trenutne potrebe uporabniških oddelkov, nadzira napredovanje in status okrevanja ter koordinira okrevalne aktivnosti med ekipami posameznih poslovnih enot in ekipami za tehnično okrevanje IT. EUU vključuje vodilne člane ekip poslovnih enot.
- Ekipe poslovnih enot (EPE) so sestavljene iz ključnih uporabnikov kritičnih sistemov in virov v posameznih poslovnih enotah. Naloga EPE je oceniti trenutne potrebe enote in pomagati tehnični okrevalni ekipi za IT pri povrnitvi izgubljenih podatkov in virov. EPE pomaga pri ročnem vnašanju shranjenih podatkov in potrdi uspešnost okrevanja.

Skupina za tehnično in operativno okrevanje

Skupina za tehnično in operativno okrevanje je sestavljena iz ekip za okrevanje virov IT in drugih virov, ki jih med seboj usklajuje koordinator neprekinjenega poslovanja:

- Ekipe za tehnično okrevanje IT (ETOIT) vključujejo različne ekipe (ekipa za operacijske sisteme, mrežna ekipa, ekipa za baze podatkov, aplikacijska ekipa, ekipa za arhiviranje, varnostna ekipa, itd.), od katerih se vsaka posveča okrevanju specifičnega tehničnega področja.
- Ekipe za tehnično okrevanje proizvodnje (ETOP) vključujejo različne ekipe (ekipa za odpravljanje okvar na opremi, ekipa za testiranje, ekipa za nadzor varnosti, podporna

ekipa, inženirska ekipa, električarji, itd.), ki so odgovorne za okrevanje kritičnih proizvodnih virov in opreme.

- Ekipa za varnost in rokovanje z nevarnimi materiali (EVRNM) pomaga pri okrevalnih aktivnostih na rezervni lokaciji in obnovi prizadete lokacije. Ekipa je odgovorna za pregled in ugotavljanje nezdravih pogojev in kontaminacij ter za izvedbo ustreznih varnostnih kontrol. Glede na tip nevarnosti lahko vključi tudi strokovnjake in inšpektorje za delo z nevarnimi materiali, ognjem, plini, vodo, elektriko in mikrobiologe.
- Ekipa za reševanje in okrevanje vitalnih zapisov (EROVZ) se ukvarja z reševanjem prizadetih zapisov. Preprečuje nadaljnjo izgubo in izvaja procedure za obnovitev zapisov v originalno stanje. Pri obnovitvenih postopkih pomaga ekipa za varnost in rokovanje z nevarnimi materiali.
- Ekipa za restavriranje podatkov in kritičnih zapisov iz arhivov (ERPKZA) je odgovorna za restavriranje operacijskih sistemov, aplikacij, podatkov, kritičnih zapisov, navodil in dokumentov iz arhivov. Ekipa je odgovorna tudi za zagotavljanje varnosti arhivskih medijev.
- Administrativna ekipa za koordinacijo podpore (AEKP) je zadolžena za usklajevanje okrevalnih procesov z rezervno lokacijo, lokacijo za shranjevanje podatkov in z dobavitelji strojne in programske opreme. Ekipa je zadolžena za preskrbo s hrano, nastanitev, potovanja in beleženje stroškov.
- Ekipa za restavriranje (ER) je odgovorna za pospeševanje in lajšanje tranzicije iz rezervne lokacije nazaj na primarno ali na neko novo lokacijo.

13.7. Kontaktne informacije

Komuniciranje z razpršenim osebjem znotraj podjetja je velikokrat težko že v normalnih razmerah, v kriznih situacijah pa je komunikacija z ekipami in njihovimi člani še veliko težja. Za zagotovitev uspešne komunikacije je zelo pomembno, da se zagotovi ažurnost kontaktnih informacij znotraj NNP.
Običajno se za organizacijo kontaktnih informacij uporabljata klicna drevesna struktura in kontaktna lista.
Obveščanje poteka od zgoraj navzdol. Nadrejeni član v drevesni strukturi obvešča vse člane, s katerimi je povezan in se v strukturi nahajajo pod njim. Obveščeni člani informacije dalje posredujejo povezanim članom, ki so v drevesni strukturi pod njimi. Postopek obveščanja se nadaljuje do dna drevesne strukture. Vsakemu članu v drevesni strukturi mora biti dodeljen tudi rezervni član, s katerim se pveže, če primarni član ni dosegljiv.
Kontaktne lista vsebujejo potrebne informacije za kontaktiranje posameznih članov. Obstaja lahko več kontaktnih list. Na primer, glavna kontaktna lista z imeni vseh kontaktov, ki so sortirani po abecednem vrstnem redu, in kontaktne liste za posamezne ekipe, kjer so za vsakega posameznika navedeni naslednji podatki:

- Ime ekipe
- Ime člana
- Vloga člana
- Službena telefonska številka
- Številka prenosnega telefona
- Domača telefonska številka
- Elektronski naslov
- Pričakovana obvestila in komunikacije vsebujejo korespondenco, ki jo bo član prejel, ko se bo začel izvajati NNP.

13.8. Izvršilne faze NNP

Načrt neprekinjenega poslovanja sestavlja zaporedje izvršilnih faz, ki si sledijo po prekinitvenem dogodku.

Začetni odgovor in objava

Začetni odgovor in objava predstavljata prvo fazo, ki se izvede takoj po prekinitvenem dogodku. Obvesti se koordinatorja neprekinjenega poslovanja in aktivira načrt. Po potrebi se obvesti gasilsko in reševalno službo, mobilizira se ekipo za oceno škode, naredi se uvodno poročilo, v katerem se oceni tip in obseg škode, aktivira se ekipo za obveščanje in obvesti ekipo za krizno upravljanje.

Ocena problema in eskalacija

V drugi fazi se na osnovi uvodnega poročila predhodne faze najprej ugotovi obseg problema. Sledi odločitev o eskalaciji problema in izvedbo naslednje faze. Rezultat faze je detajlno poročilo o problemu.

Razglasitev nesreče

Odločitev o razglasitvi nesreče temelji na detajlnem poročilu, ki je bilo izdelano v predhodni fazi. Izbere se ustrezen okrevalni pristop in pripravi izjavo o razglasitvi nesreče, ki služi kot vodilo pri izvajanju preostalih izvršilnih faz NNP. Obvesti se ustrezno osebje.

Logistika

Četrto faza se posveča logističnim aktivnostim. Pripravi se okrevalno okolje, mobilizira se ekipe za neprekinjeno poslovanje, varnostne arhive, opremo in kritične vire za fazi okrevanja in normalizacije. Izjava o razglasitvi nesreče iz predhodne faze služi kot vodilo za aktivnosti te faze.

Okrevanje kritičnih virov in procesov

V peti fazi sledi okrevanje kritičnih virov IT in drugih virov ter ponovna vzpostavitev delovanja kritičnih procesov. Planirane aktivnosti se izvajajo v sledečih okoljih:

- Na primarni, poškodovani lokaciji izvaja okrevalne aktivnosti skupina za tehnično in operativno okrevanje, ki je zadolžena za reševanje vitalnih zapisov in kritičnih virov IT in drugih virov. Aktivnosti na poškodovani lokaciji sestavljajo štirje koraki: priprava, pregled in ocena, reševanje in obnova, transport;
- Na rezervni lokaciji IT so aktivnosti sestavljene iz treh korakov: priprava, izgradnja kritičnih sistemov IT in infrastrukture, restavriranje kritičnih aplikacij IT;
- Aktivnosti na rezervni lokaciji za pisarniško delo sestavljajo naslednji koraki: priprava, izgradnja rezervnega okolja z pisarniško opremo in računalniško infrastrukturo, restavriranje procesov;
- Aktivnosti na rezervni proizvodni lokaciji so sestavljene iz naslednjih korakov: priprava, izgradnja proizvodnega okolja, testiranje opreme in produktov;

- V kriznem centru za upravljanje se najprej pripravi okolje za aktivnosti kriznega upravljanja. Ko so pripravljalne aktivnosti končane, lahko ekipa za krizno upravljanje začne z načrtovanimi aktivnostmi, ki lahko pokrivajo področja kot so rezervna lokacija, krizno komuniciranje, človeški viri, finance, zavarovanje in pravno področje.

Normalizacija

Zadnjo izvršilno fazo NNP predstavlja normalizacija. Njen namen je vrnitev dejavnosti z rezervne lokacije nazaj na primarno lokacijo ali pa na neko novo lokacijo in vzpostavitev stanja in pogojev, ki so vladali pred nesrečo. Normalizacijo sestavljajo štirje sklopi aktivnosti: pregled originalne lokacije, popravilo, priprava in tranzicija. Z izjemo tranzicije se ostale aktivnosti lahko izvajajo vzporedno z aktivnostmi faze za okrevanje kritičnih virov in procesov. Tranzicija pa se lahko začne šele, ko je faza za okrevanje kritičnih virov in procesov zaključena.

13.9. Povezava virov s fazami, aktivnostmi, postopki in nalogami

Namen poglavja je povezati vire z izvršilnimi fazami NNP, aktivnostmi, postopki in nalogami, v katerih se viri uporabljajo. Za izvedbo povezave sta potrebna dva koraka:

- V prvem koraku se ugotovi postopke in naloge, ki jih zahteva posamezna aktivnost v izvršilnih fazah NNP. Vsaka aktivnost znotraj izvršilne faze NNP lahko vsebuje enega ali več postopkov na nižjem nivoju. Podobno lahko vsebuje vsak postopek eno ali več nalog na nižjem nivoju. Upoštevati je treba vse potrebne postopke in naloge za izpolnitev aktivnosti, ki so bile predvidene v izvršilnih fazah NNP.
- V drugem koraku se poveže posamezni vir z izvršilnimi fazami NNP, z aktivnostmi, postopki in nalogami.

13.10. Dodelitev aktivnosti, postopkov in nalog

Načrt neprekinjenega poslovanja specificira organizacijo ekip za neprekinjeno poslovanje in njihove naloge ter odgovornosti. Izvršilne faze NNP pa specificirajo potrebne aktivnosti za končanje teh faz.
Naloge desetega poglavja v NNP so:

- Dodeliti aktivnosti ekipam za neprekinjeno poslovanje.
- Dodeliti postopke in naloge članom ekip, ki omogočajo izvedbo aktivnosti.
- Zagotoviti dodatne koristne informacije za upravljanje in kontroliranje aktivnosti (npr. časovni potek aktivnosti).

13.11. Kontrola sprememb NNP

Podjetja se soočajo s nenehnimi spremembami procesov, tehnologij in ljudi. NNP mora biti usklajen s temi spremembami. Spremembe NNP morajo biti kontrolirane s kontrolnimi postopki, da se zagotovi integriteto in veljavnost načrta. Enajsto poglavje v NNP predpisuje postopke za posodobitev in kontrolo veljavnosti NNP ter seznam vseh izvedenih sprememb.

13.12. Dodatki NNP

Dodatki NNP nudijo dodatne podrobnosti in sklicevanja na druge dokumente, ki nadgrajujejo informacije enega ali več področij načrta. V nadaljevanju so našteti možni dodatki NNP:

- Načrt nujnega odgovora
- Načrt kriznega komuniciranja
- Zunanji kontakti
- Kritična oprema za pisarniško delo in viri
- Kritični sistemi IT in informacije o infrastrukturi
- Kritična proizvodna oprema in viri
- Kritični proizvodni produkti
- Kritični podatki in zapisi
- Informacije o rezervni lokaciji IT
- Informacije o rezervni proizvodni lokaciji
- Informacije o rezervni lokaciji za pisarniško delo
- Kritična oprema kriznega centra za upravljanje in viri
- Procedure za restavriranje kritičnih podatkov in zapisov
- Informacije o zavarovanju
- Informacije o storitvenih pogodbah
- Informacije o standardih
- Obrazci
- Reference na poročilo o oceni tveganja
- Reference na poročilo o analizi vpliva na poslovanje
- Reference na poročilo o strategiji
- Distribucijska lista NNP
- Slovar

14. Testiranje načrta neprekinjenega poslovanja

S testiranjem se preveri in potrdi strategijo, predvidevanja, aktivnosti, procedure in smernice, določene v načrtu neprekinjenega poslovanja. Na ta način se identificira morebitne pomanjkljivosti načrta in se tako izogne presenečenjem, do katerih bi sicer lahko prišlo med izvajanjem procedur v slučaju nesreče. S testiranjem se tudi ugotovi, ali NNP omogoča okrevanje poslovanja v predvidenem časovnem okvirju.
Testiranje potrdi funkcionalnost, identificira pomanjkljivosti, preveri ažurnost NNP in usposablja ljudi, ki so predvideni za izvajanje postopkov NNP (Musaji, 2001, str. 501).
Testiranje načrta neprekinjenega poslovanja sestavljajo razvojne, pripravljalne, izvajalne in ocenjevalne faze. V razvojni fazi se pripravi načrt testiranja, ki je osnova vsem drugim fazam, in omogoči oceno uspešnosti testiranj. Pripravljalna faza vsebuje spoznavanje članov okrevalne skupine z zunanjimi partnerji, rezervno lokacijo, sistemi, opremo in viri, ki jih bo zajemalo testiranje. Med izvajalno fazo se izvede dejanska testiranja. Na koncu se rezultate testiranj oceni z vidika uspešnosti ter opredeli pomanjkljivosti testiranj in načrta neprekinjenega poslovanja. Ugotovitve zadnje faze omogočijo izboljšave NNP, bodočih testiranj, učinkovitosti okrevalne skupine in zmanjšajo stroške prihodnjih testiranj.

14.1. Metode testiranj

Metode testiranj se razlikujejo z vidika stroškov, vloženega truda in motenja izvajanja normalnih poslovnih operacij med testiranjem.

- Kontrolni seznam je najbolj osnovna oblika testiranj in se navadno uporabi pred izvedbo kompleksnejših testov. Namen testa je, da osebje pregleda NNP in preveri korektnost informacij in potrebnih virov za izvedbo načrta. Preveri se dokumente o sistemih in aplikacijah, korektnost telefonskih številk, zasilne procedure, aplikacijska namestitvena navodila, itd.
- Spoznavni test je poceni metoda, ki se navadno izvede pred simulacijskim testom. Skupina za testiranje se zbere in na skupnem sestanku opiše aktivnosti, procedure in naloge, ki bodo sledile. Test omogoči članom skupine, da se spoznajo z NNP, okrevalnimi viri in drugimi člani skupine. Članom skupine so podane naloge in obveznosti. Seznanijo se s scenarijem testiranj in skupinsko pregledajo in potrdijo korektnost procedur NNP.
- Simulacijski test simulira izpad poslovanja. Omogoča, da okrevalna skupina potrdi in hkrati vadi izvajanje NNP. Simulacijski test lahko kombinira simulacijsko in dejansko izvajanje aktivnosti NNP. Vključuje lahko testiranja na rezervni lokaciji. Od posameznih poslovnih enot lahko zaradi testiranja zahteva prekinitev izvajanja normalnih operacij. Simulacijski test zmanjšuje stroške testiranja in prekinitve normalnih operacij s tem, da določene aktivnosti iz NNP raje simulira kot dejansko izvede. Zmanjšuje potrebno število ljudi, ki morajo odpotovati na rezervno lokacijo. Testiranje se posveča samo izbranim področjem NNP.
- Vzporedni test se izvaja na rezervni lokaciji in poteka hkrati, vendar neodvisno in nemoteče za produkcijsko okolje primarne lokacije, ki med testiranjem deluje normalno. Podatke na sistemih rezervne lokacije se pridobi s pomočjo replikacije ali restavriranja arhiva. Medtem ko poteka okrevalni postopek rezervne lokacije, se na primarni lokaciji nove transakcije zapisujejo tudi ročno. Te transakcije se po končanem okrevalnem postopku vnesejo v sisteme na rezervni lokaciji. Na koncu testa se primerjata okolji primarne in rezervne lokacije in če sta z vidika procesiranih podatkov enaki, se smatra, da je bil test uspešen.
- Prekinitveni test aktivira vse komponente NNP in predvideva, da je prišlo do izpada vseh kritičnih poslovnih procesov. Test vključuje vse predvideno osebje za okrevanje, rezervno lokacijo in zunanje partnerje. Takšna oblika testiranja zaradi visokih stroškov in morebitnih prekinitev poslovanja zahteva dobro pripravo in je priporočljiva šele potem, ko so bili izvedeni vsi predhodni, enostavnejši in cenejši testi.
- Testiranja so lahko napovedana ali nenapovedana. Pri napovedanih testih se osebje lahko pripravi na testiranje in s tem zmanjša potencialne prekinitve normalnih operacij. Po drugi strani pa napovedana testiranja ne morejo preveriti pričakovane konstantne pripravljenosti in delovanj osebja v kritičnih trenutkih. Nenapovedani testi se zaradi previdnosti navadno izvajajo na posameznih poslovnih enotah in se sčasoma širijo na druge enote. Uporabijo se šele takrat, ko je osebje dovolj izvežbano.

