

(ЛОГО-ФИРМА)	ПРОЦЕДУРА-ПОЛИТКА-ПЛАН	(НУМЕРАЦИЈА)
Класиф.(ограничено...)		Верзија

ОКВИР ПЛАНА КОНТИНУИТЕТА ПОСЛОВАЊА ЗА ЦЕРТ ПЛАТФОРМУ

	Назив/име	позиција	датум
Усвојио
Одобрио
Направио
Власник/одговоран	<i>(Одељење)</i>		
Важи од			...
Примењује се на	...		

ИСТОРИЈА ДОКУМЕНТА

ВЕРЗИЈА	ДАТУМ	АУТОР	ОПИС	

САДРЖАЈ

1	ПРЕГЛЕД	4
1.1	Увод.....	4
1.2	Циљ	4
1.3	Опсег	4
2	ПЛАН ЗА КОНТИНУИТЕТ ПОСЛОВАЊА	5
2.1	Преглед.....	5
2.2	Пријављивање прекида сервиса	5
2.2.1	Пријављивање недоступности људства	5
2.2.2	Пријављивање прекида у сервисима	5
2.3	Процена ситуације-прекида	6
2.3.1	Сазивање тима за процену ситуације	6
2.3.2	Процена недоступности људства	6
2.3.3	Процена недоступности сервиса.....	7
2.3.4	Преглед утицаја-последица прекида сервиса	8
2.3.5	Комуницирање одлуке након процене	9
2.4	Одзив за проглашење Катастрофе	10
2.4.1	Одзив на проглашење Катастрофе за људство	10
2.4.2	Одзив на проглашење Катастрофе за техничке сервисе.....	10
2.5	Преглед одзива	12
2.5.1	Спровођење прегледа након догађаја	12
2.5.2	Ажурирање планова континуитета и техничких планова за опоравак.....	12
2.6	Улоге и одговорности	12
3	ПОВРАТАК НА ПРИМАРНУ ЛОКАЦИЈУ	14
3.1	Процена потребе транзиције (повратка) на примарну локацију	14
3.2	Покретање транзиције натраг на примарну локацију	14
3.3	Праћење транзиције.....	14
3.4	Завршетак транзиције	14
4	ОДРЖАВАЊЕ ПЛАНА ЗА КОНТИНУИТЕТ ПОСЛОВАЊА И ТЕХНИЧКИХ ПЛАНОВА ОПОРАВКА	15
4.1	Управљање Планом континуитета пословања	15
4.1.1	Преглед и ажурирање Плана континуитета пословања	15
4.1.2	Тестни сценарији	15
4.2	Управљање техничким плановима	16
4.2.1	Период прегледа	16
4.2.2	Идентификовање RTO i RPO.....	16

4.2.3	Идентификовање кључних контаката.....	16
4.2.4	Спровођење прегледа и постављања приоритета пословних процеса и сервиса (функција) 16	
4.2.5	Документовање техничког опоравка.....	16
4.2.6	Валидација техничког опоравка.....	17
4.2.7	Повратак на примарну локацију	17
4.2.8	Историја резултата годишњег тестирања.....	17
5	ТЕСТИРАЊЕ ПЛАНА КОНТИНУИТЕТА ПОСЛОВАЊА.....	18
6	ПРИЛОГ 1 : ДЕФИНИЦИЈЕ	19
7	ПРИЛОГ 2 : КОНТАКТ ЛИСТА.....	20
8	ПРИЛОГ 3 : ЛИСТА ЗА ПОМОЋ У ПРОЦЕНИ	21

1 ПРЕГЛЕД

1.1 Увод

Овај План треба да омогући континуитет сервиса у случају значајног прекида рада. План описује приступ процени прекида, планирања опоравка од прекида, и сталног праћења опоравка.

Процеси описани у овом документу развијени су да умање последице и поставе основу за наставак рада и опоравак од непланираних прекида пословних функција. План за обезбеђивање континуитета пословања (ВСП) користи се као подршка процесу одлучивања у случају неког прекида који може ескалирати од нивоа Проблема до проглашавања Катастрофе.

