# Развој на континуитетот во работењето во секторот на информатичко-комуникациските технологии (ИКТ) во судството

(Името на овој документ е: „*Развој на континуитетот во работењето во ИКТ_КОНЕЧНА_2020*“, користениот фонт на текст е Arial 11, единечен проред, 6 pt пред и потоа)

*Миодраг Перишиќ, MSEE, ИКТ експерт, проект „Поддршка на реформите во правосудниот сектор“*

јуни 2020 г.

**Финансирано од Европската Унија**

Владимир Полежиновски, 22/12, Скопје,
Република Северна Македонија
Тим лидер д-рДевил: +389 (0) 70 22 40 44
Е-пошта: deville@planet.gr

Проектот го реализира NIRAS и партнерот воконзорциумот Planet

# Table of Contents

**Кратенки:**

| | |
|---|---|
| ИКТ | Информатичко-комуникациска технологија |
| ЈО | Јавно обвинителство |
| ITIL | поранешен акроним за Библиотека на информатичко-технолошката инфраструктура, претставува збир од детални практики за управување со ИКТ услугите (ITSM) чиј фокус е усогласување на ИКТ услугите со потребите на деловното работење. |
| АКМИС | Автоматизиран Систем за управување со судски предмети, кој се спроведува во сите судови во Северна Македонија |
| HW | Хардвер на компјутерски системи, опрема што се користи за вршење ИТ активности |
| SW | Софтвер на компјутерски системи, програми, апликации и разни програмски алатки, кои работат на хардвер |
| ИСУКПИ | Интегриран систем за управување со казнено поправните институции, кој се користи во сите истражни затвори и затвори во државата. |
| Служба за корисничка поддршка | систем што им помага на корисниците на компјутерските системи и на ИКТ персоналот |
| ДИТ | Директор за информатички технологии, висока раководна позиција во една организација, одговорна за сите информатички услуги, складирање и безбедност |
| Структура за одговорност „матрица“ | структура за одговорност во една организација, каде одредени лица имаат повеќе од едно претпоставено лице пред кое се одговорни |
| Процес на обновување | процес на периодично заменување на ИКТ опремата, каде секоја година фиксен процент на HW се заменува со нов, обично 20-25% |
| Сервер | хардверски уред, со процесор, меморија и складиште, кој се користи за разни функции за компјутерска обработка, а се чува на полици со многу поврзани сервери во нив |

## Извршно резиме

Овој документ, откако ќе се изготви, треба да стане дел од збирот различни документи, предлози и рамки, изготвени како резултати на спецификацијата на бараните услуги во рамките на проектната задача (ToR), за компонентата 3 (ИКТ) од проектот „Поддршка на реформите во правосудниот сектор“

*Документот првично беше изготвен од страна на проектниот консултант, ИКТ експертот, по што беше споделен со голем број лица од ИКТ секторот низ целата земја, истакнати членови на ИКТ заедницата и во судовите и во обвинителствата, кои дадоа дополнителни, конкретни коментари и детали, со цел да биде целосно применлив и во согласност со моменталната состојба во овие организации и нивните идни потреби и можните насоки поврзани со ИКТ.*

*Покрај ова, во документот беа земени предвид и претходно изразените мислења и предлози, документирани во извештајот за обуката „Отворен простор“, која се одржа во Скопје, кон крајот на јануари 2020 година, а вклучуваше над 20 избрани ИКТ-професионалци од различни судови и обвинителства во Северна Македонија (повеќе детали во продолжение)*

Овој документ претставува предлог за спроведувањето на Планот за континуитет во работењето во рамките на секторот на информатичко-комуникациските технологии во судството на Северна Македонија, прилагоден на специфичната состојба во правосудните институции во Северна Македонија, како што се судовите и обвинителствата.Онаму каде што е можно или применливо, се вметнуваат кратки белешки, со конкретни коментари за состојбата во овие институции.

На крајот, ќе биде предложен конкретен пакет мерки што треба да се преземат во правосудните организации во Северна Македонија, а кои се засноваат врз инпутите обезбедени од страна на Советот за ИКТ и поширокатa ИКТ заедница во овие организации.

## 1. Вовед и дефиниции

### Резултати од испитувањето на мислењата на обуката за ИКТ „Отворен простор“

На обуката „Отворен простор“, што нашиот проект ја организираше кон крајот на јануари 2020 година, за членовите на Советот за ИКТ и други вработени во ИКТ секторот во разни судски институции во Северна Македонија, од присутните беше побарано да дадат свои мислења за неопходните приоритетни активности и иницијативи на неколку теми.Во однос на темата „Организација на ИКТ“, овие беа нивните ставови:

1. Електронска размена на информации помеѓу различните институции во рамките на системот (тековни проблеми, активности и сл.); во моментот, ова се прави само на состаноците на  Работно тело за стандардизација на постапките во судовите, на секои 2-3 месеци;
2. Систематизација и документирање на сите ИКТ активности;
3. Создавање систем за корисничка поддршка за сите вработени во ИКТ, како лесен, достапен метод за размена на искуства и решавање на заедничките проблеми (сега, единствената локална алатка е ИТ Форумот (Битола));
4. Дефинирање и воспоставување јасна хиерархија за ИКТ во рамките на судството, одговорност и поле на надлежности на секое ниво, создавање ефикасни процеси на комуникација (нова организација);
5. Централизирано, долгорочно планирање на сите потреби за ИКТ;
6. Обезбедување задолжителна (сертифицирана) обука за ИКТ за целиот ИКТ персонал, најмалку еднаш годишно;

7. Структура на организацијата на ИКТ за правосудството – да биде јасно воспоставена, според принципот на најголема ефикасност.

Сметаме дека е важно да се земат предвид овие предлози кога се препорачуваат решенија за континуитетот во работењето во секторот на информатичко-комуникациските технологии (ИКТ) во судството, и да се применат со цел постигнување најдобри можни ефекти.

**Управување со ризик**

Деловните процеси сè повеќе се поврзуваат преку информатичко-комуникациската технологија.Ова е придружено со зголемувањето на комплексноста на техничките системи и сè поголемата зависност од правилното работење на технологијата (БСИ Стандард 100-2: 2005) [IT Grundshutz].

Ризиците за континуитетот се очекува да се откријат преку процес на управување со ризици во организацијата.Со овие ризици може да се управува за да се намали нивната веројатност и/или влијание, но може да биде потребно и да се воспостават планови за справување со ефектите од ризикот доколку се појави.

Континуитет во работењето е термин што се однесува на збирот процеси на управување и интегрирани планови што го одржуваат континуитетот на клучните процеси на една организација, доколку се случи подривачки настан што влијае на способноста на организацијата да продолжи да ги обезбедува своите клучни услуги.ИКТ системите и електронските податоци се клучни компоненти на процесите и нивната заштита и навремено обновување е од најголемо значење.