14.2. Razvoj načrta testiranja

Razvoj načrta za testiranja NNP je strukturiran proces, sestavljen iz naslednjih korakov:
- Pregled predhodnih testov in rezultatov
- Določitev objektov in področij testiranja
- Omejitve testiranja
- Razvoj strategije testiranja
- Določitev logistike
- Določitev poteka testiranja
- Identifikacija tveganj
- Integracija komponent testiranja

Pregled predhodnih testov in rezultatov

Predhodni testi in njihovi rezultati so lahko v veliko pomoč pri razvoju novih testov. Identificirajo področja in komponente NNP, ki še niso bile testirane, in opišejo, kako so se med testiranjem odrezale. Področja in komponente, ki še niso bile testirane, ali pa so bili rezultati slabi, postanejo predmet novega testiranja.
Iz predhodnih testov je mogoče povzeti posamezne korake razvoja načrta za testiranje in tako poenostaviti proces načrtovanja testiranja.

Določitev objektov in področij testiranja

Objekti testiranja se delijo na primarne in sekundarne. Primarni objekti so usmerjeni v dele NNP, ki morajo biti izpolnjeni, da je testiranje uspešno. Sekundarni objekti vključujejo dele NNP, ki bi jih bilo zaželeno testirati, vendar niso ključnega pomena za uspešnost testa. Sekundarni objekti imajo z vidika testiranj nižjo prioriteto in se jih testira samo če čas in viri to dovoljujejo.
Področje testiranja se lahko opredeli na posamezne dele ali na celoten NNP. Določa posamezne faze, aktivnosti, procedure NNP, poslovne enote, skupine, dobavitelje, proizvajalce in poslovne partnerje, ki bodo pri testiranju sodelovali.

Omejitve testiranja

Omejitve zmanjšujejo razpoložljive možnosti za izvedbo testov. Finančne omejitve lahko, na primer, vplivajo na število ljudi, ki sodelujejo pri testiranju, na trajanje testov in izbiro razpoložljivih sistemov in opreme za testiranje. Testiranje mora upoštevati in zmanjšati na najnižjo možno raven morebitne prekinitve poslovnih operacij. Varnostne omejitve zmanjšujejo možnost dostopa do zaupnih podatkov in sistemov. Omejitve zaradi pomanjkanja osebja nastanejo takrat, ko ni mogoče zagotoviti ustreznega števila usposobljenih ljudi za testiranje.

Razvoj strategije testiranja

Pri razvoju strategije je potrebno testiranje časovno opredeliti, določiti metodo, scenarij, ocenjevalne kriterije in stroške testiranja.
Pri časovni opredelitvi je potrebno določiti datum, čas in trajanje testiranja. Pri določitvi metode se izbere eno izmed v predhodnem poglavju opisanih metod testiranj. Določi se tudi ali bo testiranje najavljeno ali nenajavljeno. Določitev scenarija predvidi tip namišljene prekinitve (poplava, potres, požar, itd.), opis prekinitve (datum, čas in zaporedje dogodkov, ki si sledijo po prekinitvi) in povzročeno škodo. Na osnovi ocenjevalnih kriterijev se oceni rezultate testiranja. Z oceno stroškov testiranja se predvidi in razporedi potrebna sredstva za testiranje.

Določitev logistike

Logistika je proces, ki zagotavlja formiranje skupin za testiranje, dobavlja testne vire in opremo, mobilizira osebje in pripravi rezervne objekte.
Skupine za testiranje pripravijo, spremljajo in upravljajo testiranje. Skupine za testiranje so sestavljene iz članov skupin za neprekinjeno poslovanje. Skupine in posameznike se izbere

glede na področje, ki ga pokrivajo in ki sovpada s področjem testiranja. Skupine za testiranje imajo lahko tudi dodatne člane, na primer predstavnike dobaviteljev ter notranje in zunanje opazovalce.
Ekipa za preskrbovanje zagotovi vse potrebne vire in opremo za izvedbo testiranja.
Testiranje NNP ponavadi zahteva mobilizacijo osebja na rezervne lokacije. Določiti je treba kdo gre kam, kdaj, kako dolgo bo tam in kaj potrebuje za pot.
Pri pripravi rezervnih objektov se oceni zahteve za rezervno lokacijo, sledi ocena trenutnih zmožnosti rezervne lokacije, na koncu pa se izvede analiza pomanjkljivosti rezervne lokacije.

Določitev poteka testiranja

Potek testiranja je predstavljen z listo okrevalnih aktivnosti, procedur, nalog, prioritet, odvisnosti, začetnih in končnih datumov in časov. Testiranje je sestavljeno iz pripravljalne, izvajalne in ocenjevalne faze.

Identifikacija tveganj

Glavna naloga načrta za testiranje NNP je v zmanjševanju verjetnosti za neuspeh testiranja. Identifikacija tveganj išče in nadzira potencialna tveganja za neuspeh testiranj na osnovi temeljitega pregleda vseh v predhodnih korakih zbranih informacij. Ko je tveganje identificirano, se lahko rangira z oznako nizko, srednje ali visoko. Za identificirana tveganja se poišče možne rešitve, ki se jih vnese v načrt za testiranje NNP.

Integracija komponent testiranja

Vse rezultate iz predhodnih korakov se na koncu združi v dokument, ki predstavlja načrt za testiranje NNP.

15. Vzdrževanje načrta neprekinjenega poslovanja

Pogoste notranje in zunanje spremembe, ki vplivajo na poslovanje podjetja, lahko povzročijo, da postane načrt neprekinjenega poslovanja delno ali v celoti neuporaben. Zato je potrebno načrt nenehno spreminjati in prilagajati morebitnim novim okoliščinam. Naloga vzdrževanja načrta neprekinjenega poslovanja je zagotoviti veljavnost, natančnost, popolnost in konstantno pripravljenost za izvajanje. Za uresničitev te naloge se uporabljajo naslednji procesi:

- Upravljanje sprememb NNP
- Testiranje NNP
- Izobraževanje o NNP
- Revidiranje NNP

15.1. Upravljanje sprememb NNP

Proces upravljanja sprememb NNP je sestavljen iz treh korakov in se ukvarja s spremljanjem sprememb znotraj in izven podjetja ter s kontroliranjem teh sprememb.
Prvi korak predstavlja nenehen nadzor notranjih sprememb na procesih, ljudeh in virih, ki lahko vplivajo na načrt neprekinjenega poslovanja in zahtevajo spremembo le tega. Poleg

sprememb, ki se pojavljajo znotraj podjetja, pa na načrt neprekinjenega poslovanja vplivajo tudi zunanje spremembe, ki se lahko pojavijo pri zunanjih poslovnih partnerjih, proizvajalcih, dobaviteljih in rezervnih prostorih.
V drugem koraku se naredi temeljito analizo informacij, pridobljenih iz prvega koraka in informacij, ki so rezultat raznih testiranj in revizij NNP. S pomočjo analize se ugotovi, ali imajo informacije kakšen vpliv na NNP.
Tretji korak zagotavlja, da se spremembe, ki so posledica prvih dveh korakov, v načrtu neprekinjenega poslovanja dejansko izvedejo.

15.2. Testiranje NNP

Testiranje načrta neprekinjenega poslovanja zagotavlja učinkovitost in točnost načrta. Rezultati testiranja lahko prikažejo tako prednosti kot tudi pomanjkljivosti načrta.
Pri testiranju je zelo pomembno, da se določijo intervali testiranj. Vsakemu testnemu intervalu se nato dodeli izbrana metoda za testiranje. Večja kompleksnost metode se izraža tudi v daljšem časovnem intervalu med testiranji (Hiatt, 2000, str. 78). Povedano drugače, enostavnejše metode se običajno izvajajo bolj pogosto (mesečni ali četrtletni intervali) kot zahtevnejše metode testiranj (polletni ali letni intervali). Med enostavnejše metode spadata uporabi kontrolnega seznama in spoznavnega testa, med srednje in zahtevnejše metode pa spadajo simulacijski, vzporedni in prekinitveni testi. Enostavnejši in hkrati pogostejši testi običajno pokrivajo posamezne dele oz. področja NNP, odpravljajo pomanjkljivosti in pomagajo pri postopnem usposabljanju skupin za izvedbo zahtevnejših metod testiranj.

15.3. Izobraževanje o NNP

Načrt neprekinjenega poslovanja je brez vrednosti, če zaposleni, ki so za njegovo izvajanje odgovorni, nimajo zadovoljivega nivoja zavesti in znanja za izvajanje načrta. Faza za vzdrževanje NNP se ukvarja z razširjanjem vsesplošne zavesti in z izobraževanjem o NNP v podjetju. Program ozaveščanja in izobraževanja mora podpirati vodstvo podjetja, ki vsako leto zagotovi sredstva za izvajanje programa, in poskrbi, da se zaposleni udeležujejo izobraževanj.
Izobraževalni proces ugotavlja, kdo v podjetju potrebuje izobraževanje in kakšno znanje potrebuje za izpolnitev svojih nalog in odgovornosti. Oceni se nivo trenutnega znanja in nivo zahtevanega znanja. Za vsakega posameznika se določi izobraževalne metode in termine izobraževanj.
Za zagotavljanje ozaveščenosti in znanja o NNP se lahko uporabljajo publikacije, dokumenti, knjige, zgibanke, plakati in jasna politika podjetja glede neprekinjenosti poslovanja. Organizirati in obiskovati je možno tečaje, seminarje in konference. Zelo veliko vlogo v procesu izobraževanja pa imajo tudi v predhodnih poglavjih opisane aktivnosti v zvezi z razvojem, testiranjem in vzdrževanjem NNP.

15.4. Revidiranje NNP

Revidiranje neprekinjenosti poslovanja vključuje nepristranski pregled programa in načrta neprekinjenega poslovanja podjetja z namenom ugotovitve skladnosti z notranjimi smernicami podjetja in zunanjimi zakoni in standardi. Področje revidiranja pokriva vse faze procesa načrtovanja neprekinjenega poslovanja. Pomanjkljivosti, odkrite v katerikoli fazi procesa NNP, zahtevajo ponovno obravnavo faze. Izvedba priporočil revidiranja se

izvede kjerkoli je možno. Ugotovljene spremembe se vnesejo v načrt neprekinjenega poslovanja.

16. Programska oprema NNP

Poleg klasičnega pristopa pri razvoju načrta za neprekinjeno poslovanje, ki ne zahteva drugega kot pisalni stroj ali urejevalnik besedila, se mnoga podjetja in svetovalci poslužujejo tudi namenske programske opreme za načrtovanje neprekinjenega poslovanja. V času, ko se poslovanje podjetja neprestano spreminja in prilagaja tržnim razmeram in potrebam, je s klasičnim načinom statičnih tabel in zamrznjenih podatkov izredno težko slediti spremembam, ki jim morajo slediti tudi načrti za neprekinjeno poslovanje (Beser, 2002, str. 27). Programska oprema za načrtovanje neprekinjenega poslovanja znižuje nivo vloženega truda in hkrati povečuje učinkovitost. Programska orodja nam pomagajo učinkovito organizirati podatke in jih analizirati. Dobra programska orodja so razvili priznani strokovnjaki s področja neprekinjenega poslovanja. Rezultat so aplikacije, ki uporabnika vodijo skozi celotni proces načrtovanja (Toigo, 1996, str. 47). Pripravljeni so vzorčni načrti, tabele, dokumenti in procedure, ki jih je mogoče prilagoditi vsakemu podjetju. V enem samem paketu so združene funkcije analize, načrtovanja in testiranja. Postopek analize vpliva na poslovanje vsebuje množico pripravljenih vprašanj za določitev finančnega vpliva s strani različnih dogodkov. Zaradi možnosti dodajanja novih vprašanj aplikacije nimajo mej in jih je mogoče sproti prilagajati potrebam.

Programska oprema za načrtovanje neprekinjenega poslovanja lahko avtomatizira:

- Analizo vpliva na poslovanje.
- Povezavo relacijskih podatkovnih baz s procesom analize tveganja in izdelave načrta.
- Upravljanje, iskanje in ažuriranje dokumentov načrta neprekinjenega poslovanja.
- Distribucijo načrtov v posamezne poslovne enote.
- Integracijo NNP procesov z drugimi strategijami upravljanja.

16.1. Tipi programske opreme za NNP

Programska oprema za NNP se deli v štiri kategorije (Noakes, Diamond, 2003. str. 2):

1. Orodja za analizo vpliva na poslovanje dobijo od vodstva, skozi ekspertni sistem vprašalnikov, potrebne podatke za določitev prioritet in časovnih kritičnosti posameznih funkcij. Značilnosti in zmogljivosti orodij so:
   - Prilagodljiv ekspertni sistem vprašalnikov
   - Časovni razpored dogodkov pri okrevanju po nesreči
   - Modeliranje KAJ-ČE scenarijev
   - Poročila finančnih in operativnih ranljivosti in vplivov
   - Grafične predstavitve analiz
   - Izvoz rezultatov v orodja za izgradnjo NNP
2. Orodja za izgradnjo NNP delujejo na principu ekspertnih sistemov, kjer s pomočjo vprašalnikov in široke baze podatkov pogosto direktno posredujejo odgovore v sam načrt. Značilnosti in zmogljivosti orodij so:
   - Seznam standardiziranih postopkov in procedur
   - Različnost verzij, glede na velikost podjetja
   - Orodja za upravljanje projektov
   - Vzorčni vprašalniki, tabele in šablone
   - Slovarji izrazov NNP

- Ocene tveganja
- Vgrajena orodja za analizo vpliva na poslovanje
- Okrevalne strategije
- Izdelava načrta
- Testiranje načrta

3. Podatkovne baze NNP uporabljajo ekspertni sistem vprašalnikov. Informacije, ki so bile zajete v ekspertni sistem, se nahajajo v relacijskih bazah. Značilnosti in zmogljivosti so:
   - Fleksibilna poročila.
   - Izvoz in uvoz različnih formatov poročil.
   - Integriteta podatkov (ni podvajanj).
   - Povezava z zunanjimi bazami podatkov.
   - Centralna administracija in kontrola.
   - Zagotovitev avtorizacije pri spreminjanju.
   - Mrežni dostop.
   - Varnostne kontrole.
   - Preoblikovanja obstoječih NNP .
4. Orodja za skupinsko načrtovanje NNP se opirajo na standardna komunikacijska orodja, ki koordinatorju NNP omogočajo, da zbere in posreduje informacije v več-lokacijskem, mednarodnem okolju. Značilnosti in zmogljivosti orodij so:
   - Izmenjevanje informacij ne glede na lokacijo.
   - Sodelovanje.
   - Integracija uveljavljenih dokumentov.

16.2. Zmogljivosti in prednosti programske opreme za NNP

- Metodologija, teorija, procedure za določitev prioritet, tveganj in strategij pomagajo razumeti organizacijske principe in procese NNP.
- Zmožnost priponk oz. dodajanja Microsoft Word in Visio dokumentov omogoča, da so liste s telefonskimi številkami in naslovi izvajalcev shranjene v Word tabelah, procesni diagrami pa v Visio.
- Možnost integracije podatkov načrta s podatkovno bazo odpravlja podvajanje.
- Primeri s smernicami načrtovanj.
- Možnost prilagajanja terminologij, dokumentov, vzorčnih form in podatkovnih baz specifičnostim okolja.
- Orodja za projektno vodenje in poročanje.
- Določitev verzije načrta in iskanje sprememb glede na čas, vzrok in odgovorno osebo.

16.3. Izbira orodja

Izbira orodja je odvisna predvsem od tega ali gre za prvi NNP ali pa podjetje nadgrajuje že vpeljan NNP:

1. Če gre za prve aktivnosti razvoja NNP, je smiselno poiskati orodje, ki zagotavlja:
   - Nezahtevno učenje
   - Razumljive vprašalnike in primere
   - Tehnično pomoč, tečaje in svetovanje proizvajalca
   - Uvoz in izvoz v podatkovne baze okolja, ki ga podjetje že uporablja
   - Uvoz in izvoz dokumentov v aplikacije, ki jih podjetje že uporablja
   - Možnost nadgrajevanja

2. V kolikor gre za nadgradnjo NNP, je smiselno poiskati orodje, ki zagotavlja:
   - Avtomatsko konverzijo zmožnosti originalnega načrta
   - Tehnično pomoč proizvajalca pri konverziji in izgradnji novih elementov načrta
   - Uvoz in izvoz v podatkovne baze okolja, ki ga podjetje že uporablja
   - Uvoz in izvoz dokumentov v aplikacije, ki jih podjetje že uporablja
   - Uvoz in izvoz poročil v aplikacije, ki jih podjetje že uporablja
   - Zagotovitev izobraževanja za podporno tehnično osebje in skupino za upravljanje tveganj
   - Možnost inicialnega razvoja načrta s strani proizvajalca in kasnejšo ustrezno predajo v upravljanje osebju podjetja

16.4. Proizvajalci in produkti

Vodilni proizvajalci programske opreme za načrtovanje neprekinjenega poslovanja se prilagajajo vsem oblikam podjetij. Prilagajanje je vidno tako v kompleksnosti, ceni in podpori, ki naj bi zagotovila potrebe različno velikih podjetij, ne glede na to ali se z načrtovanjem neprekinjenega poslovanja srečujejo prvič ali pa gre za nadgradnjo. Med vodilnimi proizvajalci programske opreme NNP so Strohl, SunGard, Computer Security Consultants Inc. (CSCI) in RSM McGladrey.

