

УНИВЕРЗИТЕТ У БЕОГРАДУ  
ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

Милица М. Лабус

**Модел адаптивног управљања континуитетом  
електронског пословања**

докторска дисертација

Београд, 2020

UNIVERSITY OF BELGRADE  
FACULTY OF ORGANIZATIONAL SCIENCES

Milica M. Labus

**Model for Adaptive E-Business Continuity  
Management**

Doctoral Dissertation

Belgrade, 2020

Ментор:

**др Маријана Деспотовић-Зракић,**

ред. проф. Факултета организационих наука Универзитета у Београду

Чланови комисије:

**др Божидар Раденковић,**

ред. проф. Факултета организационих наука Универзитета у Београду

**др Марко Богатовић,**

доцент Саобраћајног факултета Универзитета у Београду

Датум одбране: \_\_\_\_\_

## Модел адаптивног управљања континуитетом електронског пословања

### **Сажетак:**

Предмет ове докторске дисертације је иновативни модел адаптивног управљања континуитетом електронског пословања, који је емпиријски тестиран у три финансијске организације. Истраживање је фокусирано на управљање континуитетом пословања у организацијама које користе савремене технологије електронског пословања: интернет, мобилно рачунарство, електронске сервисе и виртуалну инфраструктуру, због чега уводи прелазак са традиционалног управљања континуитетом пословања (енгл. *Business Continuity Management*, скраћено *BCM*) на управљање континуитетом електронског пословања (енгл. *e-Business Continuity Management*, скраћено *eBCM*) које јегодно за модерна технолошка окружења.

Како се у данашње време технологије електронског пословања брзо мењају и развијају, предложени модел обезбеђује адаптивни *eBCM*, узимајући у обзир промене окружења у коме организација послује. Модел је развијен у складу са *ISO 22301* стандардом. Мотив за истраживање је дефинисање општег оквира за успостављање адаптивног *eBCM*-а. Модел се састоји од практичних корака за дефинисање елемената система управљања континуитетом пословања: анализе утицаја на пословање, процене ризика у вези са континуитетом електронског пословања и плана континуитета пословања.

Модел је примењен у пракси у три финансијске организације, након чега је спроведено његово оцењивање. Кључни резултат оцењивања је да је модел ефикасан у успостављању адаптивног *eBCM*-а, а да су за његову ефикасност најзначајније две компоненте: метод за спровођење анализе утицаја на пословања и метод за континуирано унапређење система управљања континуитетом пословања. Остале компоненте модела имају мањи, али не и занемарљив, ефекат. Предложени модел је општи и може се применити на било коју организацију која користи савремене технологије електронског пословања.

**Кључне речи:** Управљање континуитетом електронског пословања, анализа утицаја на пословање, план континуитета пословања, *ISO 22301*, електронско пословање, процена ризика

**Научна област:** Електронско пословање

**Ужа научна област:** Управљање континуитетом пословања

## *Model for Adaptive E-Business Continuity Management*

### **Abstract:**

*The doctoral dissertation research subject is an innovative model for adaptive e-business continuity management, which has been empirically tested in three financial organizations. The research is focused on business continuity management in organizations that use modern e-business technologies: the Internet, mobile computing, e-services, and virtual infrastructure, for which reason it introduces the shift from traditional Business Continuity Management (BCM) towards “e-Business Continuity Management” (eBCM) suitable for modern technological environments.*

*Since e-business technologies are rapidly changing and developing, the proposed model provides adaptive e-business continuity management, taking into account changes in the environment in which the organization operates. The model is developed in accordance with the ISO 22301 standard. The motive for this research is to define a general framework for the establishment and continuous improvement of an adaptive eBCM. The model consists of practical steps for defining elements of a business continuity management system (BCMS): business impact analysis, business continuity risk assessment and a business continuity plan.*

*The model was implemented and evaluated within three financial organizations. The key finding is that the model is effective in establishing an adaptive eBCM and that the following two model components are the most important for its effectiveness: the Business Impact Analysis Method and the Method for Continual BCMS Improvement. Other model components have a smaller, but not negligible, effect on the implementation of an adaptive eBCM. The proposed model is general and can be applied to any organization that uses modern e-business technologies.*

**Key words:** *E-Business Continuity Management, Business Impact Analysis, Business Continuity Plan, ISO 22301, E-Business, Risk Assessment*

**Scientific field:** *E-Business*

**Scientific subfield:** *Business Continuity Management*

## Садржај:

<b>1</b>	<b>УВОД</b> .....	<b>1</b>
1.1	ДЕФИНИСАЊЕ ПРЕДМЕТА ИСТРАЖИВАЊА.....	1
1.2	ЦИЉЕВИ ИСТРАЖИВАЊА.....	2
1.3	ПОЛАЗНЕ ХИПОТЕЗЕ.....	3
1.4	МЕТОДОЛОГИЈА ИСТРАЖИВАЊА.....	3
1.5	СТРУКТУРА И ОРГАНИЗАЦИЈА ДИСЕРТАЦИЈЕ.....	5
<b>2</b>	<b>УПРАВЉАЊЕ КОНТИНУИТЕТОМ ЕЛЕКТРОНСКОГ ПОСЛОВАЊА</b> .....	<b>6</b>
2.1	ЕЛЕКТРОНСКО ПОСЛОВАЊЕ.....	6
2.2	КОНТИНУИТЕТ ЕЛЕКТРОНСКОГ ПОСЛОВАЊА.....	8
2.2.1	<i>Типови инцидента</i> .....	11
2.2.2	<i>Регулатива</i> .....	12
2.2.3	<i>Међународни стандарди за управљање континуитетом пословања</i> .....	14
2.3	ЦИЉЕВИ УПРАВЉАЊА КОНТИНУИТЕТОМ ЕЛЕКТРОНСКОГ ПОСЛОВАЊА.....	19
2.4	СИСТЕМ УПРАВЉАЊА КОНТИНУИТЕТОМ ПОСЛОВАЊА.....	20
2.5	КАРАКТЕРИСТИКЕ УСПЕШНОГ УПРАВЉАЊА КОНТИНУИТЕТОМ ЕЛЕКТРОНСКОГ ПОСЛОВАЊА.....	20
2.6	МОДЕЛИ ЗА УПРАВЉАЊЕ КОНТИНУИТЕТОМ ПОСЛОВАЊА.....	21
2.6.1	<i>Карактеристике модела за управљање континуитетом пословања</i> .....	21
2.6.2	<i>Опити модели</i> .....	23
2.6.3	<i>Квантитативни модели</i> .....	27
2.6.4	<i>Доменски специфични модели</i> .....	28
2.6.5	<i>Модели везани за инциденте великих размера</i> .....	28
<b>3</b>	<b>РАЗВОЈ МОДЕЛА ЗА АДАПТИВНО УПРАВЉАЊЕ КОНТИНУИТЕТОМ ЕЛЕКТРОНСКОГ ПОСЛОВАЊА</b> .....	<b>30</b>
3.1	МОДЕЛ АДАПТИВНОГ УПРАВЉАЊА КОНТИНУИТЕТОМ ЕЛЕКТРОНСКОГ ПОСЛОВАЊА.....	30
3.2	ПАРАМЕТРИ МОДЕЛА.....	32
3.2.1	<i>Циљеви управљања континуитетом пословања</i> .....	33
3.2.2	<i>Делокруг BCMS-а</i> .....	34

3.2.3	Контекст организације.....	34
3.2.4	Потенцијалне претње.....	35
3.2.5	Присутне рањивости.....	36
3.2.6	Скала за дефинисање трајања прекида у раду.....	38
3.2.7	Финансијски утицај.....	38
3.2.8	Оперативни утицаји.....	38
3.2.9	Нивои критичности пословних процеса.....	39
3.2.10	Категорије финансијских вредности ресурса.....	39
3.2.11	Прихватљив ниво ризика.....	40
3.2.12	Класе приоритета ризика.....	40
3.3	МЕТОД ЗА СПРОВОЂЕЊЕ АНАЛИЗЕ УТИЦАЈА НА ПОСЛОВАЊЕ.....	40
3.3.1	Прикупљање и анализа података на нивоу организационих јединица.....	42
3.3.2	Анализа података и документовање резултата на нивоу организације.....	45
3.4	МЕТОД ЗА ПРОЦЕНУ РИЗИКА У ВЕЗИ СА КОНТИНУИТЕТОМ ЕЛЕКТРОНСКОГ ПОСЛОВАЊА.....	46
3.4.1	Анализа ризика.....	48
3.4.2	Вредновање ризика.....	49
3.5	МЕТОД ЗА ИЗРАДУ ПЛАНА КОНТИНУИТЕТА ПОСЛОВАЊА.....	53
3.5.1	Дефинисање стратегије управљања континуитетом пословања.....	54
3.5.2	Дефинисање плана континуитета пословања.....	57
3.6	МЕТОД ЗА КОНТИНУИРАНО УНАПРЕЂЕЊЕ ВСМС-А.....	62
3.6.1	Третман ризика.....	64
3.6.2	Тестирање плана континуитета пословања.....	65
3.6.3	Праћење и преиспитивање ВСМС-а.....	66
3.6.4	Одржавање и унапређење ВСМС-а.....	67
<b>4</b>	<b>ПРИМЕНА РАЗВИЈЕНОГ МОДЕЛА У ПРАКСИ.....</b>	<b>68</b>
4.1	ПРИМЕНА МОДЕЛА.....	68
4.2	ВРЕДНОВАЊЕ МОДЕЛА.....	68
4.3	УПИТНИК ЗА ВРЕДНОВАЊЕ МОДЕЛА.....	71
4.4	МЕТОДОЛОГИЈА ВРЕДНОВАЊА МОДЕЛА.....	73

4.5	АНАЛИЗА РЕЗУЛТАТА .....	75
4.5.1	Оцена ефикасности модела .....	75
4.5.2	Оцена PLS-SEM модела латентне варијабле .....	82
4.5.3	Оцена PLS-SEM структурног модела и тестирање хипотеза евалуације .....	85
4.6	ДИСКУСИЈА РЕЗУЛТАТА .....	88
<b>5</b>	<b>НАУЧНИ И СТРУЧНИ ДОПРИНОСИ .....</b>	<b>91</b>
<b>6</b>	<b>БУДУЋА ИСТРАЖИВАЊА .....</b>	<b>92</b>
<b>7</b>	<b>ЗАКЉУЧАК .....</b>	<b>93</b>
<b>8</b>	<b>ЛИТЕРАТУРА .....</b>	<b>94</b>
<b>9</b>	<b>ПРИЛОЗИ.....</b>	<b>106</b>
9.1	Прилог 1 – Упитник за спровођење анализе утицаја на пословање (ВИА упитник).....	106
9.2	Прилог 2 - Садржај документа Анализа утицаја на пословање .....	116
9.3	Прилог 3 - Садржај документа Стратегија управљања континуитетом пословања .....	118
9.4	Прилог 4 - Садржај документа План континуитета пословања .....	120
9.5	Прилог 5 - Упитник за вредновање модела .....	122
9.6	Прилог 6 - Одговори испитаника .....	127
9.7	Прилог 7 - Статистичка анализа питања из Упитника за вредновање модела.....	130
<b>10</b>	<b>БИОГРАФИЈА АУТОРА.....</b>	<b>134</b>



## Списак табела:

Табела 1 - Основне карактеристике електронског пословања .....	6
Табела 2 - Доступност сервиса као функција „броја деветки“ (извор: [31], [32]) .....	10
Табела 3 - Типови инцидената .....	11
Табела 4 - Преглед идентификованих група ВСМ модела и методолошких оквира .....	22
Табела 5 - Параметри модела .....	32
Табела 6 - Пример дефиниције категорија финансијских вредности ресурса .....	39
Табела 7 - Пример дефиниције класа приоритета ризика .....	40
Табела 8 - Вредновање ресурса .....	51
Табела 9 - Вероватноћа настанка ризика .....	52
Табела 10 - Потенцијални утицај ризика .....	52
Табела 11 - Ниво озбиљности инцидента .....	59
Табела 12 - Ниво утицаја инцидента .....	59
Табела 13 - Класа инцидента .....	59
Табела 14 - Дефиниција класе инцидента .....	60
Табела 15 - Хипотезе евалуације и теоријска основа .....	71
Табела 16 - План вредновања модела .....	72
Табела 17 - Кораци у вредновању модела .....	74
Табела 18 - Вредновање основних карактеристика еВСМ модела .....	76
Табела 19 - Резултати оцене модела латентне варијабле .....	83
Табела 20 - Дискриминаторна валидност: Fornell-Larcker критеријум .....	84
Табела 21 - Резултати реузорковања .....	87
Табела 22 - Резултати тестирања хипотеза евалуације .....	88
Табела 23 - Статистичка анализа питања из Упитника за вредновање модела (индикатори за рефлексивно мерење конструката PLS-SEM модела) .....	130

## Списак слика:

Слика 1 - Фазе у истраживању.....	4
Слика 2 - Нивои зрелости управљања континуитетом пословања у организацији.....	26
Слика 3 - Модел адаптивног управљања континуитетом електронског пословања.....	30
Слика 4 - Основне компоненте модела (параметри у круговима; методи у правоугаонцима са испрекиданим ивицама; поступци, као саставни делови метода, у правоугаонцима са заобљеним ивицама) и њихове најважније међузависности .....	31
Слика 5 - Матрица утицаја и интереса заинтересоване стране .....	34
Слика 6 - Метод за спровођење анализе утицаја на пословање .....	41
Слика 7 - Циљни параметри опоравка .....	45
Слика 8 - Најважније везе између метода за процену ризика (M2) и осталих компонената модела.....	47
Слика 9 - Метод за процену ризика у вези са континуитетом електронског пословања.....	48
Слика 10 - Метод за израду плана континуитета пословања .....	54
Слика 11 - Метод за континуирано унапређење BCMS-а.....	63
Слика 12 - Хипотезе евалуације (структурни PLS-SEM модел) .....	70
Слика 13 - Средње вредности и проценат поуздања одговора из групе питања.....	78
Слика 14 - Однос варијабилитета и појединачних оцена испитаника.....	79
Слика 15 - Хипотетичко тестирање величине узорка .....	80
Слика 16 - Хипотетичко тестирање величине узорка за четири метода модела .....	81
Слика 17 - Резултати PLS алгоритма (унутрашњи модел: тотални ефекти; спољашњи модел: коефицијенти спољног оптерећења, конструкти: Average Variance Extracted - AVE).....	82
Слика 18 - Резултати реузорковања (унутрашњи модел: коефицијенти путање и у заградама t-вредности).....	86
Слика 19 - Део I: Вредновање основних карактеристика модела .....	127
Слика 20 - Део II: Вредновање Метода за спровођење анализе утицаја на пословање .....	127

Слика 21 - Део III: Вредновање Метода за процену ризика у вези са континуитетом е-пословања .....	128
Слика 22 - Део IV: Вредновање Метода за израду плана континуитета пословања.....	128
Слика 23 - Део V: Вредновање Метода за континуирано унапређење BCMS-а .....	129

# 1 Увод

## 1.1 Дефинисање предмета истраживања

Континуитет пословања је способност организације да настави са испоруком производа и/или пружањем услуга на прихватљивим, унапред дефинисаним, нивоима након инцидентног догађаја [1]. Инцидентни догађај или инцидент је сваки непланирани и нежељени догађај који може довести до прекида или поремећаја пословних процеса, губитка ресурса, ванредне или кризне ситуације (на пример пожар, квар инсталација, квар техничке опреме, земљотрес, поплава, терористички напад, ванредно или ратно стање, и др.).

Управљање континуитетом пословања (енгл. *Business Continuity Management*, скраћено BCM) јесте холистички процес управљања којим се идентификују потенцијалне претње којима је изложено пословање, утврђују њихови потенцијални утицаји на пословне активности, и дефинише оквир за развијање отпорности организације и способности ефикасног опоравка од последица инцидентног догађаја. То је континуирани процес који мора бити у складу са свим променама у пословању организације. На тај начин се штите интереси кључних заинтересованих страна, репутација организације и њен бренд.

На основу анализе литературе, може се закључити да нема довољно података о моделима управљања континуитетом пословања. ISO 22301 стандард дефинише смернице за успостављање, примену, одржавање и унапређење континуитета пословања у произвољној организацији [1], али не дефинише поступке и методе који се могу применити у пракси. Дисертација уводи нови појам у постојећу научно-истраживачку област: управљање континуитетом електронског пословања (енгл. *e-Business Continuity Management*, скраћено eBCM) који се односи на организације које користе савремене технологије електронског пословања. Основни циљ истраживања је развој модела који дефинише општи оквир за успостављање и континуирано унапређење eBCM-а.

Модел у складу са ISO 22301 стандардом, обухвата методе за дефинисање важних компонената система управљања континуитетом пословања (енгл. *Business Continuity Management System*, скраћено BCMS):

1. Метод за спровођење анализе утицаја на пословање,
2. Метод за процену ризика у вези са континуитетом електронског пословања,
3. Метод за израду плана континуитета пословања,
4. Метод за континуирано унапређење BCMS-а.

Анализа утицаја на пословање је саставни део BCMS<sup>1</sup>-а и има за циљ утврђивање нивоа критичности пословних процеса са становишта континуитета пословања и њихове међузависности, утврђивање неопходних ресурса који су потребни за одвијање кључних

---

<sup>1</sup> У складу са SRPS ISO 22301:2012 преводом ISO 22301:2012 стандарда на српски језик, скраћеница BCMS се не преводи [169].

пословних процеса, процену финансијских и оперативних утицаја на целокупно пословање организације у случају прекида у раду сваког од идентификованих кључних пословних процеса и утврђивање циљних параметара опоравка кључних пословних процеса (најдужи прихватљив прекид, циљна тачка опоравка, циљно време опоравка).

Процена ризика у вези са континуитетом електронског пословања је уско повезана са анализом утицаја на пословање и најчешће се реализује паралелно. Процена ризика обухвата анализу и вредновање ризика који могу довести до прекида у пословању организације. Анализа ризика обухвата идентификовање потенцијалних претњи и рањивости, а вредновање ризика обухвата одређивање потенцијалног утицаја и вероватноће настанка ризика, као и израчунавање вредности ризика над ресурсима кључних пословних процеса.

Важна компонента ВСМС-а је *План континуитета пословања* (енгл. *Business Continuity Plan*, скраћено ВСП). То је документ који дефинише поступке у кризној ситуацији којима се организација усмерава да одговори, да се опорави и да настави са пословањем на унапред дефинисаном нивоу активности/пружања услуга након инцидентног догађаја.

Развој савремених технологија електронског пословања значајно утиче на промене у пословању организација, па самим тим и на управљање континуитетом пословања у организацији. Параметри модела за адаптивно управљање континуитетом електронског пословања треба да омогуће прилагођавање ВСМС-а променама окружења у коме организација послује. У оквиру докторске дисертације анализирани су и истражени потенцијални параметри модела, укључујући и следеће:

- критеријуми за рангирање производа и услуга организације,
- критеријуми за утврђивање степена критичности пословних процеса/функција,
- потенцијалне групе претњи и рањивости којима је изложено пословање,
- прихватљив ниво ризика за организацију,
- саставни делови плана континуитета пословања.

## 1.2 Циљеви истраживања

Примарни циљ докторске дисертације је истраживање могућности побољшања управљања континуитетом електронског пословања путем развоја модела који ће олакшати успостављање континуитета електронског пословања и, захваљујући адаптивној компоненти, омогућити успешније управљање континуитетом електронског пословања. Пошто се технологије електронског пословања брзо развијају, предложени модел треба да буде флексибилан и прилагодљив променама у пословном окружењу организација.

Циљеви истраживања су:

- дефинисање новог концепта управљања континуитетом електронског пословања (енгл. *e-Business Continuity Management*, скраћено eBCM),
- проучавање карактеристика и могућности постојећих модела за управљање континуитетом пословања,
- дефинисање модела за адаптивно управљање континуитетом електронског пословања у складу са променама у окружењу у коме послује организација,
- дефинисање метода за спровођење анализе утицаја на пословање,

- дефинисање метода за процену ризика у вези са континуитетом електронског пословања,
- дефинисање метода за израду плана континуитета пословања,
- дефинисање метода за континуирано унапређење BCMS-а,
- примена предложеног модела за адаптивно управљање континуитетом електронског пословања у пракси,
- прикупљање и анализа резултата вредновања ефикасности предложеног модела у пракси.

### 1.3 Полазне хипотезе

**Главна хипотеза истраживања:** Могуће је развити модел адаптивног управљања континуитетом електронског пословања који је прилагодљив променама у окружењу у коме послује организација, чија примена олакшава успостављање континуитета електронског пословања и омогућава успешније управљање континуитетом електронског пословања.

Помоћне хипотезе истраживања су:

1. Модел дефинише јасан и ефикасан поступак за успостављање континуитета електронског пословања (eBCM).
2. Модел свеобухватно сагледава специфичности пословања организације, а посебно употребу савремених технологија електронског пословања.
3. Модел олакшава успостављање континуитета пословања у организацији која користи савремене технологије електронског пословања.
4. Модел омогућава адаптивно управљање континуитетом електронског пословања у складу са променама у окружењу у коме послује организација.
5. Модел доприноси повећању позитивног става према управљању континуитетом електронског пословања у организацији.

Помоћне хипотезе истраживања представљају основу адаптивног eBCM-а.

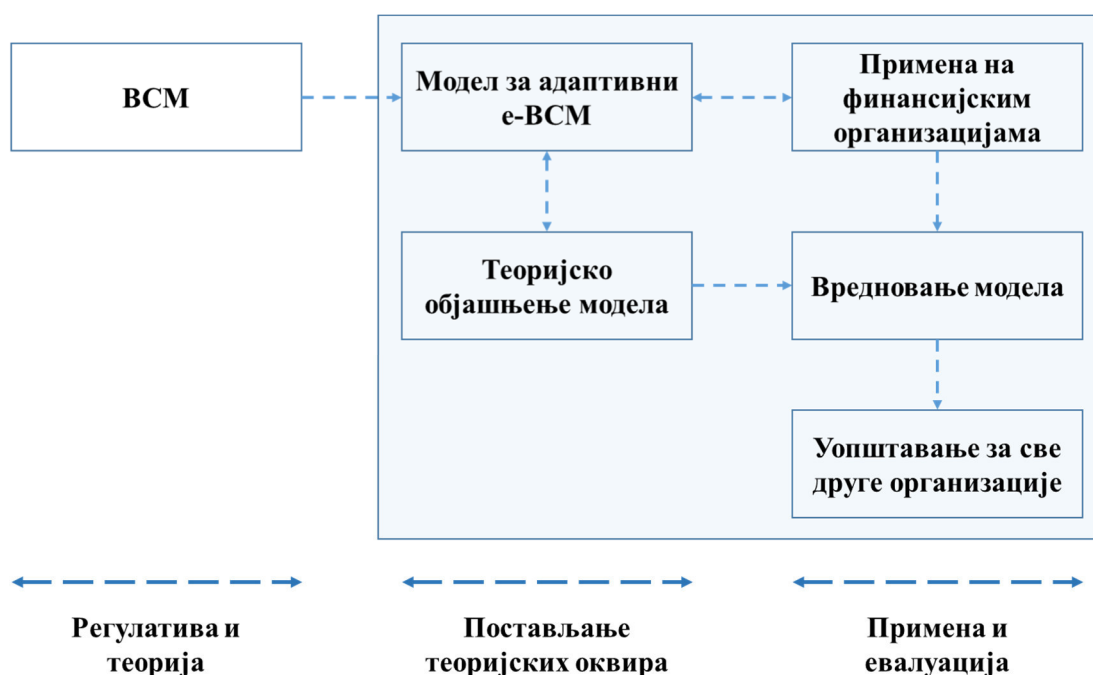
### 1.4 Методологија истраживања

Методологија истраживања у дисертацији обухватила је сложен и организован поступак истраживања полазећи од логичких начела и принципа по прецизно утврђеним фазама рада. У оквиру истраживања коришћене су следеће опште и посебне научне методе:

- Систематизовано прикупљање и анализа постојећих научних резултата из области управљања континуитетом пословања;
- Систематизација и анализа постојећих модела за управљање континуитетом пословања;

- Дефинисање модела адаптивног управљања континуитетом електронског пословања у складу са променама у окружењу у коме послује организација;
- Примена развијеног модела у три организације које делују у финансијском сектору у Србији;
- Вредновање развијеног модела за адаптивно управљање континуитетом електронског пословања путем упитника и интервјуа у организацијама у којима је модел примењен;
- Статистичке методе прикупљања и обраде података добијених путем упитника и интервјуа (основне статистичке анализе и *Partial Least Squares Structural Equation Modeling*, скраћено PLS-SEM анализа);
- Методе научног објашњења (анализа, синтеза, апстракција и генерализација).