Континуитетот во работењето (*Business Continuity* – BC) сега се смета за составен дел на добрата практика на раководењето и корпоративното управување.[1]

Ако изразот „континуитет во работењето“ го разгледаме според неговото буквално значење, најочигледно значење ќе биде способноста на деловниот субјект или претпријатието да продолжи да работи во континуитет многу долго време.Но, терминот всушност значи повеќе од буквалното значење на зборовите.

**Управување со континуитетот во работењето (*Business Continuity Management* – BCM)**

Меѓународната организација за стандардизација, во ИСО 22300, го дефинира „континуитетот во работењето“ како способност на една организација да продолжи со испорака на своите производи или услуги, на прифатливо и претходно дефинирано ниво, по подривачки инцидент.Тоа подразбира дека сопствениците на деловниот субјект и неговото раководствоимаат обврска да се погрижат тој да си ги плаќа обврските и да постигнува напредок и покрај сите пречки или проблеми со кои се соочува.Оваа обврска е дел од поопштиот процес на управување со деловното работење, што се нарекува и „Управување со континуитетот во работењето“ или BCM.

ИСО јасно го опишува BCMдека има цел да обезбеди рамка за градење на отпорноста на организацијата, што ќе ѝ овозможи на организацијата соодветно да реагира, на начин што

[1] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-plan/it-service-continuity-plan

ќе го заштити работењето, нејзиниот углед и сите други засегнати страни.Како процес на управување, BCM опфаќа неколку **клучни активности**:

- Идентификување и анализа на клучните производи и услуги на деловниот субјект
- Идентификување и анализа на најнеодложните активности и процеси на деловниот субјект
- Идентификување на потенцијалните закани и нивните влијанија врз деловното работење
- Изготвување планови и стратегии за брзо и делотворно закрепнување од какво било нарушување и продолжување на деловното работење

**Управување со континуитетот на ИТ услугите (IT *Service Continuity Management* - ITSCM)**

Неколку рамки во оваа област се однесуваат исклучивона ИТ аспектот на BCM, наречен континуитет на ИТ услугите.Управувањето со континуитетот на ИТ услугите (ITSCM) е дисциплина што произлегува од Закрепнувањето од ИТ катастрофи (IT *Disaster Recovery* – ITDR), но е повеќе ориентирана кон клиентот.Парадигмата е слична, но основните претпоставки на ИКТ во однос на приоритетите, временските рокови и важните компоненти се заменуваат со точни податоци од деловните единици.ITSCM е контролата што ја трансформира ИКТ во проактивна услужна организација, која ги задоволува потребите на своите клиенти, ги разбира нивните барања и ги исполнува овие барања.Во случај на инцидент, плановите и системите што се воспоставени треба да обезбедат продолжување на услугата во рамките на склучените договори за нивото на услугите (SLA), со што ќе се обезбеди усогласеност и задоволство на клиентите, како и поддршка на континуитетот во работењето.

Планот за континуитет во деловното работење за услугите од областа на информатичката технологија претставува збир на политики, стандарди, процедури и алатки со кои организациите не само што ја подобруваат својата способност да реагираат во случај на поголеми дефекти на системот, туку и ја подобруваат својата отпорностна поголеми инциденти, осигурувајќи дека клучните системи и услуги нема да откажат или дека дефектите ќе се санираат во рамките на еден прифатлив процес.

Плановите за закрепнување се хиерархиски организирани.Планот за закрепнување од уништување на локација ги опишува системите што ќе бидат опфатени со уништувањето на градбата.Посебен план за секоја услуга треба да обезбеди детални процедури и упатства во чекори за секоја фаза на инцидентот со цел тимовите за закрепнување да можат да ги обноват услугите и со тоа да го исполнат договорениот процес и составните цели за времето на закрепнување.

Плановите треба да бидат јасни и концизни и да очекуваат одредено ниво назнаење, но не да претпоставуваат експлицитно локално знаење, во случај да се бара надворешна помош за обнова на системите (истото важи и за плановите за закрепнување од катастрофи)[2].Секоја постапка треба да биде самостојна со цел да може да се искористи за

*[2]Овие проблеми и преклопувања се опфатени со најновите стандарди и рамки, но ова се развива во сложена мрежа на процедури и политики, на пример ITIL [ITIL] е Рамка за информатичко-технолошката (ИТ) инфраструктура, при што v2 е поделена на 9 области; иако идејата е да се искористат областите што се релевантни за организацијата, постоењето врски меѓу областите значи дека земањето една, а не друга може да создаде грешки. Ова се гледа и во стандардите, каде односите сега почнуваат да се дефинираат. На пример, управувањето со континуитетот на ИТ услугите PAS 77 [PAS 77] ја потврдува потребата за управување со континуитетот во работењето (BCM) пред да се изготват плановите за континуитет на ИТ услугите (ITSC) . Исто така, се наведува дека доколку не постои континуитет во*

да се изврши закрепнувањето на еден систем или компонента (на пр., серверот работи успешно, но системот за управување со базата на податоци е паднат).Секој документ, исто така, мора да содржи детали за предусловите; ова значи дека во случај на дефекти во повеќе компоненти, може да се следи правилната секвенца (на пр., да се замени дефектниот диск, дасе обнови оперативниот систем, да се инсталира базата на податоци, да се конфигурираат поставките за безбедност и потоа да се вратат податоците).

Накратко, Планот за континуитет на ИТ услугите обично ги содржи следниве информации:

- Детали за комбинираните составни цели за времето на закрепнување (RTO) и цели за рокот за закрепнување (RPO) и вклучување на Анализата на недостатоците на ИТ барањата.
- ИТ архитектурата
- Улогите и обврските
- Постапките за повикување
- Проценатa на штетите
- Дијаграм на текот на ескалацијата и процесите
- Детални процедури што прецизираат како да се обнови секоја компонента на ИТ системот
- Планови за тестирање што прецизираат како да се провери дали секоја компонента е успешно обновена
- Датотеки за евиденција на инциденти
- Податоци за контакт
- Процедури за враќање во стабилна состојба (*failback*)
- План за тестирање за ИТ

Овие планови детално ги опишуваат четирите фази:

- **Првичен одговор:** процена на штетите и повикување на соодветните тимови за управување со инциденти.
- **Обновување на услугите:** ова може да се изведе на начин што ќе се понуди деградирана услуга.
- **Испорачување услуги во абнормални околности:** привремените мерки може да вклучуваат преместување на услугите на друга локација или користење резервна опрема (честопати и обуки или тест сервери).Ова е привремена мерка за обезбедување ограничена услуга сè додека не се продолжи состандардната услуга.
- **Продолжување состандардната услуга:** враќање на вообичаената услуга, враќање во стабилна состојба по абнормалното испорачување услуги.