1.2 Циљ

Циљ ВСП за ЦЕРТ платформу је да:

- документује како ЦЕРТ институција треба да процењује прекид рада ЦЕРТ платформе укљ. и разумевање опсега и последица;
- опише како тим треба да реагује на проглашавање Катастрофе укљ. и планирање и постављање приоритета активности опоравка;
- обезбеди процес за процену одзива тима након Катастрофалног догађаја;
- пружи одреднице техничким тимовима за опоравак шта би требало да укључе технички планови;
- пружи одреднице тиму за Управљање инцидентима како да приступе опоравку уколико је тим угрожен директно (пандемија или катастрофални догађај) или индиректно (губитак конективности).

1.3 Опсег

Опсег Плана је фокусиран на континуитет техничке и пословне оперативности ЦЕРТ сервиса

Документ се не бави континуитетом платформи које су у власништву институција изван ЦЕРТ-а над којима су сервиси надграђени. План континуитета ових платформи и инфраструктурних сервиса је одговорност њихових техничких и пословних тимова. За утврђене међузависности, ЦЕРТ тим ће радити са тим тимовима уколико је неопходно у циљу што бржег опоравка ових сервиса.

Опсег овог плана јесте само континуитет пословања и планирање активности опоравка на вишем нивоу. За сваки појединачни сервис одн. функцију очекује се да постоји припремљен додатни документ „Технички или опоравак од катастрофалних догађаја“ и који је власништво сваког појединачног сервиса одн. функције.

2 ПЛАН ЗА КОНТИНУИТЕТ ПОСЛОВАЊА

2.1 Преглед

ВСП за ЦЕРТ платформу дефинише оквир и основне процесе за процену последица и одзива на прекид пословне оперативности.

Веома је битно прво сагледати и разумети како поступити када се открије или је пријављен прекид. Након разумевања опсега прекида, морају се донети одлуке о даљим корацима. За све пријављене прекиде потребан је план за преглед активности одзива како би се обезбедио напредак процеса.

2.2 Пријављивање прекида сервиса

Одмах по препознавању прекида сервиса, та особа мора то пројавити руководству коришћењем најпримеренијег метода за конкретну ситуацију.

- за мање озбиљне прекиде – е-пошта, евентуално интерни chat;
- за озбиљне прекиде – телефон, евентуално интерни *chat*.

Листа особа којима се пријављује и *chat* група налазе се у прилозима документа.

2.2.1 Пријављивање недоступности људства

Значајна недоступност људства треба да буде пријављена одмах Координатору за континуитет пословања и руководству ЦЕРТ-а.

Уколико је доступна било информација о прекидима и недоступности, озбиљности последица на људство које је укључено у конкретну ситуацију и потенцијалне последице на пословну оперативност исту треба укључити у ову комуникацију.

2.2.2 Пријављивање прекида у сервисима

Уколико се деси технички прекид, особа која препозна овакву ситуацију треба без одлагања да:

Пријави прекид тиму надлежном за сервис претходно договореним методом

Контактира вођу тима за Управљање инцидентима или надлежну особу за сервис

Надлежна особа за сервис ће извршити прелиминарну процену пријављеног прекида и одлучити о потреби за даљу ескалацију. Иницијална процена треба да садржи следеће информације:

Утицај на конституенте (ев. листу погођених конституената)

- која је локација погођена;
- платформа која је погођена ;
- датум и време уочавања одн. пријаве прекида;
- први утисак о прекиду и потенцијалним последицама;
- предузете активности до тог тренутка.

Уколико се ова ситуација ескалира, контактира се Координатор за континуитет пословања. Координатор тада иницира ВСП процес.

2.3 Процена ситуације-прекида

Током ове фазе, врши се процена прекида како би се одредиле и категорисале последице. Последице могу бити екстремне у случају неких природних катастрофа (пандемија, земљотрес, поплаве, урагански ветар, ...), али могу се појавити и због других догађаја као што су незгоде (губитак везе са Интернетом, квар, људска грешка, пуцање цеви, ... и др. непредвиђене ситуације) и малициозна дела (безбедносни пробој, паљевине, терористички напад итд.).

Листа за помоћ у процени дата је у **Прилогу 3**. Координатор ВСП за ЦЕРТ платформу користиће ову листу како би се обезбедило да се ВСП процес прати и документује.