Модел адаптивног управљања континуитетом електронског пословања је настао комбинацијом теоријског и практичног рада. Модел је еволуирао са сваком следећом применом. На слици 1 приказане су фазе у истраживању.



Слика 1 - Фазе у истраживању

У експерименталном делу извршена је оцена развијеног модела за адаптивно управљање континуитетом електронског пословања. Добијени резултати на основу експеримента потврдили су хипотезу да је могуће развити модел адаптивног управљања континуитетом електронског пословања који је прилагодљив променама у окружењу у коме послује организација.

Ово истраживање се може класификовати по општости као посебно, по критеријуму својства предмета као комплексно, по припадности науци као интердисциплинарно, а по актуелности предмета као актуелно истраживање.

Резултати истраживања су презентовани текстуално (описивањем) и графички (приказивањем путем табела, слика и графикона).

## 1.5 Структура и организација дисертације

У првом поглављу дефинисани су предмет истраживања, циљеви, методологија и полазне хипотезе. У другом поглављу дефинисано је управљање континуитетом електронског пословања, дефинисани су типови инцидената, дат је приказ регулативе и међународних стандарда у вези са управљањем континуитетом пословања, анализирани су постојећи модели и методолошки оквири за управљање континуитетом пословања и дефинисане су карактеристике модела за управљање континуитетом пословања.

У трећем поглављу дефинисан је модел адаптивног управљања континуитетом електронског пословања који се састоји од 12 параметара и 4 метода модела. Све компоненте модела су детаљније описане. Параметри модела су: Циљеви управљања континуитетом пословања, Делокруг BCMS-а, Контекст организације, Потенцијалне претње, Присутне рањивости, Скала за дефинисање трајања прекида у раду, Финансијски утицај, Оперативни утицаји, Нивои критичности пословних процеса, Категорије финансијских вредности ресурса, Прихватљив ниво ризика и Класе приоритета ризика. Методи модела дефинишу кључне елементе BCMS-а: Метод за спровођење анализе утицаја на пословање, Метод за процену ризика у вези са континуитетом електронског пословања, Метод за израду плана континуитета пословања, и Метод за континуирано унапређење BCMS-а.

У четвртном поглављу анализирани су резултати примене предложеног модела у пракси, а у петом поглављу наведени су научни и стручни доприноси докторске дисертације. Будућа истраживања су наведена у поглављу шест, а у поглављу седам је дат закључак.

На крају докторске дисертације дат је списак коришћене литературе, прилози документа и биографија аутора.



## 2 Управљање континуитетом електронског пословања

### 2.1 Електронско пословање

Развој интернета и електронска револуција, као последица комерцијализације интернета почетком деведесетих година прошлог века, довели су до развоја електронског пословања као новог пословног модела заснованог на коришћењу савремених информационо-комуникационих технологија [2]. Електронско пословање је резултат примене савремених информационо-комуникационих технологија: интернет технологија, мобилних технологија, *cloud computing*-а и рачунарских мрежа следеће генерације (енгл. *Next generation networks*), као и концепата развијених на поменутиим технологијама: интернет интелигентних уређаја (енгл. *Internet of things*), прикупљање и масовна обрада великих количина података (енгл. *Big data*) и свеprisутно рачунарство (енгл. *Ubiquitous computing*). Управо због тога се у контексту пословања савремене информационо-комуникационе технологије називају и технологије електронског пословања или скраћено технологије е-пословања.

„Данас се електронско пословање у ширем смислу односи на скуп електронских услуга и примену савремених информационих технологија у образовању, здравству, јавној управи, науци и другим областима људског деловања“ [2].

Савремене информационо-комуникационе технологије и њихов такоређи свакодневни развој, утичу на промене у пословању организација и стварају нове пословне моделе. Основне карактеристике електронског пословања и њихов утицај на пословање организације дате су у табели 1 [2], [3].

**Табела 1 - Основне карактеристике електронског пословања**

<b>Карактеристика електронског пословања</b>	<b>Утицај на пословање организације</b>
Свеprisутност (енгл. <i>Ubiquity</i> ) - пословање је омогућено у било које време и са било које локације	Првенствено утиче на тржиште које није више ограничено физичком локацијом организације
Глобални обухват (енгл. <i>Global reach</i> ) – савремене информационо-комуникационе технологије су присутне свуда	Превазилазе се географске, временске, културне и националне границе – потенцијално тржиште је цео свет
Универзални стандарди (енгл. <i>Universal standards</i> ) – првенствено се односи на интернет	Интернет стандарди су присутни свуда и омогућавају универзалну платформу за развој електронског пословања
Информационо богатство (енгл. <i>Richness</i> ) – информације су доступне у текстуалном, аудио и видео формату	Обједињене видео, аудио и текстуалне поруке утичу на развој маркетинга и омогућавају нове маркетиншке стратегије

## Карактеристика електронског пословања Утицај на пословање организације

Интерактивност (енгл. <i>Interactivity</i> ) - технологије електронског пословања омогућавају интеракцију са корисницима/клијентима	Корисници/ клијенти постају фокус пословања и активни учесници у процесу испоруке производа/услуге
Квалитет информација (енгл. <i>Information density</i> ) – развој технологија електронског пословања смањује цену и повећава квалитет информација	Цене обраде, чувања и преноса информација се смањују, док се тачност и благовремена доступност информација повећава
Персонализација (енгл. <i>Personalization/ Customization</i> ) – технологије електронског пословања омогућава креирање персонализованих порука индивидуалним корисницама и групама корисника	Персонализација маркетиншких порука и производа/сервиса у односу на индивидуалне карактеристике клијента
Друштвене мреже (енгл. <i>Social technology</i> ) – технологије друштвених мрежа омогућавају да корисници генеришу садржај	Друштвене мреже утичу на развој нових пословних модела у коме корисници креирају садржај и начин дистрибуције информација правећи нове и учвршћујући постојеће везе (унутар друштвених мрежа)

Електронско пословање омогућава организацијама да унапреде интерне процесе и интеракцију са трећим странама коришћењем савремених информационо-комуникационих технологија. Значајне користи и покретачи развоја електронског пословања су [4]:

- Повећање продаје услед приступа већем тржишту (нови клијенти) и квалитетнијом корисничком подршком (постојећи клијенти),
- Смањење трошкова маркетинга захваљујући продаји путем интернета,
- Смањење трошкова везаних за ланац снабдевања (краћи период наручивања, мање залиха),
- Смањење административних трошкова (аутоматизација пословних процеса) и
- Бројне нематеријалне користи као што су промоција брэнда, бржи и бољи одзив маркетинга, квалитетније управљање односима са јавношћу, боље информисање, бржи развој производа и квалитетнији кориснички сервис.

Поред нових праваца у пословању, савремене информационо-комуникационе технологије стварају и нове ризике у пословању, а посебно ризике у вези са континуитетом пословања [5]–[8]. Ту посебно треба истаћи ризике везане за безбедност информација, имајући у виду количину, брзину креирања и доступност информација у савременом пословању. Што је организација више зависна од савремених технологија, то је подложнија утицајима свих типова инцидената [9]. Употреба савремених информационо-комуникационих технологија ствара пословне системе који су сложени, због чега се сматрају природно (инхерентно) ризичним [6]. Један од циљева континуитета пословања у таквим околностима постаје и

способност прилагођавања новим ризицима које доноси примена савремених информационо-комуникационих технологија, како би се заштитили ови природно ризични системи [6].

Из свега наведеног можемо закључити да развој електронског пословања, као последица развоја савремених информационо-комуникационих технологија (технологија е-пословања), утиче на развој и промену приступа у управљању континуитетом пословања (BCM) која ствара потребу да се дефинише нови правац истраживања: управљање континуитетом електронског пословања (eBCM).

## 2.2 Континуитет електронског пословања

У складу са дефиницијом из [1], континуитет пословања је способност организације да настави са испоруком производа и/или пружањем услуга на прихватљивим, унапред дефинисаним, нивоима активности након инцидентног догађаја. Управљање континуитетом пословања је ефикасан вид предострожности у пословању са циљем ублажавања последица инцидентних догађаја и развијања отпорности организације на могуће инцидентне догађаје [10].

Управљање континуитетом пословања (BCM) се као посебна дисциплина развија од 1970-их година као одговор на техничке и оперативне ризике којима су организације изложене током опоравка од инцидентних догађаја [11]. Herbane дефинише четири историјске фазе у развоју управљања континуитетом пословања [11]:

1. **Фаза новог законодавства – „прикривени долазак“** обухвата период од средине 1970-их до средине 1990-их година чији почетак је обележио амерички Закон против подмићивања у иностранству (*US Foreign Corrupt Practices Act, FCPA*) [12] из 1977. године. Иако је донет првенствено ради спречавања и гоњења случајева корпоративног подмићивања страних званичника, FCPA је покренуо доношење низа прописа који су имплицитно или експлицитно захтевали увођење BCM у организације и развој индустрије опоравка информационих система јер су се подаци све више чували у електронском облику што је захтевало обезбеђивање процеса за израду резервних копија и опоравак података. Прописи су се у почетку углавном односили на финансијски сектор [13], [14], али су се убрзо проширили и на сектор здравства [15], телекомуникација [16], јавни сектор [17] и критичну инфраструктуру [18].
2. **Фаза настајања стандарда – „шири утицај“** обухвата период од средине 1990-их година до 2001. године и обележена је појавом стандарда намењених свим привредним гранама. У оквиру ове фазе локални стандарди су се трансформисали у међународне стандарде кроз развој ISO/IEC интернационалне организације. Међу значајнијим документима насталим у овој фази су „*Control objectives for information and related technology [COBIT]*“, верзија 4.0 из 1992. године, прописан од стране организација *IT Governance Institute (ITGI)* и *Information Systems Audit and Control Association (ISACA)*, и NFPA 1600 стандард „*Standard on disaster/emergency management and business continuity programs*“ дефинисан прво као сет препорука 1995. године, а затим и као стандард 2000. године од стране *National Fire Protection Association (NFPA)*.
3. **Фаза после 11. септембра 2001. године (9/11) – „убрзање и фокус“** обухвата период од 2002. до 2005. године и започела је великом кризом која је уследила после терористичких напада у Њујорку и Вашингтону, САД, у септембру 2001. године.

Догађаји од 11. септембра имали су утицај на широк спектар организација и сектора мимо финансијског сектора и владиних агенција. Дошло је до поновне процене континуитета пословања организација и њихове спремности за катастрофе великих размера, а посебно у доменима процене ризика и управљања кризном ситуацијом. Током ове фазе приметно је убрзање у доношењу смерница, прописа и стандарда у вези са континуитетом пословања, и то посебно у финансијском, јавном и комуналном сектору, како у Америци, тако и у остатку света [19]–[25].

4. **Фаза интернационализације** – „конкурентски стандарди и пробој“ обухвата период од 2006. године до данас и обележена је увођењем стандарда и смерница које превазилазе индустријске и националне границе. Стандарди и смернице који су се појавили у овој фази истичу важност сарадње између организација у кризним ситуацијама [26]–[28].

Употреба савремених информационо-комуникационих технологија у електронском пословању је довела до нових критеријума поузданости и доступности информација. Корисници данас очекују да им електронски сервиси буду на располагању 24/7 (24 сата дневно, седам дана у недељи). Појединци, организације и друштва све више зависе од сложених и динамичких информационих система уз помоћ којих треба поуздано да пружају важне сервисе и услуге [29].

ISO/IEC 25000 стандард, познат под називом SQuaRE (енгл. *System and Software Quality Requirements and Evaluation*) [30], дефинише поузданост информационих система и софтвера као „степен до којег систем, производ или компонента обавља одређене функције под одређеним условима током одређеног временског периода“. У складу са истим стандардом, „поузданост се састоји од следећих поткарактеристика:

- Зрелост (енгл. *maturity*) – степен до којег систем, производ или компонента задовољава потребе за поузданошћу у нормалном раду;
- Доступност (енгл. *availability*) - степен до којег је систем, производ или компонента оперативан и доступан када је то потребно за употребу;
- Толеранција на грешке (енгл. *fault tolerance*) - степен до којег систем, производ или компонента раде онако како је предвиђено упркос присутности грешака у хардверу или софтверу;
- Обнављање (енгл. *recoverability*) - степен до којег производ или систем у случају прекида у раду или квара може опоравити податке који су директно погођени и поново успоставити жељено стање система“ [30].

За крајње кориснике доступност је један од важних аспеката квалитета електронског сервиса. Доступност у основи значи да сервис „ради“ или „не ради“. Доступност сервиса се израчунава једноставном математичком формулом [31]:

$$(1) \quad \text{Доступност} = \frac{\text{Време нормалног рада}}{(\text{Време нормалног рада} + \text{Време прекида у раду})}$$

Доступност сервиса се најчешће изражава у процентима, нпр. 99,999% или „пет деветки“. У табели 2 дат је преглед значења „броја деветки“ и периода недоступност, тј. прекида у раду сервиса на годишњем нивоу.

**Табела 2 - Доступност сервиса као функција „броја деветки“ (извор: [31], [32])**

Број деветки	Доступност	Тип система са аспекта доступности	Трајање прекида у раду на годишњем нивоу (у минутима)	Практично тумачење трајања прекида у раду на годишњем нивоу
1	90%	Неуправљачки	52596.00	5 недеља
2	99%	Управљачки	5259.60	4 дана
3	99.9%	Добро управљачки	525.96	9 сати
4	99.99%	Толеранција на грешке	52.60	1 сат
5	99.999%	Висока доступност	5.26	5 минута
6	99.9999%	Веома висока доступност	0.53	30 секунди
7	99.99999%	Ултрависока доступност	0.05	3 секунде

Различити информациони сервис и апликације захтевају различите нивое доступности. Висока доступност од 99,999% („пет деветки“) уобичајено се сматра очекиваном доступношћу за критичне системе [32].

С тим у вези, и ослањајући се на дефиницију континуитета пословања [1], континуитет електронског пословања можемо дефинисати као способност организације да настави са пружањем електронских услуга на прихватљивим, унапред дефинисаним, нивоима поузданости и доступности након инцидентног догађаја [33].

### 2.2.1 Типови инцидената

Инциденти се дешавају свуда у свету и то најчешће онда када их најмање очекујемо [34]. Већина организација ће искусити неки тип инцидента, било да се ради о нестанку електричне енергије, прекиду у раду информационог система, поплави, пожару или прекиду у раду телекомуникационих веза. Оно што је основна непозната околност није „да ли ће се прекид десити“, већ „када ће се прекид десити“ [9].

Постоји три основна типа инцидента: природне катастрофе, инциденти изазвани људским фактором и несреће/технолошки инциденти [35], [36]. Сви ови типови инцидената могу утицати на ресурсе организације и онемогућити организацију да нормално испоручује своје производе и услуге. Типови инцидената дефинисани су у табели 3.

Табела 3 - Типови инцидената

Тип инцидента	Опис
Природне катастрофе (енгл. <i>natural hazards</i> )	Инциденти настали под утицајем елементарних непогода или катастрофа. Примери: пожар, поплава, удар грома, земљотрес, итд.
Инциденти изазвани људским фактором (енгл. <i>human-caused hazards</i> )	Инциденти настали чињењем или нечињењем, свесним или несвесним деловањем запослених, странака или других лица. Обухватају и инкриминисане радње, девијантна или асоцијална понашања и/или злоупотребу и кршење прописаних норми и процедура у вези са физичком безбедношћу и безбедношћу информација. Примери: злоупотребе информационог система, злоупотреба класификованих информација, превара, проневера, крађа, разбојништво, терористички напад итд.
Несреће и технолошки инциденти (енгл. <i>accidents and technological hazards</i> )	Инциденти у вези са техничком инфраструктуром организације. Примери: нестанак основних енергената (електричне енергије, воде, горива, итд.), квар опреме, прекид комуникација, прекид у раду информационог система, итд.

## 2.2.2 Регулатива

Међу законима и прописима од међународног значаја, који обухватају аспекте управљања континуитетом пословања, издвајају се:

- ***The European Programme for Critical Infrastructure Protection (EPCIP)*** - После две године јавне расправе [37], Европска унија донела је директиву 2008. године о идентификацији и заштити европске критичне инфраструктуре (ЕКИ) - „*Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*“ [38]. У складу са овом директивом, свака ЕКИ локација мора да има оперативни план безбедности у склопу кога ће се идентификовати важна имовина, анализу ризика засновану на главним сценаријима претњи и рањивости сваке имовине, као и идентификацију, избор и одређивање приоритета противмера и поступака у кризним ситуацијама.
- ***Solvency II (Directive 2009/138/EC)*** [39] - Европски парламент и Савет Европе су 2009. године усвојили Директиву о покретању и обављању послова осигурања и реосигурања. Ово је основни акт којим се уређује делатност осигурања у Европској унији на основу кога државе чланице дефинишу националне регулативе. Један од главних аспеката Директиве је транспарентност пословања која се обезбеђује објављивањем прописаних информација кроз Извештај о солвентности и финансијском стању (*SFCR-Solvency and Financial Condition Report*). Извештај између осталог обухвата систем управљања ризицима и профил ризика.
- ***High Level Principles for Business Continuity*** - Базелски комитет за супервизију банака (енгл. *Basel Committee for Banking Supervision*, скраћено BCBS), при Међународној банци за поравнања (енгл. *Bank for International Settlements*, скраћено BIS), 2006. године је објавио смернице које дефинишу важне принципе континуитета пословања [40]. Како је BIS у власништву 60 централних банака из свих делова света, документ је настао са циљем побољшања глобалне отпорности финансијског система на могуће инцидентне догађаје. Смернице дефинишу седам важних принципа који се заснивају на традиционалним концептима ефикасног управљања континуитетом пословања:
  1. Највише руководство организације је одговорно за управљање континуитетом пословања;
  2. Организације треба посебно да размотре и планирају пословање у случају инцидентних догађаја великих размера;
  3. Финансијске организације треба да успоставе циљеве опоравка који су у складу са оперативним ризицима њиховог пословања;
  4. Важан део планова континуитета пословања је дефинисање правила интерне и екстерне комуникације, у циљу успешног управљања кризном ситуацијом и одржавања поверења јавности;
  5. Финансијске институције треба да дефинишу и посебне прекограничне комуникационе протоколе имајући у виду све већу међузависност финансијских система на глобалном нивоу;
  6. Како би се обезбедила ефикасност планова континуитета пословања потребно је периодично спровођење њиховог тестирања и, у складу са резултатима, утврђивање потребних побољшања;
  7. Регулаторна тела треба да укључе у своје редовне контроле пословања финансијских институција и контролу управљања континуитетом пословања.

- **Basel II** [41] - Базелски комитет за супервизију банака је 2004. године у циљу отклањања недостатака Базела I [42] и даљег унапређења стабилности међународног банкарског система, усвојио ревидирани оквир (енгл. *Framework*). Између осталог, Базел II пружа низ могућности за одређивање капиталних захтева за кредитни ризик и оперативни ризик како би банке и супервизори могли да одаберу приступе који су најприкладнији за њихово пословање и инфраструктуру њиховог финансијског тржишта. Оперативни ризик се дефинише као „ризик губитка који настаје услед неадекватних или неуспелих унутрашњих процеса, људи и система или спољних догађаја“.
- **Basel III** [43] - Базелски комитет за супервизију банака је као последицу светске економске кризе после неколико година ревизија актуелних докумената, 2011. усвојио коначну верзију Базел III оквира под називом „*Basel III: A global regulatory framework for more resilient banks and banking systems*“. Међу најзначајнијим новинама издвајају се увођење минималних стандарда за управљање ризиком ликвидности и побољшање процеса идентификовања свих врста ризика.

Наведена регулатива од међународног значаја се углавном односи на финансијске институције (изузев [38]), али се може применити на све организације од значаја, што посебно важи за принципе континуитета пословања дефинисане у [40].

У већини земаља постоји регулатива која од организација, а посебно од финансијских институција, захтева да изграде планове континуитета пословања како би се ограничили губици у случају озбиљнијих прекида у раду информационих система и осталих инцидентних ситуација. Међу најважнијим прописима у САД спадају „*Implementing Recommendations of the 9/11 Commission Act of 2007*“ [44], „*Sarbanes-Oxley Act (SOX)*“ [45], „*Consumer Credit Protection Act (CCPA)*“, *Section 2001 Title IX* („*Electronic Fund Transfer Act*“) [46], „*E-Government Act of 2002*“, *Title III* („*Federal Information Security Modernization Act*“) [47], у Канади „*Emergency Management and Civil Protection Act*“ [48], а у Великој Британији „*Civil Contingencies Act (CCA)*“ [49].

*Implementing Recommendations of the 9/11 Commission Act of 2007* [44] закон Сједињених Држава из 2007. године законодавно регулише планове континуитета пословања и акредитацију и сертификацију тих планова од стране овлашћених организација.

*Sarbanes-Oxley Act (SOX)* [45] закон Сједињених Држава из 2002. године се првенствено односи на јавна предузећа, а у мањем делу и на компаније у приватном власништву. Закон дефинише нове стандарде у рачуноводству са циљем заштите инвеститора побољшањем тачности и поузданости информација које компаније објављују. Настао је као одговор на многобројне корпоративне и рачуноводствене афере, и сматра се законом које је стао на пут корпоративним преварама. Једна од најважнијих мера које доноси је лична одговорност највишег руководства компаније за тачност финансијских извештаја. У складу са овим Законом, највише руководство компаније је одговорно и за континуитет пословања. Закон између осталог дефинише и основу за успостављање управљања оперативним ризицима [50].

*Electronic Fund Transfer Act* је подсекција IX (енгл. *Title IX*) закона *Consumer Credit Protection Act (CCPA)* [46] која утврђује права, обавезе и одговорности учесника у системима који користе електронски трансфер средстава. Закон захтева од финансијских институција да на одређен начин дефинишу трансакције приликом електронских преноса средстава, као и да



спровode ревизије података укључујући и податке са продајних места. У складу са овим Законом, план континуитета пословања треба да задовољи „разуман стандард сигурности“ (енгл. „reasonable standard of care“).

*Federal Information Security Modernization Act (FISMA)* је подсекција III (енгл. *Title III*) закона *E-Government Act of 2002* [47] која дефинише детаљне захтеве за процену ризика, одређивање нивоа сигурности који су потребни да би се заштитили подаци, периодично тестирање и процену контрола и техника безбедности информација.

*Emergency Management and Civil Protection Act* [48] закон у Канади дефинише законодавни оквир и овлашћења која су на располагању за поступање у ванредним ситуацијама на националном нивоу.

*Civil Contingencies Act (CCA)* [49] закон у Великој Британији се односи на јавни сектор. Закон дефинише различите категорије одговорних за управљање у кризним ситуацијама и даје мандат свим институцијама од значаја, као и локалним властима, да дефинишу управљање континуитетом пословања.

Народна банка Србије је усвајањем Одлуке [51], [52] дефинисала оквир за управљање информационом системом финансијских институција, и посебан акценат је ставила на управљање континуитетом пословања. У складу са овом Одлуком, финансијске институције у Републици Србији су у обавези да, ради обезбеђивања несметаног и континуираног функционисања свих својих значајних система и процеса, као и ограничавања губитака у ванредним ситуацијама, успоставе процес управљања континуитетом пословања који је заснован на анализи утицаја на пословање и процени ризика.

Слична регулатива постоји и у околним земљама. У Хрватској Закон о саставу цивилне заштите [53] прописује да сва правна лица морају имати планове континуитета пословања, док се Смјернице за управљање информацијским саставом у циљу смањења оперативних ризика [54], које је усвојила Хрватска народна банка 2006. године односе само на банкарски сектор. У Републици Српској постоји Одлука о управљању информационом системима у банкама [55] коју је 2017. године усвојила Агенција за банкарство Републике Српске. Слична одлука постоји и у Федерацији Босне и Херцеговине, такође усвојена 2017. године од стране Агенције за банкарство Федерације БиХ [56].

### **2.2.3 Међународни стандарди за управљање континуитетом пословања**

ISO 22301 стандард [1] данас се сматра основним стандардом за управљање континуитетом пословања, из следећих разлога:

- први међународни стандард усмерен искључиво на континуитет пословања,
- може се применити на било коју организацију, без обзира на њену величину, делатност и локацију,
- јасно дефинише циљеве и делокруг управљања континуитетом пословања,
- ставља велики акценат на ангажовање руководства организације (Plan-Check-Do-Act модел) и
- подразумева континуирано унапређење.

ISO 22301 стандард је усвојен 2012. године [1], а ревидиран 2019 [57], [58]. У писању овог стандарда учествовало је преко 60 земаља, чиме је сумирана добра пракса на међународном нивоу и обухваћени су сви важни аспекти управљања континуитетом пословања [59].