---

*работењето, тогаш мора да се реализира дел од анализата на влијанијата врз работењето (BIA) со цел да се разберат деловните барања и да се усогласат ИТ услугите со деловните барања.*

*Новите стандарди (и постојните што се развиваат) ги рефлектираат своите корени и затоа мора да се знае целната публика за секој од нив за најдобро да се разбере нивната основа. Американскиот стандард NFPA 1600 доаѓа од Националното здружение за заштита од пожари [NFPA] и претставува стандард за програмите за управување со катастрофи и вонредни состојби и програмите за континуитет на деловното работење. Раните верзии се повеќе за зачувување на животната средина отколку за ИТ, но најновата верзија (2007 г.) се движи во насока на континуитетот во работењето. Ова е во спротивност со BS 25999-1, кој беше напишан чисто како стандард за континуитет во работењето со цел да им овозможи на деловните субјекти да закрепнат од инциденти што се движат од мали (прекин на неколку часа) до големи инциденти поради кои е потребно преместување на услугите [BS 25999-1].*

*https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience*

**Планирање на континуитетот во работењето**

Со оглед на реалноста дека економскиот и деловен пејзаж е непредвидлив и непостојан, деловните субјекти сега преземаат многу мерки на претпазливост за осигурат дека нивното работење и натаму ќе има шанса да опстои и во услови на неочекувани нарушувања.Обично слушаме за овие мерки на претпазливост во форма на планирање закрепнување од катастрофи, кое првенствено е насочено кон обновување на ИТ инфраструктурата и ИТ операциите на фирмата. Овој поглед е прилично ограничен, акоја погледнете поголемата слика, бидејќи деловниот субјект и неговото работење се повеќе од неговата ИТ инфраструктура.

Затоа, повеќе внимание се посветува на планирањето на континуитетот во работењето (*Business Continuity Planning* - BCP), што ја става компанијата во проактивна позиција при планирањето како да осигури дека и натаму ќе може безбедно и непречено да ги испорачува своите клучни производи и услуги, притоа исполнувајќи ги своите законски, регулаторни и други обврски.

Веројатно можеме да наведеме повеќе од десетина причини зошто деловните субјекти би требало да изготват и одржуваат иницијативи за BCP, но, на крајот на краиштата, има само една крајна цел за тоа, а тоа е да помогне да се осигури дека организацијата, деловниот субјект или компанијата ги има потребните ресурси, информации и можности за справување со итни случаи и слични неочекувани настани, а особено со нивните последици.

**Придобивки од планирањето на континуитетот во работењето**

Веројатно ќе можете уште повеќе да го цените BCP доколку имате појасна претстава за тоа што можат од него да добијат деловните субјекти.

- **BCP ја подобрува перцепцијата и прифаќањето на организацијата кај јавноста.**Со прикажување проактивен став и демонстрирање иницијатива да биде добро подготвена, корисниците и поширокатa јавност ќе имаат поволен и позитивен впечаток за организацијата.Ова ќе доведе до одредено ниво на доверба, што веројатно ќе ги претвори во лојални клиенти што ќе имаат доверба.
- **BCP ќе го зајакне моралот на персоналот и ќе ја обезбеди нивната лојалност кон организацијата.**Вработените се склони да бараат стабилност во организацијата на која припаѓаат, а солидниот BCP е еден начин за раководството да им ја даде сигурноста што ја бараат. Исто така, ќе доведе до тоа вработените да се гордеат со својата работа и ќе ги мотивира да ја зголемат продуктивноста како членови на организацијата.
- **BCP го подобрува односот на организацијата со другите засегнати страни.**Засегнатите страни, вклучувајќи ги и високите функционери, ќе ѝ веруваат на организацијата доволно за да се охрабрат и натаму да доделуваат значителни буџетски средства, доколку знаат дека се прават сите напори да биде подготвена за неочекуваното.
- **BCP ја подобрува целокупната ефикасност на организацијата.**Во случај да се појави криза, која резултира со нарушување во работењето, солидниот BCP ќе ѝ овозможи на организацијата брзо и соодветно да реагира, одржувајќи ги загубите и трошоците на минимум затоа што веќе постои план.

**Закани за континуитетот во работењето**

Ризиците се својствени за деловните субјекти, а еден од нив е и ризикот да се соочат со потенцијални катастрофи и подривачки вонредни состојби.Кои се некои примери за овие потенцијални ризици или закани?

- **Природни катастрофи**(виша сила, или „Божји дела“), како урагани или тајфуни, бури или цунами, поплави, земјотреси, пожари, снежни бури, песочни бури
- **Вештачки катастрофи** со влијанија врз животната средина, како што се излевање на нафта, излевање на опасни материи, загадување, неправилно отстранување хемиски и друг индустриски отпад
- **Несреќи** предизвикани од непредвидени настани, како што се пожари и слични инциденти на работното место
- **Кога комуналните претпријатија и други слични даватели на услуги не ги испорачуваат своите услуги,** како на пример, при исклучување на снабдувачите на електрична и друг вид енергија, прекинување на услугите на водоснабдување и нефункционирање на комуникациските линии
- **Резултати од саботажа** и слични кривични дела (со намера деловниот субјект да се стави во опасност), како што е подметнување пожар,
- **Напади на кибер-безбедноста,** при што информатичкиот систем е мета на напади од хакерски активности и други слични упади

Сите овие закани мора сериозно да се сфатат, со оглед на големиот број ефекти или влијанија што ги имаат кога доведуваат до нарушување на деловното работење.

## 2. Чекори за изготвување план за континуитет во работењето

Пред да почнете да го пишувате Планот, мора да се извршат неколку чекори.

### Чекор 1: Утврдување на опсегот на Планот

Како и во повеќето процеси на планирање на работењето, првото нешто што мора да се направи е да се дефинираат опсегот и целите на планот што се изготвува.Во овој случај, тоа е планот за континуитетот во работењето (BCP).

Покрај тоа, потребно е и да се дефинираат претпоставките што ќе бидат застапени при спроведувањето на BCP.Исто така, во текот на оваа фаза се спроведува и буџетирањето, при што првичниот програмски буџет ги зема предвид трошоците што би можеле да настанат при процесот на изготвување на планот.Тие вклучуваат трошоци за истражување, обуки и семинари, како и други услуги што се потребни во процесот на спроведување на планот.

### Чекор 2: Формирајте го својот тим за континуитет во работењето.

Потребно е да се воспостави структура на управување во рамките на BCP со цел раководството да има ред и контрола во спроведувањето.Ова подразбира грижа и претпазливост при изборот на лицата на кои ќе им биде доделена задача да го планираат континуитетот во работењето.

Обично, се назначува претставник за секој клучен процес или функција, како и за процесите и функциите за поддршка.

Нема ограничување за тоа од колку лица треба да биде составен тимот или комисијата за континуитет во работењето.Тимот би можел да брои само пет лица, или да има дури 20, па

дури и 30 члена.Бројот на луѓе и големината на тимот во голема мера ќе зависи од природата на деловниот субјект и големината и обемот на неговото работење.

**Чекор 3: Вршење анализа на влијанијата врз работењето (*Business Impact Analysis* - BIA)**

Спроведувањето на BIA е од клучно значење бидејќи резултатите од неа ќе бидат главен инпут при планирањето на континуитетот во работењето.Со помош на BIA, тимот ќе може да ги предвиди или прогнозира потенцијалните влијанија или последици врз деловното работење.Исто така, таа ќе му помогне на тимот да собере информации што ќе бидат корисни за развој на стратегии што компанијата би можела да ги усвои со цел закрепнување од кризата.