Podjetje Continuity Planning & Analysis, Consultancy & Software, krajše CPACS, je bilo ustanovljeno leta 1984 in ponuja programsko opremo RecoveryPAC, ki jo uporablja več kot 1400 srednje velikih in velikih podjetij v javnem in privatnem sektorju v 40 državah sveta.

- Programska oprema RecoveryPAC vsebuje orodje za izgradnjo NNP in podatkovno bazo. Omogoča integracijo z zunanjimi orodji za analizo vpliva na poslovanje (RiskPAC)
- Podjetje ponuja tudi spletno različico RecoveryPAC Web, ki ima vse značilnosti opreme RecoveryPAC, hkrati pa omogoča dostop preko svetovnega spleta.

Programska oprema deluje v operacijskem sistemu Microsoft Windows, Linux in SUN Solaris (Unix). Preko svetovnega spleta je do orodja mogoče dostopati s pomočjo spletnih brskalnikov Internet Explorer in Netscape Navigator (CPACS Software Products, 2006).

RSM McGladrey oz. RSM International je po velikost osmo največje svetovno svetovalno podjetje in največji ponudnik programske opreme NNP. Podjetje ima več kot 600 poslovalnic v 75 državah.

- Programska oprema Business Continuity Planning System (BCPS) vsebuje orodja za izdelavo analize vpliva na delovanje, za izgradnjo NNP in podatkovno bazo NNP.

Programsko oprema deluje v operacijskem okolju Microsoft Windows in podpira formate najpogostejših urejevalnikov teksta.

Podjetje Strohl Systems ima svojo programsko opremo v več kot 1500 podjetjih, v več kot 60 državah.

- Living Disaster Recovery Planning System (LDRPS) vsebuje orodje za izgradnjo NNP, ima tudi module za tuje jezike ter avtomatsko importiranje in tiskanje. Ima varnostne mehanizme in omogoča objavo načrta ter potrditev. Programska oprema uporablja za NNP relacijske baze podatkov in omogoča skupinsko načrtovanje.
- BIA Professional omogoča izvedbo analize vpliva na poslovanje. Obstaja tudi v spletni različici.
- Incident Manager je oblika spletnega ukaznega centra.

- NotiFind je system za obveščanje v primeru nevarnosti.

Programska oprema deluje v operacijskem okolju Microsoft Windows. Podpira podatkovne baze Sybase, Oracle in SQL Server (BCP Software, 2006).

Podjetje SunGard je vodilno podjetje na področju NNP. Usmerjeno je predvsem v IT rešitve finančnega sektorja in elektronskega poslovanja. Svoje produkte (več kot 20000 klientov) ima v 50 državah in pokriva 47 od 50 največjih finančnih institucij. Produkti vsebujejo tudi dele programske opreme nekdanjega tekmeca Comdisco (Business Continuity, 2006).

- PreCovery programska oprema tipa klient/strežnik avtomatizira vse stopnje načrtovalnega procesa. Omogoča izdelavo analize neprekinjenega poslovanja, izgradnjo načrta neprekinjenosti, uporabo podatkovnih baz NNP in skupinsko načrtovanje.
- Eplanner vsebuje vse funkcije opreme PreCovery hkrati pa omogoča dostop preko svetovnega spleta. Podpira 128 bitno SSL kodiranje.
- ComPAS je MS Windows več-uporabniška aplikacija za podporo zaposlenim v zavarovalniških in finančnih institucijah.
- Revolution Release je produkt, ki temelji na Visual Basicu in omogoča načrtovanje in administracijo s pomočjo spletnih brskalnikov preko svetovnega spleta.

Programska oprema deluje v okolju MS Windows in ima integrirano SQL bazo podatkov, podporo za vse večje urejevalnike teksta. Vsebuje restavracijske skripte za vse večje platforme (IBM, HP, SUN).

Podjetje Business Protection Systems International se ukvarja izključno z načrtovanjem neprekinjenega poslovanja. Prilagodljiva orodja zadovoljujejo potrebe različno velikih podjetij. BPSI je strateški partner podjetja IBM.

- Programska oprema Business Protector obstaja v dveh izvedbah. Različica Professional je namenjena uporabi na osebnem računalniku, različica Gateway pa je namenjena uporabi preko svetovnega spleta.

Programska oprema deluje v okolju MS Windows in je v celoti integrirana s pisarniško zbirko MS Office (Business Protector, 2006).

17. Praktični prikaz NNP za podjetje ABC d.d.

V nadaljevanju je prikazan praktični primer NNP za podjetje ABC d.d. Podjetje ABC d.d. je srednje veliko podjetje, ki ima svoj sedež v Ljubljani, manjši predstavništvi pa ima tudi v Kopru in Mariboru. Ukvarja se s kataloško spletno prodajo različnih tipov izdelkov. Načrt neprekinjenega poslovanja se nanaša na področje informacijske tehnologije. NNP prikazuje praktični primer izdelave načrta, ki lahko služi kot model za načrte drugih podjetij.

Prva stran vsakega načrta je ponavadi prilagojena oblikovnim zahtevam posameznega podjetja, zahteva pa se jasna navedba, katero področje NNP obravnava in ime avtorizirane osebe, ki je potrdila veljavnost načrta (Adney, 2002, str. 6).

Nadzorna stran vsebuje imena odgovornih oseb in oznako zaupnosti. Vsebuje tudi seznam vseh prejšnjih različic dokumenta s kratkimi opisi sprememb in oznako trenutne različice. Nadzorna stran poleg kazala vsebuje vidno izpisano opozorilo, da se v slučaju nesreče začne z branjem poglavja, ki opisuje izvršilne faze načrta za neprekinjeno poslovanje.

Namen in področje NNP

Načrt neprekinjenega poslovanja predpisuje vnaprej pripravljene procedure, ki jih podjetje uporabi v slučaju krize in tako zmanjša vpliv na poslovanje. Naloga NNP je vzpostaviti delovanje kritičnih procesov znotraj določenega časovnega okvira.
NNP se nanaša na področji informacijskih sistemov in infrastrukture ter podatkov podjetja ABC d.d.

Definicija nesreče

Manjša nesreča:
Nesreča je omejena na manjše dele kritičnih poslovnih procesov. Poslovne enote, ki so odvisne od prizadetih kritičnih procesov, lahko pogojno še vedno nadaljujejo z izvajanjem svojih osnovnih operacij. Vzrok prekinitve je pogosto okvara posamezne komponente, sistema ali servisa. Primeri manjših nesreč so okvare računalniških diskov in mrežnih komponent.

Srednja nesreča:
Srednja nesreča moti normalno delovanje posameznih, vendar ne vseh poslovnih enot. Do motenja delovanja pride zaradi večjih okvar na več sistemih in opremi. Primer nesreče srednjega tipa je vdor vode v sistemski prostor zaradi okvare na napravah za hlajenje.

Velika nesreča:
Velika nesreča prekine delovanje večine ali vseh kritičnih poslovnih procesov. Posledice se kažejo v nedelovanju ali nedosegljivosti večine ali vseh sistemov in opreme. Primer velike nesreče predstavlja nedosegljivost sistemskega prostora zaradi požara, potresa ali sabotaže.

Povzetek upravljanja s tveganji

Ocena tveganja

V tabeli 14 so navedene identificirane grožnje, ki lahko vplivajo na delovanje IT. Vsaka grožnja je kategorizirana glede na nastanek. Sledi opis dogodkov in posledice realizirane grožnje. Letni pojav grožnje opisuje verjetnost, da se grožnja uresniči (vrednost »1/10« označuje, da se bo grožnja enkrat v desetih letih gotovo uresničila). Letni pojav grožnje temelji na preteklih izkušnjah. Pričakovani enkratni vpliv temelji na subjektivni oceni in označuje izpostavljenost kritičnih delov posledicam grožnje.

LPG – letni pojav grožnje
PEV – pričakovani enkratni vpliv (1-100)
PLV - pričakovan letni vpliv (PLV = LPG * PEV)

Tveganje je visoko, če je PLV vrednost med 67 in 100. Če je PLV med 34 in 66, je tveganje srednje. Če je PLV med 1 in 33, je tveganje nizko.

Izbrani nivo še sprejemljivega tveganja (ST), ki ga podjetje ABC d.d. sprejema in dopušča, predstavljajo vrednosti tveganja manjše, od 10. Vse grožnje, ki imajo vrednost tveganja manjšo od 10, podjetje ABC d.d. sprejema in za njih ne predvideva dodatnih kontrolnih možnosti. Grožnje, ki imajo vrednost tveganja 10 ali več, zahtevajo nadaljnjo obravnavo in so v tabeli 14 označene z rdečo barvo.

Tabela 14: **Identifikacija groženj in opredelitev tveganja**

Grožnja	Kategorija	Opis	Posledice	LPG	PEV	PLV/tveganje
Požar	Naravna	Uničenje opreme IT	Izpad IS	1/10	100	10 nizko
Potres	Naravna	Uničenje opreme IT	Izpad IS	1/80	90	1,12 nizko
Poplava	Naravna	Uničenje opreme IT	Izpad IS	1/50	95	1,9 nizko
Prekinitev el. voda	Tehnična	Izpad elektrike	Izpad IS	1/5	80	16 nizko
Okvara diska	Tehnična	Prenehanje delovanja strežnika	Izguba podatkov	1	60	60 srednje
Okvara strežnika	Tehnična	Prenehanje delovanja strežnika	Izpad strežnika	1	70	70 visoko
Aplikacijska napaka	Tehnična	Nepravilno delovanje aplikacije	Izpad aplikacije	1	50	50 srednje
Okvara naprave za hlajenje	Tehnična	Pregretje in zaustavitev opreme IT	Izpad IS	1/5	70	14 nizko
Napaka na vodnem omrežju	Tehnična	Izliv vode in uničenje opreme IT	Izpad IS	1/10	85	8,5 nizko
Mrežna okvara	Tehnična	Nedostopnost strežnikov	Izpad IS	1	90	90 visoko
Padec aviona	Tehnična	Uničenje opreme IT	Izpad IS	1/500	100	0,2 nizko
Virus	Človeška	Poškodbe programske opreme	Izguba podatkov	1	70	70 visoko
Maščevanje zaposlenih	Človeška	Poškodbe opreme IT, aplikacij in podatkov	Izpad dela ali celega IS	1/8	70	8,75 nizko
Računalniški vdor	Človeška	Neavtoriziran dostop	Odtujitev ali izguba podatkov	1/2	70	35 srednje
Rop	Človeška	Odtujitev opreme IT	Izpad dela ali celega IS	1/7	60	8,5 nizko
Vandalizem	Človeška	Poškodbe opreme IT	Izpad dela ali celega IS	1/10	50	5 nizko
Terorizem	Človeška	Uničenje opreme IT	Izpad IS	1/40	100	2,5 nizko
Vojna	Človeška	Uničenje opreme IT	Izpad IS	1/50	100	2 nizko

Vir: Lasten

Ocena kontrolnih stroškov in učinkovitosti

Za vse grožnje, ki imajo vrednost tveganja 10 ali več, so določene kontrolne možnosti, ki zmanjšujejo stopnjo tveganja (tabela 15). Kontrolne možnosti so kategorizirane glede na zmanjšanje stopnje tveganja (sprejemanje, izogibanje, zmanjševanje, prenos). Sledijo stroški izvedbe kontrolnih možnosti in nove subjektivne ocene letnih pojavov groženj po izvedbi kontrolnih možnosti.
Nova vrednost pričakovanega letnega vpliva je produkt nove vrednosti letnega pojava grožnje in pričakovanega enkratnega vpliva iz tabele 14 ($PLV^2 = LPG^2 * PEV$).
Zmanjšanje tveganja pove za koliko se je zmanjšalo tveganje zaradi uporabljenih kontrolnih možnosti (zmanjšanje tveganja = stara vrednost PLV – nova vrednost PLV^2).
Stroški zmanjšanja tveganja na enoto ovrednotijo stroške in koristi posameznih kontrolnih možnosti.

SZTE – stroški zmanjšanja tveganja na enoto (SZTE = kontrolni stroški / zmanjšanje tveganja)

Manjša vrednost SZTE predstavlja boljšo izbiro. V tabeli 15 so z zeleno barvo označene izbrane kontrolne možnosti.

Tabela 15: **Ocena kontrolnih stroškov in učinkovitosti**

Grožnja	Kontrolna možnost	Kontrolna kategorija	Stroški (EUR)	LPG^2	PLV^2	Zman-jšanje	SZTE (EUR)
Požar	Protipožarni sistem	Zmanjše-vanje	10.000	1/20	5	5	2.000
	Sistemski prostor se prestavi na varnejšo lokacijo	Zmanjše-vanje	100.000	1/15	6,66	3,34	29.940
	Zavarovanje pri zavarov-alnici	Prenos	22.000 (obdobje 10 let)	0	0	10	2.200
Prekinitev el. voda	Dva ločena vira napajanja	Izogibanje	50.000	1/50	1,6	14,4	3.472
	Naprava za neprekinje-no napajanje	Zmanjše-vanje	6.000	1/10	8	8	750
	Zavarovanje pri zavarov-alnici	Prenos	13.000 (obdobje 10 let)	0	0	16	812
Okvara diska	Dodatni disk in RAID tehnologija	Izogibanje	1.000	1/15	4	56	17,8
	Gruče	Zmanjše-vanje	20.000	1/10	6	54	370
	Diagnostika	Zmanjše-	10.000	1/3	20	40	250

	napak z nadzornim sistemom	vanje					
	Vzdrževalna pogodba	Prenos	2.000	0	0	60	33,3
Okvara strežnika	Podvojitev vseh komponent	Izogibanje	5.000	1/13	5,38	64,62	77,4
	Gruče	Zmanjše-vanje	20.000	1/10	7	63	317,5
	Diagnostika napak z nadzornim sistemo	Zmanjše-vanje	10.000	1/2	35	35	285,7
	Vzdrževalna pogodba	Prenos	10.000	0	0	70	142,8
Aplikacijska napaka	Vzdrževalna pogodba	Prenos	5.000	0	0	50	100
Okvara naprave za hlajenje	Podvojen sistem hlajenja	Izogibanje	20.000	1/30	2,33	11,67	1713,8
	Sistem za obveščanje	Zmanjše-vanje	3.000	1/10	7	7	428,5
	Vzdrževalna pogodba	Prenos	5.000	0	0	14	357,1
Mrežna okvara	Podvojitev vseh komponent	Izogibanje	40.000	1/40	2,25	87,75	455,8
	Diagnostika napak z nadzornim sistemom	Zmanjše-vanje	10.000	1/2	45	45	222,2
	Vzdrževalna pogodba	Prenos	15.000	0	0	90	166,7
Virus	Proti-virusni programi	Zmanjše-vanje	1.000	1/7	10	60	16,7
Računalniški vdor	Sistemi za odkrivanje vdorov	Zmanjše-vanje	25.000	1/10	7	28	892,9
	Požarne pregrade	Zmanjše-vanje	20.000	1/7	10	25	800

Vir: Lasten

Povzetek analize vpliva na poslovanje

Analiza vpliva na poslovanje identificira kritična področja poslovanja in potrebo po neprekinjenosti delovanja. Analiza vpliva na poslovanje je bila narejena za poslovne funkcije prodaje, marketinga, uporabniških storitev in transporta v podjetju ABC d.d.

a) Identifikacija poslovnih funkcij in procesov z oceno dnevnega finančnega izpada ob nedelovanju (tabela 16). Stopnje pomembnosti (0 – nepomembno, 3 – zelo pomembno) so usklajene z vrednostmi dnevnih finančnih izpadov.

Tabela 16: **Identifikacija poslovnih funkcij in procesov**

Poslovna funkcija	Poslovni proces	Finančni izpad (dnevni)	Stopnja pomembnosti
Prodaja	Generiranje naročil	700.000 EUR	3
	Prodajna poročila	0 EUR	0
Marketing	Promocija produktov	2.000 EUR	1
	Prodajni katalogi	5.000 EUR	1
Uporabniške storitve	Podpora uporabnikom	5.000 EUR	1
	Izvedba naročil	500.000 EUR	3
Transport	Pakiranje produktov	15.000 EUR	2
	Pošiljanje produktov	20.000 EUR	2

Vir: Lasten

b) Ocena operativnih vplivov (ni, nizek, srednji, visok, najvišji) in identifikacija kritičnih poslovnih procesov, ki so v tabeli 17 označeni z rdečo barvo. Kritični poslovni procesi so izbrani na osnovi stopnje pomembnosti iz tabele 16 in ocene operativnih vplivov iz tabele 17. Proces je kritičen, če je izpolnjuje kateregakoli od naslednjih pogojev:

- Stopnja pomembnosti finančnega vpliva je ocenjena z vrednostjo 2 ali 3.
- Vsaj tri ocene operativnih vplivov so označene z oznako »visok«.
- Vsaj dve oceni operativnih vplivov sta označeni z oznako »visok« in vsaj ena z oznako »najvišji«.
- Vsaj dve oceni operativnih vplivov sta označeni z oznako »najvišji«.