ISO 22301 фамилија стандарда обухвата следећа документа:

- ISO 22300:2018 „*Security and resilience - Vocabulary*“ [60] - речник који дефинише 277 израза који се користе у стандардима у вези са безбедношћу и отпорношћу (енгл. *Resilience*);
- ISO 22301:2019 стандард „*Security and resilience - Business continuity management systems – Requirements*“ [57] - дефинише захтеве за планирање, успостављање, примену, функционисање, надгледање, преглед, одржавање и континуирано унапређивање документованог система управљања како би се заштитили, смањили вероватноћу појаве, припремили се, одговорили на могуће инциденте и опоравили се од њих када настану;
- ISO 22311:2014 стандард „*Societal Security – Video Surveillance – Export Interoperability*“ [61] – дефинише стандардни формат за прикупљање, чување и обраду дигиталног садржаја из система видео-надзора;
- ISO/TR 22312:2011 стандард „*Societal Security – Technological Capabilities*“ [62] - попис постојећих технологија које су релевантне за стандардизацију у оквиру области друштвене безбедности;
- ISO 22313:2012 стандард „*Societal security — Business continuity management systems — Guidance*“ [63] - смернице за успостављање програма реаговања на инцидент и континуитета пословања, подржава имплементацију стандарда ISO 22301;
- ISO 22315:2014 стандард „*Societal security — Mass evacuation — Guidelines for planning*“ [64] - смернице за планирање масовне евакуације у смислу успостављања, примене, надгледања, оцењивања, прегледа и побољшања спремности;
- ISO/TS 22317:2015 стандард „*Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*“ [65] - упутство за спровођење анализе утицаја на пословање, подржава имплементацију стандарда ISO 22301;
- ISO/TS 22318:2015 стандард „*Societal security — Business continuity management systems — Guidelines for supply chain continuity*“ [66] - упутство за успостављање програма континуитета пословања ланаца снабдевања;
- ISO 22320:2018 стандард „*Security and resilience — Emergency management — Guidelines for incident management*“ [67] – дефинише минималне захтеве за ефикасно реаговање на инцидент и пружа основе успостављања одговорности, контроле, оперативних информација, координације и сарадње у оквиру тима за реаговање на инцидент;
- ISO 22322:2015 стандард „*Societal security — Emergency management — Guidelines for public warning*“ [68] - дефинише смернице за развој, управљање и спровођење обавештавања јавности пре, за време и после инцидента;

- ISO 22324:2015 стандард „*Societal security — Emergency management — Guidelines for colour-coded alerts*“ [69] – дефинише смернице за употребу боја приликом информисања о потенцијалној опасности и за изражавање тежине ситуације;
- ISO 22397:2014 стандард „*Societal security — Guidelines for establishing partnering arrangements*“ [70] - дефинише смернице за успостављање партнерских уговора између организација у вези са управљањем инцидентима који утичу на друштвену безбедност; обухвата принципе и описује процес планирања, развоја, примене и ревизије партнерских уговора;
- ISO 22398:2013 стандард „*Societal security — Guidelines for exercises*“ [71] – дефинише смернице за планирање, спровођење и побољшавање пројеката тестирања који се могу организовати у оквиру програма тестирања; намењен је за употребу свима који су одговорни за обезбеђивање компетенција запослених организације, посебно руководству организације и особама одговорним за управљање програмима и пројектима тестирања;
- ISO/PAS 22399:2007 стандард „*Societal security - Guideline for incident preparedness and operational continuity management*“ [26] – дефинише опште смернице за развој приправности на инциденте и систем управљања у циљу обезбеђења континуитета пословања; омогућава организацији да на доследан начин оцени своју отпорност на инциденте.

ISO 22301 стандард је настао од британског стандарда BS 25999:

- BS 25999-1:2006 Правилник [28]
- BS 25999-2:2007 Спецификација [27]

Основни елемент система управљања континуитетом пословања, према BS 25999 стандарду, јесте управљање програмом, као контролним елементом дефинисања области одговорности и обезбеђивања континуираних пословних процеса.

Поред наведених општеприхваћених стандарда, постоји још много других релевантних стандарда и смерница везаних за управљање континуитетом пословања. Неки од значајнијих су:

- *Good Practice Guidelines (GPG)* [72] — смернице које је дефинисао *Business Continuity Institute (BCI)* представљају најбољу глобалну праксу у животном циклусу управљања континуитетом пословања;
- *BSI-Standard 100-4: Business Continuity Management* [73] — стандард дефинисан од стране *Federal Office for Information Security (BSI)*, Централне агенција савезне владе у Немачкој, дефинише успостављање управљања у ванредним ситуацијама, како би се осигурао континуитет пословања;
- *COBIT 5* стандард „*Control Objectives for Information & Related Technology 5*“ [74] — дефинише општеприхваћене циљеве управљања информационим системима; обухвата принципе, политике, оквире, процесе, организациону структуру, културу, етику, понашање, информације, услуге, инфраструктуру, апликације, људе, вештине и компетенције;

- ITIL V3 (скраћеница од „*IT Infrastructure Library*“) објављен је 2007. године од стране британске владине агенције *Office of Government Commerce (OGC)*; састоји се од пет публикација [75]–[79] и представља глобални стандард за дизајн, имплементацију и управљање услугама информационих технологија (скраћено ИТ) на основу најбољих пракси из јавног и приватног сектора; садржи опсежну јавно доступну специјалистичку документацију о планирању, пружању и подршци ИТ услугама; управљање континуитетом ИТ услуга је део књиге „Дизајн услуга“ [78] у оквиру ITIL V3 верзије;
- ISO 9001:2015 стандард „*Quality management systems — Requirements*“ [80] – дефинише захтеве за систем менаџмента квалитетом у циљу доследног пружања производа и услуга, обезбеђивања усаглашености са важећим законским и регулаторним захтевима, и побољшавања задовољства корисника ефикасном применом система, укључујући процесе за унапређење система;
- ISO/IEC 27001:2013 стандард „*Information technology - Security techniques -- Information security management systems - Requirements*“ [81] – дефинише детаљне захтеве за систем управљања безбедношћу информација (енгл. *Information Security Management System*, скраћено ISMS), са мањим фокусом на процес управљања континуитетом пословања, писање и спровођење планова континуитета пословања, оквир за планирање континуитета пословања, спровођење анализе утицаја на пословање и тестирање и одржавање планова континуитета пословања;
- ISO/IEC 27002:2013 (некадашњи ISO/IEC 17799) стандард „*Information technology - Security techniques - Code of practice for information security controls*“ [82] – дефинише смернице за стандарде и праксе управљања безбедношћу информација унутар организације, укључујући избор, примену и управљање контролама у складу са окружењем и безбедносним ризицима којима је изложена организација;
- ISO/IEC 27003:2017 стандард „*Information technology — Security techniques — Information security management systems — Guidance*“ [83] – дефинише критичне аспекте потребне за успешан дизајн и имплементацију система управљања безбедношћу информација (ISMS), у складу са ISO/IEC 27001:2013;
- ISO/IEC 27004:2016 стандард „*Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*“ [84] - дефинише смернице за процену перформанси безбедности информација и ефикасности система управљања безбедношћу информација (ISMS), како би се испунили захтеви ISO/IEC 27001:2013;
- ISO/IEC 27035-1:2016 „*Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*“ [85] и ISO/IEC 27035-2:2016 „*Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*“ [86] – дефинише основне концепте и фазе управљања инцидентима у вези са безбедношћу информација, дефинише структурирани приступ у откривању, пријављивању, оцењивању и реаговању на инциденте, као и примену научених лекција;
- ISO/IEC 27036-1:2014 стандард „*Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*“ [87] - дефинише упутства намењена заштити информација и информационих система у контексту односа са добављачима, из перспективе и купаца и добављача;

- ISO/IEC 27036-2:2014 стандард „*Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements*“ [88] – дефинише основне захтеве у вези са безбедношћу информација за дефинисање, примену, функционисање, надгледање, преглед, одржавање и унапређење односа између купца и добављача;
- ISO/IEC 27036-3:2013 стандард „*Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*“ [89] - дефинише смернице у вези са безбедношћу информација у ланцу снабдевања информационим и комуникационим технологијама;
- ISO/IEC 27031:2011 стандард „*Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*“ [90] - описује концепте и принципе спремности информационих и комуникационих технологија (ИКТ) унутар организације за континуитет пословања и пружа оквир метода и процеса за идентификацију и спецификацију свих аспеката побољшања ИКТ спремности организације да осигура континуитет пословања;
- NIST SP 800-34 стандард „*Contingency Planning Guide for Federal Information Systems*“ [91] објављен 2010. од стране National Institute of Standards and Technology (NIST) – дефинише основне принципе планирања и развијања способности одговора на инциденте укључујући прелиминарно планирање, спровођење анализе утицаја на пословање, избор алтернативних локација и дефинисање стратегије опоравка;
- ISO/IEC 25000:2014 стандард „*Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE*“ [30] – даје смернице за употребу SQuaRE серије међународних стандарда у вези са захтевима и проценом квалитета софтвера;
- ISO/IEC 20000-1:2018 стандард „*Information technology — Service management — Part 1: Service management system requirements*“ [92] - дефинише захтеве за успостављање, примену, одржавање и континуирано побољшање система управљања услугама; захтеви наведени у овом документу укључују планирање, дизајн, транзицију, испоруку и унапређење услуга како би се задовољили захтеви купаца и испоручила вредност;
- ISO/IEC TS 17021-6:2014 стандард „*Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems*“ [93] - дефинише посебне захтеве за компетенције особа укључених у процес сертификације система управљања континуитетом пословања (BCMS);
- ISO 31000:2018 стандард „*Risk management — Guidelines*“ [94] – дефинише основне принципе и опште смернице за управљање ризиком;
- ISO GUIDE 73:2009 „*Risk management — Vocabulary*“ [95] - дефинише генеричке појмове у вези са управљањем ризиком;
- IEC 61508:2010 стандард „*Functional Safety of Electrical, Electronic and Programmable Electronic Safety Related Systems*“ [96] – дефинише захтеве за управљање ризицима приликом развоја софтвера за аутоматизацију процеса;

- IEC 60300-1:2014 стандард „*Dependability management - Part 1: Guidance for management and application*“ [97] - успоставља оквир и дефинише смернице за управљање поузданошћу производа, система, процеса или услуга које укључују хардвер, софтвер и људске ресурсе или било које интегрисане комбинације ових елемената.

## 2.3 Циљеви управљања континуитетом електронског пословања

Основни циљ управљања континуитетом електронског пословања је заштита пословања која се огледа у:

1. идентификовању потенцијалних претњи којима је изложено пословање организације и њихове могуће утицаје на пословне процесе,
2. развијање способности организације да се ефикасно опорави од последица потенцијалних инцидената и
3. обезбеђивање заштите интереса заинтересованих страна и репутације организације.

У данашње време пословање сваким даном постоје све глобалније, сложеније и ризичније [98]. Управљање континуитетом електронског пословања, као одговор на поменуте изазове, успоставља планове континуитета пословања који су базирани на идентификованим ризицима прекида пословања, обезбеђује проактивно управљање и развија спремност на одговор у случају инцидентне ситуације.

Одсуство управљања континуитетом пословања може довести до губитка прихода или чак и до престанка пословања организације [99]. Аутори у наведеном раду истичу да у оквиру процеса успостављања континуитета пословања свака организација треба да размотри следећа важна питања:

- Који је најгори могући сценарио који може да задеси наше пословање?
- Са које локације бисмо сутра обављали пословање уколико нас задеси катастрофа?
- Колико брзо наше пословање може да дође до тачке са које нема повратка?
- Колико брзо након инцидентног догађаја можемо да успоставимо редовно пословање?

Приликом дефинисања плана континуитета пословања неопходно је разумевање посебних потреба организације, њеног контекста пословања, али и заштита података организације као једног од најважнијих производа пословања [100].

## 2.4 Систем управљања континуитетом пословања

Управљање континуитетом пословања је дефинисано системом управљања континуитетом пословања (BCMS) који обухвата организациону структуру, политику, активности планирања, нивое одговорности, поступке, процесе и ресурсе којима организација умањује ризике свог пословања [1]. BCMS дефинише смернице за примену, спровођење, праћење, преиспитивање, одржавање и побољшавање континуитета пословања организације.

BCMS, у складу са међународним стандардом ISO 22301, омогућава:

- успостављање континуитета пословања организације,
- управљање способношћу организације за опоравак од последица инцидената,
- праћење и преиспитивања перформанси и ефикасности управљања континуитетом пословања,
- континуирано унапређење управљања континуитетом пословања на основу објективног мерења.

Важне компоненте BCMS-а, као и сваког другог систем менаџмента, су:

- Политика континуитета пословања;
- Људи са дефинисаним улогама, одговорностима и овлашћењима;
- Процеси менаџмента (управљања) који се односе на:
  - политику,
  - планирање,
  - примену и функционисање BCMS-а,
  - оцењивање перформанси BCMS-а,
  - преиспитивање BCMS-а од стране руководства организације и
  - унапређење управљања континуитетом пословања;
- Сет докумената који су подложни преиспитивању (ревизији);
- Сви остали процеси менаџмента који су релевантни за управљање континуитетом пословања организације.

## 2.5 Карактеристике успешног управљања континуитетом електронског пословања

Карактеристике успешног управљања континуитетом електронског пословања су висок ниво отпорности (енгл. *Resilience*) организације према могућим инцидентним догађајима, превентивно деловање, инкорпорираност (интегрисаност) и стратешка улога у очувању конкурентске предности.

Висок ниво отпорности организације према могућим инцидентним догађајима подразумева велику могућност успешног опоравка од последица инцидентног догађаја [101]. Организација са високим нивоом отпорности има могућност да [102]:

- реагује на робусан, али и флексибилан начин на широк дијапазон очекиваних, али и неочекиваних претњи,
- ефикасно прати поступак опоравка, укључујући и своје перформансе,
- предвиди ризичне догађаје и препозна пословне могућности и

- извуче поуку из искуства.

Укључивање континуитета пословања у све аспекте пословања битно утиче на успешност управљања континуитетом пословања [103]. Резултати ове студије показују да је интегрисаност континуитета пословања од суштинске важности за умањења негативних последица инцидената, и да чисто технички приступ, која само подразумева постојање планова опоравка, није довољан. Посвећеност и свест о континуитету пословања су потребни на свим организационим нивоима – од највишег руководства до свих запослених у организацији.

Примарна улога система управљања континуитетом пословања је превентивно деловање. Превентивно деловање захтева стратешки приступ, добро разумевање пословних процеса организације и окружења у коме организација послује, подизање свести о значају континуитета пословања код запослених и развијање посебне ВСП културе [5], [104].

Континуитет пословања, поред тога што активно обезбеђује континуитет пословних операција, има и стратешку улогу у очувању конкурентске предности организације [105]. Организације које могу брзо и темељно да се опораве од последица кризе неће имати озбиљније последице по репутацију. Са друге стране, уколико организација није у стању да се брзо опорави од последица инцидената или ако важне заинтересоване стране сматрају да је процес опоравка неефикасан, ефекти по репутацију организације могу бити знатно већи од директних ефеката кризе.

Аутори у раду [106] иду и корак даље и предлажу да делокруг управљања континуитетом пословања обухвати и пословни модел компаније, у циљу холистичког и стратешког приступа ВСМ-а. Њихов предлог стратешког управљање континуитетом пословања се састоји од два дела: (1) очување континуитета пословног модела компаније (очување вредности) и (2) оцењивање и ревидирање пословног модела (стварање вредност).

## **2.6 Модели за управљање континуитетом пословања**

### **2.6.1 Карактеристике модела за управљање континуитетом пословања**

Релевантна литература из јавно доступних база података нуди различите моделе и методолошке оквире (енгл. *Framework*) који се баве разним аспектима успостављања и управљања континуитетом пословања, али недостаје специфичан модел који дефинише практичне кораке и процедуре у успостављању континуитета пословања код организација које користе савремене технологије електронског пословања: интернет, мобилно рачунарство, електронске сервисе, виртуалну инфраструктуру и сл.

Осим тога, детаљи и резултати успостављања континуитета пословања се често сматрају поверљивим информацијама, па организације имају потешкоћа да пронађу опробана искуства и практичне смернице у успостављању е-ВСМ-а.

Након анализе релевантне литературе и доступних истраживачких радова, идентификоване су четири групе ВСМ модела и методолошких оквира. Преглед идентификованих група ВСМ модела и методолошких оквира дат је у табели 4.



**Табела 4 - Преглед идентификованих група ВСМ модела и методолошких оквира**

<b>Р. Бр. Групе</b>	<b>Назив групе и релевантни радови</b>	<b>Карактеристике и предности модела из групе</b>	<b>Недостаци модела из групе</b>
1	Општи модели [9], [99], [103], [105], [107]–[112][113], [114]	Опште смернице, применљиве на произвољне индустрије	Недостају практични кораци за успостављање континуитета пословања, а посебно за спровођење анализе утицаја на пословање и за процену ризика
2	Квантитативни модели [104], [115]–[118]	Модел базиран на статистичким и математичким квантитативним прорачунима	Компликовано за примену у произвољној организацији
3	Доменски специфични модели [119]–[122]	Модел који се баве специфичним индустријама, пословним питањима и захтевима	Приступ је превише специфичан за одређену индустрију или делатност; недостају практични кораци за успостављање континуитета пословања
4	Модел везани за инциденте великих размера [123]–[125]	Модел базиран на утицају природе и људских разарања на градове	Приступ није применљив у произвољној организацији

Након анализе четири идентификоване групе ВСМ модела и методолошких оквира, можемо закључити да недостају практични кораци у успостављању континуитета пословања у организацијама које користе савремене технологије е-пословања. Следећи потенцијални проблеми су идентификовани у постојећим моделима и приступима:

- 1) фокус је искључиво на дефинисању и планирању програма континуитета пословања [109] или искључиво на једном аспекту управљања континуитетом пословања [115], [117], [122], [123],
- 2) недостају практични кораци у успостављању управљања континуитетом пословања [105], [111]–[113], [117], [121] а посебно, недостају практични кораци за спровођење анализе утицаја на пословање и за процену ризика [9], [105], који су битни елементи ВСМС-а,
- 3) приступ је превише специфичан за одређену индустрију или делатност [120], [121] и
- 4) приступ је превише компликован да би се применио у произвољној организацији [115], [117].

Предложени модел адаптивног управљања континуитетом електронског пословања [33], [126] испуњава наведене критеријуме и адресира идентификоване проблеме. Анализиране групе ВСМ модела и методолошких оквира су детаљније описане у наставку овог поглавља, а предложени модел је описан у наредном поглављу (поглавље бр. 3).

## 2.6.2 Општи модели

Прва група ВСМ модела дефинише опште оквире и начине успостављања континуитета пословања који су применљиви у произвољним индустријама.

Један од првих свеобухватних оквира за управљање континуитетом пословања, предложен 2006. године [99], наглашава важност усклађивања ИТ инфраструктуре, података и услуга са укупном пословном стратегијом и свим компонентама ВСМ стратегије. Аутори Gibb и Buchanan су развили методолошки оквир за дефинисање, примену и праћење управљања континуитетом пословања у контексту информационе стратегије. Пословни процеси су високозависни од информација и информационих система. Прекиди у раду информационог система организације поред материјалне штете могу довести до велике репутационе штете. Управљање континуитетом пословања је алат који обезбеђује веће поверење да излази из пословних процеса могу бити испоручени и под утицајем ризика. Њихов методолошки оквир се превасходно бави идентификацијом и управљањем ризицима који прете да поремете најважније пословне процесе, ублажавањем ефеката ових ризика, и обезбеђивањем опоравка пословних процеса без значајног нарушавања пословања организације.

Gibb и Buchanan-ов методолошки оквир обухвата девет (9) фаза које су описане одређеним корацима, активностима, улазима и излазима. Фазе, од којих се неке преклапају, су:

1. Покретање програма управљања континуитетом пословања (обухвата дефинисање повеље управљања континуитетом пословања и плана програма);
2. Покретање пројекта успостављања континуитета пословања;
3. Анализа ризика (обухвата идентификацију ризика, оцену ризика и анализу утицаја на пословање);
4. Одабир метода ублажавања ризика (обухвата трансфер ризика, умањење ризика, прихватање ризика и дефинисање планова опоравка – енгл. *Disaster recovery plans*);
5. Праћење и контрола (преплиће се са преосталим фазама);
6. Примена;
7. Тестирање;
8. Образовање и обука;
9. Преиспитивање.

Овај методолошки оквир даје смернице за планирање и дефинисање планова опоравка који су у складу са информационом стратегијом организације и који на првом месту штите информациону имовину и омогућавају организацији да ефективно опорави кључне пословне системе.

Сличан методолошки оквир за успостављање континуитета пословања је предложио и Cook [9] на основу изучавања релевантне литературе објављене у протеклих 20 година (укупно 105 чланака), спровођења полуструктурираних интервјуа (укупно 21 интервју) са представницима финансијског сектора, сектора производње, хране, институција образовања, здравства, државних органа и организација којима су поверене пословне активности од стране трећих

лица (енгл. *Outsourcers*), као и два практична случаја у којима је методолошки оквир успешно проверен и примењен. Његов методолошки оквир има шест фаза: дефиниција структуре управљања (подршка руководства организације), иницијација (плана), анализа утицаја на пословање са проценом ризика, дизајн плана, тестирање и тренинг, и одржавање.

Значај ИТ инцидената у модерним стратегијама ВСМ-а указана је у [103]. Предложени оквир за управљање континуитетом информационог система (енгл. *Information System Continuity Management*, скраћено ISCM) обухвата спољне захтеве заинтересованих страна, подршку руководства, будност организације и укључивање континуитета пословања у све аспекте пословања како би се уочио и свео на минимум утицај ИТ инцидената на пословање. Аутор истиче да је подршка највишег руководства кључни фактор успешног управљања континуитетом пословања, као и да су посвећеност и свест о континуитету пословања потребни на свим организационим нивоима.

Herbane, Elliott и Swartz су развили проактивни методолошки оквир за управљање континуитетом пословања [105] који је базиран на следећим факторима који повезују управљање континуитетом пословања са стратешким управљањем:

- брзина опоравка: критична детерминанта предности опоравка,
- еластичност: умањење рањивости пословања у вези са ланцем снабдевања и пословне умрежености,
- екстерне обавезе: законске, уговорне и остале обавезе,
- инкорпорираност (интегрисаност): неопходан фактор којим се постиже прелаз од планирања до управљања континуитетом пословања.

Основна идеја њиховог истраживања је да у данашње време - које је окарактерисано растућим претњама (терористички напади, корпоративни финансијски скандали, интернет криминал и променљиви/непредвидиви временски услови) - управљање континуитетом пословања, поред систематског супротстављања последицама прекида пословања, има и стратешки потенцијал. Стратешки потенцијал се огледа у очувању конкурентске предности организације која се постиже способношћу очувања вредности које су створене од стране организације.

Вајгорис предлаже систематски оквир за имплементацију ВСМ-а заснован на концепту системске имплементације „увек доступног“ информационог система (енгл. *“always on”*) [107]. Модел објашњава да данашње организације користе континуиране рачунарске технологије како би понудиле већу доступност и поузданост сервиса својим клијентима.

У студији [108], уз референцу на [1], Sanchez Dominguez износи свеобухватан преглед холистичког оквира за ВСМ, са водичем за његову примену. Аутор закључује да одговарајућа примена ВСМ-а мора бити усклађена са свим кључним производима и процесима организације.

Комплексност пословања и промене пословних процеса, улога, односа и примена савремених технологија присиљавају пословне системе да постојеће ВСМ стратегије прилагоде новим условима и окружењу [109]. Wong предлаже инкрементални концепт који укључује три врсте стратегија: процесно оријентисане, програмски оријентисане и стратегије управљања отпорношћу организације. За сваку од ових стратегија, аутор предлаже листу специфичних техника.

Lindström, Samuelsson и Hägerfors су развили методолошки оквир који је првенствено намењен руководству организације како би на прави начин разумели њихову улогу у успостављању континуитета пословања [110]. Методолошки оквир је настао као резултат практичних пројеката и дефинише седам (7) фаза које се посебно примењују на нивоу организације и на нивоу појединачних организационих делова: од одређивања оквира и циљева управљања континуитетом пословања, преко идентификовања критичних пословних процеса и процене ризика, до дефинисања планова опоравка, тренинга запослених, као и редовног тестирања и одржавања. Фазе уједно представљају и нивое зрелости организације у погледу успостављања континуитета пословања.