Накратко, да ги разгледаме основните теми од интерес на BIA:

- **Клучните деловни области**или основните активности на деловниот субјект;
- **Функциите и процесите на деловниот субјект** што се сметаат за клучни и/или временски ограничени;
- Потребните **ресурси** за да се обезбеди континуитет на овие клучни деловни области и клучните процеси и функции;
- **Врските на зависност** (и меѓузависност) помеѓу деловните области и функциите или процесите;
- Прифатливото или **поднесливото време на застој** за секој клучен процес или функција

BIA ќе ја олесни приоретизацијата на клучните процеси и функции (или клучни производи и услуги) на компанијата, така што раководството ќе има појасна претстава на кои области им е потребна поголема распределба на ресурси при итни случаи.Обично, проценките и апроксимациите се прават во однос на финансиските варијабли, како што се изгубените приходи, дополнителните трошоци и други можни загуби.

**Чекор 4: Изготвување стратегија и планирање**

Врз основа на резултатите од BIA, тимот потоа ќе ги утврди стратегиите и плановите за одговор и закрепнување со цел решавање на ефектите од нарушувањето, и детално ќе ги претстави.Токму во оваа фаза тимот обезбедува детали за плановите и мерките што компанијата ќе ги преземе за да ги ублажи заканите и ризиците.

За секоја клучна функција, процес, услуга или производ, треба да има соодветни реакции, мерки или планови за континуитет.Треба да бидат вклучени и процени на трошоците.Оваа фаза треба да биде исклучително детална.

Исто така, треба да се осврне и на процедурите за подготвеност што мора да се спроведат и за тоа како тие ќе се спроведат.

**Чекор 5: Составување и документирање**

Ова вклучува пишување на Планот за континуитет во работењето.Обично, ќе има прв нацрт со оглед на тоа што последователните чекори вклучуваат тестирање на плановите и стратегиите за закрепнување, вршење прилагодувања и повторно тестирање сè додека не се финализира Планот.

Исто така, важно е да се напомене дека BCP е тековен процес.Тоа значи дека Планот мора често да се тестира и да се ажурира кога е потребно.Оттаму, Планот е предмет на промени, колку што е потребно.

**Чекор 6: Спроведување и тестирање**

Тука се применуваат стратегиите за превенција и ублажување, формулирани во Чекор 4. Ова подразбира соопштување на планот на сите членови на организацијата, информирајќи ги за нивната улога дел во него.Ова опфаќа обука за нивните улоги доколку таков настан навистина се случи.Надворешните засегнати страни, исто така, треба да бидат запознаени со планот.

Стратегиите за одговор и закрепнување при итни случаи ќе бидат предмет на тестирања, главно преку вежби и симулации за кои е потребно учество на засегнатите вработени или членови на организацијата.Преку тестирање, тимот за континуитет во работењето ќе може да процени дали планот ќе биде ефективен или не.Ова е нивна можност да ги направат потребните прилагодувања и корекции.

Периодично мора да се врши тестирање и евалуацијатокму поради непостојаната природа на деловните активности.

**Чекор 7: Прилагодување и унапредување**

Програмата можеби ќе треба да се прилагоди заради следново:

- Евалуацијата и тестирањето на стратегиите може да откријат дека тие се неделотворни или неефикасни
- Може да има недостатоци во стратегиите
- Некои улоги и обврски се нејасни и треба да се појаснат
- Промена во улогите и членовите на тимот за континуитет во работењето
- Воведување или појава на нови или дополнителни фактори или околности, како што се нова опрема, отворање на нова филијала, преместување на деловните активности и нова технологија или систем што ги модифицира клучните процеси.

Бидејќи тестирањето и евалуациите се вршат периодично, постои еднаква шанса програмата да мора да се прилагоди неколку пати.Произлегува дека Планот за континуитет во работењето ќе мора одново да се напише за да одговара или да ги одрази овие прилагодувања.

## 3. Пишување на Планот за континуитет во работењето

Откако ќе ги извршите првите три чекори споменати погоре, ќе бидете подготвени да ги составите и документирате активностите за планирање на континуитетот во работењето во Планот за континуитет во работењето, при што ќе го модифицирате за да добиете финална верзија по тестирањето и ревизијата.Во суштина, сè што сте реализирале во рамките на BCM ќе биде документирано во Планот.

Во зависност од природата на деловните активности, Планот може да има посебни карактеристики или дополнителни делови. Но, генерално, Планот за континуитет во работењето ги има следниве делови:

**1. Спроведување на програмата**

Обично, ова доаѓа во форма на Изјава за мисијата што го содржи следново:

- Целта на планот, наведена за од него да има корист и да се вклучи организацијата во целост, а не во делови
- Опсегот, долгорочните и краткорочните цели на BCP на организацијата
- Методите за евалуација што ќе се користат
- Буџетот, поточно предвидените и проценетите трошоци што ќе бидат потребни
- Други барања за ресурси
- Предвидениот временски распоред на спроведувањето на BCP
- Усогласеноста со сите релевантни правни и/или регулаторни барања

**Специфики на судството во Северна Македонија (спроведување на програмата):**

Тука се внесуваат некои конкретни коментари и предлози во врска со ситуацијата во оваа област, обезбедени од страна на дел од ИКТ вработените во судовите во Северна Македонија:

Планот за континуитет во деловното работење за услугите од областа на ИКТ претставува збир на политики, стандарди, процедури и алатки, па во таа насока во продолжение следат правилниците и процедурите кои веќе се усвоени од највископто раководство на институциите и истите се применуваат во судскиот систем на РСМ. Со дополнителна обработка и прилагодување во зависност од потребите, истите би можеле да се искористат при изработка на планот за континуитет во деловното работење.

Согласно предвидените обврски со **Законот за заштита на лични податоци** сите судови ги имаат изготвено актите кои следат. За истите добиена е согласност од Дирекцијата за заштита на лични податоци дека по својата содржина се во согласност со постојните прописи:

1. Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци
2. Правилник за начинот на вршење на видео надзор
3. Процедура за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци
4. Процедура за за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите
5. Процедура за пријавување, реакција и санирање на инциденти
6. Процедура за определување на обврските и одговорностите на судскиот службеник-информатичар кој го администрира информацискиот систем

Дирекцијата за заштита на лични податоци на секои три години врши редовен инспекциски надзор во сите судови после кој доставува до судовите решение за евентуално утврдени повреди со задолжение да се преземат дејствија и активности за отстранување на истите во зададен рок, во спротивно следуваат парични казни.

Секој суд има обврска еднаш годишно да врши внатрешна контрола на работењето на судскиот службеник-информатичар кој го администрира информацискиот систем како и проверка на евидентирање на авторизираниот пристап и на овластените лица при пристапување до предметите, за што изготвува извештај во кој се содржани евентуалните констатирани неправилности и предложените мерки за нивно отстранување.