Намера процене и категорисања обима прекида јесте да се одреди како ЦЕРТ треба да реагује.

- уколико је процена да су последице прекида ниске (отказ који траје мање од 4 сата), Управа може одлучити да прође узрок и прихвати друге потенцијалне последице (неиспуњавање обавезе извештавања, трошкови или др. због неиспуњавања договореног нивоа сервиса – SLA);
- уколико је процена да су последице веће и да прекид може трајати дуже, Управа ће одлучити о томе да ли је неопходно прогласити „катастрофалну ситуацију“.

Сви ови фактори морају се посматрати у светлу процењених трошкова и времена у случају проглашавања Катастрофе и одлуке да се пређе на другу локацију.

За потребе овог плана, Катастрофа се дефинише као тачка у којој губитак система или ресурса који подржавају апликације и пословне процесе постаје критичан по континуитет оперативности ЦЕРТ платформе.

2.3.1 Сазивање тима за процену ситуације

Тим за процену прекида критичан је за даље разумевање последица прекида пословних сервиса.

Тим треба да сачињавају следећи представници:

- координатор ВСП за ЦЕРТ платформу;
- представници погођеног сервиса;
- представници сектора за безбедност;
- представници пружаоца услуга за платформу над којом је надграђен сервис (ако је применљиво).

Тим за процену ситуације са свим кључним контакт детаљима наведен је Прилогу 2.

2.3.2 Процена недоступности људства

Наредна табела даје узорак разлога недоступности људства.

Догађај	Препоручени одзив
Губитак конективности на примарној локацији	Упутити људство на рад од куће
Пандемија која утиче на могућност тима за управљање инцидентима да раде са примарне локације	Тражити да људство ради од куће
Пандемија која директно утиче на тим за управљање инцидентима због недостатка неопходних људи	Периодично проверавати стање и доступност људства Ре-алоцирати људство из других тимова или са других локација како би се привремено превазишао проблем.

2.3.3 Процена недоступности сервиса

Детаљна процена се довршава. Процена садржи детаљне информације од људи са терена.

Управа ЦЕРТ-а мора сагледати и разумети последице прекида прегледањем добијених детаљних информација . Тим за процену сазива се и биће одговоран за ову процену. Чланови тима се узимају из сектора за безбедност, управљања инцидентима и тимова који су погођени прекидом. Тим за процену ће:

- довршити иницијалну процену последица;
- идентификовати ниво прекида и сервисе одн. конституенте на које ово утиче;
- радити са одговарајућим ресурсима из тимова за управљање data центром и платформама како ни се проценили утицаји и последице;
- проценити време потребно за опоравак основне инфраструктуре, платформи од којих постоји зависност, сервиса и др. повезаних области;
- идентификовати алтернативна решења;
- дати препоруке.

Обично недоступност људства не утиче директно на доступност пословних сервиса. Људство је критично да би се осигурала континуална доступност и стабилност пословних сервиса.

Тим за процену ће доделити ниво озбиљности на основу своје процене. Иницијална процена мора бити завршена и прегледана од стране одговарајућег руководства у року од 1-2 сата од пријаве.

Прекид једног сервиса потенцијално може утицати на стабилност ЦЕРТ платформе за коју је дефинисан циљани ниво доступности од 99.95%. Критично је а процена буде завршена што је пре могуће како би други тимови могли што пре кренути са својим активностима у случају проглашења Катастрофе.

Ниво озбиљности	Опис
НИЗАК (очекиван мање утицај одн. последице)	Очекивани прекид < 4 сата Потребне неке измене у раду одн. распоређивању послова. Нема или је потребна врло мала мобилизација из домена који се односи на опоравак од катастрофалних догађаја.