Savage дефинише неопходне елементе плана континуитета пословања и разматра важна питања која је потребно адресирати како би се испунили стварни захтеви опоравка пословних процеса након инцидентног догађаја [111]. У складу са његовим методолошким оквиром, који је базиран на анализи утицаја на пословање и процени ризика, неопходно је да се приликом писања плана континуитета пословања размотре следећа питања:

- алтернативне локације на којима је могуће обављати пословање у кризној ситуацији,
- начини опремања алтернативних локација,
- неопходне компоненте информационог система и пословни процеси/пословне функције које од њих зависе,
- минимални ниво корисничког сервиса у кризној ситуацији,
- неопходни оперативни/административни послови,
- евентуалне полисе осигурања у вези са инцидентним догађајима и њиховим последицама,
- неопходни људски ресурси за спровођење плана,
- локације на којима се чувају копије важне документације,
- начин комуникације са медијима и осталим важним заинтересованим странама у кризној ситуацији,
- дефинисање трошкова у вези са имплементацијом плана,
- начини тестирања и ревизије плана,
- непосредан одговор на инцидент и координација са хитним службама и органима власти.

Tammineedi је дефинисао методолошки оквир за успостављање континуитета пословања у складу са BS 25999 стандардом [112] који има основне три фазе: припрема (енгл. *Pre-Event Preparation*), управљање инцидентом и успостављање континуитета пословања (енгл. *Post-Event Continuity*). Он посебан акценат ставља на организациону структуру, тј. на улоге и тимове који су ангажовани у кризној ситуацији. Посебно је интересантан *Business Continuity Maturity Model*®, који је развила организација *Virtual Corporation* на основу којег је могуће проценити зрелост успостављеног управљања континуитетом пословања у организацији [127]. Модел дефинише шест нивоа зрелости: саморазвијајући, на нивоу одсека, кооперативан, у складу са стандардом, интегрисан и синергистичан (видети слику 2). Сличне нивое зрелости система управљања континуитетом пословања дефинишу и [128].

Нивои зрелости управљања континуитетом пословања	Ниво 1 Само-развијајући	Ниво 2 На нивоу одсека	Ниво 3 Кооперативан	Ниво 4 У складу са стандардом	Ниво 5 Интегрисан	Ниво 6 Синергистичан
<b>Корпоративне компетенције</b>	<b>Карактеристике организације на сваком нивоу зрелости</b>					
Руководство	ВН	Н	С	В	В	В
Свест запослених	ВН	Н	Н	С	В	В
Структура ВСМ програма	ВН	Н	Н	С	В	В
Свеприсутност програма	ВН	ВН	Н		С	В
Метрике	ВН	Н	С	С	В	В
Алокација ресурса	ВН	Н	С	В	В	В
Координација	ВН	Н	Н	С	В	В
<b>Садржај ВСМ програма</b>	<b>Карактеристике управљања континуитетом пословања на сваком нивоу зрелости</b>					
Управљање инцидентима	ВН	Н	С	В	В	В
Опоравак инф. система	ВН	Н	С	В	В	В
Опоравак пословања	ВН	Н	С	В	В	В
Управљање безбедношћу	ВН	Н	С	В	В	В

Веома ниска	Ниска	Средња	Висока
-------------	-------	--------	--------

Слика 2 - Нивои зрелости управљања континуитетом пословања у организацији (извор: [127])

Већина радова представља практичну имплементацију модела и методолошких оквира унутар компанија, класификованих као велике. Чини се да су мала и средња предузећа (МСП) испала из интереса, иако, представљају удео од 99% у Немачкој и од преко 95% у Европској унији [129]. Аутори у [129] испитују зашто је ВСМ недовољно заступљено у малим и средњим предузећима и између осталог закључују да су сложеност и трошкови имплементације битни фактори.

Botha и Von Solms су развили теоријски модел ВСР методологије која може да се примени и у великим и малим организацијама и предлажу циклични приступ у планирању континуитета пословања који у свакој од итерација покрива одређене аспекте континуитета пословања [113]. Анализом постојећих методологија, аутори посебно наглашавају недостатак смерница за имплементацију постојећих ВСР методологија, и као одговор предлажу циклични приступ у примени методологије која обухвата седам (7) фаза:

1. Планирање пројекта;
2. Спровођење анализе утицаја на пословање (ВИА);
3. Анализа различитих стратегија континуитета пословања;
4. Имплементација одабраних стратегија континуитета пословања;
5. Обуке;
6. Тестирање;
7. Одржавање плана континуитета пословања.

Фазе се примењују у четири циклуса: 1) циклус обезбеђивања резервних копија података, 2) циклус опоравка информационих система, 3) циклус планирања континуитета пословних процеса и 4) циклус имплементације свеобухватног континуитета пословања. Сваки од циклуса обухвата одређене делове свих фаза методологије. Циклуси су раздвојени и примењују се сукцесивно чиме дају могућност произвољној организацији да имплементира ВСР методологију на одређеном нивоу у складу са својим потребама и могућностима.

Cerullo и Cerullo [114] су дефинисали смернице за развој и унапређење плана континуитета пословања (ВСР), који се састоји од три компоненте: анализе утицаја на пословање, плана опоравка од катастрофе (енгл. *Disaster Contingency and Recovery Plan*, скраћено DCRP) и

компоненте за обуку и тестирање. Аутори посебно наглашавају да је тестирање пресудно за развој ефикасног ВСП-а и за процену ефикасности ВСП-а пре него што се догоди стварна инцидентна ситуација.

### 2.6.3 Квантитативни модели

У другој групи ВСМ модела истраживачи предлажу оквире обogaћене статистичким и математичким квантитативним прорачунима. Sahebjamnia, Torabi и Mansouri предлажу оквир за интегрисано планирање континуитета пословања и опоравка од катастрофа ради ефикасног и ефективног наставка и опоравка критичних операција након прекида у раду [104]. Аутори су користили оквирни и интерактивни модел за доношење одлуке у оквиру проблема расподеле ресурса. Предложени модел бави се проблемима одлучивања на свим стратешким, тактичким и оперативним нивоима. Концепт су успешно примењивали у организацији произвођача мењача.

Torabi, Rezaei Soufi и Sahebjamnia су развили методолошки оквир за спровођење анализе утицаја на пословање на структуриран и квантификован начин, који је примењен у организацији за производњу ауто делова [115]. Њихов методолошки оквир користи разне *multi attribute decision making (MADM)* технике и састоји се од следећих корака:

1. Идентификовање и рангирање кључних производа организације (коришћењем теорије графова и унапред дефинисаних критеријума);
2. Идентификовање пословних функција које су неопходне за испоруку кључних производа (WBS методом, тј. хијерархијском структуром);
3. Рангирање пословних функција по критичности на основу унапред дефинисаних критеријума (на сличан начин као и код кључних производа организације);
4. Одређивање циљних параметара опоравка, узимајући у обзир прихватљиви ниво ризика за организацију, за све:
  - а. кључне производе организације и
  - б. критичне функције организације.

Zeng и Zio предлажу интегрисани ВСМ оквир [116] који користи квантитативне метрике кроз фазе заштите, ублажавања, ванредне ситуације и опоравка и примењује их на критични догађај ометања светлости на фарми складишта нафте.

Bryson, Millar, Joseph, и Mobolurin су у свом истраживању показали да MS/OR (енгл. *Management Science/ Operational Research*) методе моделовања могу да се искористе за стратешку подршку у одлучивању приликом избора стратегије опоравка, у оквиру планирања континуитета пословања [117]. Циљ овог модела је да избором одговарајућих потпланова опоравка пословања обезбеди максималну укупну вредност покривености, тј. заштите пословања.

Van de Walle и Rutkowski [118] развили су помоћу fuzzy релационог моделовања прототип система за подршку у одлучивању. Прототип је развијен за потребе управљања континуитетом ИТ услуга, у домену идентификовања ризика и одговарајућих мера њиховог ублажавања. Основни циљ је превазилажење проблема у одлучивању услед различитог сагледавања утицаја, обима и вероватноћа претњи од стране представника разних заинтересованих страна које учествују у процесу.

#### 2.6.4 Доменски специфични модели

Трећа идентификована група BSM модела обухвата моделе који се баве специфичним индустријама, пословним питањима и пословним захтевима. Montshiwa, Nagahira и Ishida су развили BSM оквир посебно прилагођеним сложеним ланцима снабдевања у аутомобилској индустрији [119]. У оквиру истраживања спровели су свеобухватну квантитативну студију која је обухватила 75 произвођача аутомобилских делова у регионима подложним катастрофама и увели нов појам - *Supply Chain Cooperation* (SCC) - у план континуитета пословања (BCP). Они потврђују да је BIA камен темељац BSM-а, јер има снажан утицај на остале факторе и компоненте BSM-а.

Blos, Hoeflich и Miyagi су развили општи методолошки оквир за управљање континуитетом ланца снабдевања: *A General Supply Chain Continuity Framework* [120]. Њихов методолошки оквир обухвата шест фаза: управљање ризицима, анализа утицаја на пословање, развој стратегије управљања континуитетом ланца снабдевања, развој плана континуитета ланца снабдевања, тестирање плана континуитета ланца снабдевања и одржавање плана континуитета ланца снабдевања. Методолошки оквир је заснован на ISO 22301 стандарду и посебно је фокусиран на анализу ризика који могу довести до прекида у ланцу снабдевања. Новина коју уводе у односу на ISO 22301 стандард је осам оперативних параметара у вези са ланцем снабдевања: кориснички сервис, управљање залихама, флексибилност, време пласирања (енгл. *Time to Market*), финансирање, време испоруке (енгл. *Ordering Cycle Time*), квалитет и тржиште. Оперативни параметри се разматрају у свакој од наведених фаза.

Агенција за међународну сарадњу Јапана (*Japan International Cooperation Agency*, JICA) покренула је пројекат дефинисања „*Area BCP (Business Continuity Plan)*“, као новог концепта управљања ризиком од катастрофа у густо изграђеним индустријским зонама [121]. Овај методолошки оквир дефинише координиране мере ублажавања ризика и активности опоравка од стране свих заинтересованих страна, укључујући појединачне организације, менаџере индустријске зоне, локалне власти и администраторе/испоручиоце потребне инфраструктуре, а у циљу континуитета пословања индустријске зоне као целине. Први експериментални „*Area BCP*“ планови дефинисани су у Индонезији, Филипинима и Вијетнаму, где постоје густо изграђене индустријске зоне посебно изложене ризицима од природних катастрофа.

Lozupone [122] је описао концепте плана опоравка информационог система (DR plan) и репликације података у компанијама које пружају ИТ услуге болницама, медицинским лабораторијама и другим здравственим организацијама („*The Medical Record Company*“). Рад је фокусиран на анализи рањивости информационог система и даје одговоре у виду стратегије ублажавања ризика, DR плана и дизајна детекције упада у информациони систем. Аутор посебно наглашава да успостављање планова опоравка није једнократан пројекат. Планови опоравка су „живи“ документи које треба редовно ревидирати и тестирати.

#### 2.6.5 Модели везани за инциденте великих размера

Четврта група BSM модела фокусирана је на утицаје природе и људских разарања на градове. Torabi, Giah и Sahebjamnia [123] предложили су побољшани оквир за процену ризика у контексту BCMS-а, истовремено узимајући у обзир посебне кораке и захтеве BCMS-а. Процена ризика (RA) је, поред BIA, једна од основних компоненти BCMS-а. Аутори су оценили оквир у стварној услужној организацији задуженој за услуге управљања катастрофама у граду Техерану у Ирану. Jinguе и Takehiro [124] дискутују о концепту паметног

управљања континуитетом пословања (енгл. *Smart Business Continuity Management*, скраћено SBCM) на примеру инфраструктуре паметног града за Олимпијске игре у Јапану 2020. Аутори разрађују аспекте сигурности и одрживог развоја инфраструктуре града за предстојеће игре.

Kato и Charoenrat у [125] расправљају о доступности BSM подршке за мала и средња предузећа у ризичним подручјима. У истраживању је учествовало 136 малих и средњих предузећа са Тајланда. Истраживање је показало да иако је ово подручје претрпело значајне катастрофе у периоду од 2004. до 2014. године, управљање континуитетом пословања је на релативно ниском нивоу. Студија указује на значај пружања подршке малим предузећима од стране јавног и приватног сектора, и истиче да основни разлог за недостатак BCP-а нису финансијска ограничења, већ мањак ресурса и недостатак знања.

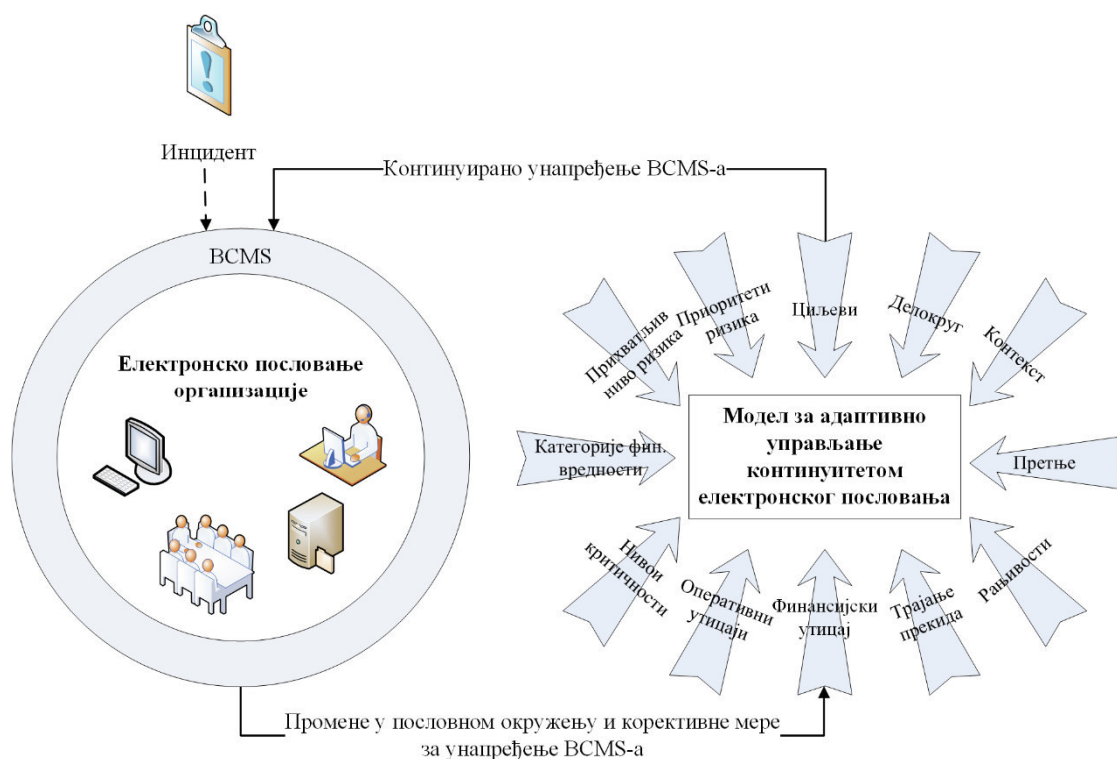


### 3 Развој модела за адаптивно управљање континуитетом електронског пословања

#### 3.1 Модел адаптивног управљања континуитетом електронског пословања

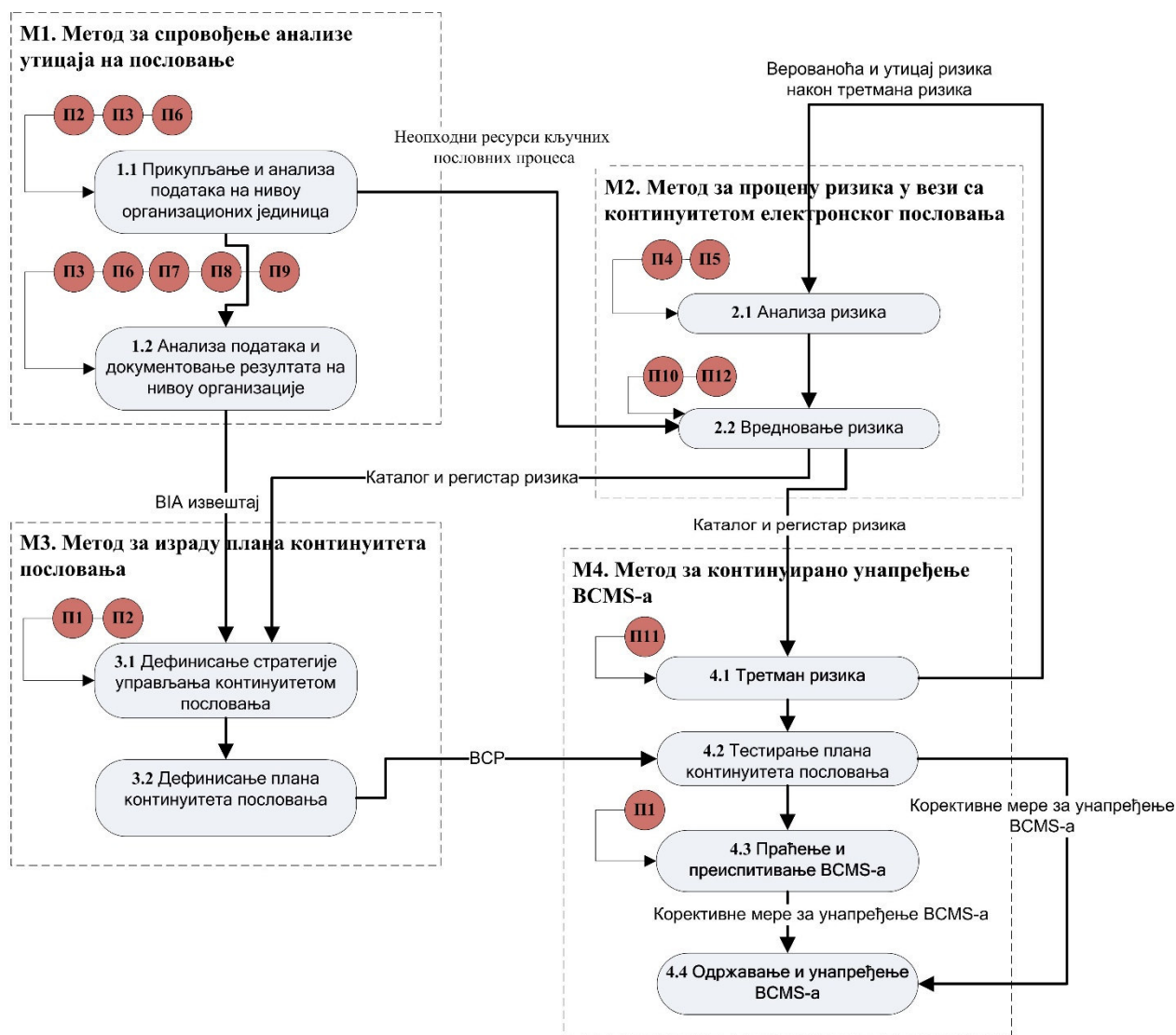
Модел адаптивног управљања континуитетом електронског пословања дефинисан је у складу са ISO 22301 стандардом, након систематског прикупљања, прегледа и анализа литературе о континуитету пословања и постојећих модела. У оквиру истраживања и рада на докторској дисертацији, модел је имплементиран у три организације из финансијског сектора у Србији.

Модел адаптивног управљања континуитетом електронског пословања се састоји од дванаест (12) параметара и четири (4) метода. Модел је концептуално приказан на слици 3, док слика 4 илуструје основне компоненте модела и њихове најважније међузависности.



Слика 3 - Модел адаптивног управљања континуитетом електронског пословања (извор: [33])

Параметри модела осликавају основне карактеристике пословног окружења организације [1], [59], [130], као и главне карактеристике технологија електронског пословања: свеприсутност, глобализација, универзални стандарди, богатство информација, интерактивност, густина информација, персонализација/прилагођавање и употреба друштвених мрежа [3]. Параметри модела су П1) Циљеви управљања континуитетом пословања, П2) Делокруг BCMS-a, П3) Контекст организације, П4) Потенцијалне претње, П5) Присутне рањивости, П6) Скала за дефинисање трајања прекида у раду, П7) Финансијски утицај, П8) Оперативни утицаји, П9) Нивои критичности пословних процеса, П10) Категорије финансијских вредности ресурса, П11) Прихватљив ниво ризика и П12) Класе приоритета ризика.



**Слика 4 - Основне компоненте модела (параметри у круговима; методи у правоугаоницима са испрекиданим ивицама; поступци, као саставни делови метода, у правоугаоницима са заобљеним ивицама) и њихове најважније међузависности (извор: [33])**

У складу са ISO 22301 стандардом, одговор организације на промене у пословном окружењу се заснива на систему управљања континуитетом пословања (BCMS), који штити организацију од потенцијалних инцидентних догађаја (видети слику 3). Методи модела дефинишу кључне елементе BCMS-а:

- M1. Метод за спровођење анализе утицаја на пословање,
- M2. Метод за процену ризика у вези са континуитетом електронског пословања,
- M3. Метод за израду плана континуитета пословања,
- M4. Метод за континуирано унапређење BCMS-а.

Метод M1 за спровођење анализе утицаја на пословање обухвата анализу на нивоу организационих јединица и анализу и документовање резултата на нивоу организације (видети слику 4). У оквиру овог метода на првом месту се идентификују кључни пословни процеси организације. То су пословни процеси који су најзначајнији за остваривање улоге и основних циљева организације. Затим се идентификују потенцијални губици који могу настати као

результат инцидента и утврђује се којом брзином кључни пословни процеси организације морају да се опораве да би поново почели да пружају потпуну пословну функцију након прекида у раду. У склопу овог метода идентификују се и неопходни ресурси за кључне пословне процесе над којима се врши анализа и вредновање ризика у оквиру метода М2 - Метод за процену ризика у вези са континуитетом електронског пословања. Ризици се документују у каталогу и регистру ризика који су неопходан улаз за преостала два метода: Метод за израду плана континуитета пословања (М3) и Метод за континуирано унапређење ВСМС-а (М4). У оквиру метода М3 дефинишу се планови континуитета пословања, док метод М4 обухвата третман ризика, тестирање планова континуитета пословања и све остале активности у циљу одржавања и унапређења ВСМС-а. Сва четири метода модела су описана у наставку овог поглавља.

Модел је потребно прилагодити и применити при свакој промени неког од параметара модела, чиме се омогућава управљање континуитетом електронског пословања које је прилагодљиво променама у пословном окружењу организације. У оквиру Метода за континуирано унапређење ВСМС-а (М4) дефинишу се корективне мере за унапређење ВСМС-а.

Прилагодљивост променама у пословном окружењу организације заједно са корективним мерама за унапређење ВСМС-а обезбеђује адаптивно управљање континуитетом електронског пословања.

### 3.2 Параметри модела

Параметри модела за адаптивно управљање континуитетом електронског пословања дефинисани су у табели 5.

**Табела 5 - Параметри модела**

<b>Р.бр.</b>	<b>Параметар</b>	<b>Опис</b>
П1	Циљеви управљања континуитетом пословања	Дефинише основне циљеве управљања континуитетом пословања
П2	Делокруг ВСМС-а	Дефинише пословне процесе који су обухваћени системом управљања континуитетом пословања
П3	Контекст организације	Обухвата најважније заинтересоване стране и правно-регулаторни оквир организације
П4	Потенцијалне претње	Обухвата списак релевантних претњи по пословање организације
П5	Присутне рањивости	Обухвата списак идентификованих рањивости пословања организације

Р.бр.	Параметар	Опис
П6	Скала за дефинисање трајања прекида у раду	У зависности од природе пословања организације дефинише адекватну временску скалу за анализу последица прекида у раду
П7	Финансијски утицај	Дефинише да ли се у оквиру анализе утицаја на пословање спроводи процена финансијских утицаја на пословање услед прекида у раду
П8	Оперативни утицаји	Дефинише оперативне утицаје који се процењују у оквиру анализе утицаја на пословање
П9	Нивои критичности пословних процеса	Дефинише четири нивоа критичности пословних процеса (врло критичан, критичан, виталан и важан) на основу вредности најдужег прихватљивог прекида (МАО време)
П10	Категорије финансијских вредности ресурса	Дефинише четири категорије финансијских вредности ресурса (врло висока, висока, средња и ниска) на основу новчаних вредности
П11	Прихватљив ниво ризика	Дефинише вредност прихватљивог нивоа ризика за организацију
П12	Класе приоритета ризика	Дефинише четири класе приоритета ризика (врло висок, висок, средњи и низак) на основу вредности ризика

Параметри модела описани су детаљније у наставку поглавља.

### 3.2.1 Циљеви управљања континуитетом пословања

Неопходан предуслов за успешну имплементацију BCMS-а је да циљеви управљања континуитетом пословања буду успостављени и усаглашени са стратешким циљевима организације [59], [99]. Могући циљеви управљања континуитетом пословања су:

- обезбеђивање континуитета пословања организације, а специјално континуитета пословања кључних пословних процеса,
- заштита запослених и других лица, као и материјалних ресурса и друге имовине организације,
- смањење вероватноће настанка прекида пословања уз помоћ BCMS-а и управљања ризиком у вези са континуитетом пословања,
- смањење утицаја на пословање, свођење на прихватљиву меру потенцијалних губитака и смањење потенцијалне штете везане за репутацију организације, у случају кризне ситуације,
- обезбеђење високог степена способности организације за опоравак од последица кризне ситуације,

- очување и одржавање односа са заинтересованим странама,
- обезбеђење финансијских ресурса организације у циљу испуњења законских, уговорних и осталих обавеза.