Tabela 17: **Ocena operativnih vplivov in identifikacija kritičnih procesov**

Poslovna funkcija	Poslovni proces	Ocena operativnih vplivov				
		Pretok denarja	Zaupanje investitorjev	Tržni delež	Konkuren-čnost	Zadovoljstvo uporabnikov
Prodaja	Generiranje naročil	visok	visok	najvišji	visok	ni
	Prodajna poročila	ni	najvišji	nizek	ni	ni
Marketing	Promocija produktov	nizek	visok	visok	najvišji	srednji
	Prodajni katalogi	nizek	nizek	visok	najvišji	visok
Uporabniške storitve	Podpora uporabnikom	srednji	nizek	nizek	srednji	visok
	Izvedba naročil	najvišji	srednji	nizek	srednji	najvišji
Transport	Pakiranje produktov	visok	srednji	nizek	visok	visok
	Pošiljanje produktov	visok	srednji	nizek	visok	visok

Vir: Lasten

c) V tabeli 18 so predstavljeni največji sprejemljivi časi prekinitev (NSČP) za posamezne poslovne procese in prioritete okrevanja (nižja vrednost predstavlja večjo prioriteto okrevanja).

Tabela 18: **Določitev največjih sprejemljivih časov prekinitev in prioritet okrevanja**

Poslovna funkcija	Poslovni proces	NSČP	Prioriteta okrevanja
Prodaja	Generiranje naročil	3 ure	1
Marketing	Promocija produktov	5 dni	3
	Prodajni katalogi	7 dni	4
Uporabniške storitve	Izvedba naročil	3 ure	1
Transport	Pakiranje produktov	1 dan	2
	Pošiljanje produktov	1 dan	2

Vir: Lasten

d) V tabeli 19 so navedeni kritični sistemi IT in aplikacije, ki jih uporabljajo v tabeli 17 identificirani kritični poslovni procesi.

Tabela 19: **Identifikacija kritičnih sistemov IT in aplikacij**

Poslovna funkcija	Poslovni proces	Kritični sistemi IT in aplikacije
Prodaja	Generiranje naročil	Uporabniški informacijski sistem
		Sistem za vnos naročil
		Elektronska pošta
		Aplikacija za elektronsko izmenjavo podatkov
		Sistem za sledenje prodajnih povpraševanj
Marketing	Promocija produktov	Uporabniški informacijski sistem
		Elektronska pošta
	Prodajni katalogi	Aplikacija za interaktivni katalog
Uporabniške storitve	Izvedba naročil	Sistem za vnos naročil
		Sistem za upravljanje zalog
		Računovodski sistem
Transport	Pakiranje produktov	Sistem za vnos naročil
		Sistem za upravljanje pakiranja in prevoza
	Pošiljanje produktov	Sistem za upravljanje pakiranja in prevoza
		Sistem za upravljanje zalog
		Sistem za vnos naročil

Vir: Lasten

Opisi identificiranih kritičnih sistemov IT in aplikacij:

- Uporabniški informacijski sistem skrbi za uporabniške podatke. Vsebuje imena podjetij, kontaktne informacije, elektronske naslove, naslove za pošiljanje, zgodovino, itd. Uporabniški informacijski sistem je povezan s sistemom za vnos naročil in s sistemom za sledenje prodajnih povpraševanj.
- Sistem za vnos naročil se uporablja za vnos, procesiranje in sledenje naročil.
- Elektronska pošta se uporablja za notranjo in zunanjo komunikacijo.
- Aplikacija za elektronsko izmenjavo podatkov se uporablja za sprejemanje elektronskih uporabniških naročil. Aplikacija je povezana s sistemom za vnos naročil.

- Sistem za sledenje prodajnih povpraševanj vsebuje podatke o potencialnih prodajnih priložnostih. Vsebuje imena podjetij, kontaktne informacije, datume povpraševanj, potencialna prodajna naročila, vrednosti naročil, itd. Sistem za sledenje prodajnih povpraševanj je povezan z uporabniškim informacijskim sistemom in sistemom za vnos naročil.
- Aplikacija za interaktivni katalog je spletni katalog, v katerem uporabniki pridobijo informacije o izdelkih preko svetovnega spleta.
- Računovodski sistem vsebuje uporabniške račune, prejemke plačil, kontrolo kreditov, itd. Računovodski sistem je povezan s sistemom za vnos naročil in sistemom za upravljanje pakiranja in prevoza.
- Sistem za upravljanje pakiranja in prevoza vsebuje ključne podatke, ki so potrebni za pošiljanje produktov strankam. Vsebuje podatke o času pošiljanja, teži, merah, karakteristikah, sledenju, itd. Sistem je povezan z računovodskim sistemom in sistemom za upravljanje zalog.
- Sistem za upravljanje zalog upravlja s podatki o zalogah. Za vsak produkt vsebuje podatke od trenutka sprejema od dobavitelja do trenutka, ko se pošlje stranki. Sistem za upravljanje je povezan s sistemom za upravljanje pakiranja in prevoza ter s sistemom za vnos naročil.

e) V tabeli 20 so predstavljeni objektivni časi okrevanja (OČO), delovni časi okrevanja (DČO) in objektivne točke okrevanja (OTO).

Tabela 20: **Določitev okrevalnih časov**

Poslovna funkcija	**Poslovni proces**	**Kritični sistemi IT in aplikacije**	**OČO**	**DČO**	**OTO**
Prodaja	Generiranje naročil	Uporabniški informacijski sistem	2.5 ure	0.5 ure	1 ura
		Sistem za vnos naročil	1.5 ure	1.5 ure	1 ura
		Elektronska pošta	2.5 ure	0.5 ure	1 ura
		Aplikacija za elektronsko izmenjavo podatkov	2 uri	1 ura	1 ura
		Sistem za sledenje prodajnih povpraševanj	2.8 ure	0.2 ure	1 ura
Marketing	Promocija produktov	Uporabniški informacijski sistem			
		Elektronska pošta			
	Prodajni katalogi	Aplikacija za interaktivni katalog	6.5 dni	0.5 dni	1 dan
Uporabniške storitve	Izvedba naročil	Sistem za vnos naročil			
		Sistem za upravljanje zalog	2 uri	1 ura	1 ura
		Računovodski sistem	1.5 ure	1.5 ure	1 ura
Transport	Pakiranje produktov	Sistem za vnos naročil			
		Sistem za upravljanje pakiranja in prevoza	0.8 dni	0.2 dni	2 uri
	Pošiljanje produktov	Sistem za upravljanje pakiranja in prevoza			
		Sistem za upravljanje zalog			
		Sistem za vnos naročil			

Vir: Lasten

Povzetek strategije neprekinjenega poslovanja

Identifikacija okrevalnih zahtev, možnosti in časovne razpoložljivosti:

V tabeli 21 so predstavljene okrevalne možnosti za kritične sisteme IT. Za vsako okrevalno možnost je naveden opis in predviden čas okrevanja. Okrevalne možnosti, pri katerih je okrevalni čas v mejah zahtevanih časov iz AVP, so v tabeli označene z zeleno barvo.

Tabela 21: **Okrevalne možnosti za kritične sisteme IT**

Kategorija	Možnosti	Opis	Okrevanje
Metode zagotavljanja rezervnih sistemov IT	Nadomestni sistemi	Nadomestne sisteme predstavljajo vnaprej pripravljenimi sistemi (pred nesrečo), ki služijo samo za primer izpada.	Nekaj ur do največ nekaj dni.
	Vnaprejšnji dogovor	Možnost predvideva vnaprejšnji dogovor (pred nesrečo) z dobaviteljem o hitri dobavi sistemov v slučaju nesreče.	Dva do sedem dni.
	Naročanje po potrebi	Možnost predvideva naročanje kritičnih sistemov pri dobaviteljih glede na potrebo, ki se pojavi po izpadu delovanja.	Več dni, tednov ali celo mesecev.

Vir: Lasten

V tabeli 22 so predstavljene okrevalne možnosti za rezervno lokacijo. Ustrezne okrevalne možnosti so v tabeli označene z zeleno barvo.

Tabela 22: **Okrevalne možnosti za rezervno lokacijo**

Kategorija	Možnosti	Opis	Okrevanje
Lastništvo lokacije	Lastni prostori	Rezervna lokacija v lastnih prostorih na oddaljeni lokaciji podjetja.	Odvisno od razdalje
	Mobilna lokacija	Mobilno lokacijo predstavlja vozilo, opremljeno z najnujnejšo strojno in programsko opremo.	Odvisno od poti in razdalje
	Skupna raba	Dogovor o skupni rabi prostorov z drugim podjetjem.	Odvisno od razdalje in pripravljenosti
	Najem lastne rezervne lokacije	Najem lastne rezervne lokacije pri komercialnem ponudniku.	Odvisno od razdalje
	Najem skupne rezervne lokacije	Najem skupne rezervne lokacije pri komercialnem ponudniku. Uporablja in deli si jo več podjetij.	Odvisno od razdalje in pripravljenosti
Opremljenost lokacije	Mrzla lokacija	Mrzla lokacija ne vsebuje nobene opreme.	Dva do tri tedne
	Topla lokacija	Topla lokacija ima nekaj najpotrebnejše strojne, programske in komunikacijske opreme že nameščene.	Nekaj dni do dveh tednov.
	Vroča lokacija	Vroča lokacija je v celoti opremljena in pripravljena za uporabo.	Nekaj ur.

Vir: Lasten

V tabeli 23 so predstavljene okrevalne možnosti za kritične podatke. Ustrezne okrevalne možnosti so v tabeli označene z zeleno barvo.

Tabela 23: **Okrevalne možnosti za kritične podatke**

Kategorija	Možnosti	Opis	Okrevanje
Pogostost arhiviranja	Nepretrgoma	Podatki se s pomočjo replikacije shranjujejo na pomnilniško enoto oddaljene lokacije.	OTO=ura
	Dnevno	Podatki se arhivirajo enkrat dnevno.	OTO=dan
	Tedensko	Podatki se arhivirajo enkrat tedensko.	OTO=teden
	Mesečno	Podatki se arhivirajo enkrat mesečno.	OTO=mesec
Način arhiviranja	Popolno	Napravi se kompleten arhiv vseh podatkov	Hitrejše restavriranje kot pri inkrement-alnem in difer-enetnem načinu
	Inkrementalno	Arhivirajo se samo podatki, ki so bili kreirani ali spremenjeni od zadnjega popolnega ali inkrementalnega arhiviranja	Dolgotrajnejše restavriranje
	Diferentno	Arhivirajo se samo podatki, ki so bili kreirani ali spremenjeni od zadnjega popolnega arhiviranja	Hitrejše restavriranje kot pri diferenetnem načinu
Metode arhiviranja	Zrcaljenje med lokacijami	Podatki se zrcalijo med primarno in rezervno lokacijo.	OČO=0 OTO=0
	Globalne gruče	Multipliciranje strežnikov z uporabo globalnih gruč.	OČO<8 ur OTO<30 minut
	Omrežna diskovna polja	Zelo hitra in zmogljiva diskovna polja z RAID tehnologijo omogočajo priklop strežnikov z različnimi operacijskimi sistemi.	
	Virtualizacija diskovnih polj	Združevanje več diskovnih polj v eno navidezno enoto.	
	Lokalno zrcaljenje diskov	Hkratno zapisovanje podatkov na več lokalnih diskov.	
	Senčenje diskov	Senčenje ali kloniranje diskov na diskovnih poljih.	
	Replikacija podatkov	Sinhrona ali asinhrona replikacija podatkov med diskovnimi polji.	
	Avtomatično arhiviranje	Avtomatično arhiviranje na oddaljeno lokacijo.	OČO>8 ur in OČO<72 ur OTO<24 ur
	Arhiviranje na kasete	Tradicionalna metoda arhiviranja podatkov na kasete.	OČO>72 ur OTO>24 ur

Vir: Lasten

V tabeli 24 so predstavljene okrevalne možnosti lokacije za shranjevanje podatkov. Ustrezne okrevalne možnosti so v tabeli označene z zeleno barvo.

Tabela 24: **Okrevalne možnosti lokacije za shranjevanje podatkov**

Kategorija	Možnosti	Opis	Okrevanje
Lokacija za shranjevanje	Lastna lokacija	Podatke se arhivira na oddaljeni lokaciji v lasti podjetja.	Odvisno od razdalje
	Komercialna lokacija	Sklene se dogovor z zunanjim ponudnikom, ki razpolaga s posebej opremljenimi prostori za arhiviranje podatkov.	Odvisno od razdalje

Vir: Lasten

Z vidika stroškov in sposobnosti ustrezne okrevalne možnosti:

V tabeli 25 so okrevalne možnosti, ki se v celoti ali delno skladajo z zahtevanimi časi okrevanja, ocenjene z vidika stroškov izvedbe, kvalitete, vloženega truda in nivoja kontrole, ki jo ima podjetje pri izgradnji. Izbrane okrevalne možnosti so v tabeli označene z zeleno barvo.

Tabela 25: **Kriterijska ocena ustreznih okrevalnih možnosti**

Kategorija	Možnosti	Stroški	Kvaliteta	Trud	Kontrola
Zagotavljanje rezervnih sistemov IT	Nadomestni sistemi	visoki	visoka	visok	visoka
	Vnaprejšnji dogovor	srednji	visoka	nizek	nizka
Lastništvo rezervne lokacije	Lastni prostori	nizki	visoka	visok	visoka
	Najem lastne rezervne lokacije	visoki	visoka	visok	srednja
Opremljenost rezervne lokacije	Topla lokacija	srednji	srednja	srednji	visoka
	Vroča lokacija	visoki	visoka	visok	visoka
Pogostost arhiviranja podatkov	Nepretrgoma	visoki	visoka	visok	visoka
	Dnevno	srednji	srednja	nizek	visoka
Način arhiviranja podatkov	Popolno	nizki	visoka	nizek	visoka
	Inkrementalno	srednji	visoka	srednji	visoka
	Diferentno	srednji	visoka	srednji	visoka
Metode arhiviranja podatkov	Zrcaljenje med lokacijami	visoki	visoka	visok	visoka
	Globalne gruče	visoki	visoka	visok	visoka
	Omrežna diskovna polja	visoki	visoka	srednji	visoka
	Virtualizacija diskovnih polj	visoki	visoka	visok	visoka
	Lokalno zrcaljenje diskov	nizki	visoka	nizek	visoka
	Senčenje diskov	srednji	visoka	srednji	visoka
	Replikacija podatkov	visoki	visoka	srednji	visoka
	Avtomatično arhiviranje	visoki	visok	visok	visoka
	Arhiviranje na kasete	nizki	srednja	nizek	visoka
Lokacija za shr. podatkov	Lastna lokacija	nizki	visoka	visok	visoka
	Komercialna lokacija	visoki	visoka	srednja	nizka

Vir: Lasten

Izbrane okrevalne možnosti za področje okrevanja: informacijski sistemi in infrastruktura

- Kritični sistemi IT in infrastruktura:
  Za zagotovitev rezervnih sistemov IT za sisteme, ki imajo največji sprejemljiv čas prekinitve manjši od enega dneva, se uporabi vnaprej pripravljene nadomestne sisteme, ki služijo samo za primer izpada.
  Za zagotovitev rezervnih sistemov IT za sisteme, ki imajo največji sprejemljiv čas prekinitve daljši od enega dneva, se izvede vnaprejšnji dogovor z dobaviteljem o hitri dobavi sistemov v slučaju izpada.

  Za računovodski sistem, sistem za vnos naročil, aplikacijo za elektronsko izmenjavo podatkov, sistem za upravljanje zalog, uporabniški informacijski sistem, elektronsko pošto, sistem za sledenje prodajnih povpraševanj in sistem za upravljanje pakiranja in prevoza se zagotovi vnaprej pripravljene nadomestne sisteme, ki se jih namesti na rezervno lokacijo in se uporabijo samo v slučaju izpada delovanja primarne lokacije.
  Za sistem z aplikacijo za interaktivni katalog se z dobaviteljem SNT d.d. sklene pogodbo o hitri dobavi sistema, če pride do izpada na primarni lokaciji. Dobavitelj zagotovi enakovreden strežnik, ki ga namesti na rezervni lokaciji in ustrezno usposobi najkasneje v 6 dneh, tako da lahko prevzame polno funkcionalnost okvarjenega strežnika.

- Rezervna lokacija:
  Za rezervno lokacijo se uporabijo lastni prostori podjetja v mestu Maribor (ABC d.d., Vrablova ulica 48, 2000 Maribor). Rezervno lokacijo se opremi s pripravljenimi nadomestnimi sistemi, rezervnim diskovnim poljem, arhivsko knjižnico in vso potrebno komunikacijsko opremo.