<p>УМЕРЕН (очекиван умерен утицај одн. последице)</p>	<p>Озбиљан проблем и опоравак пословних функција и/или ИКТ сервиса може потрајати > <u>4 сата</u>; може бити потребе за имплементацијом на локацијама за опоравак.</p> <p>Потребне су измене у раду раду одн. распоређивању пословакак оби се обезбедило да приоритетне пословне функције и апликације могу прорадити што је пре могуће. Може бити потребе за делимичном или потпуном мобилизацијом одговарајућих ресурса (тим за управљање инфраструктуром и локацијама).</p> <p>Зависно од опсега штете, изводе се активности опоравка за неке од система и продукционих апликација. Већина пословних функција и/или сервиса радиће уобичајено након опоравка.</p>
<p>ВИСОК (потпуни прекид)</p>	<p>Проблем је озбиљан, опоравак пословних функција и/или ИКТ сервиса може потрајати и више од <u>24 сата</u> и спровешће се на алтернативној локацији (за опоравак) – према дефинисаном распореду приоритизације за сваки сервис кроз дефинисане планове за опоравак од катастрофалних ситуација</p> <p>Потребна је потпуна мобилизација ресурса за опоравак. Проглашава се катастрофа и све пословне функције, информациони сервис и др. функције за подршку раде у Режиму опоравка.</p>

2.3.4 Преглед утицаја-последича прекида сервиса

Користе се одреднице из претходне табеле и Упутства за процену утицаја (из прилога) како би управа одредила ниво озбиљности и применила адекватне планове.

Доношење одлуке о проглашењу Катастрофе није неопходно ако Тим за процену сматра да опоравак од прекида неће трајати дуже од 48 сати.

За озбиљније прекиде – очекивано преко 48 сати – акција која ће се применити у случају прекида пословне оперативности мора примарно бити базирана на процени процењеног трајања прекида у односу на дефинисани RTO (*Recovery Time Objective*).

- уколико је разлика у времену између RTO и очекиваног времена оправка већа од 48 сати, проглашава се Катастрофа и обавештавају се технички тимови за опоравак да започну са својим активностима опоравка на алтернативној локацији;
- уколико је разлика у времену између RTO и очекиваног времена оправка између 24 сата и 48 сати, Тима за управљање континуитетом пословања може одлучити да ли ће чекати разрешење прекида или прогласити Катастрофу;

- уколико је одлука да се сачека разрешење прекида а прекид се настави и наон дозвољеног периода, управа одлучује о томе да ли ће бити проглашена Катастрофа;
- тим за процену прати актуелну ситуацију, имајући у виду да иста може ескалирати до вишег нивоа озбиљности.

Одобрење управе ЦЕРТ-а не неопходно за проглашавање Катастрофе, у случају да :

- погођени су сви пословни процеси и/или апликације (било да није могуће испунити предвиђени ниво сервиса или неки системи повремено нису доступни);
- тим за процену сматра да је прекид ширег размера и да неће бити могуће враћање на „нормално“ стање на примарној локацији унутар дефинисаног RTO периода;
- штета је толика да је јасно да није потребна непосредна процена;
- неопходно људство из Тима за управљање инцидентима није више доступно.

По проглашавању Катастрофе, управа ће:

- ауторизовати процес опоравка од катастрофа;
- покренути план комуникације – интерни, за конституенте и за јавност.

2.3.5 Комуницирање одлуке након процене

Без обзира на проглашавање Катастрофе или не, вероватно је да ће особе задужене за комуникацију са конституентима и корисничка подршка бити оптерећени додатним упитима због проблема у коришћењу сервиса.

Да би се осигурао координирани приступ, потребно је извршити следеће кораке.

- координатор за комуникацију координира и управља комуникацију ка конституентима, интерним и екстерним тимовима, другим релевантним институцијама;
- координатор за комуникацију саопштава погођеним тимовима стање и активности које треба да предузму;
- координатор за комуникацију саопштава конституентима стање погођених сервиса и да ли је проглашена Катастрофа
 - саопштава конституентима актуелно стање;
 - наговештава када ће уследити наредна комуникација;
 - појашњава и даје више детаља о прекидима пословне оперативности;
 - појашњава који су наредни кораци.

Контакт информације тима за Континуитет пословања и др. неопходни контакти објављени су на безбедној локацији тако да информације које нису јавне не би доспеле у јавност. У оквирима сваког од сервиса наведена је техничка документација потребна за опоравак и листа надлежних контаката (укљ. и управу) који треба да буду обавештени о проглашењу катастрофе.