Од особена важност е да се истакне дека за време траење на припремата за исполнување на предвидените обврски со Законот за заштита на лични податоци, се организираа обуки и работилници со присуство на претставници од Дирекцијата за

заштита на лични податоци кои даваа насоки, изготвуваа теркови за изработка на потребната документација итн.

Врховниот суд, Судскиот совет и четирите апелациони судови имаат **ИСО 9001:2015 сертификација** во чии рамки изготвени се и усвоени од страна на највисокото раководство дополнителни процедури во областа на ИКТ. Конкретно во Врховниот суд во делот на ИКТ усвоени се и се применуваат следните процедури:

1. Процедура за пристап до просториите каде се сместени ИКТ системите
2. Процедура за учество, изработка и следење на ИКТ проекти за судовите на РМ и Судскиот совет на РМ
3. Процедура за одржување на ИКТ проекти и координација со ИТ одделенија во судовите на РМ и Судскиот совет на РМ
4. Процедура за ажурирање на централните номенклатури
5. Процедура за инсталирање, конфигурирање, администрирање, мониторинг и одржување на ИКТ системот во ВСРМ
6. Процедура за користење, надградба и обнова на ИКТ системот во ВСРСМ
7. Процедура за пријавување, реакција и санирање на ИКТ инцидент
8. Процедура за креирање и управување со сигурносни копии
9. Процедура за сигурносен излез на интернет и е-пошта
10. Процедура за доделување на кориснички привилегии

Еднаш годишно се врши внатрешна и надворешна контрола од страна на овластена компанија со цел утврдување на евентуални недоследности после чие отстранување следи продолжување на сертификатот за наредната година.

Усвоените процедури континуирано се надополнуваат и менуваат во зависност од потребите и проблемите кои се појавуваат.

Од особена важност е да се истакне дека за време траење на процесот за спроведување на ИСО сертификацијата, беше ангажирана овластена компанија која вршеше обуки, даваше насоки, изготвуваше теркови за изработка на потребната документација и раководеше со целокупната постапка за сертификација.

Во продолжение следи листа на констатирани ризици во судскиот систем на РСМ:

1. Недостаток на доволен број стручни ИТ лица вработени во Центарот за информатика на ВСРСМ. Поради специфичноста на работата која ја извршува истиот, пополнувањето на работни места треба да биде со стручни и соодветно едуцирани ИТ лица
2. Недостатокот на соодветна и континуирана едукација во овластени едукативни центри на ИТ лицата вработени во судскиот систем на РСМ
3. Недостаток на дополнителни (backup) интернет линкови (во случај на пад на интернет линкот, да продолжи функционалноста на ИКТ ситемите)
4. Недостаток на локација за закрепнување од катастрофи (Disaster recovery site според моделот актив – актив)
5. Недостаток на High-availability clusters на ниво на секој суд
6. Недостаток на навремена и континуирана HW и SW надградба или обнова согласно амортизациониот период или по истекот на животниот циклус
7. Недостатокот од работни станици за ново вработените судски службеници
8. Недостаток на соодветна опрема и софтвер за централизирано мониторирање на сите сервери во ВСРСМ и сите сервери во судовите на РСМ
9. Недостатокот на услуга од страна на овластена компанија за чување на медиумите со сигурносни копии за ВСРСМ на дислоцирана локација, за останатите судови обезбедено е дислоцирано чување на бекапираните податоци во Центарот за информатика на ВСРСМ

10. Недостаток на обуки за подигнување на свесноста за безбедност кај сите вработени
11. Недостаток на соодветна и/или навремена информација: за евентуален физички пристап на неовластено лице до ИКТ опремата, за евентуално појавен проблем или настанат ИКТ инцидент
12. Недоволно почитување на сите безбедносни аспекти при користење на дадените овластувања за работа со АКМИС системот
13. Недоволно почитување на безбедносните правила од страна на корисниците на интернет и Е-пошта

*Целите на BCP/ITSBCP ќе бидат да се зголеми ефикасноста, транспарентноста и отчетноста на информатичките системи во судството, да се зголеми пристапноста, навременоста и леснотијата на користењето на судските услуги за сите корисници, да се подобри квалитетот на податоците и да се обезбеди непречено функционирање на централизираниот ИТ систем во целина.*

*Да се направи функционална анализа и процена на можните ризици (кои веќе се дадени во ISO документацијата во правосудните институции каде се применува овој сертификат) со дефинирање на степенот на секој од ризиците, веројатноста за нивно појавување, како и редовно следење и ажурирање на табелата со потенцијални ризици.*

*„Планот за континуитет во работењето од областа на информатичката технологија претставува збир на политики, стандарди, процедури и алатки“ (страница 2)*

*Можеме да зборуваме за еден генерален BCP само како ITSBCP, со акцент на најважните процедури за закрепнување од катастрофи во случај на: губење податоци, дефекти на серверите и мрежите, напади на безбедноста…*

*Сите постојни ИСО процедури со дефинирани стратешки цели и ризици, други внатрешни процедури и многу други акти треба да бидат обработени и прилагодени, според правилата на предложеното ITSCM, водејќи сметка за компатибилноста со Судскиот деловник и другите законски пропишани правила.*

*Паралелното постоење и континуирано одржување на два (или повеќе) независни системи – ISO и ITSBCP би било бесмислено.*

**2. Управување**

Тука ќе се прецизира формирањето на тимот за континуитет во работењето.Акцентот мора да се стави на следниве информации:

- **Членовите на тимот**, нивните титули или позиции, како и нивните улоги и обврски како членови на тимот за BCP.Наведете ги нивните информации за контакт.
- **Хиерархиската поставеност** и преземањето на управувањето, при што јасно ќе се покаже доделувањето на овластувањата и одговорностите.
- **Надворешни субјекти** или организации со кои деловниот субјект ќе комуницира во спроведувањето на BCP.Тие вклучуваат продавачи, дистрибутери, изведувачи, добавувачи и слично.

Презентирањето на овој дел се зајакнува со вклучување организациска или функционална шема што ги прикажува низите и меѓусебните врски помеѓу членовите на тимот и надворешните страни.