Izbrane okrevalne možnosti za področje okrevanja: podatki

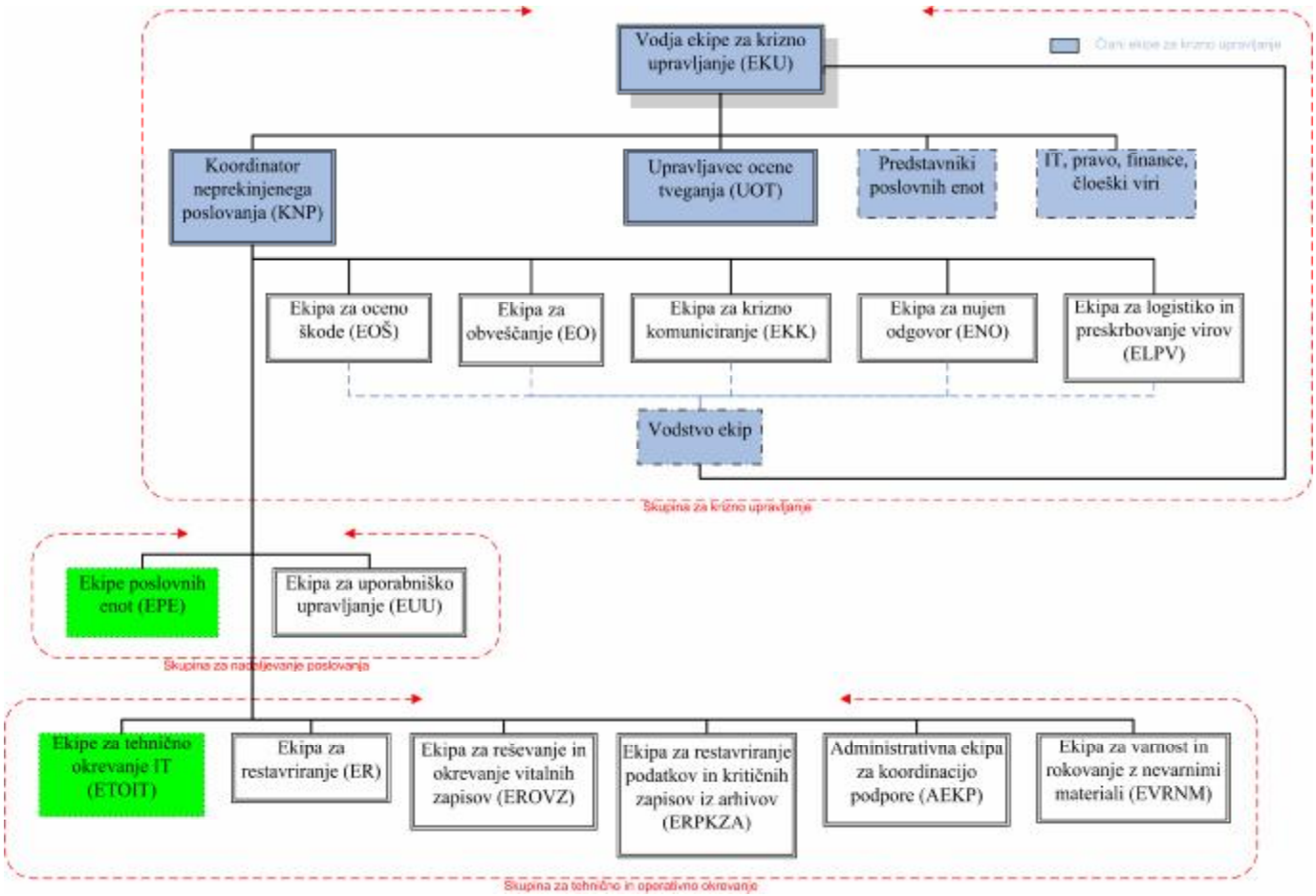
- Kritični podatki:
  Podatki se s pomočjo replikacije nepretrgoma shranjujejo na pomnilniško enoto oddaljene lokacije. Enkrat dnevno se izvede tudi popolno arhiviranje podatkov na kasete. Uporabi se omrežna diskovna polja z RAID tehnologijo. Eno diskovno polje se nahaja na primarni lokaciji podjetja, drugo diskovno polje pa se nahaja na rezervni lokaciji podjetja. Med diskovnima poljema je vzpostavljena asinhrona replikacija podatkov. Kot dodatno varovalo se uporabi senčenje diskov na diskovnih poljih. Za varovanje podatkov na lokalnih diskih strežnikov se uporabi zrcaljenje diskov.

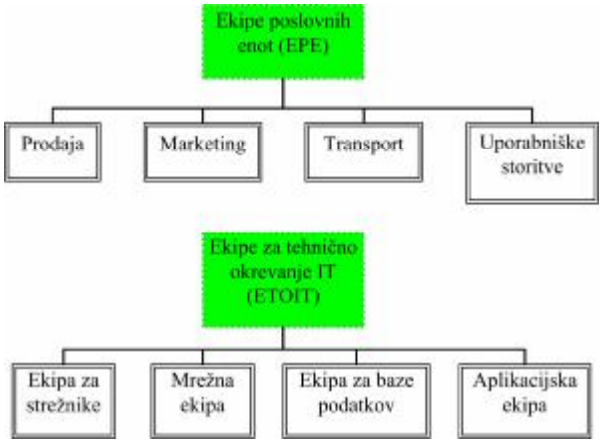
- Lokacija za shranjevanje podatkov:
  Za shranjevanje podatkov se uporabi lastna lokacija podjetja. Gre za rezervno lokacijo, ki se uporablja tudi za kritične sisteme IT in infrastrukturo.

Skupine za neprekinjeno poslovanje

Slika 25 prikazuje organizacijo skupin za neprekinjeno poslovanje. Skupine so razdeljene v tri nivoje. Skupina za krizno upravljanje vključuje ekipe, ki jih usmerja vodja ekipe za krizno upravljanje in med seboj koordinira koordinator neprekinjenega poslovanja. Skupina za nadaljevanje poslovanja je sestavljena iz ekip, katerih delovanje usklajuje koordinator neprekinjenega poslovanja. Skupina za tehnično in operativno okrevanja je sestavljena iz ekip za okrevanje virov IT in drugih virov. Delovanje usklajuje koordinator.

Slika 25: **Struktura skupin za neprekinjeno poslovanje**





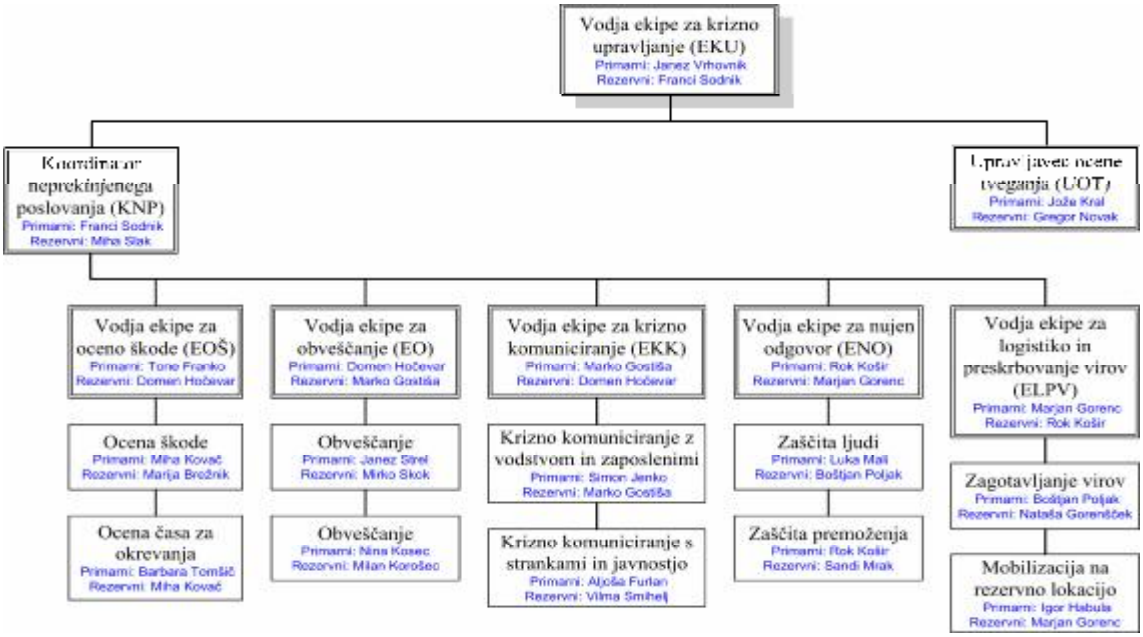
Vir: Lasten

Kontaktne informacije

a) Klicna drevesna struktura

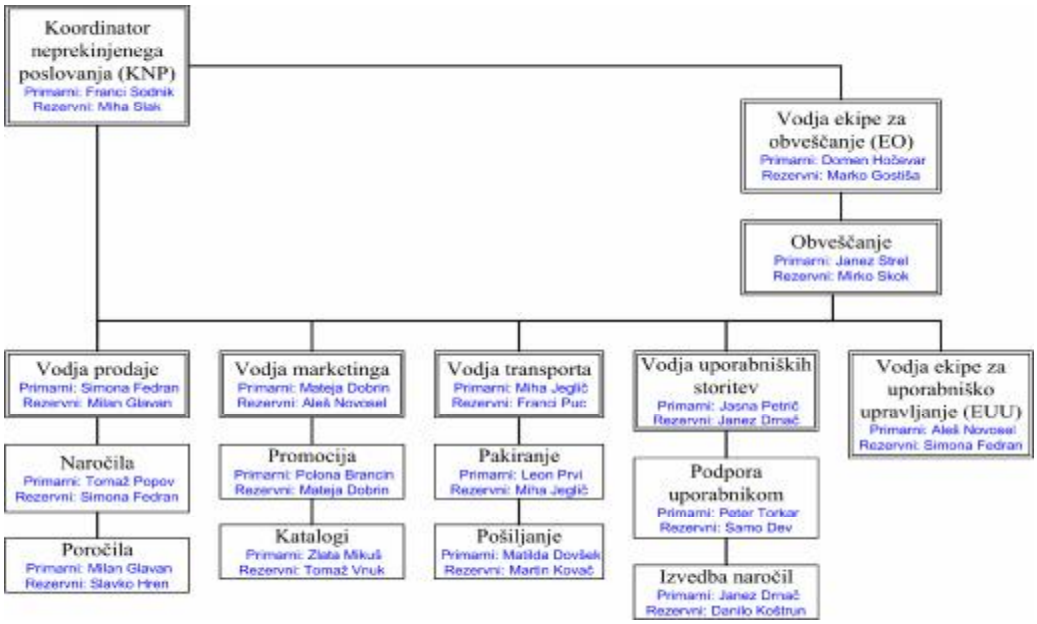
Slike 26, 27 in 28 prikazujejo klicne drevesne strukture. Obveščanje poteka od zgoraj navzdol. Nadrejeni član v drevesni strukturi obvešča vse člane, s katerimi je povezan in se v strukturi nahajajo pod njim. Obveščeni člani informacije dalje posredujejo povezanim članom, ki so v drevesni strukturi pod njimi. Postopek obveščanja se nadaljuje do dna drevesne strukture. V kolikor primarni član ni dosegljiv, se kontaktira rezervnega.

Slika 26: **Klicna drevesna struktura skupine za krizno upravljanje**



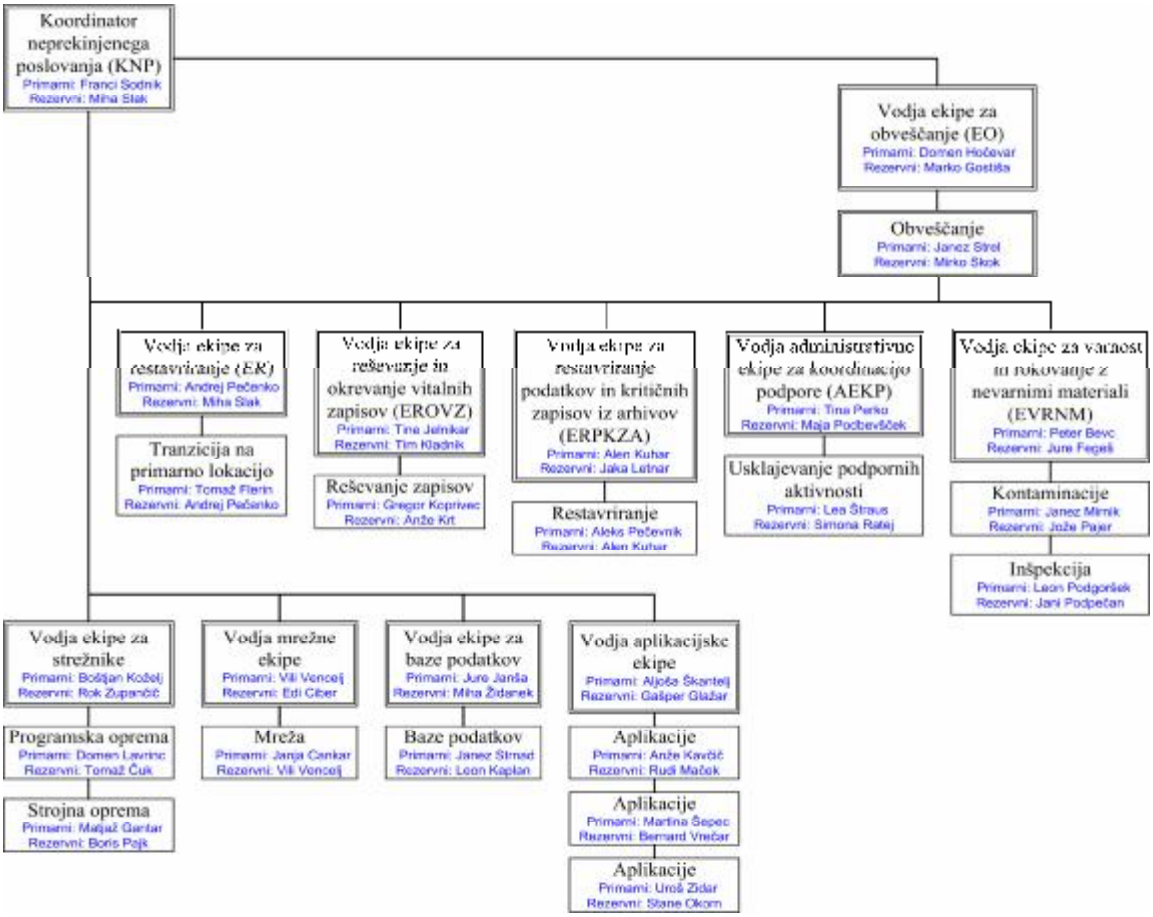
Vir: Lasten

Slika 27: **Klicna drevesna struktura skupine za nadaljevanje poslovanja**



Vir: Lasten

Slika 28: **Klicna drevesna struktura skupine za tehnično in operativno okrevanje**



Vir: Lasten

b) Kontaktna lista

Glavna kontaktna lista z imeni članov. Imena so sortirana po abecednem vrstnem redu.

1. **Bevc Peter**
   Ime ekipe: **Ekipa za varnost in rokovanje z nevarnimi materiali**
   Vloga člana: **Primarni vodja ekipe**
   Službeni tel.: **01 5582142**
   Prenosni tel.: **031 453656**
   Domači tel.: **01 5764255**
   E-naslov: **Bevc.Peter@abc.si**
2. **Brancin Polona**
   Ime ekipe: **Poslovna enota marketing**
   Vloga člana: **Primarni član za promocijo**
   Službeni tel.: **01 5582436**
   Prenosni tel.: **040 54322**
   Domači tel.: **01 5454651**
   E-naslov: **Brancin.Polona@abc.si**
3. **Brežnik Marija**
   Ime ekipe: **Ekipa za oceno škode**
   Vloga člana: **Rezervni ocenjevalec škode**
   Službeni tel.: **01 5582332**
   Prenosni tel.: **041 542756**
   Domači tel.: **01 5654344**
   E-naslov: **Breznik.Marija@abc.si**
4. **Cankar Janja**
   Ime ekipe: **Ekipa za tehnično okrevanje mrež**
   Vloga člana: **Primarni član za mreže**
   Službeni tel.: **01 5582431**
   Prenosni tel.: **041 543265**
   Domači tel.: **01 5243211**
   E-naslov: **Cankar.Janja@abc.si**
5. **Ciber Edi**
   Ime ekipe: **Ekipa za tehnično okrevanje mrež**
   Vloga člana: **Rezervni vodja ekipe za tehnično okrevanje mrež**
   Službeni tel.: **01 5582553**
   Prenosni tel.: **041 234666**
   Domači tel.: **01 5564321**
   E-naslov: **Ciber.Edi@abc.si**
6. **Čuk Tomaž**
   Ime ekipe: **Ekipa za tehnično okrevanje strežnikov**
   Vloga člana: **Rezervni član za programsko opremo**
   Službeni tel.: **01 5582342**
   Prenosni tel.: **040 432111**
   Domači tel.: **01 5543255**
   E-naslov: **Cuk.Tomaz@abc.si**
7. **Dev Samo**
   Ime ekipe: **Poslovna enota uporabniške storitve**
   Vloga člana: **Rezervni član za podporo uporabnikom**
   Službeni tel.: **01 5582441**
   Prenosni tel.: **041 452551**
   Domači tel.: **01 5235231**
   E-naslov: **Dev.Samo@abc.si**
8. **Dobrin Mateja**
   Ime ekipe: **Poslovna enota marketing**
   Vloga člana: **Primarni vodja poslovne enote marketing**
   Službeni tel.: **01 5582523**
   Prenosni tel.: **051 532561**
   Domači tel.: **01 5653767**
   E-naslov: **Dobrin.Mateja@abc.si**
9. **Dovšek Matilda**
   Ime ekipe: **Poslovna enota transport**
   Vloga člana: **Primarni član za pošiljanje**
   Službeni tel.: **01 5582324**
   Prenosni tel.: **041 654771**
   Domači tel.: **01 5655643**
   E-naslov: **Dovsek.Matilda@abc.si**

:

Recepcija ljubljanske poslovalnice podjetja ABC d.d.: 01 5582100, 041 694367
Recepcija mariborske poslovalnice podjetja ABC d.d.: 02 1526100, 041 456733
Gasilci: 112
Reševalci: 112
Policija: 113

Izvršilne faze NNP z opredelitvijo in dodelitvijo postopkov in nalog

a) Začeten odgovor in objava

Začeten odgovor in objava se izvede takoj po prekinitvenem dogodku. Izvedejo se vse predvidene aktivnosti izvršilne faze NNP za začeten odgovor in objavo (tabela 26).