Циљеви континуитета пословања се најчешће одређују у посебном документу под називом Политика континуитета пословања (енгл. *Business Continuity Policy*), која треба да буде доступна свим заинтересованим странама и адекватно представљена у оквиру организације [1].

### 3.2.2 Делокруг BCMS-а

Потребно је дефинисати делокруг BCMS-а имајући у виду:

- организационе делове,
- пословне функције и
- локације на којима послује организација.

Управљање континуитетом електронског пословања омогућава континуитет пословних процеса који су обухваћени делокругом BCMS-а.

### 3.2.3 Контекст организације

Контекст организације, у складу са [131], обухвата:

- најважније заинтересоване стране и њихов утицај на пословање организације,
- правно-регулаторни оквир.

Процена важности идентификованих заинтересованих страна реализује се на основу матрице утицаја и интереса заинтересоване стране [132], [133]. На слици 5 приказана је једна варијанта ове матрице.

<b>Утицај</b>	Велики	7	8	9
	Средњи	3	4	6
	Мали	1	2	5
		Мали	Средњи	Велики
		<b>Интерес</b>		

**Слика 5 - Матрица утицаја и интереса заинтересоване стране**

Утицај заинтересоване стране (мали, средњи, велики) јесте показатељ колико заинтересована страна утиче на пословање организације. Интерес заинтересоване стране (мали, средњи, велики) показатељ је колико је пословање организације важно или корисно за идентификовану заинтересовану страну.

### 3.2.4 Потенцијалне претње

Претња (енгл. *threat*) јесте сваки потенцијално остварив нежељен и/или штетан догађај. Претње у присуству рањивости (видети поглавље 3.2.5) постају ризици. Ризике, па самим тим и претње, могуће је класификовати на разне начине [36], [134]. У наставку овог поглавља дефинисана је једна од могућих класификација претњи посебно прилагођена организацијама која користи савремене технологије електронског пословања.

Могућа класификација потенцијалних претњи по пословање организације:

#### 1. Природне катастрофе:

- поплава,
- пожар,
- гром,
- ветар,
- земљотрес;

#### 2. Инциденти изазвани људским фактором

##### 2.1. Екстерни инциденти изазвани људским фактором:

- рат, друштвени немири, нарушена безбедност државе,
- терористички напад,
- епидемија,
- штета проузрокована од треће стране,
- отмица запосленог,
- уцена запосленог,
- разбојништво,
- претећи позив, писмо/дојава о бомби,
- медијско деловање усмерено негативно према организацији,
- шпијунажа, прислушкивање, социјални инжењеринг,
- неовлашћени приступ информационом систему,
- неовлашћени физички приступ,
- експлозивне направе;

##### 2.2. Интерни инциденти изазвани ненамерни људским деловањем:

- пожар,
- штрајк запослених,
- кршење закона, подзаконских аката и унутрашњих правних аката организације,
- неизвршење уговорних обавеза,
- неовлашћено инсталирање софтвера,
- неовлашћено коришћење ауторских материјала,
- неовлашћено коришћење софтвера,
- одлазак запосленог,
- повреда на раду,
- погрешан унос података;

##### 2.3. Интерни инциденти изазвани намерним људским деловањем:

- активирање малициозног програма,
- злоупотреба информационог система,
- превара, проневера, крађа,

- прикривање корисничког идентитета,
- разоткривање лозинки,
- фалсификовање записа, уништење записа,
- физичко уништење медија,
- злоупотреба класификованих информација;

### 3. Несреће и технолошки инциденти

#### 3.1. Инциденти на инфраструктури:

- нестанак електричне енергије,
- прекид комуникација,
- екстремна влажност ваздуха и температура;

#### 3.2. Инциденти на информационо-комуникационој инфраструктури:

- прекид у раду информационог система,
- престанак рада треће стране,
- електромагнетно зрачење,
- квар опреме,
- коришћење застарелих верзија софтвера,
- коришћење неауторизованог или нетестираног софтвера,
- коришћење неауторизованог или нетестираног хардвера,
- нерасположивост ресурса,
- грешке у апликацијама - софтверска грешка,
- губитак података.

#### 3.2.5 Присутне рањивости

Рањивост (енгл. *vulnerability*) јесте слабост у информационом систему, имовини или осталим ресурсима која може бити искоришћена, тј. експлоатисана од стране одређене претње. У наставку овог поглавља предложена је једна од могућих класификација рањивости по угледу на класификацију ризика дефинисану у [135].

Могуће рањивости организације која користи савремене технологије електронског пословања су:

##### 1. Стратешке рањивости:

- јединствена тачка прекида,
- мањак људских ресурса,
- неадекватна заштита физичког приступа,
- неадекватна локација,
- неадекватни уговори са трећим странама,
- неадекватно радно окружење,
- неадекватно управљање безбедношћу и здрављем на раду,
- нејасно одређене надлежности унутар организације,
- немотивисани или незадовољни запослени,
- непостојање адекватне класификације и заштите информација;

## 2. Организационе рањивости:

- дуг период за набавку добара и/или услуга,
- информације изложене неовлашћеним лицима,
- коришћење заједничког административног налога,
- неадекватна интерна правила,
- неадекватна обука запосленог,
- неадекватна овлашћења запосленог,
- неадекватна процедура за пријем запосленог,
- неадекватно управљање инцидентима,
- недостатак кризног менаџмента,
- некомпетентност запосленог,
- непримерен надзор рада запослених;

## 3. Рањивости информационог система:

- безбедносни пропусти,
- екстерно одржавање,
- компликовано корисничко упутство,
- неадекватан информациони систем,
- неадекватан ниво ИТ сервиса,
- неадекватне лозинке,
- неадекватно документоване пословне апликације,
- неадекватно лиценцирање,
- неадекватно одржавање,
- неадекватно тестирање,
- неадекватно управљање корисничким правима,
- неадекватно управљање променама,
- нејасни и непотпуни захтеви за развој пословних апликација,
- некомпетентно тестирање софтвера
- непримерено раздвајање надлежности,
- непримерено управљање капацитетом,
- нераздвајање тестног од продукционог окружења,
- неукидање корисничких налога после раскида радног односа,
- позната грешка (bag) у софтверу,
- прекомерна овлашћења администратора система;

## 4. Оперативне рањивости:

- грешка запосленог,
- запослени не поштује политике безбедности,
- коришћење туђег налога,
- неадекватно руковање опремом,
- непоштовање интерних правила,
- непоштовање правила заштите од пожара;



## 5. Техничке и инфраструктурне рањивости:

- дозвољено коришћење приватних преносивих медија и уређаја,
- каблирање - могуће оштећење кабловске инсталације,
- коришћење преносивих медија,
- неадекватно расходовање ИТ опреме,
- неадекватно чување резервних копија података,
- неажурирање база за заштиту од малициозног кода,
- незаштићен пренос информација,
- некомпатибилност опреме,
- некомпатибилност софтвера,
- неконтролисано скидање података са интернета (енгл. *download*),
- неконтролисано копирање електронских података,
- немогућност приступа ресурсима,
- неодговарајућа заштитна полиса (енгл. *Firewall*),
- неодговарајуће управљање РКИ инфраструктуром,
- непостојање алтернативног извора енергије,
- непостојање резервних копија података,
- нередовно ажурирање „закрпа“ и надоградњи софтвера,
- нередовно тестирање резервних копија података,
- преносива опрема изложена крађи,
- укључена аутоматска надоградња софтвера,
- употреба застареле опреме,
- фабрички постављени кориснички налози и лозинке.

### 3.2.6 Скала за дефинисање трајања прекида у раду

Скала за дефинисање трајања прекида у раду је параметар који у зависности од природе пословања организације дефинише адекватну временску скалу за анализу последица прекида у раду. Пример скале за дефинисање трајања прекида у раду је: 1 минут, 5 минута, 30 минута, 1 сат, 4 сата, 8 сати, 24 сата, 48 сати, 72 сата, 7 дана, 14 дана.

### 3.2.7 Финансијски утицај

Овај параметар дефинише да ли се у оквиру анализе утицаја на пословање спроводи процена директног финансијског утицаја услед прекида у раду пословних процеса. Процене директних финансијских утицаја није увек могуће прецизно спровести.

### 3.2.8 Оперативни утицаји

Овај параметар дефинише оперативне утицаје који се оцењују у оквиру анализе утицаја на пословање услед прекида у раду пословних процеса. Могући оперативни утицаји су:

- репутација организације,
- поверење грађана,
- поверење уговорних страна,
- новчани токови,

- законске обавезе,
- повећање расхода,
- морал запослених и сл.

### 3.2.9 Нивои критичности пословних процеса

Нивои критичности пословних процеса дефинишу се на основу вредности најдужег прихватљивог прекида (енгл. *Maximum Acceptable Outage*, скраћено МАО).

Постоји четири нивоа критичности пословних процеса и овај параметар их дефинише помоћу вредности МАО времена:

1. Врло критични: пословни процеси неопходни за остваривање најважнијих функција организације; расположивост ових процеса захтева се у најкраћем могућем временском року након инцидента (нпр. МАО време < 2 сата);
2. Критични: пословни процеси неопходни за остваривање важних функција организације; расположивост ових процеса потребно је обезбедити у најкраћем могућем року, одмах након успешног успостављања процеса из најкритичније групе (нпр. МАО време < 24 сата);
3. Витални: пословни процеси неопходни за нормално пословање организације (нпр. МАО време < 72 сата);
4. Важни: организација може пословати одређено време без ових пословних процеса (нпр. МАО време < 7 дана).

### 3.2.10 Категорије финансијских вредности ресурса

Овај параметар дефинише четири категорије финансијских вредности ресурса (врло висока, висока, средња и ниска) на основу новчаних вредности. Пример могућих вредности дат је табели 6.

**Табела 6 - Пример дефиниције категорија финансијских вредности ресурса**

<b>Финансијска вредност ресурса</b>	<b>Новчани износ</b>
Врло висока	Преко 10.000.000 €
Висока	Од 1.000.000 € до 10.000.000 €
Средња	Од 100.000 € до 1.000.000 €
Ниска	Од 10.000 € до 100.000 €

### 3.2.11 Прихватљив ниво ризика

Параметар дефинише вредност прихватљивог нивоа ризика за организацију. Израчунавање вредности ризика је дефинисан у оквиру метода за процену ризика у вези са континуитетом пословања (видети поглавље 3.4.2). Вредност ризика може бити нумеричка вредност од 1 до 64.

Ризици чија је вредност мања од прихватљивог нивоа ризика сматрају се прихватљивим и као такви не улазе у даљу обраду ризика (видети поглавље 0), тј. у њиховом случају није потребно умањивати могуће последице остваривања претње. Организација свесно прихвата постојање ових ризика.

### 3.2.12 Класе приоритета ризика

Параметар дефинише четири класе приоритета ризика (врло висок, висок, средњи и низак) на основу вредности ризика. Пример могућих вредности дат је у табели 7.

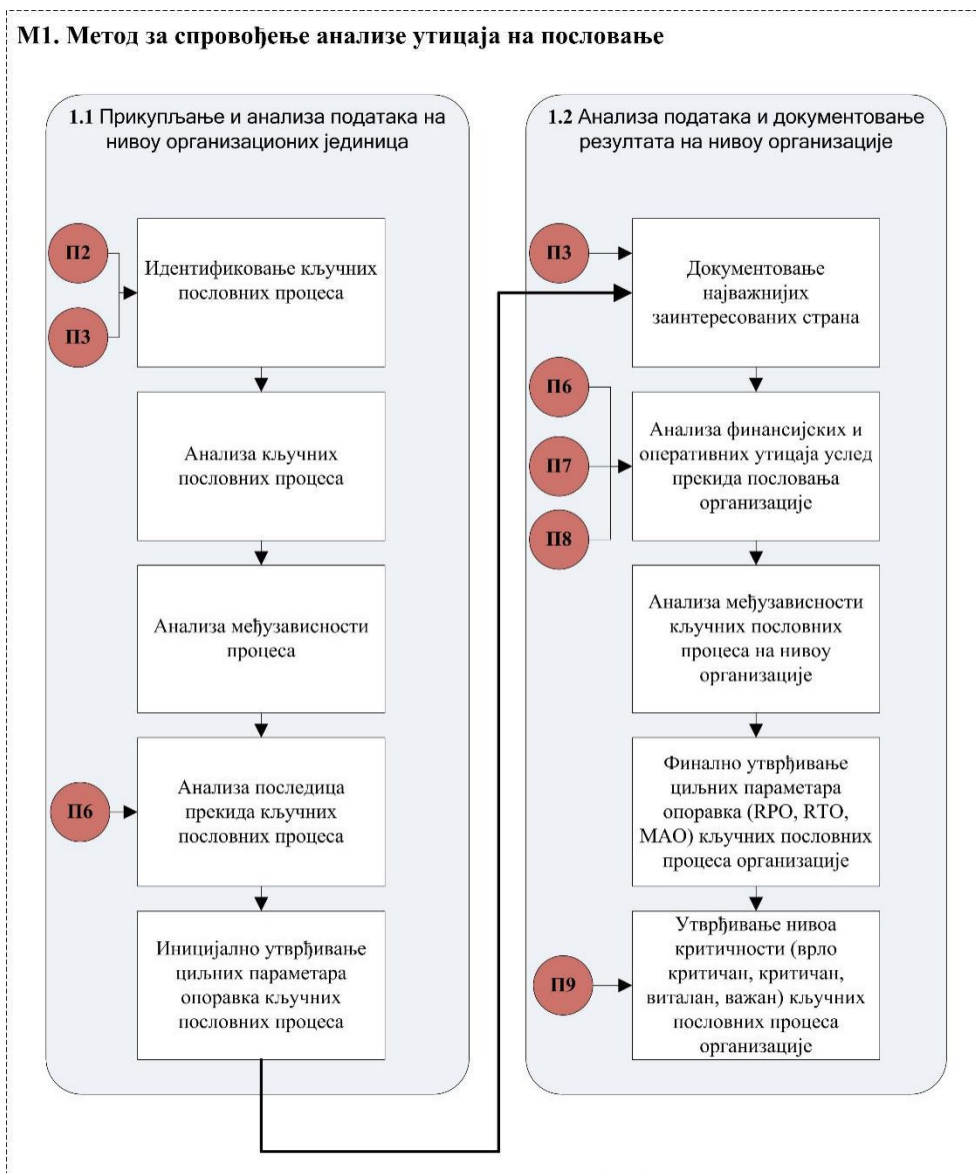
Табела 7 - Пример дефиниције класа приоритета ризика

Приоритет ризика	Вредност ризика
Врло висок	Већа од 41 ( $\geq 41$ )
Висок	31 -40
Средњи	21-30
Низак	Мања од 20 ( $\leq 20$ )

## 3.3 Метод за спровођење анализе утицаја на пословање

Анализа утицаја на пословање (енгл. *Business Impact Analysis*, скраћено BIA) саставни је део свеобухватног BCMS-а. Сврха BIA анализе је идентификација кључних пословних процеса организације и утврђивање којом брзином ти пословни процеси морају да се опораве да би поново почели да пружају потпуну пословну функцију након прекида рада, у случају инцидента. Метод за спровођење анализе утицаја на пословање је приказан на слици 6.

Анализом утицаја на пословање, идентификују се потенцијални губици који могу настати као резултат инцидента. Ови губици могу имати утицај на пословање организације кроз финансијске, оперативне, регулаторне, репутационе и друге губитке [59], [136]. Параметар Финансијски утицај (П7), дефинише да ли се у склопу BIA анализе процењују финансијски губици по пословање, док параметар Оперативни утицаји (П8) дефинише све оперативне утицаје који се процењују. Поред тога, у склопу BIA анализе идентификују се неопходни ресурси за кључне пословне процесе, и дефинишу се приоритети приликом опоравка.



**Слика 6 - Метод за спровођење анализе утицаја на пословање**

Циљеви анализе утицаја на пословање су:

- идентификовање кључних пословних процеса организације, тј. пословних процеса који су најзначајнији за остваривање улоге и основних циљева организације,
- утврђивање неопходних ресурса који су потребни за одвијање кључних пословних процеса,
- процена финансијског и оперативног утицаја на целокупно пословање организације у случају прекида у раду сваког од идентификованих кључних пословних процеса, према најгорем могућем сценарију,
- утврђивање нивоа критичности кључних пословних процеса са становишта континуитета пословања и њихове међузависности,
- утврђивање циљних параметара опоравка (најдужи прихватљив прекид, циљна тачка опоравка, циљно време опоравка) кључних пословних процеса и
- утврђивање приоритета приликом опоравка (поновног успостављања кључних пословних процеса након инцидентног догађаја).

Метод за спровођење анализе утицаја на пословање, слично као и код [137], обухвата два поступка: Прикупљање и анализу података на нивоу организационих јединица и Анализу података и документовање резултата на нивоу организације.

Прикупљање података и анализа се прво обавља на нивоу организационих јединица (поступак 1.1). Анализирају се само пословни процеси који су обухваћени делокругом ВСМС-а (дефинисано параметром П2), узимајући у обзир најважније заинтересоване стране и правно-регулаторни оквир организације, што је дефинисано параметром Контекст организације (П3). Анализа последица прекида у раду спроводи се у складу са временском скалом (нпр. минути, сати, дани), дефинисаном параметром П6, имајући у виду природу пословања организације.

Резултати се накнадно анализирају и документују на нивоу организације (поступак 1.2). Нивои критичности идентификују се за све кључне пословне процесе на основу вредности њиховог најдужег прихватљивог прекида (МАО време), у складу са параметром П9.

### 3.3.1 Прикупљање и анализа података на нивоу организационих јединица

Први поступак у оквиру метода за спровођење анализе утицаја на пословање је прикупљање и анализа података на нивоу организационих јединица. Поступак се спроводи низом структурираних интервјуа са представницима организационих јединица на основу Упитника анализе утицаја на пословање (VIA упитник) који је дефинисан у **Прилогу 1**. Упитник VIA анализе спроводи се кроз следеће кораке:

1. Улога и основни циљеви организационе јединице
2. Идентификација кључних пословних процеса
3. Анализа кључних пословних процеса
  - 3.1. Основне карактеристике кључних процеса
  - 3.2. Неопходни ресурси кључних пословних процеса
  - 3.3. Обрада критичних података (енгл. *Critical Record Management*)
  - 3.4. Важно извештавање
4. Анализа међузависности процеса
  - 4.1. Зависност од других процеса (енгл. *Upstream Dependencies*)
  - 4.2. Утицај на друге процесе (енгл. *Downstream Dependencies*)
5. Анализа последица прекида кључних пословних процеса
  - 5.1. Директни финансијски утицај
  - 5.2. Оперативни утицаји
  - 5.3. Опоравак кључних пословних процеса
6. Иницијално утврђивање циљних параметара опоравка.

Упитници за спровођење анализе утицаја на пословање се попуњавају посебно за сваку организациону јединицу из делокруга ВСМС-а са циљем да се на свеобухватни начин сагледају размере потенцијалних губитака у случају инцидентних и ванредних ситуација.

Поступак прикупљања и анализе података у оквиру организационе јединице се састоји од пет корака који су шематски приказани на слици 6 и детаљније описани у наставку поглавља.

### 3.3.1.1 Идентификовање кључних пословних процеса

Први корак у оквиру поступка је идентификовање кључних пословних процеса. Кључни пословни процеси су они пословни процеси који су најзначајнији за остваривање улоге и основних циљева организације. Фокус управљања континуитетом пословања је на кључним пословним процесима организације [137]. За сваки од идентификованих кључних пословних процеса дефинише се циљни ниво активности и анализира се постојање евентуалног алтернативног сценарија.

### 3.3.1.2 Анализа идентификованих кључних пословних процеса

Наредни корак је анализа идентификованих кључних пословних процеса која се састоји од:

- документовања основних карактеристика процеса,
- идентификовања неопходних ресурса за функционисање процеса,
- анализе обраде критичних података (енгл. *Critical Record Management*) у оквиру процеса,
- анализе регулаторног и другог важног извештавања у оквиру процеса.

Ресурси су сва имовина, људи, вештине, технологије, опрема, просторије, залихе и информације (било да су електронске или не) које организација мора да има на располагању за коришћење, када је то потребно, како би функционисала и испуњавала своје циљеве.

### 3.3.1.3 Анализа међузависности процеса

Анализа међузависности процеса се састоји од анализе зависности једног процеса од других процеса у организацији (енгл. *Upstream Dependencies*) и анализе његовог утицаја на друге процесе у организацији (енгл. *Downstream Dependencies*). Разматрају се преваходно кључни пословни процеси у осталим организационим јединицама. Ниво зависности пословних процеса се класификује као низак, средњи или висок.

### 3.3.1.4 Анализа последица прекида кључних пословних процеса

Анализа последица прекида у раду кључних пословних процеса се састоји од:

- процене директних финансијских утицаја на пословање,
- процене оперативних утицаја на пословање и
- анализе опоравка пословних процеса (опоравак изгубљених критичних података и обрада заосталог посла).

Процена финансијских и оперативних утицаја се спроводи према најгорем могућем сценарију у случају немогућности обављања пословне функције, тј. у случају прекида у раду пословних процеса, за сваки од идентификованих кључних пословних процеса посебно или за групе идентификованих процеса.

Финансијски утицаји се процењују уколико је тако дефинисано одговарајућим параметром модела. Оперативни утицаји су такође дефинисани одговарајућим параметром модела и оцењују на скали од 0 до 4, где 0 = нема утицаја, а 4 = велики утицај.

### 3.3.1.5 Иницијално утврђивање циљних параметара опоравка кључних пословних процеса

У последњем кораку се на основу свих прикупљених података иницијално утврђују циљни параметри опоравка кључних пословних процеса.

Циљни параметри опоравка су:

- Циљна тачка опоравка - RPO (енгл. *Recovery Point Objective*) представља количину губитка информација и трансакција коју је могуће толерисати. Ово је, уопште узевши, дефиниција прихватљивог губитка података у случају отказа система [138], [139]. RPO време се одређује само за пословне процесе који обрађују информације, тј. који генеришу нове информације;
- Циљно време опоравка - RTO (енгл. *Recovery Time Objective*) означава период током којег треба да буде постигнут одговарајући ниво опоравка пословног процеса [138], [139]. У пракси то представља потребно време за опоравак неопходних ресурса пословног процеса;
- Најдужи прихватљиви прекид - MAO (енгл. *Maximum Acceptable Outage*) означава најдужи прихватљив период нерасположивости пословног процеса, односно критично време за опоравак тог процеса [139]. Опоравак процеса обухвата и опоравак изгубљених критичних података и обраду заосталог посла.

На слици 7 представљени су односи између циљних параметара опоравка на временској оси од момента последње израде резервне копије (енгл. *backup*) до момента поновног успостављања редовног пословања.

RPO се иницијално одређује анализом на основу:

- постојања алтернативног сценарија за одвијање пословног процеса (тачка 2 ВИА упитника),
- обраде критичних података (тачка 3.3 ВИА упитника),
- важног извештавања (тачка 3.4 ВИА упитника) и
- опоравка кључних пословних процеса (тачка 5.3 ВИА упитника).

RTO се иницијално одређује анализом на основу:

- постојања алтернативног сценарија за одвијање пословног процеса (тачка 2 ВИА упитника),
- основних карактеристике кључних процеса (тачка 3.1 ВИА упитника),
- неопходних ресурса кључних процеса (тачка 3.2 ВИА упитника),
- анализе међузависности процеса (тачка 4. ВИА упитника),
- директних финансијских утицаја (тачка 5.1 ВИА упитника) и
- оперативних утицаја (тачка 5.2 ВИА упитника).



Слика 7 - Циљни параметри опоравка  
(извор: [139])

MAO се иницијално одређује анализом на основу:

- RTO времена и
- опоравка кључних пословних процеса (тачка 5.3 ВИА упитника).

### 3.3.2 Анализа података и документовање резултата на нивоу организације

Након спроведених интервјуа са представницима организационих јединица из делокруга BCMS-а, прикупљени подаци се анализирају и сумирају на нивоу организације у оквиру документа Анализа утицаја на пословање (садржај документа дефинисан је у **Прилогу 2**).

Поступак анализе података и документовање резултата на нивоу организације се састоји од пет корака који су шематски приказани на слици 6 и детаљније описани у наставку поглавља.