2.4 Одзив за проглашење Катастрофе

2.4.1 Одзив на проглашење Катастрофе за људство

Управа мора да одреди како најбоље одговорити на ситуације које се односе на људство у Тиму за управљање инцидентима. Минимално, потребно је контактирати:

- Кадровску службу
- Управу РАТЕЛ
- Руководство ЦЕРТ
- Надлежно министарство

Како би се ублажиле потенцијалне последице недоступности људства, могуће је:

- тражити од расположивог људства да преузме додатне обавезе и задатке на себе
- прераспоредити део људства из других сервиса да „ускоче“
- тражити друге техничке ресурсе који би помогли по потреби

Одлука треба јасно да буде комуницирана свим укљученим странама – директно или индиректно.

2.4.2 Одзив на проглашење Катастрофе за техничке сервисе

Именује се Тим за одзив који ће одредити како је најбоље реаговати на проглашење катастрофе. Чланови Тима за одзив су:

- координатор континуитета пословања;
- додељена особа из управе;
- координатор за комуникацију;
- представници погођених сервиса.

Тим за одзив прво одређује какве и које акције ће се применити. Развија се план који се комуницира како унутар институције тако и (главним) конституентима преко Координатора за комуникацију. Тим је такође одговоран за праћење статуса техничког опоравка.

2.4.2.1 Планирање и постављање приоритета

Тим прво утврђује који сервиси су погођени. Информације које су потребне Тиму за опоравак су:

- која је локација погођена;
- који сервиси су погођени;
- да ли постоје нека регулаторна ограничења и захтеви која се односе на опоравак сервиса.

Са овим прикупљеним информацијама, Тим за одзив припрема план приоритета опоравка сервиса. Тим за одзив мора да разуме основну архитектуру погођених сервиса и препозна да ли постоји нека дељена одн. заједничка платформа или инфраструктура која је потребна пре него се опорављају појединачни сервиси. План треба да узме у обзир напоре и време потребно за опоравак различитих окружења.

Фокус је на опоравку инстанци сервиса које користе спољашњи корисници. Уколико је примарни *data* центар значајно погођен, потребно је размотрити и опоравак не-продукционих инстанци. Одлука о овоме се одлаже док се не заврши опоравак свих продукционих инстанци.

По завршетку припреме плана опоравка, исти се прегледа и одобрава од стране управе.

2.4.2.2 Комуникација

Уз одобрени план опоравка, извршава се и план за комуникацију са конституентима, другим релевантним институцијама и са управом. Координатор комуникације прикупља информације како би се омогућила адекватна комуникација узевши у обзир и:

- потребне капацитете за hardware (сервери, storage, мрежни уређаји) и пропусни опсег за сваки *data* центар;
- процењено време опоравка – за конституенте и за тимове за подршку одн. оне који комуницирају са екст. странама;
- план опоравка за погођене тимове;
- план опоравка за Управу.

2.4.2.3 Технички опоравак

По проглашавању катастрофе, план опоравка се комуницира сваком техничком тиму за опоравак. Ови тимови – који су одговорни за технички опоравак – идентификовани су при техничкој документацији за сваки појединачни сервис.

Листа за проверу опоравка припрема се за сваки од сервиса и прати током процеса опоравка. Измене се уносе у документацију и стално комуницирају управи и координатору за континуитет.

Уколико постоји заједнички одн. дељени сервиси, исти се морају узети у обзир и њихов распоредити тако да претходи другим појединачним сервисима.

По техничком опоравку сваког од сервиса ЦЕРТ платформе, изводи се основна провера функционалне исправности. Ажурне информације о успешном опоравку сваког од сервиса се комуницирају Тиму за континуитет.

Сви технички тимови остају на својим местима док се стање комуницира са конституентима и др. екст. корисницима и почињу да користе ове сервисе.

2.4.2.4 Завршетак

Како се закључује прекид оперативности, постоји више активности које треба спровести.

Одговорни тим:

- комуницира стање опоравка конституентима;
- спроводи анализу узрока прекида и комуницира резултате одговарајућим тимовима (који су били погођени, руководству, итд.);
- комуницира са тимовима интерних сервиса и сервиса за подршку о стању опоравка;
- комуницира са управом о статусу опоравка укљ. и параметре о броју погођених сервиса и страна, обавештених институција, итд.