**Специфики на судството во Северна Македонија (управување):**

*BCP мора да содржи список на надворешни добавувачи што склучиле договор за одржување хардверска опрема со судовите и за секој добавувач треба прецизно да се*

*дефинира точното време на испорака на сите резервни хардверски делови во случај на катастрофа на хардверот.*

*Сите можни планови се поврзани со постојното планирање на централниот буџет, предводено од Судскиот буџетски совет.*

*За многу ИКТ проблеми и инциденти, судовите зависат од повисоки инстанци и надворешни субјекти, така што поголемиот дел од планирањето на ИКТ во судовите е тесно поврзано со централизираното планирање на ИКТ.*

Тука се внесуваат конкретни коментари и предлози во врска со ситуацијата во оваа област, обезбедени од страна на дел од ИКТ персоналот за реакција на инциденти во Северна Македонија:

На годишно ниво Врховниот суд на Република Северна Македонија спроведува централизирани јавни набавки за одржување на следната ИКТ опрема наменета за потребите на сите судови:

- Одржување на софтверот за АКМИС системот во судовите вклучително и сите функционални надградби интегрирани во истиот
- Одржување на ИКТ опремата и софтверското решение за Web порталите и нивната интеграција со АКМИС системите на сите судови
- Одржување на системот за прецизна климатизација во Систем салата на Врховниот суд на РСМ каде е сместена целокупната ИКТ опрема за судот и дел за сите судови на РСМ
- Одржување и софтверска обнова на уредите за заштита на сите судови на РСМ
- Одржување на ИКТ опремата, платформата за витуализација, оперативни системи, бази на податоци, Active Directory архитектура итн. наменета за функционирање на АКМИС системот во сите судови на РСМ
- Одржување на системот за централизиран backup / restore наменет за заштита на АКМИС базите на сите судови на РСМ
- Набавка на анти-вирусни и анти-спам лиценци наменети за сите судови на РСМ
- Одржување на системот за електронска пошта наменет за Врховниот суд на РСМ
- Одржување на софтверот за евиденција на настани со корелирање на логови од ИКТ уредите сместени во Врховниот суд на РСМ
- Одржување на системот за непрекинато напојување со електрична енергија (УПС) сместен во зградата на Врховен суд на РСМ

Откако ќе се склучи договор за одржување со некоја компанија, Центарот за информатика по е-маил ги известува вработените ИТ лица во судовите за контакт адресата на help desk-от на компанијата каде треба да се обраќаат за пријавување на проблем или барање помош. Со цел да се контролира ажурноста и времето на одзив на компаниите, копија од пријавувањето на проблемот како и копија од преземената активност се доставува до е-маил сметката на Центарот за информатика.

Досегашните искуства се воглавно позитивни во однос на ажурноста и одзивот на компаниите. Во случај на нефункционалност на цел сервер компанијата задолжена за одржување го заменува со резервен сервер, додека во случај на нефункционалност на некој хардверски дел компанијата врши замена на истиот со резервен и дополнително набавува резервни делови. Во случај на сериозен проблем со системскиот софтвер компаниите во координација со support-от на производителите и со вработените ИТ лица успешно го надминуваат проблемот и во најкраток можен рок ја враќаат функционалноста.

Пријавување на проблем или барање помош од компанијата која го одржува АКМИС системот се одвива преку тикетинг систем такашто вработените ИТ лица во судовите имаат искуство со работа на ваков систем.

### 3. Анализа на влијанијата врз работењето

Документирајте ги сите резултати од BIA спроведена од тимот.Повторно, бидете колку што можете подетални.

Треба да бидат вклучени сите резултати од претходни процедури за процена на ризици што ги спровела компанијата бидејќи тие ќе имаат значајна улога во спроведувањето на BIA.Со утврдување на слабостите на компанијата и нивното потенцијално влијание врз нејзиното работење, компанијата ќе може да ја утврди својата состојба на подготвеност и реактивност во случај да се случи катастрофа што може да предизвика нарушувања.

Други точки што мора да се истакнат во овој дел се:

- **Цели за времето на закрепнување (RTO) за деловните процеси и функции,** во случај на нарушување.Ова, во основа, претставува проценка на максималното времетраење или период до кога нарушените процеси и функции мора да се обноват или да закрепнат, пред сериозно да се загрози континуитетот во работењето.
- **Цели за рокот за закрепнување (RPO) за обновување на податоците.**Ова е максималниот период за време на кој податоците во ИТ инфраструктурата или базата на податоци на една организација може да бидат изгубени или недостапни поради итен случај или катастрофа.Кога системските дизајнери и аналитичари ќе бидат повикани да работат на закрепнување или обновување на податоците, тие ќе знаат колку време им се дава за тоа да го постигнат.

**Специфики на судството во Северна Македонија (Анализа на влијанијата врз работењето):**

Тука се внесуваат конкретни коментари и предлози во врска со ситуацијата во оваа област, обезбедени од страна на дел од ИКТ персоналот за реакција на инциденти во Северна Македонија:

Со цел да се постигне најкраток можен прекин на функционалноста (down time), од особена важност е при планирање и набавка на потребната ИКТ опрема да им се даде предност на новите технологии како што се **High – Availability clusters, Disaster Recovery site** според моделот актив – актив итн.

Во Центарот за информатика ИКТ опремата на која е сместено решението за Казнена евиденција конфигурирана е како High – Availability clusters, додека Disaster Recovery site, резервна локација конфигурирана е во Основниот кривичен суд и се однесува на ИКТ опремата на која е сместено решението за Web порталите на судовите и Електронската достава. Во останатите судови ИКТ опремата е застарена и ги нема наведените можности.

*Ова е највисок критичен ризик, така што времето за закрепнување за процесите и обновување на податоците е многу кратко.Оттука, исто така е важно да се процени времето потребно за да се врати системот во функција во случај на пад.*

*Постапката за враќање на податоците од резервните копии треба детално да се опише, со точно дефинирани параметри за својствата на вратените податоци.*

*Мора да имаме ефикасен план за закрепнување, на пример во случај на ваков инцидент, идниот Централен систем за управување со предмети мора итно да обезбеди целосна испорака на услуги, сè до целосно обновување на стандардните услуги.*

*Оттука, можна сугестија е да постојат два физички сервери, наместо само виртуелни, во секој суд, така што вториот ќе може да преземе во случај на дефект на примарниот*

*сервер!Оваа мерка би можела да се изведе со претстојната голема набавка на нови сервери.*

**4. Стратегии и барања за континуитетот во работењето**

Сите планови, мерки, процедури и подготовки, како и ресурсите и другите барања за нивно спроведување, мора да бидат документирани во овој дел, и тоа многу детално.

Имајте предвид дека BCM е тековен процес, што подразбира планирање на стратегиите што ќе се користат пред, за време и по подривачкиот настан.

Примерите се **детални стратегии и барања за ресурси** за:

- Спроведување и извршување **стратегии за превенција и контрола**, или активности што ќе бидат преземени пред да се случи настанот.Примери за тоа се:
    - Инсталирање објекти, системи и мерки за физичка заштита, како што се генератори за итни случаи и капаци за прозорци за заштита од невреме.
    - Диверзификација на снабдувачите со ресурси и проширување на синџирот на снабдување, преку потенцијално барање други алтернативни добавувачи и продавачи за да се избегне целосна зависност од еден извор.
    - Поставување објекти надвор од локацијата како резервни или алтернативни локации за сервери, меморија и складирање, меѓу другото (локација за закрепнување од катастрофи)
- Спроведување и извршување **стратегии за одговор при итни случаи** или активности за време на настанот.Примери за ваквите одговори при итни случаи се:
    - Формирање команден центар за одговор на инциденти
    - Постапки за евакуација
    - Дистрибуција на информации до медиумите и пошироката јавност
    - Доставување известувања и ажурирања на статусот до добавувачите, продавачите, дистрибутерите и клиентите
- Спроведување и извршување **стратегии за закрепнување** или активности по настанот, како и напори за продолжување со операциите.Пример стратегии се:
    - Преместување или пренесување на операциите во друга географска област
    - Алтернативни методи или процеси, како што се мануелни заобиколувања, или привремени методи што ги применува или користи компанијата за да се олесни продолжувањето на клучните процеси и функции во отсуство на стандардни системи и персонал
    - Обновување на податоците, особено кога нарушувањето е најмногу на товар на единиците за информатичка технологија во компанијата.