#### 3.3.2.1 Документовање најважнијих заинтересованих страна

Најважније заинтересоване стране су дефинисане параметром модела. У оквиру документа Анализа утицаја на пословање документују се оцене утицаја и интереса идентификованих најважнијих заинтересованих страна узимајући у обзир комплетно пословање организације.

#### 3.3.2.2 Анализа финансијских и оперативних утицаја услед прекида пословања организације

Процењени финансијски и оперативни утицаји у оквиру сваке организационе јединице се сумирају и документују на нивоу организације.



### 3.3.2.3 Анализа међузависности кључних пословних процеса на нивоу организације

Међузависности идентификованих кључних пословних процеса се утврђује анализом на основу:

- неопходних ресурса кључних процеса - тачка 3.2 ВИА упитника,
- идентификованих зависности пословних процеса (енгл. *Upstream Dependencies*) – тачка 4.1 ВИА упитника и
- идентификованих утицаја пословних процеса (енгл. *Downstream Dependencies*) – тачка 4.2 ВИА упитника.

### 3.3.2.4 Финално утврђивање циљних параметара опоравка (*RPO, RTO, MAO*) кључних пословних процеса организације

Након спроведене анализе међузависности кључних пословних процеса ревидирају се иницијално процењени циљни параметри опоравка пословних процеса и утврђују се финалне вредности параметара опоравка (*RPO, RTO, MAO*), узимајући у обзир све средње и високе зависности између процеса.

### 3.3.2.5 Утврђивање нивоа критичности (врло критичан, критичан, виталан, важан) кључних пословних процеса организације

Нивои критичности пословних процеса дефинисани су параметром модела на основу најдужег прихватљивог прекида у раду пословних процеса (*MAO* времена). На основу те дефиниције и утврђених параметара опоравка, за сваки од идентификованих кључних пословних процеса утврђује се ниво критичности (врло критичан, критичан, виталан, важан).

Последњи корак поступка је утврђивање приоритета приликом опоравка кључних пословних процеса, тј. редоследа поновног успостављања пословних процеса након инцидентног догађаја. Приоритети опоравка кључних пословних процеса утврђују се на основу:

- критичности процеса,
- неопходних ресурса за њихово функционисање и
- међузависности процеса.

## 3.4 **Метод за процену ризика у вези са континуитетом електронског пословања**

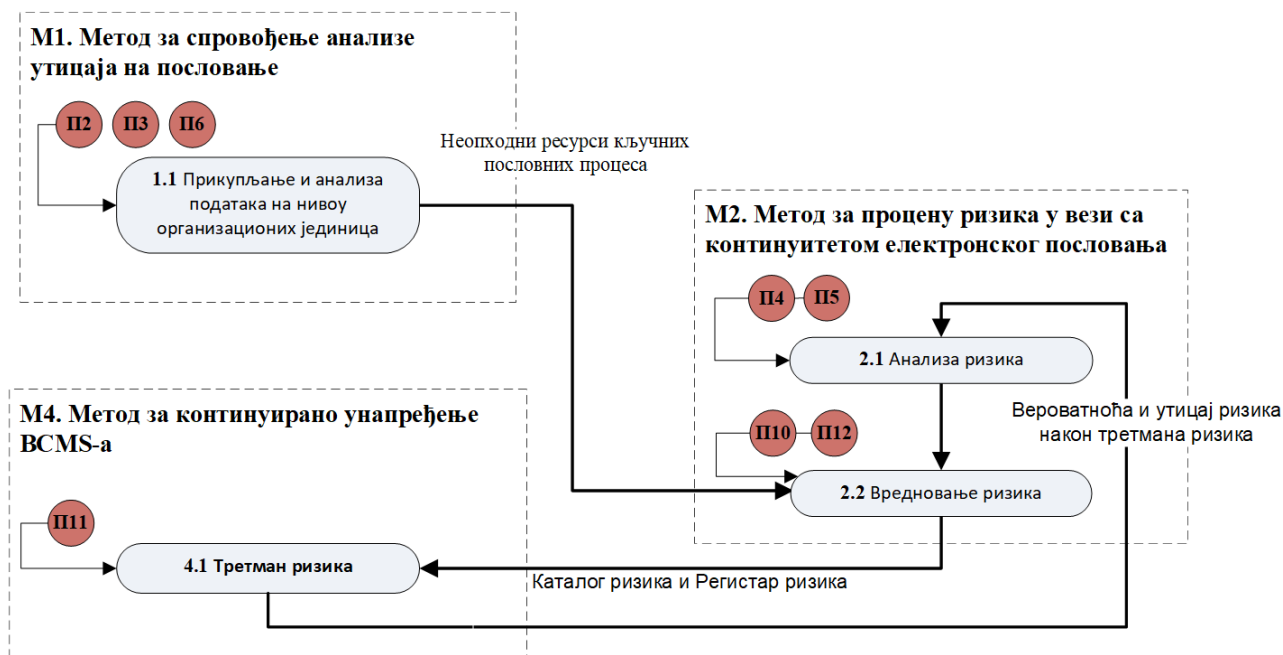
Процена ризика у вези са континуитетом електронског пословања је саставни део BCMS-а и примењује се на целокупно пословање организације, а не само на ИТ сектор [140]. Процена ризика је саставни део прикупљања неопходних информација приликом доношења важних стратешких и оперативних одлука у организацији [141].

Процена ризика у вези са континуитетом електронског пословања, као део BCMS-а, је блиска са процесом управљања ризицима. Основа разлика је у фокусу: у оквиру система управљања континуитетом електронског пословања фокус је на ризицима који могу довести до прекида у пословању, док је процес управљања ризицима најчешће фокусиран на безбедносним инцидентима [142]. У оквиру овог метода примењен је интегрисани приступ који обухвата и безбедносне инциденте.

Метод за процену ризика у вези са континуитетом електронског пословања (скраћено Метод за процену ризика) обухвата поступке за анализу и вредновање ризика над неопходним ресурсима кључних пословних процеса организације који су идентификовани у оквиру анализе утицаја на пословање. Неизвесност је кључни концепт у анализи и вредновању ризика и у пракси се користе разни математички модели из теорије вероватноће како би се она превазишла [141]. У овом методу коришћен је квалитативни приступ у процени ризика, за разлику од квантитативних и полуквантитативних (комбинованих) приступа, тј. метода.

На основу резултата процене ризика дефинише се третман ризика у циљу умањења ризика чија вредност превазилази унапред одређени ниво прихватљивости, што је саставни део метода за континуирано унапређење ВСМС-а.

Најважније везе између метода за процену ризика (М2) и осталих компонената модела приказана је на слици 8. Анализа и вредновање ризика се спроводи над неопходним ресурсима кључних пословних процеса који су идентификовани у оквиру метода М1. Резултати метода М2 документују се у каталогу и регистру ризика, који су основа за третман ризика у оквиру метода М4. На основу одабраних начина третмана ризика, поново се у оквиру метода М2 процењује преостали (тзв. резидуални) ризик.



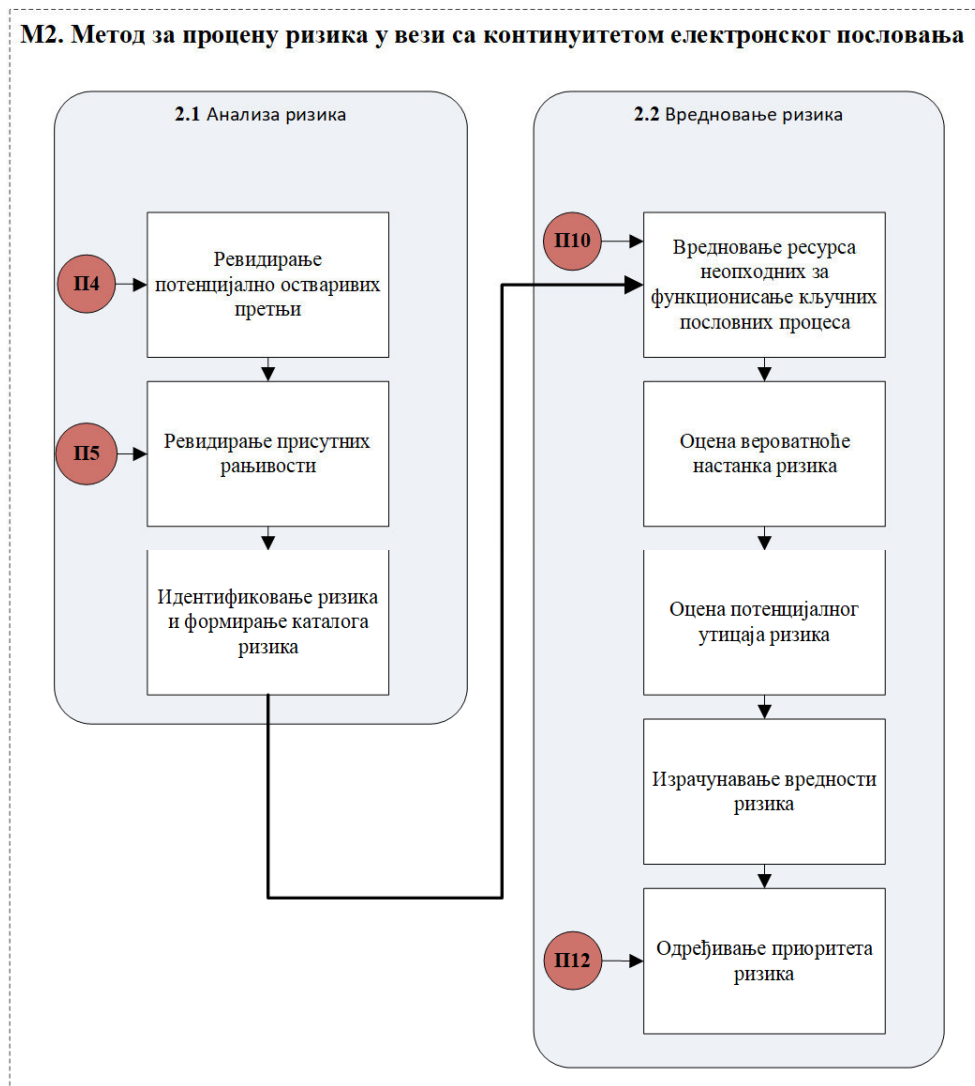
**Слика 8 - Најважније везе између метода за процену ризика (М2) и осталих компонената модела**

Циљеви процене ризика у вези са континуитетом електронског пословања су:

- идентификовање потенцијално остваривих претњи узимајући у обзир присутне рањивости кључних пословних процеса,
- одређивање потенцијалног утицаја и вероватноће настанка идентификованих ризика и
- вредновање ризика над неопходним ресурсима кључних пословних процеса.

Метод за процену ризика у вези са континуитетом електронског пословања је приказан на слици 9. Метод обухвата два поступка: Анализа ризика и Вредновање ризика.

## M2. Метод за процену ризика у вези са континуитетом електронског пословања



Слика 9 - Метод за процену ризика у вези са континуитетом електронског пословања

Анализа ризика идентификује потенцијално оствариве претње (дефинисане параметром П4) на основу постојећих рањивости кључних пословних процеса (дефинисане параметром П5). Вредновање ризика укључује процену вероватноће ризика и утицаја на ресурсе потребне за кључне пословне процесе и резултира израчунавањем вредности ризика. Важни улазни параметри за вредновање ризика су Категорије финансијских вредности ресурса (П10) и Класе приоритета ризика (П12). Категорије финансијских вредности ресурса (врло висока, висока, средња и ниска) заснивају се на новчаним вредностима ресурса и дефинишу се посебно за сваку организацију. Ризици су категорисани у четири нивоа приоритета (врло високи, високи, средњи и ниски) на основу вредности ризика, као што је дефинисано параметром П12.

### 3.4.1 Анализа ризика

Поступак анализе ризика обухвата идентификовање потенцијалних претњи и рањивости којима је изложено пословање организације. Неопходни улазни елементи за овај поступак су каталог кључних пословних процеса и њихови неопходни ресурси.

Анализа ризика је први поступак у процени ризика. Ризик је концепт који укључује догађај, вероватноћу појаве догађаја и озбиљност негативног утицаја догађаја. У присуству рањивости, претња постаје ризик.

Поступак анализе ризика се састоји од три корака који су шематски приказани на слици 9 и детаљније описани у наставку поглавља.

#### 3.4.1.1 Ревидирање потенцијално остваривих претњи

Први корак је ревидирање потенцијално остваривих претњи. Потенцијалне претње су дефинисане параметром модела П4. Ревидирање потенцијалних претњи се спроводи најчешће на основу следећих улазних докумената и активности:

- Списак кључних пословних процеса;
- Неопходни ресурси кључних пословних процеса, а посебно ИТ сервиси;
- Анализа претходних инцидената у вези са континуитетом пословања у организацији;
- Резултати ревизија;
- Разговори са власницима пословних процеса;
- Стандарди ISO 27001 [81], ISO 27005 [143], ISO 31000 [94];
- Светске статистике и каталози претњи и рањивости (нпр. PWC, Gartner, Ernst & Young, CERT и сл.).

На крају овог корака ажуриран је параметар модела Потенцијалне претње (П4).

#### 3.4.1.2 Ревидирање присутних рањивости

Следећи корак је ревидирање присутних рањивости кључних пословних процеса. Присутне рањивости су дефинисане параметром модела П5. Присутне рањивости се ревидирају и допуњују најчешће на основу истих улазних докумената као и потенцијалне претње (видети претходно поглавље).

На крају овог корака ажуриран је параметар модела Присутне рањивости (П5).

#### 3.4.1.3 Идентификовање ризика и формирање каталога ризика

На основу ревидираних потенцијално остваривих претњи и присутних рањивости кључних пословних процеса, идентификују се ризици у вези са континуитетом пословања. Приликом ове активности узимају се у обзир сви неопходни ресурси кључних пословних процеса.

Идентификоване комбинације претњи и рањивости се документују у каталогу ризика. Каталог ризика се састоји од пописа претњи, пописа рањивости и њихове међузависности у тренутку анализе ризика.

### 3.4.2 **Вредновање ризика**

Вредновање ризика је поступак одређивања потенцијалног утицаја и вероватноће настанка ризика, као и израчунавања вредности ризика над неопходним ресурсима кључних пословних процеса.

Поступак вредновања ризика се састоји од пет корака који су шематски приказани на слици 9 и детаљније описани у наставку поглавља.

#### 3.4.2.1 Вредновање ресурса неопходних за функционисање кључних пословних процеса

Вредност ресурса је мера потребног времена и додатних ресурса потребних да се неки ресурс кључних пословних процеса замени или врати у претходно стање. Еквивалентан термин је цена замене ресурса. Начин вредновања ресурса доприноси правилној оцени нивоа критичности нерасположивости ресурса по пословне процесе, који би могли да доведу до прекида испоруке производа и/или услуга организације, у складу са [144].

Вредновање ресурса се спроводи на основу добијених информација од представника организационих јединица који дефинишу начине коришћења неопходних ресурса и њихову важност за кључне пословне процесе. Приликом вредновања ресурса процењује се потенцијална (финансијска, материјална, репутациона или слична) штета по пословање организације, која настаје у случају нерасположивости ресурса. При процени штете узима се у обзир увек најгори могући сценарио.

За сваки од идентификованих неопходних ресурса кључних пословних процеса одређује се вредност ресурса у односу на следећих пет аспеката вредности ресурса:

- Поверљивост - подразумева заштиту од неовлашћеног приступа ресурсима, у било ком облику. Неовлашћене су све особе (или организације) које немају директну дозволу приступа од стране власника ресурса (тј. од стране одговорне особе за одговарајући ресурс);
- Интегритет - представља очување тачности и целовитости ресурса током манипулације, исправно коришћење и заштиту од неовлашћене модификације (нпр. под интегритетом рачунарских мрежа и система, као и телефонске мреже, разматра се, осим исправног преноса података, и аутентичност извора или одредишта);
- Расположивост - дефинише потребу за доступношћу ресурса овлашћеним лицима, узимајући у обзир време и место доступности, тј. у ком временском периоду и на којим локацијама ресурси морају бити доступни;
- Финансијска вредност – дефинише финансијску вредност ресурса; категорија финансијских вредности ресурса је један од параметара модела (P10);
- Репутациона вредност – анализира негативан утицај нерасположивости ресурса на кршење правних и регулаторних обавеза организације, као и последице по репутацију организације.

Дефиниције вредновања ресурса за сваки од пет аспеката дате су у табели 8.

**Табела 8 - Вредновање ресурса**

<b>Описна (нумеричка) вредност ресурса:</b>	<b>Ниска (1)</b>	<b>Средња (2)</b>	<b>Висока (3)</b>	<b>Врло висока (4)</b>
Поверљивост	Ресурс доступан свим запосленима	Ресурс за који је потребно овлашћење	Ресурс који располаже поверљивим подацима о партнерима и клијентима	Ресурс на нивоу класификоване информације
Интегритет	Оштећење, случајна или намерна измена узрокује додатни посао и заостатке у раду	Оштећење, случајна или намерна измена узрокује проблеме у раду и могући финансијски губитак	Оштећење, случајна или намерна измена узрокује сигурни финансијски губитак	Оштећење, случајна или намерна измена узрокује значајне проблеме и представља потенцијални губитак тржишне позиције
Расположивост	Недоступност узрокује гомилање посла и заостатке у раду	Недоступност узрокује значајне проблеме у раду и могући финансијски губитак	Недоступност узрокује сигурни финансијски губитак	Недоступност узрокује значајне проблеме и представља потенцијални губитак тржишне позиције
Финансијска вредност	Занемарива и мање значајна вредност ресурса (нпр. од 10.000 € до 100.000 €)	Релативно значајна вредност ресурса (нпр. од 100.000 € до 1.000.000 €)	Озбиљна вредност ресурса (нпр. од 1.000.000 € до 10.000.000 €)	Критична вредност ресурса (нпр. преко 10.000.000 €)
Репутациона вредност	Мање значајан негативан утицај на репутацију	Релативно значајан негативан утицај на репутацију	Озбиљан негативан утицај на репутацију	Веома озбиљан негативан утицај на репутацију

Процена вредности ресурса се спроводи на следећи начин:

- За сваки ресурс се дефинише оцена утицаја губитка поверљивости, интегритета и расположивости ресурса, финансијска вредност и репутациона вредност према дефиницијама из табеле 8;
- Вредност ресурса је максимална вредност од пет добијених вредносних оцена.

#### 3.4.2.2 Оцена вероватноће настанка ризика

Након вредновања ресурса, следећи корак је оцена вероватноће настанка ризика, тј. вероватноћа остваривања претње узимајући у обзир присутне рањивости. Вероватноћа настанка ризика се оцењује према дефиницијама из табеле 9.

**Табела 9 - Вероватноћа настанка ризика**

Нумеричка вредност	Вероватноћа настанка	Опис
1	Ниска	Ризик је мање вероватан због имплементираних контрола
2	Средња	Недостатак контрола чини овај ризик вероватним, иако се још није појавио
3	Висока	Недостатак контрола је за последицу већ имао појављивање овог ризика
4	Врло висока	Овај ризик представља хронични проблем који се континуирано појављује

#### 3.4.2.3 Оцена потенцијалног утицаја ризика

Оцена потенцијалног утицаја ризика на идентификоване ресурсе се изражава према дефиницијама из табеле 10.

**Табела 10 - Потенцијални утицај ризика**

Нумеричка вредност	Потенцијални утицај	Опис
1	Низак	Ресурс није значајније угрожен
2	Средњи	Могућ привремени губитак расположивости ресурса
3	Висок	Могућ трајни губитак ресурса
4	Врло висок	Сигуран трајни губитак ресурса

#### 3.4.2.4 Израчунавање вредности ризика

Ризик се израчунава за сваки ресурс неопходан за одвијање кључних пословних процеса. Вредност ризика се израчунава према следећој формули:

$$(2) \quad P = VP \times V \times U$$

где је:

- **P** – вредност ризика
- **VP** – вредност ресурса
- **V** – вероватноћа настанка ризика
- **U** – потенцијалан утицај ризика.

Вредност ризика може бити нумеричка вредност од 1 до 64. Прихватљив ниво ризика је максимална вредност ризика која је прихватљива за организацију у смислу могућих последица њиховог остваривања. То је један од параметара модела (П11).

За све ризике чија је вредност једнака или већа од прихватљивог нивоа ризика потребно је одредити ефикасно и усмерено превентивно деловање које се дефинише Планом обраде ризика (видети поглавље 0). Овим планом могу бити обухваћени и ризици који су прихватљивог нивоа, уколико организација процени да је то потребно или сврсисходно за континуитет пословања.

#### 3.4.2.5 Одређивање приоритета ризика

Приоритет ризика се одређује на основу вредности ризика и класа приоритета ризика дефинисаних у оквиру параметара модела П12. Приоритет ризика може бити: врло висок, висок, средњи или низак.

Вредновање ризика се документује у регистру ризика. Регистар ризика садржи списак идентификованих кључних пословних процеса, ресурсе неопходне за одвијање кључних пословних процеса, процењену вредност ресурса, идентификоване ризике, њихове вероватноће настанка, потенцијалне утицаје и вредности над неопходним ресурсима кључних пословних процеса, као и приоритете ризика. Каталог ризика је део регистра ризика.

### 3.5 **Метод за израду плана континуитета пословања**

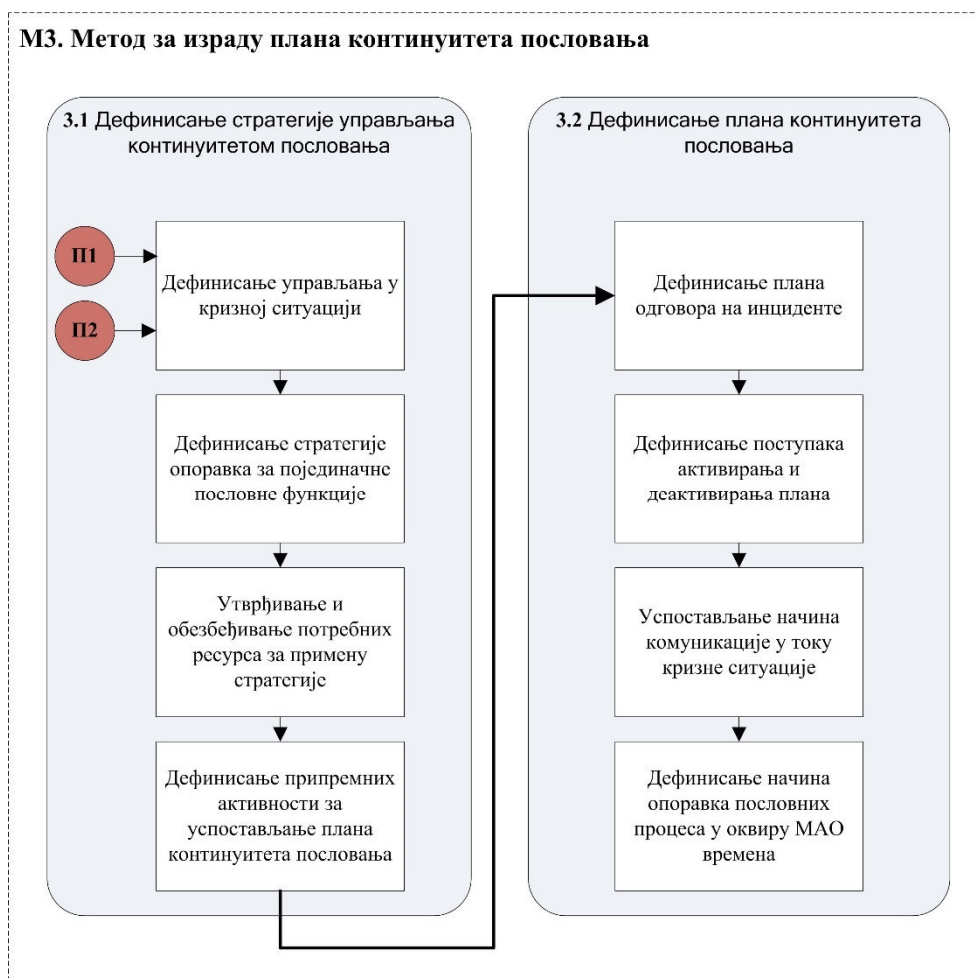
План континуитета пословања (енгл. *Business Continuity Plan*, скраћено BCP) дефинише поступке у кризној ситуацији којима се организација усмерава да одговори, да се опорави и да настави са пословањем на унапред дефинисаном нивоу активности након инцидентног догађаја. Планом континуитета пословања се успоставља функционисање кључних пословних процеса организације у оквиру дефинисаних циљних параметара опоравка (видети поглавље 3.3).