Tabela 26: **Začeten odgovor in objava**

	Aktivnost	Postopek	Naloga	Ekipa	Člani ekipe
1.	Ugotovitev nesreče.	Po potrebi se obvesti gasilce in reševalce.	Na telefonski številki 112 ali 113 se obvesti ustrezne službe.	Dežurno osebje	Zaposleni
2.	Obvesti se koordinatorja NNP.	V internem telefonskem imeniku se poišče kontaktno informacijo.	O nesreči se obvesti koordinatorja NNP.	Dežurno osebje	Zaposleni
3.	Če je do nesreče prišlo izven delovnega časa se odpotuje v podjetje.	Takoj po prejemu obvestila o nesreči se odpotuje.	Odpotuje se na lokacijo podjetja.	Koordinator neprekinjenega poslovanja	Franci Sodnik
4.	Pridobi se vse potrebne dokumente.	Pridobi se vse dokumente, vezane na načrt neprekinjenega poslovanja (NNP).	Z intraneta, v kadrovski pisarni ali v pisarni koordinatorja NNP se pridobi vse dokumente vezane na NNP.	Koordinator neprekinjenega poslovanja	Franci Sodnik
5.	Obvesti se ekipo za nujen odgovor	Ekipa se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Koordinator neprekinjenega poslovanja	Franci Sodnik
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Koordinator neprekinjenega poslovanja	Franci Sodnik
6.	Zavaruje se ljudi in premoženje.	Pregleda se dodatek NNP: načrt nujnega odgovora	Zavaruje se ljudi.	Ekipa za nujen odgovor	Luka Mali
			Zavaruje se premoženje.	Ekipa za nujen odgovor	Rok Košir
7.	Ugotovi se, če je sistemski prostor dosegljiv.	Obišče se lokacija sistemskega prostora.	Preveri se fizična dostopnost v sistemski prostor.	Koordinator neprekinjenega poslovanja	Franci Sodnik
8.	Napravi se začetno oceno vzroka za nastalo škodo.	Pregleda se sistemski prostor.	Identificira se vzrok nesreče.	Koordinator neprekinjenega poslovanja	Franci Sodnik
9.	Ovrednoti se obseg nesreče.	Pregleda se sistemske komponente.	Identificira se prizadete vire.	Koordinator neprekinjenega poslovanja	Franci Sodnik
10.	Napravi se začetno oceno škode.	Pregleda se prizadete vire.	Za prizadete dele se določi stopnjo prizadetosti.	Koordinator neprekinjenega poslovanja	Franci Sodnik
11.	Izdela se uvodno poročilo o nesreči.	Zbere se rezultate ocen.	V poročilo se vključi rezultate zgornjih vrstic.	Koordinator neprekinjenega poslovanja	Franci Sodnik
12.	Obvesti se ekipo za obveščanje (EO).	Ekipa se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Koordinator neprekinjenega poslovanja	Franci Sodnik
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Koordinator neprekinjenega poslovanja	Franci Sodnik
13.	Obvesti se ekipo za krizno upravljanje.	Ekipa se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Ekipa za obveščanje	Janez Strel
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za obveščanje	Janez Strel
14.	Obvesti in mobilizira se ekipa za oceno škode (EOŠ).	Ekipa se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Ekipa za obveščanje	Nina Kosec
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za obveščanje	Nina Kosec

Vir: Lasten

b) Ocena problema in eskalacija

Druga izvšilna faza NNP je ocena problema in eskalacija. Izvedejo se predpisane aktivnosti iz tabele 27.

Tabela 27: **Ocena problema in eskalacija**

	Aktivnost	Postopek	Naloga	Ekipa	Člani ekipe
1.	Pridobi se uvodno poročilo o nesreči.	Koordinator NNP se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Ekipa za oceno škode	Tone Franko
			Pregleda se kontaktno listo in kontaktira koordinatorja NNP.	Ekipa za oceno škode	Tone Franko
			Pridobi se uvodno poročilo o nesreči.	Ekipa za oceno škode	Tone Franko
2.	Ugotovi se obseg, moč in vzrok nesreče.	Pregleda se uvodno poročilo o nesreči.	Identificira se vzrok nesreče.	Ekipa za oceno škode	Miha Kovač
			Opredeli se moč nesreče.	Ekipa za oceno škode	Miha Kovač
			Identificira se prizadete vire.	Ekipa za oceno škode	Miha Kovač
3.	Izdela se detajlno oceno nesreče.	Pregleda se prizadeto lokacijo.	Na osnovi identificiranih virov in pregleda lokacije se naredi detajlno oceno nesreče.	Ekipa za oceno škode	Miha Kovač
4.	Oceni se zdravstvena in varnostna tveganja.	Pregleda se prizadeto lokacijo.	Identificira se morebitne nevarnosti za zdravje.	Upravljavec ocene tveganja	Jože Kral
			Ugotovi se morebitno prisotnost nevarnih materialov.	Upravljavec ocene tveganja	Jože Kral
5.	Oceni se nastalo škodo.	Pregleda se prizadeto lokacijo in funkcionalnost poslovnih procesov.	Oceni se škodo prostorov.	Ekipa za oceno škode	Miha Kovač
			Oceni se škodo na opremi.	Ekipa za oceno škode	Miha Kovač
			Oceni se možnost širjenja posledic nesreče.	Upravljavec ocene tveganja	Jože Kral
			Oceni se vpliv na delovanje poslovnih procesov.	Ekipa za oceno škode	Miha Kovač
6.	Oceni se finančno izgubo.	Pregleda se prizadeto lokacijo.	Oceni se zmanjšanje vrednosti prizadete opreme in prostorov.	Ekipa za oceno škode	Miha Kovač
7.	Definira oz. klasificira se nesrečo.	Pregleda se drugo poglavje NNP.	Na osnovi pridobljenih ugotovitev se določi stopnjo nesreče.	Ekipa za oceno škode	Tone Franko
8.	Odloči se o zaustavitvi ali nadaljevanju izvajanja NNP.	Pregleda se oceno vpliva na delovanje poslovnih procesov.	Če nesreča ni vplivala na delovanje kritičnih procesov, se izvajanje NNP zamrzne. Situacija se nadzira.	Vodja ekipe za krizno upravljanje	Janez Vrhovnik
			Če je nesreča vplivala na delovanje kritičnih procesov, se nadaljuje z izvajanjem NNP.	Vodja ekipe za krizno upravljanje	Janez Vrhovnik
9.	Izdela se detajlno poročilo o nesreči	Na osnovi predhodnih ocen se izdela detajlno poročilo o nesreči.	Opiše se klasifikacijo nesreče.	Ekipa za oceno škode	Tone Franko
			Opiše se oceno finančnega izpada.	Ekipa za oceno škode	Miha Kovač
			Opiše se vzrok nesreče.	Ekipa za oceno škode	Miha Kovač
			Opiše se obseg nesreče.	Ekipa za oceno škode	Miha Kovač
			Opiše se fizično stanje sistemskega prostora.	Ekipa za oceno škode	Miha Kovač
			Opiše se varnostni status sistemskega prostora.	Upravljavec ocene tveganja	Jože Kral
			Opiše se morebitno prisotnost nevarnih materialov.	Upravljavec ocene tveganja	Jože Kral
			Opiše se možnost širjenja posledic nesreče.	Upravljavec ocene tveganja	Jože Kral
			Opiše se oceno trajanja okrevanja.	Ekipa za oceno škode	Barbara Tomšič
10.	Obvesti se skupino za tehnično in operativno okrevanje.	Ekipa se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Ekipa za obveščanje	Janez Strel
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za obveščanje	Janez Strel
11.	Obvesti se skupino za nadaljevanje poslovanja.	Ekipa se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Ekipa za obveščanje	Nina Kosec
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za obveščanje	Nina Kosec

Vir: Lasten

c) Razglasitev nesreče

Razglasitev nesreče je tretja izvršilna faza NNP. Odločitev za razglasitev nesreče temelji na detajlnem poročilu o nesreči. Izvede se aktivnosti iz tabele 28.

Tabela 28: **Razglasitev nesreče**

	Aktivnost	Postopek	Naloga	Ekipa	Člani ekipe
1.	Za dano situacijo se izbere najboljši okrevalni pristop.	Pregleda se detajlno poročilo o nesreči.	Ugotovi se stopnja nesreče.	Ekipa za oceno škode.	Tone Franko
			Ugotovi se tveganja.	Upravljavec ocene tveganja	Jože Kral
			Ugotovi se vplive nesreče.	Ekipa za uporabniško upravljanje	Aleš Novosel
		Pregleda se peto poglavje NNP.	Izbere se najboljši okrevalni pristop.	Ekipa za krizno upravljanje	Janez Vrhovnik, Franci Sodnik, Jože Kral, Tone Franko
2.	Pripravi se izjava o razglasitvi nesreče.	Izjava o razglasitvi nesreče se izdela na osnovi predhodnih korakov in poglavij.	Definira se žarišče nesreče.	Koordinator neprekinjenega poslovanja	Franci Sodnik
			Vpiše se datum in čas nastanka nesreče.	Koordinator neprekinjenega poslovanja	Franci Sodnik
			Nesrečo se definira oz. klasificira.	Ekipa za oceno škode	Tone Franko
			Navede se prizadete vire.	Ekipa za oceno škode	Tone Franko
			Opiše se izbrano okrevalno strategijo.	Koordinator neprekinjenega poslovanja	Franci Sodnik
			Definira se lokacijo okrevanja.	Koordinator neprekinjenega poslovanja	Franci Sodnik
			Oceni se čas okrevanja.	Ekipa za oceno škode	Tone Franko
			Vpiše se imena posameznikov, ki so odgovorni za izdajo izjave o razglasitvi nesreče.	Vodja ekipe za krizno upravljanje	Janez Vrhovnik
			Vpiše se kontaktne informacije za dodatna pojasnila.	Koordinator neprekinjenega poslovanja	Franci Sodnik
3.	Izjavo o razglasitvi nesreče se razširi.	Osebje se locira v shemi skupin za neprekinjeno poslovanje	Pregleda se klicno drevesno strukturo	Ekipa za obveščanje	Janez Strel
			Pregleda se kontaktno listo in obvesti ustrezno osebje	Ekipa za obveščanje	Janez Strel
4.	Obvesti se ekipo za krizno komuniciranje.	Ekipa se locira v shemi skupin za neprekinjeno poslovanje	Pregleda se klicno drevesno strukturo	Ekipa za obveščanje	Domen Hočevar
			Pregleda se kontaktno listo in obvesti ustrezno osebje	Ekipa za obveščanje	Domen Hočevar
5.	O nesreči se obvesti vse zaposlene in javnost.	Pregleda se dodatek NNP: načrt kriznega komuniciranja	O nesreči se obvesti vse zaposlene.	Ekipa za krizno komuniciranje	Simon Jenko
			O nesreči se obvesti javnost.	Ekipa za krizno komuniciranje	Aljoša Furlan

Vir: Lasten

d) Logistika

Logistika je četrta izvršilna faza NNP. Izvede se aktivnosti za pripravo rezervne lokacije in pripravo ekip iz tabele 29.

Tabela 29: **Logistika**

	Aktivnost	Postopek	Naloga	Ekipa	Člani ekipe
Aktivnosti za pripravo rezervne lokacije					
1.	Obvesti se ekipo za logistiko in preskrbovanje virov.	Ekipa se locira v shemi skupin za neprekinjeno poslovanje	Pregleda se klicno drevesno strukturo	Ekipa za obveščanje	Nina Kosec
			Pregleda se kontaktno listo in obvesti ustrezno osebje	Ekipa za obveščanje	Nina Kosec
2.	Naroči se potrebna manjkajoča računalniška strojna in programska oprema.	Pregleda se dodatek NNP »Pogodbe z dobavitelji«	V skladu z določili pogodbe se pri zunanjem dobavitelju naroči sistem z aplikacijo za interaktivni katalog.	Ekipa za logistiko in preskrbovanje virov	Boštjan Poljak
3.	Na rezervno lokacijo se pošlje ključne dokumente.	Zbere se ključne dokumente.	Na rezervno lokacijo se pošlje detajlno poročilo o nesreči, izjavo o razglasitvi nesreče in NNP z vsemi dodatki.	Ekipa za logistiko in preskrbovanje virov	Marjan Gorenc
4.	Na rezervni lokaciji se pripravi vse za sprejem naročene opreme.	Pregleda se dodatek NNP »Pogodbe z dobavitelji« in povzetek strategije NNP.	Pripravi se prostor in mrežno povezavo za sistem z aplikacijo za interaktivni katalog.	Ekipa za logistiko in preskrbovanje virov	Boštjan Poljak
5.	Rezervno lokacijo se pripravi za sprejem okrevalnih ekip.	Pregleda se kontaktno listo.	Obvesti se recepcijo mariborske poslovalnice in omogoči vstop okrevalnim ekipam.	Ekipa za logistiko in preskrbovanje virov	Igor Habula
Aktivnosti za pripravo ekip					
6.	Ugotovi se kdo je na voljo za okrevalne operacije.	Pregleda se seznam uspešno obveščenega osebja.	V klicni drevesni strukturi se označi dosegljivo osebje.	Administrativna ekipa za koordinacijo podpore	Lea Štraus
7.	Določi se člane ekip, ki bodo odpotovali na rezervno lokacijo.	Pregleda se z dosegljivim osebjem označeno klicno drevesno strukturo.	Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za logistiko in preskrbovanje virov	Igor Habula
8.	Določi se člane ekip, ki bodo delali na primarni lokaciji, če je še dosegljiva.	Pregleda se z dosegljivim osebjem označeno klicno drevesno strukturo.	Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za logistiko in preskrbovanje virov	Igor Habula
9.	Pripravi se potovalni načrt.	Preveri se prometne informacije.	Izbere se način potovanja.	Administrativna ekipa za koordinacijo podpore	Lea Štraus
10.	Zagotovi se informacije o tem, kaj je bilo poslano na rezervno lokacijo.	Zbere se informacije o tem, kaj je bilo poslano na rezervno lokacijo.	Seznam se pošlje na rezervno lokacijo.	Ekipa za logistiko in preskrbovanje virov	Boštjan Poljak

Vir: Lasten

e) Okrevanje kritičnih virov in procesov

Aktivnosti na primarni lokaciji

Na primarni, poškodovani lokaciji izvaja okrevalne aktivnosti skupina za tehnično in operativno okrevanje, ki je zadolžena za reševanje vitalnih zapisov in kritičnih virov. Aktivnosti na poškodovani lokaciji sestavljajo štirje koraki: priprava, pregled in ocena, reševanje in obnova ter transport (tabela 30).