**Специфики на судството во Северна Македонија (стратегии и барања за континуитет во работењето):**

Тука се внесуваат конкретни коментари и предлози во врска со ситуацијата во оваа област, обезбедени од страна на дел од ИКТ персоналот за реакција на инциденти во Северна Македонија:

Во однос на стратегиите за превенција и контрола, во рамките на можностите се преземаат соодветни мерки:

- Зградата во која е сместен Врховниот суд опремена е со генератор и УПС уред на кој е приклучена целокупната ИКТ опрема сместена во Врховниот суд
- Систем салата сместена во Врховниот суд на РСМ ги задоволува пропишаните стандарди за просторни, климатски, енергетски и безбедносни услови: површина од

над 50 м$^2$ , нема прозори, дупли антистатски под, независни кабли за напојување, професионален редундантен систем за разладување, метална врата, контролиран влез со магнетна картица само за вработените ИТ лица и за судската полиција во случај на непредвидени ситуации.

- Во останатите судови целосно или делумно се запазени пропишаните стандарди за просторни, климатски, енергетски и безбедносни услови.

*Мора да се формира тим за закрепнување од катастрофи што ќе дејствува брзо според претходно подготвен план во случај на катастрофи.*Исто така е важно да се обезбеди и локација за закрепнување од катастрофи.

*Просториите на серверите не се целосно опремени во сите судови, но постепено се опремуваат според средствата обезбедени од Судскиот буџетски совет.Онаму каде што се завршени, безбедноста на просториите на серверите е веќе на високо ниво:метална врата и антистатички под, независни кабли за напојување, двојна климатизација, заклучени, со надзор од судската полиција и камери, со влез во судовите под контрола на судската полиција.*

*Постојат тековни ИСО процедури за:контрола на пристапот до просторијата на серверите, физичка заштита и видео надзор, евиденција на лицата што влегуваат во судот…*

*Некои поставки на стратегиите за закрепнување и тестирањето во голема мера зависат од повисоки инстанци.*

*Иако денес постојат регулативи што ги пропишуваат овие мерки, во многу случаи нема доволно простор во просториите на серверите, особено кога повеќе институции се под ист покрив.*

**5. Обука, тестирање и евалуација**

Во однос на обуката, Планот треба да содржи детали за следново:

- Програма за обука или курикулум што ќе ја следат членовите на тимот за континуитет во работењето и другите членови на организацијата.
- Временска рамка или распоред за обука на членовите на тимот и другиот персонал

При евалуацијата на планираните стратегии, во Планот треба да се вклучи и следново:

- Постапки за тестирање за стратегиите за закрепнување и одговор
- Распоред на тестирање или временска рамка за спроведување на постапките
- Формулари и документи што ќе се користат при тестирањето и евалуацијата
- Опис и подробности за вежбите што ќе се спроведат

**Специфики на судството во Северна Македонија (обука, тестирање и евалуација):**

Согласно предвидените обврски со Законот за заштита на лични податоци (Процедура за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци), секој суд има обврска најмалку 2 – 4 пати годишно да изврши проверка на фумкционалноста на сигурносните копии за вршење на реконструкција на личните податоци.

Судовите во РСМ не се во можност да вршат проверка на функционалноста на сигурносните копии од причина што немаат доволно ресурси на постојната ИКТ опремата, ниту имаат обука за изведување на наведената проверка која воопшто не е едноставна.

Единстено Врховниот суд најредовно врши или проверка на функционалноста на сигурносните копии или реална реконструкција на делови од ИКТ системот и враќање на бекапираните податоци во зависност од потребите. Во изминатиот период Центарот за информатика во соработка со надворешната компанија задолжена за одржување на опремата за Казнената евиденција, извршија комплетна реконфигурација на истата поради логичко пореметување, извршија враќање на бекапираните податоци и повторно воспоставување на функционалноста. За сите извршени проверки или реална реконструкција на податоците уредно се изготвуваат записници во кои се нотирани преземените активности и истите се приложуваат кога се врши редовен инспекциски надзор од страна на Дирекцијата за заштита на лични податоци.

*Планот мора да се тестира во однапред одредено време, затоа што може да биде изложен на ризик за време на реален итен случај.Тестовите треба да се вршат по пропишаните активности за закрепнување од катастрофи преземени за да се пресмета очекуваното време на закрепнување на системот или податоците и да осигурат дека ќе го добиеме очекуваниот резултат.*

*Исто така, резервните копии што се прават според тековните применливи регулативи треба да се тестираат во однапред дефиниран распоред за да се обезбеди конзистентност и функционалност на податоците, како и да се утврди времето за враќање на овие податоци во системот.*

**6. Одржување на програмата**

Планот исто така ќе служи како историски запис или упатување за следење на начинот на кој се одвивал процесот на управување со континуитетот во работењето.Оттука, кога пишувате за извршените ажурирања или прилагодувања, треба да се споменат недостатоците или проблемите што биле решавани со прилагодувањата или корективните активности.

Планот за континуитет во работењето во суштина е Светото Писмо на компанијата за време на криза или кога треба да се справи со последиците од катастрофа.Луѓето обично имаат проблем јасно да размислуваат за време на вакви големи настани и нарушувања, а Планот ќе послужи како водич што ќе ја води компанијата во вистинската насока.

Кога пишувате план за континуитет во работењето, точноста е од големо значење, од личните информации на сите вклучени лица и субјекти, до нивните улоги и обврски.Исто така, планот треба да биде релевантен во секое време, а тоа може да се постигне ако се погрижите да биде ажуриран.Конечно, кога го пишувате Планот, направете го тоа на начин што ќе биде лесно разбирлив за сите што го читаат, од високото раководство до вработениот на најниската позиција во организацијата.Нема да биде од корист ако е тешко да се разбере напишаното.