Догађај се затвара и сва документација се одлаже на предвиђену локацију.

2.5 Преглед одзива

По успостављању оперативног стања, цео процес се поновно прегледа и анализира како би се унапредила реакција у будућности. Припрема се документ са формалним налазима (‘lessons learned’) или састанак где се дискутују начини унапређења произашли из ове активности.

2.5.1 Спровођење прегледа након догађаја

Првенствена намера је да се идентификује:

- Шта је био основни узрок прекида?;
- Шта је добро функционисало?;
- Шта је могло бити боље?;
- Шта смо научили? Како можемо унапредити своје сервисе укљ. и упутства, процесе за опоравак итд.?

Фокус је на унапређењу процеса континуитета пословања и техничког опоравка.

Улазни подаци за овај преглед јесу информације прикупљене од тимова који су учествовали у опоравку као и попуњена Листа за помоћ у процени.

По комплетирању извештаја или састанка, предлози за измене се шаљу надлежном руководству.

2.5.2 Ажурирање планова континуитета и техничких планова за опоравак

Све препоручене измене се инкорпорирају и поновно прегледају. По одобрењу промена, нове верзије докумената се објављују и смештају на предвиђеним локацијама.

2.6 Улоге и одговорности

У табели је представљен Тим за опоравак и улоге процесу Континуитета пословања/ Опоравка од катастрофалних ситуација. Само један тим или особа може бити одговорна за одређену област током овог процеса.

Одговорност	Улога	Координатор ВСП	Руководство	Тим по платформи	Тим за упр. Инц.	Data центар (провајдер)	Координатор комуникације
Пријава	прекида	A	I	C	R	C	I
Покретање	ВСП	A	I	I	R	I	I
Процена	прекида	A	I	C	R	C	I
Комуникација катстрофи	о	A	R	C	R	C	I
План и приоритизација опоравка		A		I	I	I	R
План и приоритизација опоравка		A	I	C	R	C	I
Технички опоравак		A	I	C	R	C	I
Праћење техн. опоравка		A	I	I	R	I	
Валидација опоравка	техн.	A	I	C	R	C	

Комуникација о опоравку	A	I	I	I	I	R
Преглед	R	A	C	C	I	I

Легенда:

R – *responsible* = ко извршава

A – *accountable* = ко доноси одлуку

C – *consulted* = ко се консултује пре доношења одлуке или предузимања акције

I – *informed* = ко се обавештава да је одлука донета или активност извршена

3 ПОВРАТАК НА ПРИМАРНУ ЛОКАЦИЈУ

По престанку прекида одн. догађаја који су довели до прекида оперативности на примарној локацији, Тим за континуитет треба да одреди да ли је потребан прелазак на примарну локацију (примарни *data* центар).

3.1 Процена потребе транзиције (повратка) на примарну локацију

Тим за процену се састаје како би проценио потребу за повратком на примарну локацију.

Критеријуми који се користе за процену укључују:

- Близина и доступност платформи и/или инфраструктурних сервиса који су потребни
- Могућа ограничења у домену капацитета на алтернативној локацији
- Захтеви конституената
- Регулаторни и сл. захтеви

Уколико се донесе одлука о повратку, активности треба спровести у координацији са конституентима колико је то могуће. Тимови за технички опоравак се обавештавају када активности могу започети и спроводе све аспекте ових активности.

3.2 Покретање транзиције натраг на примарну локацију

Све релевантне стране се обавештавају о планираној транзицији.

Време се усаглашава и формални захтеви за промене се бележе у систему пре извођења активности.

Технички тимови за опоравак изводе техничке процедуре и валидирају успешност по завршетку.

Све стране које могу бит „погођене“ овим Координатор за комуникацију обавештава о завршетку активности.

3.3 Праћење транзиције

Током процеса повратка (*fallback*), Тим за континуитет прати прогрес и остаје доступан за случај ескалације или појаве других проблема.

3.4 Завршетак транзиције

По завршетку транзиције натраг на примарну локацију сматра се да су активности завршене. Припрема се извештај и дистрибуира надлежном руководству индицирајући да је транзиција покренута и завршена.