План континуитета пословања, између осталог, разматра потребе за различитим алтернативним локацијама за обављање (делова) пословања, израду резервних копија



података, алтернативне испоручиоце производа/услуга, као и успостављање политика и процедура у вези са важним питањима за организацију [98]. Приликом дефинисања плана континуитета пословања, фокус треба да буде на заштити и очувању података, као најважнијег производа пословања [100].

Метод за израду плана континуитета пословања је приказан на слици 10. Метод обухвата два поступка: Дефинисање стратегије управљања континуитетом пословања и Дефинисање плана континуитета пословања.



**Слика 10 - Метод за израду плана континуитета пословања**

Стратегија управљања континуитетом пословања се дефинише у складу са параметрима Циљеви управљања континуитетом пословања (П1) и Делокруг BCMS-а (П2), и заснива се на резултатима ВИА анализе и процене ризика. Стратегијом се дефинишу предуслови и обезбеђују сва потребна средства за успостављање плана континуитета пословања у кризној ситуацији.

### 3.5.1 Дефинисање стратегије управљања континуитетом пословања

Стратегија управљања континуитетом пословања се заснива на резултатима метода за спровођење анализе утицаја на пословање и процене ризика у вези са континуитетом електронског пословања.

Стратегија управљања континуитетом пословања дефинише и обезбеђује предуслове да сви неопходни ресурси буду на располагању у кризној ситуацији, тј. у ситуацији изазваној инцидентом у којој је активиран план континуитета пословања. Стратегија управљања континуитетом пословања представља основу за дефинисање плана континуитета пословања.

Стратегије управљања континуитетом пословања има за циљ да:

- дефинише начине на које се обезбеђује континуитет рада кључних пословних процеса,
- дефинише управљање у кризној ситуацији,
- дефинише стратегије опоравка за појединачне пословне функције,
- утврди и обезбеди потребне ресурсе за примену стратегије и
- дефинише припремне активности за успостављање плана континуитета пословања.

Стратегија се документује у оквиру документа Стратегија управљања континуитетом пословања (садржај документа дефинисан је у **Прилогу 3**).

Поступак дефинисања стратегије управљања континуитетом пословања се састоји од четири корака који су шематски приказани на слици 10 и детаљније описани у наставку поглавља.

#### 3.5.1.1 Дефинисање управљања у кризној ситуацији

У овом кораку дефинишу се најважнија овлашћења везана за доношење одлука и извештавање у кризној ситуацији. Потребно је дефинисати:

- кризне тимове - тимови који имају посебне улоге, одговорности и овлашћења у кризној ситуацији;
- локације са којих ће функционисати кризни тимови у случају кризне ситуације (најчешће се основна локација назива командни центар);
- план комуникације са заинтересованим странама;
- сарадњу са органима власти и хитним службама;
- средства за комуникацију која запослени организације користе у кризној ситуацији, као и одговорну особу за све активности у вези са њиховим прибављањем и одржавањем.

У оквиру стратегије управљања континуитетом пословања дефинишу се сви кризни тимови и њихове одговорности, док се у оквиру планова континуитета пословања додељују појединачне улоге у тиму запосленима унутар организације, заједно са свим потребним контакт подацима. Најчешће се дефинишу следећи кризни тимови:

- Кризни менаџмент тим (или кризни штаб) – тим је одговоран за доношење најважнијих одлука у кризној ситуацији и сви остали кризни тимови су директно одговорни овом тиму; неке од најважнијих одлука у кризној ситуацију су:
  - активирања и деактивирања планова континуитета пословања,
  - обавештавања заинтересованих страна,
  - одлука о преласку на алтернативне локације,
  - покретања набавки у кризној ситуацији;
- Тим за управљање инцидентима - тим је одговоран за управљање непосредним последицама инцидента;

- Тим (или тимови) за опоравак пословања - тим је одговоран за спровођење свих неопходних активности везаних за опоравак пословања; може постојати више тимова за опоравак пословања са јасно дефинисаним одговорностима везаним за организационе делове, пословне функције и/или локације на којима послује организација, а које су обухваћене делокругом BCMS-а (параметар модела П2);
- DR (енгл. *Disaster Recovery*, скраћено DR) тим - тим је одговоран за спровођење свих неопходних активности опоравка информационог система организације.

### 3.5.1.2 Дефинисање стратегије опоравка за појединачне пословне функције

За сваку пословну функцију/организациону јединицу/локацију у оквиру делокруга BCMS-а (параметар модела П2) дефинише се посебно стратегија опоравка како би се обезбедио континуитет рада кључних пословних процеса. Стратегија опоравка обухвата:

- кључне пословне процесе са циљним параметрима опоравка;
- неопходне ресурсе кључних пословних процеса, а посебно људске и ИТ ресурсе;
- активности неопходне за опоравак пословања, тј. поступак успостављања функционисања кључних пословних процеса (из делокруга BCMS-а) у кризној ситуацији;
- улоге у Тиму за опоравак пословања и њихове одговорности и овлашћења у кризној ситуацији;
- одредишта у случају евакуације за сваку од локација на којима послује организација;
- алтернативне локације за обављање пословања у кризној ситуацији, у случајевима када примарне локације нису на располагању (дефинише се посебно за сваку од локација на којима послује организација, а које су обухваћене делокругом BCMS-а);
- планирање превоза запослених организације до алтернативних локација (потребно је предвидети превоз за све запослене који имају улоге у плановима опоравка пословања);
- дефинисање потребне сарадње са партнерима и испоручиоцима.

За опоравак пословања сваке појединачне пословне функције/организационе јединице/локације одговоран је посебно формиран Тим за опоравак пословања.

### 3.5.1.3 Утврђивање и обезбеђивање потребних ресурса за примену стратегије

Следећи корак је утврђивање и обезбеђивање потребних ресурса за примену стратегије. Потребни ресурси за примену стратегије обухватају:

- људске ресурсе,
- информације и податке,
- радно окружење, опрему, потрошна добра и потребну инфраструктуру,
- апликативне и инфраструктурне ИТ сервисе,
- финансијске ресурсе,
- важне интерне и екстерне заинтересоване стране, partnere и испоручиоце.

Међу најважнијим задацима је обезбеђивање и опремање алтернативних локација. За сваку примарну локацију на којој послује организација потребно је дефинисати алтернативне локације и предвидети минималан потребан број радних места, као и начин потребног

опремања. У алтернативне локације спадају и све резервне локације за информациони систем организације (тзв. DR локације).

Алтернативна локација по начину опремања може бити:

- хладна (енгл. *cold*) – локација нема сопствену инфраструктуру и опрему,
- млага (енгл. *warm*) – локација има постављену основну инфраструктуру (мрежа, телекомуникације) и опрему чији је период набавке дугачак,
- топла (енгл. *hot*) – локација има постављену инфраструктуру, комплетну опрему и ИТ ресурсе,
- мобилна (енгл. *mobile*) – мобилна локација која има постављену инфраструктуру, комплетну опрему и ИТ ресурсе и
- пресликана (енгл. *mirrored*) – локација има постављену инфраструктуру, комплетну опрему, ИТ ресурсе и податке у реалном времену.

Могуће је дефинисати више алтернативних локација за једну примарну локацију организације. Додатно, одређена примарна локација организације може бити дефинисана као алтернативна локација за потребе друге примарне локације.

#### 3.5.1.4 Дефинисање припремних активности за успостављање плана континуитета пословања

Последњи корак у оквиру поступка дефинисања стратегије управљања континуитетом пословања је дефинисање припремних активности за успостављање плана континуитета пословања. Припремне активности између осталог обухватају:

- набавку потребних ресурса,
- опремање свих алтернативних локација у складу са њиховим начином опремања,
- обуку особа задужених за комуникацију са заинтересованим странама,
- прибављање инструкција органа власти и хитних служби за поступања у кризној ситуацији.

За сваку припремну активност дефинишу се почетак активности, крај активности, неопходни ресурси и одговорна особа. Потребно је на крају проценити и неопходне финансијске и друге ресурсе за реализацију свих припремних активности.

#### 3.5.2 Дефинисање плана континуитета пословања

На основу дефинисане стратегије управљања континуитетом пословања, дефинише се план континуитета пословања.

План континуитета пословања, у складу са [136], има за циљ:

- дефинисање поступака активирања и деактивирања плана,
- дефинисање улога, одговорности и овлашћења за људе и тимове који имају овлашћења у кризној ситуацији,
- успостављање начина комуникације у кризној ситуацији,
- дефинисање начина функционисања и неопходних ресурса у кризној ситуацији,

- дефинисање начина опоравка пословних процеса/активности у оквиру МАО времена: специфичних корака опоравка који без одлагања треба да се предузму током кризне ситуације,
- дефинисање алтернативних (резервних) локација,
- дефинисање превоза до алтернативних локација и
- дефинисање начина документовања информација у кризној ситуацији.

План континуитета пословања може бити један или више докумената. Оквирни садржај основног (кровног) документа дефинисан је у **Прилогу 4**.

План континуитета пословања најчешће као своје прилоге садржи и следећа докумената:

- План одговора на инциденте (енгл. *Incident Response Plan*),
- План опоравка информационог система (енгл. *Disaster Recovery Plan*, скраћено DRP),
- План опоравка пословања (енгл. *Recovery Plan*) за све пословне функције/ организационе јединице/локације из делокруга BCMS,.

Поступак дефинисања плана континуитета пословања се састоји од четири корака који су шематски приказани на слици 10 и детаљније описани у наставку поглавља.

#### 3.5.2.1 Дефинисање плана одговора на инциденте

План одговора на инциденте, као саставни део плана континуитета пословања, има за циљ благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности ресурса организације. Активности дефинисане овим планом имају сврху да обезбеде заштиту ресурса организације, и самим тим континуитет пословања.

План одговара на инциденте обухвата:

- дефинисање тима за управљање инцидентима који је одговоран за спровођење свих неопходних активности везаних за одговор на инциденте у вези са континуитетом пословања, укључујући и управљање непосредним последицама инцидента,
- дефинисање поступка откривања и пријаве инцидента,
- дефинисање поступка класификације инцидента,
- дефинисање поступка одговора на инцидент.

Класификација инцидента има за циљ процену нивоа озбиљности инцидента и нивоа утицаја инцидента. Пример могуће класификације дат је у наредне четири табеле (табеле 11 – 14).

Ниво озбиљности инцидента и ниво утицаја инцидента дефинисани су у табели 11 и табели 12.

**Табела 11 - Ниво озбиљности инцидента**

<b>Ниво озбиљности инцидента</b>	<b>Опис</b>
Висок	Инцидент има за последицу трајни губитак ресурса
Средњи	Инцидент има за последицу привремени губитак ресурса
Низак	Инцидент нема за последицу губитак ресурса

**Табела 12 - Ниво утицаја инцидента**

<b>Ниво утицаја инцидента</b>	<b>Опис</b>
Висок	Инцидент на више локација који има за последицу прекиде у функционисању кључних пословних процеса у више организационих делова
Средњи	Инцидент на једној локацији који има за последицу прекиде у функционисању кључних пословних процеса у више организационих делова
Низак	Инцидент на једној локацији који проузрокује прекиде у функционисању кључних пословних процеса у једном организационом делу

Класа инцидента на основу нивоа озбиљности инцидента и нивоа утицаја инцидента дефинисана је у табели 13.

**Табела 13 - Класа инцидента**

	<b>Висок ниво утицаја</b>	<b>Средњи ниво утицаја</b>	<b>Низак ниво утицаја</b>
<b>Висок ниво озбиљности</b>	Класа V	Класа IV	Класа III
<b>Средњи ниво озбиљности</b>	Класа IV	Класа III	Класа II
<b>Низак ниво озбиљности</b>	Класа IV	Класа II	Класа I

Дефиниција класе инцидента дата је у табели 14.

Табела 14 - Дефиниција класе инцидента

Класа инцидента	Дефиниција класе инцидента
<b>Класа V</b>	Инцидент има за последицу трајни губитак ресурса на више локација; Пример: катастрофа која ће највероватније имати за последицу проглашење ванредне ситуације, ванредно или ратно стање на нивоу РС
<b>Класа IV</b>	Инцидент има за последицу трајни губитак ресурса на једној локација или привремени губитак расположивости ресурса на више локација; Пример: пожар, прекид телекомуникационих веза или нестанак електричне енергије у делу земље
<b>Класа III</b>	Инцидент има за последицу привремени губитак расположивости ресурса на једној локација или трајни губитак на делу локације; Пример: квар опреме која утиче на расположивост више кључних пословних процеса
<b>Класа II</b>	Инцидент има за последицу привремени губитак расположивости ресурса на делу локације; Пример: квар на електричним инсталацијама или прекид телекомуникационих веза у делу зграде
<b>Класа I</b>	Инцидент не узрокује губитак расположивости ресурса, али може проузроковати проблеме у раду пословних процеса везаних за део једне локације; Пример: прокишњавање, квар штампача, квар система за дојаву пожара

Поступак одговора на инцидент треба да обухвати следеће важне активности:

- обавештавања хитних служби,
- ескалација инцидента (дефинише се у односу на класу инцидента),
- координација рада свих тимова на решавању инцидента,
- решавање инцидента,
- проглашење кризне ситуације и активирање плана континуитета пословања,
- праћење статуса инцидента,
- затварање инцидента.

### 3.5.2.2 Дефинисање поступака активирања и деактивирања плана

Кризном ситуацијом називамо ситуацију у којој је активиран план континуитета пословања. План континуитета пословања може бити активиран у целости или у деловима, у зависности од природе и озбиљности инцидента, као и од степена угрожености организације.

У оквиру плана континуитета пословања потребно је прецизно дефинисати:

- одговорности везане за доношење одлука о активирању и деактивирању плана континуитета пословања,
- поступке активирања и деактивирања плана континуитета пословања,
- план комуникације са заинтересованим странама у случају активације/деактивације плана.

За сваку заинтересовану страну, план комуникације дефинише одговорну особу за комуникацију, начин комуникације (допис, телефон, имејл, саопштење за штампу, вест на веб сајту организације итд.) и рокове у односу на активирање/деактивирање плана.

### 3.5.2.3 Успостављање начина комуникације у току кризне ситуације

Начин комуникације у току кризне ситуације дефинише се кризним тимовима и средствима за комуникацију.

Сви кризни тимови се дефинишу у оквиру Стратегије управљања континуитетом пословања. У оквиру планова континуитета пословања додељују појединачне улоге у тиму запосленима унутар организације, заједно са свим потребним контакт подацима: име и презиме, улога у тиму, пословни и приватни бројеви телефона, пословне и приватне имејл адресе, адреса становања и особа која је замена у случају недоступности примарног контакта.

Средства за комуникацију се дефинишу према редоследу доступности и приоритетом. Пример дефиниције средстава за комуникацију са приоритетима:

1. мобилни телефони (пословни и приватни)
2. фиксни телефони (пословни и приватни)
3. електронска пошта (пословни и приватни имејл, коришћењем пословних или приватних рачунара)
4. курирске службе (запослени у организацији или специјализоване службе)
5. радио-станице, и др.

### 3.5.2.4 Дефинисање начина опоравка пословних процеса у оквиру МАО времена

У оквиру овог корака дефинишу се посебни планови опоравка пословања за сваку пословну функцију/организациону јединицу/локацију у оквиру делокруга BCMS (параметар модела П2), у складу са стратегијом управљања континуитетом пословања.

План опоравка пословања обухвата:

- циљне нивое активности кључних пословних процеса из делокруга BCMS-а у кризној ситуацији,
- улоге у тиму за опоравак пословања и њихове одговорности и овлашћења у кризној ситуацији,
- поступке активирања и деактивирања плана,
- примарне и алтернативне локације,
- план мобилизације тима за опоравак пословања,



- план комуникације,
- поступак опоравка пословања, тј. поступак успостављање функционисања кључних пословних процеса (из делокруга BCMS-a) у кризној ситуацији и
- неопходне ресурсе за спровођење плана опоравка пословања.

Тим за опоравак пословања се састоји од дефинисаног минималног броја запослених ангажованих у кризној ситуацији, који је потребан за успостављање функционисања кључних пословних процеса у оквиру циљних нивоа активности и циљних времена опоравка. То је тим који реагује у складу са планом мобилизације тима за опоравак пословања, одмах по доношењу одлуке о активирању плана опоравка пословања.

Тим за опоравак пословања је одговоран и за доношење одлуке о успостављању и осталих пословних процеса, који нису обухваћени делокругом плана опоравка пословања, као и о ангажовању запослених који немају улогу у тиму за опоравак пословања, чим се за то створе услови, у конкретној кризној ситуацији. Та одлука ће првенствено зависити од утицаја кризне ситуације на здравље и животе људи, као и од степена угрожености примарне локације на којој се обавља пословање, тј. од чињенице да ли се пословање у кризној ситуацији обавља са алтернативних локација.

### **3.6 Метод за континуирано унапређење BCMS-a**

Прва три метода модела дефинишу најважније елементе BCMS-a, док се последњи метод бави сталним унапређењем BCMS-a. Разматрају се унутрашње и екстерне промене у окружењу организације и дефинишу се корективне мере за унапређење BCMS-a.

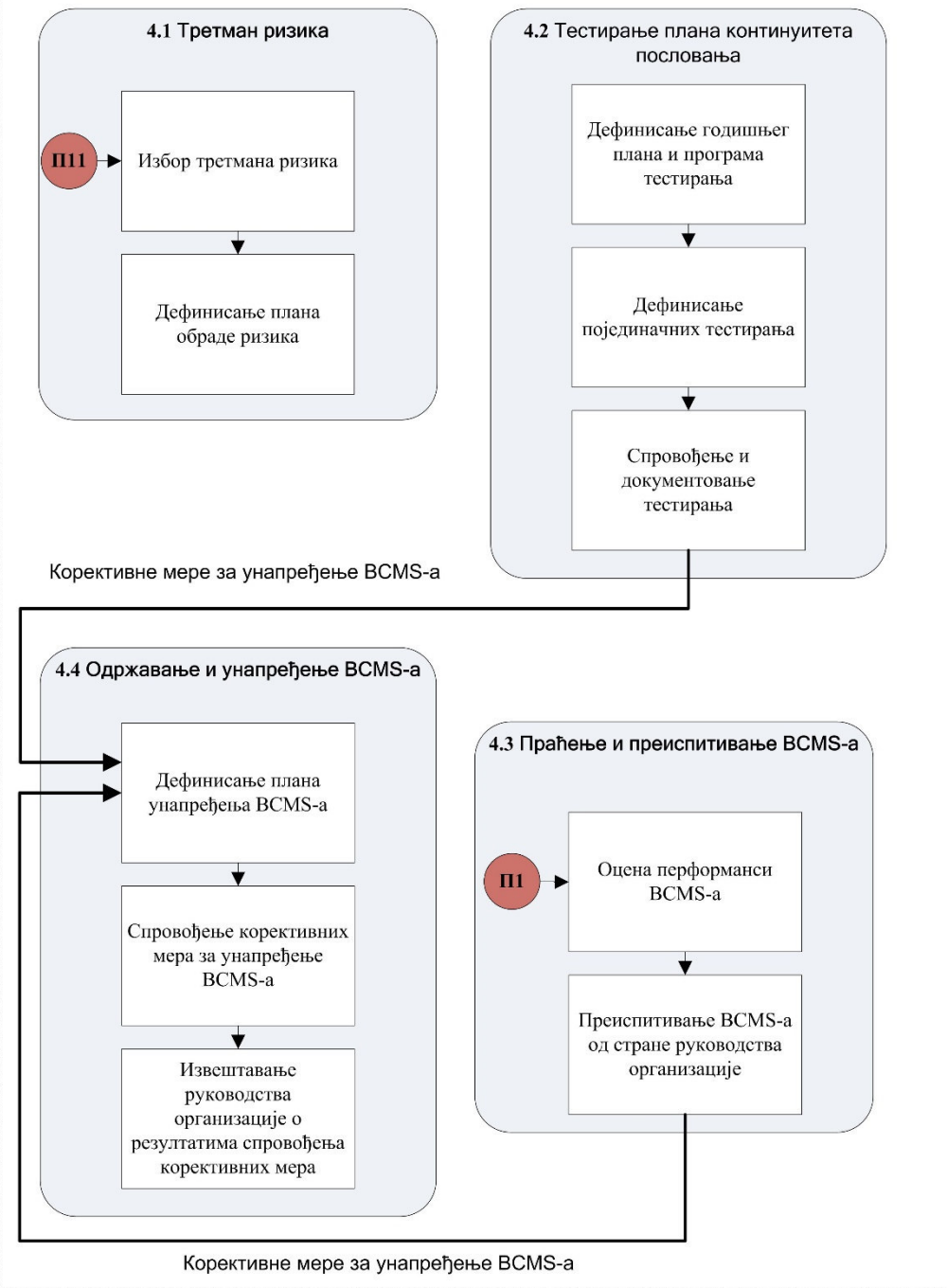
Метод за континуирано унапређење BCMS-a је приказан на слици 11. Метод обухвата четири поступка: Третман ризика, Тестирање плана континуитета пословања, Праћење и преиспитивање BCMS-a и Одржавање и унапређење BCMS-a.

Третман ризика се примењује само на ризицима чија је вредност већа од прихватљивог нивоа ризика (параметар модела П11). Тестирање плана континуитета пословања користи се за валидацију дефинисаног плана континуитета пословања пре настанка инцидентног догађаја, како би се осигурало да се опоравак може постићи у дефинисаним временским интервалима [33], [114].

Праћење и преиспитивање BCMS-a обухвата оцену перформанси BCMS-a у односу на циљеве управљања континуитетом пословања (параметар модела П1). Одржавање и унапређење BCMS-a спроводи унапред дефинисане корективне мера за унапређење BCMS-a.

Главни циљ Метода за континуирано унапређење BCMS-a је успостављање адаптивног управљања континуитетом електронског пословања, узимајући у обзир промене окружења у коме организација послује и корективне мере за унапређење BCMS-a. Метод се примењује у планираним интервалима, као и приликом сваке промене у пословном окружењу организације.

#### M4. Метод за континуирано унапређење BCMS-а



Слика 11 - Метод за континуирано унапређење BCMS-а

### 3.6.1 Третман ризика

Третман ризика има за циљ превентивно деловање на узроке појављивања ризичног догађаја и његов могући утицај на целокупно пословање организације. Неопходна претпоставка за овај поступак представља регистар ризика који је дефинисан у оквиру Метода за процену ризика у вези са континуитетом пословања (М2).

Поступак третмана ризика састоји се од два корака који су шематски приказани на слици 11 и детаљније описани у наставку поглавља.

#### 3.6.1.1 Избор третмана ризика

Могући начини третмана ризика су:

- Умањење ризика – спровођење контрола (нпр. превентивних и детективних контрола) којима се смањује потенцијални негативни утицај ризика на прихватљив ниво или се смањује вероватноћа појављивања ризика;
- Избегавање ризика – уклањање узрока и/или последица ризика (нпр. одрицање од одређених функција информационог система или престанком коришћења делова информационог система);
- Преношење ризика – уговарање накнаде штете (нпр. склапањем уговора о осигурању или уговора о циљном нивоу пружања ИТ услуге са клаузулом о накнади евентуалне штете);
- Прихватање ризика – у случају да је вредност ризика мања од прихватљивог нивоа ризика за организацију.

Заједно са одабиром начина третмана ризика, дефинишу се и нове контроле које треба спровести и процењује се преостали (резидуални) ризик уколико се примене предложене контроле.

Контрола је свака административна, управљачка, техничка или законска метода која се користи у сврху остваривања пословних циљева и спречавања или откривања нежељених догађаја. Она укључује политике, правилнике, процедуре, рачунарске програме, разне технологије и организациону структуру.

Контроле се разликују по начину примене (управљачке, техничке и физичке) и по намени (превентивне, детективне и корективне).

#### 3.6.1.2 Дефинисање плана обраде ризика

Планом обраде ризика се дефинише примена предложених контрола за све ризике за које није изабрано прихватање ризика као начин третмана.

План обраде ризика садржи:

- податке о ризику (вредност ризика, претња, рањивост, ресурс над којим је оцењен ризик и постојеће контроле),
- оцену приоритета,
- одабране контроле за примену,
- одговорне особе за примену контрола и
- временска ограничења у оквиру којих је потребно обрадити ризике, тј. применити одабране контроле.

### 3.6.2 Тестирање плана континуитета пословања

Тестирање плана континуитета пословања је једини начин провере адекватности дефинисаног плана континуитета пословања пре настанка инцидентног догађаја. Тестирање представља и начин обуке запослених за спровођење плана континуитета пословања у кризној ситуацији.

Поступак тестирање плана континуитета пословања се састоји од три корака који су шематски приказани на слици 11 и детаљније описани у наставку поглавља.