Tabela 30: **Okrevanje kritičnih virov in procesov na primarni lokaciji**

	Aktivnost	Postopek	Naloga	Ekipa	Člani ekipe
Priprava					
1.	Preveri se, ali so vse potrebne ekipe prišle na prizadeto lokacijo.	Pregleda se klicno drevesno strukturo.	Preveri in označi se prisotnost ekip.	Administrativna ekipa za koordinacijo podpore	Lea Štrus
2.	Preveri se, ali imajo ekipe seznam kritičnih virov prizadete lokacije.	Izvede se sestanek z vodji ekip.	Preveri se, ali imajo vse ekipe NNP z dodatki.	Administrativna ekipa za koordinacijo podpore	Lea Štraus
3.	Ekipe se seznani s situacijo.	Vodjem ekip se posreduje detajlno poročilo o nesreči.	Ekipe pregledajo detajlno poročilo o nesreči.	Administrativna ekipa za koordinacijo podpore	Tina Perko
4.	Ekipe se seznani se z varnostnimi procedurami in smernicami.	Pregleda se dodatek NNP: varnostne procedure in smernice.	Glede na detajlno poročilo o nesreči se pregleda ustrezne varnostne procedure.	Ekipa za varnost in rokovanje z nevarnimi materiali	Peter Bevc
Pregled in ocena					
5.	Pregleda in ugotovi se stanje prostorov.	Vstopi se v sistemski prostor.	Ugotovi se stanje prostorov.	Ekipa za varnost in rokovanje z nevarnimi materiali	Leon Podgoršek
6.	Ugotovi se morebitno prisotnost nevarnih substanc.	Pregleda se sistemski prostor.	Potrdi ali zanika se prisotnost nevarnih substanc.	Ekipa za varnost in rokovanje z nevarnimi materiali	Janez Mirnik
7.	Pregleda se vire in ugotovi tip poškodbe.	Pregleda se vire v sistemskem prostoru.	Ugotovi se tip poškodbe.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
8.	Pregleda se vire in ugotovi obseg okvare.	Pregleda se vire v sistemskem prostoru.	Ugotovi se obseg okvare.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
9.	Oceni se možnost širjenja okvar.	Pregleda se vire v sistemskem prostoru.	Naredi se oceno možnosti širjenja okvar.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
10.	Oceni se možnosti restavriranja.	Pregleda se ugotovljen tip in obseg okvar virov.	Oceni se možnost restavriranja.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
11.	Določi se razpoložljivi čas za izvedbo reševalnih procedur.	Pregleda se ugotovljen tip in obseg okvar virov.	Oceni se razpoložljivi čas okrevanja.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
12.	Ugotovitve pregleda se dokumentira.	Zbere se vse ugotovitve pregleda.	Ugotovitve se dokumentira.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
Reševanje in obnova					
13.	Po potrebi se pridobi dodatna oprema in vire za reševanje.	Pregleda se ugotovitve pregleda.	Naroči se opremo in vire za reševanje.	Ekipa za logistiko in preskrbovanje virov	Boštjan Poljak
14.	Po potrebi se odstrani prisotnost nevarnih substanc.	Pregleda se ugotovitve pregleda.	Odstrani se identificirane nevarne substance.	Ekipa za varnost in rokovanje z nevarnimi materiali	Janez Mirnik
15.	Onemogoči se nadaljnje širjenja okvar.	Pregleda se ugotovitve pregleda.	Prepreči se nadaljnje širjenje okvar.	Ekipe za tehnično okrevanje IT	Boris Pajk, Vili Vencelj
16.	Po potrebi se vire prenese v primernejše okolje za reševanje.	Pregleda se detajlno poročilo o nesreči.	Če je potrebno, se vire prenese v varnejše okolje.	Ekipe za tehnično okrevanje IT	Boris Pajk, Vili Vencelj
17.	Rezultate reševanja se dokumentira.	Vse aktivnosti reševanja se beleži.	Sestavi se dokument z rezultati reševanja.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
Transport					
18.	Določi se lokacija na katero se transportira rešene vire.	Pregleda se detajlno poročilo o nesreči, dodatek NNP s seznamom opreme na rezervni lokaciji in seznam kritičnih virov.	Rešene vire se pošlje na najprimernejšo lokacijo.	Ekipa za logistiko in preskrbovanje virov	Marjan Gorenc
19.	Pripravi se navodila za varno ravnanje z rešenimi viri.	Pregleda se stanje virov in dokument z rezultati reševanja.	Glede na tip in stanje virov se pripravi navodila za varno ravnanje z njimi.	Ekipe za tehnično okrevanje IT	Rok Zupančič, Edi Ciber
20.	Organizira se transport.	Naroči se transportno službo.	V skladu z navodili za varno ravnanje se transportira vire na izbrano lokacijo.	Ekipa za logistiko in preskrbovanje virov	Boštjan Poljak

Vir: Lasten

Aktivnosti na rezervni lokaciji

Na rezervni lokaciji IT so aktivnosti sestavljene iz treh korakov: priprava, izgradnja kritičnih sistemov IT in mrežne infrastrukture ter restavriranje kritičnih aplikacij IT (tabela 31).

Tabela 31: **Okrevanje kritičnih virov in procesov na rezervni lokaciji**

	Aktivnost	Postopek	Naloga	Ekipa	Člani ekipe
Priprava					
1.	Preveri se, ali so vse potrebne ekipe in njihovi člani prispeli na rezervno lokacijo.	Pregleda se klicno drevesno strukturo.	Preveri in označi se prisotnost ekip.	Administrativna ekipa za koordinacijo podpore	Lea Štraus
2.	Preveri se, ali imajo člani ekip seznam opreme in okrevalne procedure.	Kontaktira se vodje ekip.	Preveri se, ali imajo vse ekipe NNP z dodatki.	Administrativna ekipa za koordinacijo podpore	Lea Štraus
3.	Preveri se, ali se vsi sodelujoči zavedajo zahtevanih okrev.časov.	Kontaktira se vodje ekip.	Preveri se, ali je ekipam jasna vsebina NNP.	Administrativna ekipa za koordinacijo podpore	Lea Štraus
4.	Na rezervni lokaciji se pregleda oprema in zagotovi, da je skladna z okrevalnimi zahtevami.	Pregleda se dodatek NNP: seznam opreme na rezervni lokaciji.	Potrdi se skladnost opreme z okrevalnimi zahtevami.	Ekipe za tehnično okrevanje IT	Boštajn Koželj, Vili Vencelj
5.	Po sprejemu manjkajoče opreme se preveri skladnost s seznamom poslane opreme.	Pregleda se seznam naročene opreme.	Potrdi se ujemanje poslane opreme s seznamom	Ekipe za tehnično okrevanje IT	Boštajn Koželj, Vili Vencelj
Izgradnja kritičnih sistemov IT in mrežne infrastrukture					
6.	Zagotovi se, da so vsi kritični sistemi IT povezani v mrežo.	Pregleda se kritične sisteme IT.	Zagotovi se, da so sistemi povezani v mrežo.	Mrežna ekipa	Janja Cankar
7.	Preveri se mrežne in sistemske naslove in nastavitvene informacije.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Zagotovi se korektnost mrežnih in nastavitvenih informacij.	Mrežna ekipa	Janja Cankar
8.	Na rezervno lokacijo se preusmeri glasovni in podatkovni prenos podatkov.	Nastavi se mrežna stikala.	Mrežni pretok se preusmeri na rezervno lokacijo.	Mrežna ekipa	Janja Cankar
9.	Testira in preveri se mrežno povezljivost.	Pregleda se sisteme.	Preveri se mrežno povezljivost.	Ekipa za strežnike	Domen Lavrinc
Restavriranje kritičnih aplikacij IT					
10.	Preveri se okrevalne prioritete kritičnih sistemov IT in aplikacij.	Pregleda se povzetek analize vpliva na poslovanje v NNP.	Določi se okrevalne prioritete kritičnih sistemov IT.	Ekipa za strežnike	Boštjan Koželj
11.	Prekine se replikacija in aktivira datotečne skupine na nadomestnih sistemih.	Pregleda se dodatek NNP: Procedure za restavriranje kritičnih podatkov	Na nadomestne sisteme se importira datotečne skupine.	Ekipa za strežnike	Domen Lavrinc
12.	Vzpostavi se delovanje baz podatkov.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Na nadomestnih sistemih se aktivira podatkovne baze.	Ekipa za baze podatkov	Janez Strnad
13.	Vzpostavi se delovanje aplikacij.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Na nadomestnih sistemih se zažene aplikacije.	Aplikacijska ekipa	Anže Kavčič, Martina Šepec, Uroš Zidar
14.	Preveri se funkcionalnost aplikacij in korektnost podatkov.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Na nadomestnih sistemih se preveri korektnost delovanja.	Ekipe poslovnih enot	Simona Fedran, Mateja Dobrin, Miha Jeglič, Jasna Petrič
			Aplikacije se preda v uporabo.	Aplikacijska ekipa	Aljoša Škantelj
15.	Iz arhivskih medijev se restavrira operacijski sistem za naročeno mankajočo opremo.	Pregleda se dodatek NNP: Procedure za restavriranje kritičnih podatkov.	Iz arhivskih medijev se restavrira operacijski sistem za sistem z aplikacijo za interaktivni katalog.	Ekipa za restavriranje podatkov in kritičnih zapisov iz arhivov	Aleks Pečevnik
16.	Preveri se mrežno	Pregleda se sistem.	Preveri se mrežno	Mrežna ekipa	Janja Cankar

	povezljivost.		povezljivost.		
17.	Iz arhivskih medijev se restavrira aplikacije.	Pregleda se dodatek NNP: Procedure za restavriranje kritičnih podatkov	Iz arhivskih medijev se restavrira aplikacije.	Ekipa za restavriranje podatkov in kritičnih zapisov iz arhivov	Aleks Pečevnik
18.	Iz arhivskih medijev se restavrira podatke.	Pregleda se dodatek NNP: Procedure za restavriranje kritičnih podatkov	Iz arhivskih medijev se restavrira podatke.	Ekipa za restavriranje podatkov in kritičnih zapisov iz arhivov	Aleks Pečevnik
19.	Preveri se funkcionalnost aplikacij in korektnost podatkov.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Preveri se korektnost delovanja.	Poslovna enota marketing	Mateja Dobrin
			Aplikacije se preda v uporabo.	Aplikacijska ekipa	Aljoša Škantelj

Vir: Lasten

f) Normalizacija

Zadnjo izvršilno fazo NNP predstavlja normalizacija. Namen normalizacije je vrnitev dejavnosti z rezervne lokacije nazaj na primarno lokacijo in vzpostavitev stanja in pogojev, ki so vladali pred nesrečo. Normalizacijo sestavljajo štirje sklopi aktivnosti: pregled originalne lokacije, popravilo, priprava in tranzicija (tabela 32). Z izjemo tranzicije se ostale aktivnosti lahko izvajajo vzporedno z aktivnostmi faze za okrevanje kritičnih virov in procesov. Tranzicija se lahko začne šele tedaj, ko je faza za okrevanje kritičnih virov in procesov zaključena.

Tabela 32: **Normalizacija**

	Aktivnost	**Postopek**	**Naloga**	**Ekipa**	**Člani ekipe**
Pregled originalne lokacije					
1.	Ugotovi se možnost vrnitve na originalno lokacijo.	Izvede se temeljit pregled originalne lokacije.	Ugotovi se možnost vrnitve.	Ekipa za restavriranje	Andrej Pečenko
2.	Razišče se možnosti prehoda na drugo lokacijo.	Pregleda se vse razpoložljive lokacije.	Ugotovi se možnost prehoda na drugo lokacijo.	Ekipa za restavriranje	Andrej Pečenko
3.	V dogovoru z vodstvom se izbere lokacijo.	Primerja se rezultate predhodnih dveh korakov.	Vodstvu se predstavi rezultate.	Ekipa za restavriranje	Andrej Pečenko
			Izbere se lokacijo.	Vodja ekipe za krizno upravljanje	Janez Vrhovnik
Popravilo					
4.	Pridobi se odobritev za popravilo prizadete lokacije.	Pregleda se ugotovitve temeljitega pregleda originalne lokacije.	Vodstvu se predstavi rezultate.	Ekipa za restavriranje	Andrej Pečenko
			Odobri se popravilo.	Vodja ekipe za krizno upravljanje	Janez Vrhovnik
5.	Pridobi se potrebna dovoljenja za obnovo.	Kontaktira se pristojne organe.	Pridobi se dovoljenja za obnovo.	Administrativna ekipa za koordinacijo podpore	Tina Perko
6.	Najame se pogodbenike za popravilo prizadete lokacije.	Pregleda se ugotovitve temeljitega pregleda originalne lokacije.	V skladu z ugotovitvami se najame ustrezne pogodbenike za popravilo lokacije.	Ekipa za logistiko in preskrbovanje virov	Marjan Gorenc
7.	Preveri se stanje opremljenosti in po potrebi naroči dodatno opremo.	Pregleda se ugotovitve temeljitega pregleda originalne lokacije.	Naroči se manjkajočo opremo.	Ekipa za logistiko in preskrbovanje virov	Boštjan Poljak
8.	Fizično se namesti naročeno opremo in vire.	Sprejme in pregleda se naročeno opremo.	Namesti se mrežno opremo.	Mrežna ekipa	Vili Vencelj
			Namesti se periferno opremo.	Ekipa za strežnike	Boris Pajk
			Namesti se diskovno polje.	Ekipa za strežnike	Boris Pajk
			Namesti se sisteme.	Ekipa za strežnike	Boris Pajk
Priprava					
9.	Preveri se, da so sistemi povezani v mrežo.	Pregleda se nameščeno opremo.	Zagotovi se povezanost v mrežo.	Mrežna ekipa	Vili Vencelj
10.	Iz arhivskih medijev se restavrira mrežne sisteme.	Pregleda se dodatek NNP: Procedure za restavriranje kritičnih podatkov	Iz arhivskih medijev se restavrira podatke.	Ekipa za restavriranje podatkov in kritičnih zapisov iz arhiviv	Alen Kuhar
11.	Vzpostavi se sinhronizacija med diskovnimi polji.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in	Med diskovnimi polji se vzpostavi asinhrona replikacija.	Ekipa za strežnike	Tomaž Čuk

		aplikacij			
12.	Iz arhivskih medijev se restavrira varnostne sisteme.	Pregleda se dodatek NNP: Procedure za restavriranje kritičnih podatkov	Iz arhivskih medijev se restavrira podatke.	Ekipa za restavriranje podatkov in kritičnih zapisov iz arhiviv	Alen Kuhar
Tranzicija					
13.	Določi se časovni termin tranzicije.	Organizira se sestanek ekipe za krizno upravljanje.	Določi se datum in čas tranzicije.	Ekipa za krizno upravljanje	Janez Vrhovnik
14.	Ekipe se obvesti o času tranzicije in nalogah.	Ekipe se locira v shemi skupin za neprekinjeno poslovanje.	Pregleda se klicno drevesno strukturo.	Ekipa za obveščanje	Janez Strel
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za obveščanje	Janez Strel
15.	Produkcijsko okolje na rezervni lokaciji se zamrzne.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Zaustavi se delovanje aplikacij na rezervni lokaciji.	Aplikacijska ekipa	Anže Kavčič, Martina Šepec, Uroš Zidar
16.	Izdela se popolne arhive sistemov na rezervni lokaciji.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Izdela se popolne arhive sistemov.	Ekipa za strežnike	Domen Lavrinc
17.	Ekipe z arhivi se pošlje na originalno ali drugo lokacijo.	Pregleda se klicno drevesno strukturo.	Pregleda se klicno drevesno strukturo.	Ekipa za obveščanje	Janez Strel
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za obveščanje	Janez Strel
18.	Preveri se, ali so vse potrebne ekipe prišle na originalno ali drugo lokacijo.	Pregleda se klicno drevesno strukturo.	Preveri in označi se prisotnost ekip.	Administrativna ekipa za koordinacijo podpore	Lea Štraus
19.	Na originalni ali drugi lokaciji se restavrira sisteme, aplikacije in podatke.	Pregleda se dodatek NNP: Procedure za restavriranje kritičnih podatkov	Iz arhivskih medijev se restavrira podatke.	Ekipa za restavriranje podatkov in kritičnih zapisov iz arhiviv	Aleks Pečevnik
20.	Aktivira in preveri se delovanje mreže, sistemov, podatkovnih baz, aplikacij in podatkov.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Preveri se korektnost delovanja mreže.	Mrežna ekipa	Janja Cankar
			Zažene in preveri se korektnost delovanja sistemov.	Ekipa za strežnike	Domen Lavrinc
			Zažene in preveri se korektnost delovanja podatkovnih baz.	Ekipa za baze podatkov	Janez Strnad
			Zažene in preveri se korektnost delovanja aplikacij.	Aplikacijska ekipa	Anže Kavčič, Martina Šepec, Uroš Zidar
			Preveri se korektnost podatkov.	Ekipe poslovnih enot	Simona Fedran, Mateja Dobrin, Miha Jeglič, Jasna Petrič
21.	Glasovni in podatkovni promet se preusmeri na originalno ali drugo lokacijo.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Mrežni promet se preusmeri na originalno ali drugo lokacijo.	Mrežna ekipa	Janja Cankar
22.	Uporabnikom se določi nova gesla.		Na sistemih se zamenja uporabniška gesla.	Ekipa za strežnike	Domen Lavrinc
			Na aplikacijah se zamenja uporabniška gesla.	Aplikacijska ekipa	Anže Kavčič, Martina Šepec, Uroš Zidar
23.	Obvesti se uporabnike in začne se z izvajanjem normalnih operacij.	Pregleda se klicno drevesno strukturo.	Pregleda se klicno drevesno strukturo.	Ekipa za obveščanje	Nina Kosec
			Pregleda se kontaktno listo in obvesti ustrezno osebje.	Ekipa za obveščanje	Nina Kosec
24.	Izvede se normalne postopke za arhiviranje.	Pregleda se dodatek NNP: Nastavitve in navodila za uporabo sistemov IT in aplikacij	Izvede se postopke za arhiviranje.	Ekipa za strežnike	Domen Lavrinc

Vir: Lasten

Kontrola sprememb NNP

NNP mora biti usklajen s spremembami procesov, tehnologije in ljudi. Spremembe NNP morajo biti kontrolirane s kontrolnimi postopki, da se zagotovi integriteto in veljavnost načrta. Sledi opis kontrolnega postopka, ki obravnava spremembe NNP:

· Pregleda se zahtevo za spremembo NNP.
· Ugotovi se naravo zahtevane spremembe (procesi, tehnologija, ljudje).
· Identificira se poglavja in dele NNP, na katere vpliva sprememba.
· Identificira se osebje, ki je odgovorno za dele NNP, na katere vpliva sprememba. Osebje izdela osnutek dokumenta, ki vsebuje zahtevane spremembe NNP za svoje področje, ali pa zavrne zahtevane spremembe in ustrezno obrazloži zavrnitev.
· Osnutek dokumenta se pregleda in ugotovi morebitne odvisnosti, konflikte in pomanjkljivosti. Po potrebi se ugotovljene nepravilnosti korigira.
· Osnutek dokumenta se dokončno izoblikuje in pridobi potrditev odgovornih oseb.
· NNP se popravi in dopolni v skladu s potrjenim dokumentom.
· Vse upoštevane spremembe NNP se v okviru tega poglavja tudi dokumentira.
· NNP se razpošlje prejemnikom iz distribucijske liste NNP.