4 ОДРЖАВАЊЕ ПЛАНА ЗА КОНТИНУИТЕТ ПОСЛОВАЊА И ТЕХНИЧКИХ ПЛАНОВА ОПОРАВКА

План за континуитет и технички планови се прегледају и поновно процењују на годишњем нивоу. Поред тога, нови сервиси или промене у имплементацији сервиса захтевају да се технички планови прегледају и ажурирају.

4.1 Управљање Планом континуитета пословања

Одржавање Плана је од изузетне важности за валидацију актуелности процедура које руководе процесом опоравка. Све пословне промене морају се размотрити при ажурирању Плана.

4.1.1 Преглед и ажурирање Плана континуитета пословања

План се одржава актуелним и синхронизован са пословним променама. Све пословне промене морају се размотрити при ажурирању Плана.

План за континуитет пословања и планови за опоравак сервиса прегледају се годишње. Циљ је идентификовати и инкорпорирати у пословне функције или процес опоравка промене које су се појавиле од претходног прегледа. Елементи које треба прегледати при разматрању ажурирања плана укључују:

- пословни захтеви и приоритети;
- опсег, претпоставке и промене мисије;
- процедуре тестирања;
- нове безбедносне контроле;
- промене техничких планова;
- процедуре континуитета и опоравка;
- промене у људству.

4.1.2 Тестни сценарији

Као део годишњег тестирања Плана континуитета, треба размотрити и ове сценарије. Чак и у случају да се раде тзв. „папирни“ тестови, битно је проверити какав би могао бити одзив на догађаје који би довели до прекида у пословној оперативности.

	Сценарио	Опис
1	Недоступност главне локације	Није могућ приступ или је локација неупотребљива
2	Недоступност људства	Више од 50% људства је спречено-недоступно
3	Недоступност ИКТ сервиса	Један или више од критичних заједничких сервиса није доступан

4	Регионална катастрофа	Догађај ширих размера који спречава критичном људству приступ радној локацији и критичним ИКТ системима
---	-----------------------	---

4.2 Управљање техничким плановима

Технички планови опоравка праве се за сваки сервис. Оквир се одржава конзистентним за све сервисе. Овде се дају смернице шта треба да буде укључено у сваки технички план опоравка.

4.2.1 Период прегледа

Технички планови се прегледају на годишњем нивоу и ажурирају по потреби.

4.2.2 Идентификовање RTO и RPO

Recovery Time Objective (RTO) дефинише се као циљано време (и ниво сервиса) током којег пословни процес мора бити поново успостављен након катастрофалног догађаја (или прекида) како би се избегле неприхватљиве последице повезане са прекидом континуитета пословања.

Recovery Point Objective (RPO) дефинише се као максимално циљано време за које је могуће изгубити податке за неки ИКТ сервис због неког значајног инцидента.

ЦЕРТ има дефинисане полазне RTO и RPO и сви тимови су у обавези да буду у складу (или бољи) са овим захтевима:

Recovery Time Objective (RTO) = 24 сата

Recovery Point Objective (RPO) = 8 сати

4.2.3 Идентификовање кључних контаката

Идентификовање контаката који треба да буду (или може бити потребно) да се укључе у технички опоравак. Листа треба да буде на локацији која је лако доступна ауторизованим особама.

4.2.4 Спровођење прегледа и постављања приоритета пословних процеса и сервиса (функција)

Тим одговоран за сервис мора прегледати инвентар решења како би разумели који процеси су критични за „опстанак“.

Тим одговоран за сервис мора одредити компоненте које треба одмах опоравити а које могу бити накнадно успостављене по успостављању пословног сервиса.

Тим одговоран за сервис мора документовати редослед опоравка компоненти, одн. које компоненте треба опоравити да би се могло сматрати да је сервис опорављен.

4.2.5 Документовање техничког опоравка

Технички план опоравка састоји се од ових основних одељака:

- опоравак мрежних компоненти;
- идентификовање и опоравак минималних безбедносних захтева

Тим одговоран за сервис идентификује минималне захтеве како би се смањила изложеност. Ово мин. укључује *firewall*-е, конфигурацију мрежних зона и *gateway*-а, проверу усклађености са регулаторним захтевима;

- опоравак основне инфраструктуре

Документ мора да забележи био које конфигурације специфичне за одређени сервис. Тимови надлежни за сервис треба ово да идентификују у својим техничким документима;

- опоравак помоћних компоненти

У овом одељку налазе се детаљи везани за додатне мрежне компоненте, *backup* итд.