**Специфики на судството во Северна Македонија (одржување на програмата):**

Тука се внесуваат конкретни коментари и предлози во врска со ситуацијата во оваа област, обезбедени од страна на дел од ИКТ персоналот за реакција на инциденти во Северна Македонија:

*Планот за континуитет во работењето (BCP) треба да го води највисокото раководство на судот (претседателот, администраторот), но со оглед на тоа што овој план се однесува на содржината на ИКТ, ИКТ лицата треба да бидат длабоко вклучени во неговото создавање и управување.*

*Планот за континуитет во работењето (BCP) што овозможува функционирање во непредвидени ситуации, треба да биде резултат на комбинираните напори на*

*претседателот на судот, администраторот на судот и лидерите на ИКТ во организацијата; исто така, тој треба да се одржува и постојано да се следи од страна на сите клучни лица вклучени во сите процеси, со цел BCP да биде постојано ажуриран.Сосема е можно повеќето активности за одржување да станат друг пакет обемни задолжителни должности, додадени на веќе долгиот список на должности за вработените во ИКТ.*

## 4. Резиме на специфичните околности во Северна Македонија

Со оглед на улогата што судството денес ја има во секое цивилизирано општество, мора да се забележат специфичните околности што мора да се земат предвид при планирањето и управувањето со континуитетот во работењето од областа на ИКТ во судството во Северна Македонија:

- Како што е случај и со другите слични системи во земјите во транзиција во ЦИЕ, ЕУ посветува големо внимание на правилното, ефикасното и независното функционирање на националните судски системи, како клучен предуслов за владеењето на правото; ова е јасно видливо преку голем број проекти со висока вредност финансирани од ЕУ во оваа област
- Со денешната улога на ИКТ како столб на ефикасното национално судство, станува најзначајно ИКТ да биде способна да функционира непрекинато за време на криза предизвикана од потенцијални катастрофи и/или подривачки итни случаи
- Оттука, правилно испланираниот, напишан и спроведен план за континуитет во работењето, вклучително и закрепнување од катастрофи, може многу да постигне во насока на обезбедување континуирано работење на ИКТ во судството, како и за зголемување на довербата, како кај персоналот во судството, така и кај клиентите во судството (граѓани, правни лица, итн.)
- Денес, не постојат планови за управување со кризи за основните судови, ниту поединечно ниту колективно
- Релевантна едукација за ISO стандардите спроведена е само за апелационите судови, а не и за основните судови
- Не постојат конкретни постапки во случај на криза за заштита на личните податоци во основните судови

## 5. Акциски план

Ова е пакетот препораки, претставени во документот, со предложени дополнителни активности:

**Совет за ИКТ:**

Овој документ, кој веќе е проширен со коментарите и предлозите собрани од повеќе вработени во ИКТ низ целата земја, ќе биде испратен од нашиот проект до Советот за ИКТ, за натамошни нивни активности.Очекуваме Советот за ИКТ да продолжи со следниве активности:

a. Прегледување на документот, при што ќе се разгледаат натамошни проширувања или подобрувања, на својот следен месечен состанок;

b. Назначување на еден од членовите како известувач за управување со процесот на пополнување на овој документ;

c. Советот за ИКТ треба, при прегледот на овој документ, да ги разгледа потребните активности, дефинирани во документот, и нивните последици врз идните планови за стратегија за ИКТ, како и потребните измени на стратегијата за ИКТ, временскиот распоред и финансиските потреби;

d. Откако ова ќе се изврши, Советот треба да го вметне овој документ како дел од стратегијата за ИКТ и да го испрати комплетираниот документ, заедно со предложените активности, временскиот распоред и финансиските очекувања, за натамошно разгледување до Министерството за правда и другите релевантни тела/институции;

**Препорачан процес:**

Со оглед на горенаведеното, се чини дека постои јасен процес за подобрување на континуитетот во работењето, како во судовите така и во обвинителствата:

1. Формирање на тимот за управување со континуитетот во работењето, на ниво на Судскиот совет или Врховниот суд (за судство), или на ниво на Државното обвинителство (обвинителство);
2. Тимот треба да изготви соодветен план за сите институции, како што е опишано во овој текст, веројатно со конкретни детали за различните видови институции;
3. Планот треба да претставува извор за конкретните постапки, со јасно назначени должности;
4. Исто така, мора да се изготват и контролни постапки за да се обезбеди гаранција дека процесот ќе се почитува и редовно ќе се тестира;
5. Треба да се креираат пакет курсеви за обука и редовно да се повторуваат во просториите на Академијата за судии и јавни обвинители;
6. Постапките и подготвеноста мора редовно да се проверуваат и да се изготвуваат извештаи до раководното тело, врз основа на овие проверки, во претходно утврдени временски периоди.
7. Исто така, ве молиме разгледајте ги „Спецификите на судството во Северна Македонија“ на крајот на секое поглавје, за натамошни подетални упатства.
8. Лицата и/или институциите што треба да бидат вклучени во горенаведениот план се наведени во рамките на овие препораки, за секој елемент од плановите за континуитет во работењето/закрепнување од катастрофи.
9. Тешко е да се проценат трошоците за изготвување на ваквите планови, имајќи предвид дека тие треба да се изготват на централно ниво и на ниво на секој суд, но тие главно ги содржат трошоците за вложеното време од страна на лицата во судството, назначени за извршување на овие дејствија.

**Локација за закрепнување од катастрофи:**

Како што претходно разговаравме со г. Јане Стојанов, раководител на Секторот за телекомуникации при Министерството за внатрешни работи (МВР), постои реална можностИКТ секторот во правосудството во Северна Македонија да формира своја локација за закрепнување од катастрофи, во рамките на периметарот на новиот сопствен објект на МВР за закрепнување од катастрофи, во градот Прилеп.

До ноември минатата година, овој објект веќе ја беше завршил својата прва фаза, физичката зграда и комплетен, специјално наменетагрегат за резервно напојување; до овој рок, според проектниот план, треба да се заврши втората фаза, со целосно опремен центар за податоци, поделен на два одделни простори, со 42 полици за сместување на серверите, дисковите и целата комуникациска и безбедносна опрема.Еден од овие простори е резервиран за МВР, а другиот е достапен за сите други владини сектори (вклучувајќи ја и потенцијалната ИКТ опрема за правосудството); некои сектори веќе имаат резервирано простор, како што е Министерството за финансии, секторот за јавни приходи

и секторот за царина.Оваа локација треба да биде целосно завршена и подготвена за употреба до јули 2020 година.

Министерството за внатрешни работи нуди два модели на финансирање на овие надворешни корисници:едниот е практично „бесплатно“, доколку владата се согласи да го преземе финансирањето, а другиот е предмет на склучен меморандум за разбирање помеѓу МВР и секторот што бара употреба на центарот.

Локацијата се очекува да биде целосно поврзана со корисниците во Скопје, со користење микробранова и брза оптичка врска, која во моментот се гради.

## Прилог 1: Анализа на влијанијата врз работењето

### Анализа на влијанијата врз работењето:Рангирање на основните услуги/функции

**Единица на услуга/деловна активност: _____**

**Погодени области и степен на влијание:**

| Степен на важност на основната ИКТ активност/ услуга | Финанси и | Вработен и | Клиенти | Добавувач и/деловни партнери | Правни регулатор ни | Јавни/ заедница | Друго | Вкупен резултат (приоретизира ње и изготвување на списокот на услуги) |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

***1= слабо негативно влијание*** ***10= силно негативно влијание***