Dodatki NNP

Načrt neprekinjenega poslovanja predvideva več možnih dodatkov, ki so priloženi kot priloge in na katere se nanašajo in sklicujejo postopki izvršilnih faz NNP. Dodatki podrobno opisujejo posamezna področja in podajajo detajlna navodila, ki niso zajeta v osnovnem NNP.

- Načrt nujnega odgovora
- Načrt kriznega komuniciranja
- Informacije o rezervni lokaciji IT
- Seznam opreme na rezervni lokaciji.
- Procedure za restavriranje kritičnih podatkov
- Informacije o zavarovanju
- Pogodbe z dobavitelji
- Nastavitve in navodila za uporabo sistemov IT in aplikacij
- Informacije o standardih
- Varnostne procedure in smernice.
- Obrazci
- Reference na poročilo o oceni tveganja
- Reference na poročilo o analizi vpliva na poslovanje
- Reference na poročilo o strategiji
- Distribucijska lista NNP
- Slovar

18. Sklep

Informacijski sistem ima ključno vlogo pri zagotavljanju uspešnega poslovanja podjetja. Izpad ali motnjo v delovanju informacijskega sistema lahko povzroči načrtovana ali nenačrtovana prekinitev. Nenačrtovanih prekinitev je v primerjavi z načrtovanimi veliko manj, so pa zato toliko bolj neprijetne, včasih celo katastrofalne. Iz ankete, ki sem jo opravil med pomembnejšimi slovenskimi podjetji sledi, da se je večina podjetij že srečala z nenačrtovanimi prekinitvami v delovanju informacijskih sistemov, ki so bistveno vplivale na poslovanje podjetja. Stroški, s katerimi se srečujejo podjetja zaradi nedelovanja informacijskega sistema in posledično okrnjenega poslovanja, so tako neposredne, kot tudi posredne narave. Težje merljivi so posredni stroški. Njihove posledice so dolgotrajnejše in pogosto jih je zelo težko v celoti odpraviti.
Razlogov za izgradnjo visoko razpoložljivega informacijskega sistema je več. Najbolj učinkovit vzvod je zakonodaja. Banka Slovenije predpisuje slovenskim bankam, hranilnicam in zavarovalnicam uporabo standarda ISO/IEC 17799, ki predpisuje izgradnjo visoko razpoložljivega informacijskega sistema in okrevalnega načrta.
Znanih je več vrst načrtov in metodologij za izgradnjo načrtov neprekinjenosti poslovanja, vsem pa je skupno, da so usklajeni s priporočili, standardi in kontrolnimi ogrodji kot so Cobit, Itil, ISO/IEC 17799 in NFPA 1600. Pri izgradnji načrta je pomembno, da se podjetje osredotoči na model krovnega načrta neprekinjenega poslovanja, ki lahko kot sestavne dele ali dodatke vsebuje načrte za posamezne sklope. Taka struktura dopušča enostavno nadgrajevanje, je veliko preglednejša in odpravlja probleme, ki se sicer pojavljajo zaradi težav v koordinaciji, podvajanju in prekrivanju funkcij posameznih načrtov.
Obstaja več metodologij, ki opisujejo proces načrtovanja neprekinjenosti poslovanja. Pri izbiri metodologije imajo ključno vlogo potrebe in okolje, v katerem se podjetje nahaja. Največkrat je izbira prepuščena zunanjim svetovalcem, s katerimi podjetje sodeluje.
Proces izdelave načrta neprekinjenega poslovanja najprej oceni tveganja, ki lahko vplivajo na poslovanje podjetja, in omogoči izbiro kontrolnih možnosti za izogibanje in zmanjševanje tveganj. Sledi analiza vpliva na poslovanje, ki se ukvarja s posledicami finančnih in operativnih vplivov nepredvidenih dogodkov na poslovanje podjetja. Analiza vpliva na poslovanje identificira kritična področja in določi okrevalne čase. Za identificirana kritična področja in v skladu s predvidenimi okrevalnimi časi se določi strategija neprekinjenega poslovanja. Izberejo in izvedejo se tehnične rešitve, ki omogočajo visoko razpoložljivost informacijskih sistemov in zagotavljajo dostopnost podatkov v primeru težav. Načrt neprekinjenega poslovanja vsebuje povzetke prvih treh korakov in eksplicitno navaja postopke ravnanja v primeru nesreče. Po končani izvedbi načrta je potrebno izvesti temeljito testiranje, ki pa se ne sme končati z enkratnim testiranjem in potrditvijo. Teste je potrebno načrtovati in jih izvajati redno. Testiranje je vključeno tudi v fazo vzdrževanja, ki predstavlja zadnji korak v procesu neprekinjenega poslovanja.
Poleg klasičnega, t.i. papirnega načrtovanja, obstajajo na tržišču tudi programi, ki lahko postopek načrtovanja in izvedbe precej olajšajo. Njihova pomanjkljivost je visoka cena, manjša prilagodljivost in uporaba tujega jezika.
Iz ugotovitev magistrskega dela izhaja, da ni vprašanje ali se podati na pot visoke razpoložljivosti informacijskih sistemov in neprekinjenosti poslovanja, temveč katero pot izbrati in kako priti do cilja. Večina slovenskih podjetij se zaveda pomembnosti izdelave načrta za neprekinjeno poslovanje, soočajo pa se s kroničnim pomanjkanjem literature, navodil in predvsem izkušenj na področju, ki se pri nas uveljavlja šele v zadnjih nekaj letih. V magistrskem delu sem predstavil različne možnosti in primer izdelave načrta neprekinjenega poslovanja, ki lahko služi kot vzorčni primer podjetjem, ki se podajajo na to pot.

19. Slovar

Annualized impact expectancy (AIE) - pričakovan letni vpliv (PLV)
Annualized loss expectancy (ALE) - pričakovan letni izpad (PLI)
Annualized rate of threat occurrence (ART) - verjetnost letnega pojava grožnje (LPG)
Asset loss potential value (ALPV) - vrednost potencialnega zmanjšanja premoženja (VPZP)
Business continuity management (BCM) – upravljanje neprekinjenega poslovanja (UNP)
Business continuity plan (BCP) – načrt neprekinjenega poslovanja (NNP)
Business impact analysis (BIA) – analiza vpliva na poslovanje (AVP)
Business recovery – okrevanje poslovanja
Business resumption – nadaljevanje poslovanja
Business unit resumption plan – načrt nadaljevanja dela poslovnih enot
Cluster – gruča
Continuity of operations plan (COOP) – načrt neprekinjenosti operacij
Continuity of support plan – načrt neprekinjene podpore
Crisis communication plan - načrt kriznega komuniciranja
Crisis management plan – načrt kriznega upravljanja
Cyber incident response plan - načrt odgovorov na mrežne napade
Disaster recovery (DR) – okrevanje po nesreči
Disaster recovery plan (DRP) – okrevalni načrt
Disk mirroring - zrcaljenje diskov
Disk shadowing - senčenje diskov
Emergency response plan – načrt nujnega odgovora
Expected Availability Time (EAT) – pričakovani razpoložljivi čas (PRČ)
Exposure factor (EF) – faktor izpostavljenosti (FI)
Global cluster – globalna gruča
Information Technology (IT) – informacijska tehnologija (IT)
Interim plan – začasen načrt
IT contingency planning – načrtovanje naključij IT
Management – upravljanje
Maximum tolerable downtime (MTD) – največji sprejemljiv čas prekinitve (NSČP)
Occupant emergency plan – načrt zavarovanja lastništva
Recovery point objective (RPO) – objektivna točka okrevanja (OTO)
Recovery time objective (RTO) – objektiven čas okrevanja (OČO)
Risk assesment – ocena tveganja
Single impact expectancy (SIE) - pričakovani enkratni vpliv (PEV)
Single loss expectancy (SLE) - pričakovani enkratni izpad (PEI)
Work recovery time (WRT) – delovni čas okrevanja (DČO)

20. Literatura

1. Adney William M.: Professional's Guide to the Contents of a Business Continuity Plan, Grand Prairie. Infosolutions. 2002. 35 str.
2. Ahrens Sean A. et al.: Business Continuity Guideline. Alexandria : ASIS International, 2005. 44 str.
3. Allemon Stephan et al.: CobiT 4.0, Rolling Meadows : IT Governance Institute. 2005. 194 str.
4. Bachra Billie et al.: Veritas Cluster Server 3.5 for Solaris. Mountain View : Veritas Software Corporation, 2003. 330 str.
5. Bakshi Bhaskar Sunil et al.: CISA Review Manual 2006. Rolling Meadows : Information Systems Audit and Control Association, 2006. 586 str.
6. Baschab John, Piot Jon: Executive's Guide to Information Technology. Hoboken : John Wiley & Sons, 2003. 498 str.
7. Beser Eric: A Guide to the Perplexed Business Owner, Helping your business survive the unexpected shutdown. B.k. : Ennovate, 2002. 113 str.
8. Brooks Charlote et al.: Disaster Recovery Strategies with Tivoli Storage Management. New York : IBM, 2002. 404 str.
9. Business Continuity Management 2005. London : Chartered Management Institute, 2005. 8 str.
10. Business Continuity Planning Guide. B.k. : PACE, 1998. 245 str.
11. Business Continuity Planning. B.k. : Federal Financial Institutions Examination Council, 2003. 58 str.
12. Developing a Business Continuity Plan. B.k. : Hewlett Packard, 2003. 20 str.
13. Fulmer Kenneth L.: Business Continuity Planning. Brookfield : Rothstein Associates Inc., 2000. 134 str.
14. Gallagher Michael: Business Continuity Management. London : Prentice Hall, 2003. 150 str.
15. Guldentops Erik et al.: Aligning CobiT, ITIL and ISO 17799 for Business Benefit. B.k.: IT Governance Institute, 2005. 62 str.
16. Hiatt Charlotte J.: A Primer for Disaster Recovery Planning in an IT Environment. London : Idea Group Publishing, 2000. 276 str.
17. Hiles Andrew: Enterprise Risk Assessment and Business Impact Analysis. Brookfield : Rothstein Associates, 2002. 286 str.
18. Hines Annlee A.: Planning for Survivable Networks. Indianapolis : Wiley Publishing, 2002. 217 str.
19. Hoekstra Angeli, Conradie Nicolette: CobiT, ITIL and ISO17799: How to use them in conjunction. B.k. : Price Waterhouse Coopers, 2002. 27 str.
20. Information technology — Security techniques — Code of practice for information security management. International Organization for Standardization & International Electrotechnical Commission. Geneva, 2005. 115 str.
21. Jamar Phyllis et al.: Business Continuity Planning Guidelines. Austin : Texas Department of Information Resources, 2004. 136 str.
22. Jolly Adam: Secure Online Business. London : Kogan Page, 2003. 210 str.
23. Khosrow Pour Mehdi: Encyclopedia of Information Science and Technology. Hershey: Idea Group, 2005. 3121 str.
24. Maiwald Eric, Sieglein William: Security Planning & Disaster Recovery. Berkeley : McGraw-Hill/Osborne, 2002. 237 str.
25. Marcus Evan, Stern Hal: Blueprints for High Availability. Indianapolis : Wiley Publishing, 2003. 587 str.

26. Moskal Edward: Business Continuity Management [URL: http://www.drj.com/articles/spr06/1902-10.html], Disaster Recovery Journal, 15.9.2006
27. Musaji Yusufali F.: Auditing and Security: AS/400, NT, Unix, Networks, and Disaster Recovery Plans. New York : John Wiley & Sons, 2001. 530 str.
28. NFPA 1600 Standard. Quincy : National Fire Protection Association, 2004. 40 str.
29. Noakes Fry Kristen, Diamond Trude: Business Continuity Planning Software. B.k.: Gartner, 2003. 19 str.
30. Professional Practices for Business Continuity Planners. Falls Church : DRI International, 2003. 32 str.
31. Pušnik Matjaž, Krajnc Tomaž: Uporaba ITIL v IT organizaciji. Zbornik posvetovanja. Dnevi slovenske informatike : Slovensko društvo Informatika, 2005. str. 271-279.
32. Rudd Colin: Introductory Overview of ITIL, Reading : itSMF. 2004. 40 str.
33. Shapiro Jeffrey R., Policht Marcin: Building High Availability Windows Server 2003 Solutions. Hagerstown : Addison Wesley Professional, 2004. 504 str.
34. Sollicito Johnston Michelle: Corporate Governance, Business Continuity Planning and Disaster Recovery. [URL: http://www.ciscopress.com/articles/article.asp?p=427373&seqNum=1&rl=1], 1.12.2005.
35. Swanson Marianne et al.: Contingency Planning Guide for Information Technology Systems. Washington : NIST, 2002. 107 str.
36. Syed Akhtar, Syed Afsar: Business Continuity Planning Methodology. Mississauga : Sentryx, 2004. 307 str.
37. Toigo Jon W.: Disaster Recovery Planning. New York : John Wiley & Sons, 1996. 329 str.
38. Troppens Ulf, Erkens Rainer, Müller Wolfgang: Storage Networks Explained. Chichester : John Wiley & Sons, 2004. 400 str.
39. Vargas Enrique: High Availability Fundamentals. Palo Alto : Sun Microsystems, 2000. 17 str.
40. Wallace Michael, Webber Lawrence: The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets. New York : Amacom, 2004. 416 str.
41. Williamson John: Business Continuity Planning. B.k. : The AnyKeyNow Group, 2002. 28 str.
42. Wright Anne et al.: Good Practice Guidelines. B.k. : Business Continuity Institute, 2005. 75 str.

21. Viri

1. BCP Software. [URL: http://www.strohlsystems.com/Software/default.asp], Strohl Systems, 19.7.2006
2. BIS. [URL: http://www.bis.org/publ/joint17.htm] , Bank for International Settlements, 10.9.2006
3. Business Continuity. [URL: http://www.availability.sungard.com/Products+and+Services/ Business+Continuity], SunGard, 19.7.2006
4. Business Protector. [URL: http://www.businessprotection.com/software.html], Business Protection Systems International, 19.7.2006
5. Civil Contingencies Bill. [URL: http://www.ukresilience.info/ccbill/index.htm], UK Resilience, 21.4.2006

6. COBIT. [URL: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981], ISACA, 15.9.2006
7. CPACS Software Products. [URL: http://www.cpacsweb.com/products.html], CPACS, 19.7.2006
8. DRJ's Sample DR PLans and Outlines. [URL: http://www.drj.com/new2dr/samples.htm], Disaster Recovery Journal, 13.7.2006
9. EFA. [URL: http://www.strohlsystems.com/Education/Regulations/MoreInfo.asp?ID=11], Strohl Systems, 20.9.2006
10. Interna gradiva podjetja Hewlett Packard
11. Interna gradiva podjetja Hitachi Data Systems
12. Interna gradiva podjetja S&T Hermes Plus
13. Interna gradiva podjetja Sun Microsystems
14. Interna gradiva podjetja Veritas Software
15. Knowledge Leader. [URL: http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/BusinessContinuityManagementTheRelationshipBetweenBCMandSarbanes-Oxley!OpenDocument], Protiviti, 10.9.2006
16. NFPA 1600. [URL: http://www.davislogic.com/NFPA1600.htm], Davis Logic, 25.8.2006
17. OSH. [URL: http://www.osha.gov/pls/oshaweb/owasrch.search_form?p_doc_type=OSHACT], U.S. Department of Labor, 12.9.2006
18. Sklep o določitvi pogojev, ki jih mora izpolnjevati banka oziroma hranilnica za opravljanje bančnih oziroma drugih finančnih storitev (Uradni list RS, št. 38/06).