Како неке од помоћних компоненти нису захтеване за иницијални опоравак технички планови документују које су компоненте неопходне а за које опоравак може бити одложен (и колико дуго), као и које компоненте уопште не морају бити обновљене;

- опоравак основних (кључних) апликација

Опоравак апликација тежи да тесно прати иницијалну поставку сервиса и како се уобичајено апликације и сервери инсталирају.

У техничком плану за сваки сервис документовани су сви кораци потребни за опоравак апликација укљ. и податке и конфигурацију апликација;

- имплементација специфичних екстензија или интеграција

Како неки сервиси могу укључивати и коришћење специфичних, то је и један од последњих корака у процесу техничког опоравка. Имплементација и валидација ових екстензија може захтевати додатно укључивање додатних специфичних тимова за њихову имплементацију и подешавање.

Технички документ садржи и листу за проверу која се може користи за проверу да ли су сви потребни кораци извршени правилни редоследом. Листа садржи имена и улоге неопходне за комплетирање тих задатака.

4.2.6 Валидација техничког опоравка

По успешном опоравку, основни тестови валидације се извршавају на сервисима пре комуницирања о статусу опоравка. Ови основни тестови обично се користе за проверу и демонстрацију могућности приступа апликацији, уласка у апликацију уз додатне специфичне тестове који потврђују да је окружење функционално и спремно за употребу.

4.2.7 Повратак на примарну локацију

По разрешењу проблема који су узроковали прелазак, може бити неопходно урадити транзицију натраг на примарну локацију. Уколико се транзиција разликује на неки начин од техничких планова опоравка, ове разлике треба нагласити у техничким документима за опоравак или документима за опоравак од катастрофа (DR).

4.2.8 Историја резултата годишњег тестирања

Налази и резултати годишњих DR тестова треба да се чувају мин. 3 год.

5 ТЕСТИРАЊЕ ПЛАНА КОНТИНУИТЕТА ПОСЛОВАЊА

План континуитета - који се односи на мин. један сервис – мора се тестирати бар једанпут годишње. Додатно, годишње за сваки сервис треба тестирати технички план опоравка. Координатор континуитета мора бити укључен у било које тестирање.

За сваки тест који се спроводи (BCP, технички DR план) мора бити припремљена и објављена листа која садржи опсег; резултати морају бити доступни.

Сваки план тестирања мора да садржи:

1. Циљеви тестирања:
 - листа примарних циљева вежбе и очекиваних резултата;
 - листа секундарних циљева вежбе и очекиваних резултата;
 - постављено временско ограничење за постизање циљева.
2. Параметри тестирања:
 - учесници;
 - план обавештавања;
 - системи и подаци које треба опоравити;
 - мрежна конфигурација;
 - учешће корисника;
 - пословне функције које треба опоравити.
3. Вредности који се прате:
 - забележени почетак и завршетак вежбе и задатака;
 - документовање проблема на које се наишло;
 - одступања од плана тестирања.
4. Преглед по завршетку :
 - Да ли су параметри коректни?;
 - Да ли су постигнути циљеви?;
 - Да ли су критеријуми мерења коректни?;
 - идентификоване проблематичне области, добре стране, одступања од плана;
 - препоруке за унапређење.

Детаљни Извештај са тестирања сматра се поверљивим.

6 ПРИЛОГ 1 : ДЕФИНИЦИЈЕ

- BCP, Business Continuity Plan
- DR, Disaster Recovery Plan
- **критични сервиси** – сервиси означени првим приоритетом у Анализи утицаја на пословање (*Business Impact Analysis, BIA*).

...

7 ПРИЛОГ 2 : КОНТАКТ ЛИСТА

Тим за процену

Тим за опоравак 1

Тим за опоравак 2

...

Координатор Континуитета

Координатор Опоравка

Координатор Комуникације

...

8 ПРИЛОГ 3 : ЛИСТА ЗА ПОМОЋ У ПРОЦЕНИ

...

...

...