#### 3.6.2.1 Дефинисање годишњег плана и програма тестирања

План и програм тестирања дефинише планиране интервале у којима се спроводи тестирање (распоред тестирања) и начине тестирања. План и програм тестирања се дефинишу на годишњем нивоу. Могући начини тестирања су следећи начини који се најчешће спроводе по редоследу у ком су наведени [145]:

- провера путем читања сценарија (енгл. *desk-based evaluation*) – обухвата пролазак кроз план континуитета пословања као кроз сценарио и укључује све важне улоге (актере);
- тест припремљености – обухвата тестирање делова система;
- комплетан оперативни тест – симулација инцидентне ситуација.

#### 3.6.2.2 Дефинисање појединачних тестирања

За свако појединачно тестирање плана континуитета пословања потребно је дефинисати и предвидети одговарајући сценарио, са јасно дефинисаним намерама, циљевима и улогама. Потребно је да тестни сценарио на што реалнији начин осликава могућу инцидентну ситуацију.

#### 3.6.2.3 Спровођење и документовање тестирања

Појединачна тестирања се спроводе у планираним интервалима, као и када постоје значајне промене у организацији или у пословном окружењу. Резултати тестирања се документују у форми извештаја који обавезно садржи предлоге могућих унапређења плана континуитета пословања. То су корективне мере које се даље обрађују у поступку одржавања и унапређења ВСМС-а (видети поглавље 3.6.4).

### 3.6.3 Праћење и преиспитивање BCMS-a

Праћење и преиспитивање BCMS-a обухвата праћење и преиспитивање перформанси у односу на циљеве управљања континуитетом пословања, преиспитивање BCMS-a и дефинисање мера за унапређење BCMS-a.

Праћење и преиспитивање се спроводи у планираним интервалима као и када настану значајне промене у окружењу организације. Посебно, праћење и преиспитивање се спроводи након сваког инцидента који је проузроковао активирање плана континуитета пословања.

Поступак праћења и преиспитивања се састоји од два корака који су шематски приказани на слици 11 и детаљније описани у наставку поглавља.

#### 3.6.3.1 Оцена перформанси BCMS-a

Оцена перформанси BCMS-a обухвата:

- успостављање метрике вредновања перформанси BCMS-a која обухвата ефикасност и ефективност BCMS-a;
- утврђивање динамике провере перформанси;
- спровођење и документовање оцене перформанси и
- извештавање руководства организације о резултатима провере.

За сваку идентификовану неусаглашеност и/или лоше перформансе BCMS-a, утврђује се узрок неусаглашености и предлажу се корективне мере за унапређење BCMS-a које се даље обрађују у поступку одржавања и унапређења BCMS-a (видети поглавље 3.6.4). Резултати оцене се документују у форми извештаја који обавезно садржи предлоге корективних мера.

Неопходно је чување одговарајуће документоване информације као доказ о резултатима оцене перформанси.

#### 3.6.3.2 Преиспитивање BCMS-a од стране руководства организације

Преиспитивање BCMS-a од стране руководства организације обухвата:

- разматрање статуса корективних мера из претходних преиспитивања;
- анализу релевантних промена интерних и екстерних утицаја на BCMS;
- анализу извештаја о резултатима спроведених тестирања плана континуитета пословања;
- анализу извештаја о резултатима оцене перформанси BCMS-a;
- утврђивање потреба за променама у BCMS-у, укључујући циљеве управљања континуитетом пословања (параметар модела П1);
- идентификовање могућности за унапређење BCMS-a;
- документовање резултата у форми извештаја о спроведеном преиспитивању и
- доношење одлуке о имплементацији корективних мера за унапређење BCMS-a које се даље обрађују у поступку одржавања и унапређења BCMS-a.

### 3.6.4 Одржавање и унапређење ВСМС-а

Поступак одржавања и унапређења омогућава континуирано унапређење ВСМС-а на основу корективних мера за унапређење ВСМС-а усвојених од стране руководства организације.

Поступак одржавања и унапређења се састоји од три корака који су шематски приказани на слици 11 и детаљније описани у наставку поглавља.

#### 3.6.4.1 Дефинисање плана унапређења ВСМС-а

План унапређења ВСМС-а дефинише корективне мере за унапређење ВСМС-а и приоритете у примени корективних мера. За сваку корективну меру дефинисана је одговорна особа, рок за реализацију и потребни ресурси.

Корективне мере се дефинишу као резултат:

- тестирања плана континуитета пословања,
- оцене перформанси ВСМС-а и
- преиспитивања ВСМС-а од стране руководства организације.

#### 3.6.4.2 Спровођење корективних мера за унапређење ВСМС-а

У оквиру овог корака спроводе се следеће активности:

- спровођење корективних мера за унапређење ВСМС-а,
- преиспитивање ефикасности и ефективности предузетих корективних мера,
- спровођење измена у ВСМС-у уколико је неопходно и
- праћење прогреса и извештавање о статусу корективних мера дефинисаних планом унапређења ВСМС-а.

Спровођење корективних мера дефинисаних планом унапређења ВСМС-а се континуирано прати са становишта рокова, потребних ресурса и приоритета. Праћење напретка се документује у форми извештаја који обавезно садржи статусе свих корективних мера и евентуална одступања од планираних рокова.

#### 3.6.4.3 Извештавање руководства организације о резултатима спровођења корективних мера

Извештавање руководства о статусу корективних мера дефинисаних планом унапређења ВСМС-а се спроводи у планираним временским интервалима и обавезно пре сваког преиспитивања ВСМС-а.

## 4 Примена развијеног модела у пракси

### 4.1 Примена модела

Као што је претходно речено, предложени модел адаптивног управљања континуитетом електронског пословања је примењен у три организације које послују у финансијском сектору у Србији:

- Удружење осигуравача Србије (период увођења модела: јул 2013 - септембар 2013)
- Миленијум осигурање (период увођења модела: март 2014 – јун 2014)
- Народна банка Србије (период увођења модела: септембар 2015 – април 2016).

Примена модела обухвата дефинисање параметара модела и реализацију свих метода модела у одабраној организацији.

Прва примена модела је била 2013. године у Удружењу осигуравача Србије, регулаторној организацији чији чланови су друштва за осигурање која обављају послове обавезног осигурања у саобраћају. Пројекат имплементације је трајао три месеца. Пошто је Удружење осигуравача Србије одговорно за централизован информациони систем за продају полиса обавезног осигурања у саобраћају, током ВИА анализе спроведени су интервјуи са свим осигуравајућим друштвима у Србији која се баве овом врстом осигурања. Друга примена је била годину дана касније (2014) у Миленијум осигурању, осигуравајућој компанији са 300 запослених која пружа све врсте неживотних осигурања. Овај пројекат је трајао четири месеца. Последња примена модела је била у 2015. и 2016. години, у Народној банци Србије (НБС). Пројекат је трајао седам месеци и обухватао је ангажовање од преко 200 запослених НБС. Подршка највишег руководства НБС је била пресудна за успех пројекта.

Све три организације које су примениле модел сложиле су се да учествују у његовој евалуацији. Међутим, из разлога поверљивости, тражено је да се не објављују појединачни резултати евалуација, већ да се све три организације посматрају као јединствени узорак евалуације.

### 4.2 Вредновање модела

Главни циљ вредновања модела је процена његове ефикасности у успостављању адаптивног еВСМ. Хипотезе евалуације заснивају се на теоријској основи и процени међузависности компонената модела.

Први група хипотеза евалуације тестира да ли је свака компонента модела кључна за успостављање адаптивног еВСМ-а, и колико су значајни њени доприноси:

**H1a:** Метод за спровођење анализе утицаја на пословање (M1) доприноси успостављању адаптивног еВСМ-а.

**H1b:** Метод за процену ризика у вези са континуитетом е-пословања (M2) доприноси успостављању адаптивног еВСМ-а.

**H1c:** Метод за израду плана континуитета пословања (M3) доприноси успостављању адаптивног eBCM-а.

**H1d:** Метод за континуирано унапређење BCMS-а (M4) доприноси успостављању адаптивног eBCM-а.

Друга група хипотеза евалуације односи се на Метод за спровођење анализе утицаја на пословање (M1). Један од главних циљева ВИА анализе је идентификовање кључних пословних процеса организације и њихових неопходних ресурса, што је полазна основа за процену ризика. Стога је предложена следећа хипотеза евалуације:

**H2a:** Примена Метода за спровођење анализе утицаја на пословање (M1) доприноси примени Метода за процену ризика у вези са континуитетом е-пословања (M2).

ВИА анализом утврђују се циљни параметри опоравка кључних пословних процеса: циљна тачка опоравка (RPO), циљно време опоравка (RTO) и најдужи прихватљиви прекид (MAO). Циљни параметри опоравка одређују границе унутар којих се кључни пословни процеси морају опоравити и представљају главне циљеве BCM-а, као и почетну тачку за израду плана континуитета пословања. Отуда је изведена следећа хипотеза евалуације:

**H2b:** Примена Метода за спровођење анализе утицаја на пословање (M1) доприноси примени Метода за израду плана континуитета пословања (M3).

Следећа група хипотеза евалуације односи се на Метод за процену ризика у вези са континуитетом е-пословања (M2), који обухвата све ризике који могу довести до прекида пословања, а не само на сигурносне инциденте. Томе у прилог иду и дефиниције параметара модела П4 и П5, којима су унапред дефинисане потенцијалне претње и присутне рањивости, релевантне за дату организацију. Потенцијалне претње и рањивости фокусиране су на информационе системе и употребу савремених технологија е-пословања. Дефинисана на такав начин, процена ризика даје важан допринос стратешком и оперативном одлучивању у организацији [141]. Стога је предложена следећа хипотеза евалуације:

**H3a:** Примена Метода за процену ризика у вези са континуитетом е-пословања (M2) доприноси примени Метода за израду плана континуитета пословања (M3).

У оквиру поступка третмана ризика, дефинишу се превентивна деловања за све ризике чија вредност превазилази Прихватљив ниво ризика (параметар модела П11). Неопходан предуслов за третман ризика је постојање регистра ризика који се дефинише у оквиру Метода за процену ризика у вези са континуитетом е-пословања (M2). Третман ризика је саставни део Метода за континуирано унапређење BCMS-а (M4). Стога се предлаже следећа хипотеза:

**H3b:** Примена Метода за процену ризика у вези са континуитетом е-пословања (M2) доприноси примени Метода за континуирано унапређење BCMS-а (M4).

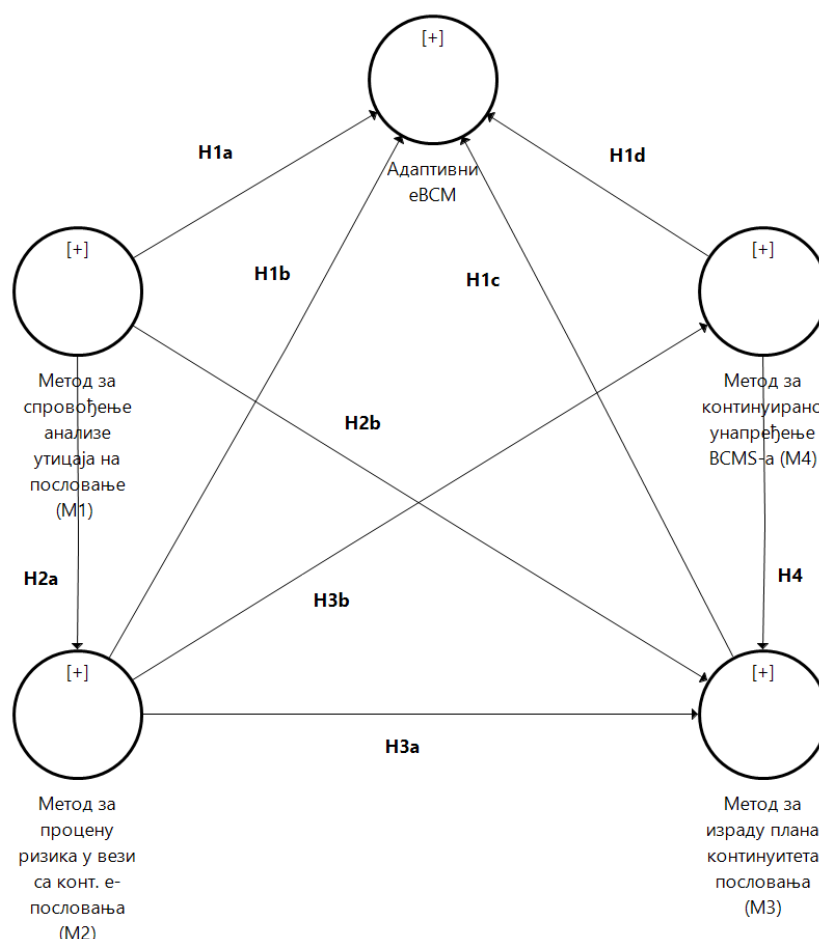
Метода за континуирано унапређење BCMS-а (M4) примењује се у планираним интервалима и након сваке важне промене у окружењу организације. У оквиру овог метода је поступак за тестирање плана континуитета пословања, што је осим самог инцидентног догађаја једини начин да се потврди садржај BCP документа и провери могућност опоравка кључних



пословних процеса у оквиру циљних параметара опоравка. Стога је коначна хипотеза евалуације:

**H4:** Примена Метода за континуирано унапређење ВСМС-а (M4) доприноси примени Метода за израду плана континуитета пословања (M3).

Све хипотезе евалуације приказане су на слици 12, док табела 15 даје преглед коришћене литературе.



Слика 12 - Хипотезе евалуације (структурни PLS-SEM модел)

**Табела 15 - Хипотезе евалуације и теоријска основа**

<b>Хипотезе евалуације</b>	<b>Теоријска основа</b>
H1a: M1 -> Адаптивни eBCM	
H1b: M2 -> Адаптивни eBCM	Сви методи модела значајно доприносе успостављању адаптивног eBCM [33]
H1c: M3 -> Адаптивни eBCM	
H1d: M4 -> Адаптивни eBCM	
H2a: M1 -> M2	
H2b: M1 -> M3	У оквиру ВИА анализе идентификовани су кључни пословни процеси [59], [63]; процена ризика врши се на ресурсима потребним за кључне пословне процесе [33], [123], [140]
H3a: M2 -> M3	ВИА анализом утврђују се циљни параметри опоравка кључних пословних процеса [1], [59], [115], [137]
H3b: M2 -> M4	План континуитета пословања се заснива на резултатима ВИА анализе и процене ризика [1], [59], [115]; резултати процене ризика важни су за стратешко и оперативно доношење одлука у организацији [141]
H4: M4 -> M3	Третман ризика је заснован на резултатима процене ризика [1], [123], [140]
	Тестирање плана континуитета пословања је неопходан део ефикасног управљања континуитетом пословања [1], [59]

### 4.3 Упитник за вредновање модела

У оквиру рада на докторској дисертацији, спроведено је вредновање модела путем упитника, који је дат у **Прилогу 5** овог документа. Сви одговори су дефинисани на петостепеној Ликертовој скали: (1) Уопште се не слажем, (2) Донекле се не слажем, (3) Немам мишљење, (4) Делимично се слажем и (5) Потпуно се слажем.

Упитник за вредновање модела (у даљем тексту „Упитник“) састоји се од пет делова:

- I. Вредновање основних карактеристика модела
- II. Вредновање Метода за спровођење анализе утицаја на пословање
- III. Вредновање Метода за процену ризика у вези са континуитетом е-пословања
- IV. Вредновање Метода за израду плана континуитета пословања и
- V. Вредновање Метода за континуирано унапређење BCMS-а.

Питања коришћена за вредновање основних карактеристика модела базирана су на основним хипотезама истраживања, како је дефинисано у [33], међународном стандарду [1] и оцени BCMS перформанси [109]. Остала питања базирана су на следећој литератури: [59], [136], [137] за вредновање Метода за спровођење анализе утицаја на пословање (М1); [99], [140], [141] за вредновање Метода за процену ризика у вези са континуитетом е-пословања (М2); [98], [100], [136] за вредновање Метода за израду плана континуитета пословања (М3); и [145] за вредновање Метода за континуирано унапређење BCMS-а (М4).

У процесу вредновања модела учествовали су представници све три организације у којима је модел примењен, и то према плану вредновања дефинисаном у табели 16. Све три организације су из финансијског сектора у Србији и све подлежу истим стандардима и правилима везаним за континуитет пословања. Због поверљивости података све три организације су разматране као јединствени узорак. Вредновање модела је спроведено између априла и јуна 2017. године. У **Прилогу 6** приказани су сви одговори испитаника у облику графикана.

**Табела 16 - План вредновања модела**

Р. Бр.	Организација	Број испитаника	Радно место или представник организационе јединице
1.	Удружење осигуравача Србије	3 испитаника (од укупно око 20 запослених)	<ul style="list-style-type: none"> <li>• Директор Информационог центра</li> <li>• Директор Гарантног фонда</li> <li>• Директор Бироа „Зелена карта“</li> </ul>
2.	Миленијум осигурање	9 испитаника (од укупно око 200 запослених)	<ul style="list-style-type: none"> <li>• Служба за информационо-комуникационе технологије</li> <li>• Служба за неживотна осигурања</li> <li>• Служба за осигурање моторних возила</li> <li>• Служба за пријаву, процену и ликвидацију штета</li> <li>• Служба за рачуноводство и финансије</li> <li>• Служба за управљање људским ресурсима, правне и опште послове</li> <li>• Интерна ревизија</li> <li>• Односи са јавношћу и информисање (ПР менаџер)</li> </ul>
3.	Народна банка Србије	26 испитаника (од укупно око 2000 запослених)	<ul style="list-style-type: none"> <li>• Директорат за економска истраживања и статистику</li> <li>• Дирекција за законодавно-правне послове</li> <li>• Дирекција за набавке</li> <li>• Дирекција за опште послове (два испитаника)</li> </ul>

Р. Бр.	Организација	Број испитаника	Радно место или представник организационе јединице
			<ul style="list-style-type: none"> <li>• Дирекција за рачуноводство и финансије</li> <li>• Завод за израду новчаница и кованог новца</li> <li>• Кабинет гувернера</li> <li>• Људски ресурси</li> <li>• Национални центар за платне картице</li> <li>• Принудна наплата</li> <li>• Сектор за девизне послове</li> <li>• Сектор за информационо-комуникационе технологије</li> <li>• Сектор за међународну сарадњу</li> <li>• Сектор за монетарне операције</li> <li>• Сектор за послове с готовином</li> <li>• Сектор за платни систем</li> <li>• Управа за надзор над финансијским институцијама</li> <li>• Филијала у Београду</li> <li>• Центар за контролинг</li> </ul>

#### 4.4 Методологија вредновања модела

Вредновање модела је спроведено у три корака, као што је приказано у табели 17. Основна статистичка анализа података [146] [147], заједно са тестом статистичке значајности (корак 1) [148], коришћена је за процену тачности хипотеза истраживања и процену да ли је модел ефикасан у имплементацији еVCM-а. За анализу је коришћен Stata софтвер (верзија 13) [149] [150].

Детаљнија анализа резултата вредновања модела (кораци 2 и 3) извршена је коришћењем структурног моделовања (енгл. *Structural Equation Modeling*, скраћено SEM), напредне технике статистичке анализе која може идентификовати односе између измерених и латентних варијабли (варијабле које се не мере директно), као и односе између латентних варијабли [151]–[154].

У дисертацији је коришћено структурно моделовање применом технике најмањих парцијалних квадрата (енгл. *Partial Least Squares SEM*, скраћено PLS-SEM), која је насупрот *Covariance-Based SEM* (CB-SEM) за процену теоретски оправданих узрочно-последичних односа у моделима, посебно погодна за истраживања код којих је мала величина узорка [155], [156]. PLS-SEM је ефикасна техника са малим величинама узорка и нема ограничења по питању дистрибуције података у узорку [151]. За анализу је коришћен SmartPLS софтвер (верзија 3.2.9) [157].

**Табела 17 - Кораци у вредновању модела**

<b>Корак</b>	<b>Метода вредновања</b>	<b>Сврха корака</b>
1. Оцена ефикасности модела	Основне статистичке анализе и тест статистичке значајности	Оцена тачности полазних хипотеза истраживања и оцена ефикасности модела у имплементацији eBCM-а
2. Оцена PLS-SEM модела латентне варијабле (спољни модел)	PLS-SEM стандардни алгоритам	Оцена поузданости и валидности Упитника за вредновање модела
3. Оцена PLS-SEM структурног модела (унутрашњи модел)	PLS-SEM <i>blindfolding</i> алгоритам и алгоритам реузорковања (енгл. <i>bootstrapping</i> )	Тестирање хипотеза евалуације

PLS-SEM анализа се састоји од процене одговарајућих PLS-SEM модела: структурног модела и модела латентне варијабле.

PLS-SEM структурни модел (енгл. *structural model*), који се назива и унутрашњим моделом, илуструје хипотезе истраживања и приказује узрочно-последичне односе између променљивих које ће бити испитиване [151]. У овом истраживању структурни модел је дефинисан на основу хипотеза евалуације (видети слику 12). У PLS-SEM анализи, променљиве које се директно не мере, тј. латентне варијабле, називају се конструкти (енгл. *constructs*) и визуално се представљају у облику кругова или овала. Индикатори (енгл. *indicators*), који се називају још и ставке (енгл. *items*) или манифестне променљиве (енгл. *manifest variables*), променљиве су које је могуће директно измерити и које садрже необрађене податке. Индикатори се визуелно представљају као правоугаоници [151].

PLS-SEM модел латентне варијабле (енгл. *measurement model*), који се назива и спољним моделом, приказује однос између конструката и индикатора [151]. Модел латентне варијабле дефинисан је помоћу питања из Упитника за вредновање модела објашњених у поглављу 4.3, а детаљније описаних у наредном поглављу 4.5 (видети слику 17).

PLS-SEM моделе није могуће оценити са јединственим критеријумом погодности. У складу са PLS-SEM смерницама [151], [158]–[162] у оквиру дисертације је коришћен двостепени приступ у евалуацији PLS-SEM модела, као што је описано у корацима евалуације 2 и 3 (видети табелу 17).

У следећем поглављу представљена су детаљније сва три корака у вредновању предложеног модела за адаптивно управљање континуитетом електронског пословања.

## 4.5 Анализа резултата

### 4.5.1 Оцена ефикасности модела

У првом кораку вредновања модела извршена је статистичка анализа заснована на средњим вредностима оцена испитаника из Упитника за вредновање модела (видети **Прилог 7** за комплетне резултате овог корака).

У оквиру анализе, извршен је тест статистичке значајности (t-тест) на средњим вредностима за свако питање из Упитника. Тест статистичке значајности се заснива на тестирању нулте хипотезе у односу на алтернативне хипотезе [148], [163]. У техничком смислу речи, тестирају се следеће хипотезе:

$$(3) \quad \Pr (H_a: \text{погрешно} \mid H_0: \text{тачно}) \\ H_0: \mu = \mu^* \\ H_a: \mu < \mu^*, H_a: \mu \neq \mu^*, H_a: \mu > \mu^*$$

где су  $H_0$  и  $H_a$  нулта и алтернативна хипотеза,  $\mu$  је средња вредност скупа података из узорка,  $\mu^*$  је референтна средња вредност, а  $\Pr$  (енгл. *Probability*) вероватноћа с којом се може одбацили нулта хипотеза у односу на алтернативну хипотезу као тачну<sup>2</sup>. Фактички, тестирају се три алтернативне хипотезе  $H_a$  ( $\mu < \mu^*$ ,  $\mu \neq \mu^*$  и  $\mu > \mu^*$ ), увек у односу на нулту хипотезу  $H_0$ , али посебан значај за тестирање модела има само једна од њих.

За овај тест од кључне важности је одређивање референтне средње вредности. Оцене испитаника из Упитника рангиране су на петостепеној Ликертовој скали: (1) Уопште се не слажем, (2) Донекле се не слажем, (3) Немам мишљење, (4) Делимично се слажем и (5) Потпуно се слажем. У том смислу свакој оцени придодата је одговарајућа вредност између 1 и 5. Имајући то у виду, средња вредност од 4 је изабрана као референтна вредност са којом се могу упоредити резултати евалуације модела. Основна претпоставка анализе је да се средња вредност од 4 сматра прагом ефикасности у имплементацији адаптивног eVCM модела. Свака оцена која има вредност испод 4 тумачи се као неефикасност одговарајуће компоненте адаптивног eVCM-а, и обрнуто, свака оцена која има вредност преко 4 тумачи се као ефикасност одговарајуће компоненте адаптивног eVCM-а.

У спроведеној анализи статистичке значајности (t-тест) на средњим вредностима узорка, нулта хипотеза је била: Средња вредност једнака је 4 ( $H_0: \mu = 4$ ). За свако питање израчунат је тест статистичке значајности за друге алтернативне хипотезе: средња вредност је мања од 4 ( $H_a: \mu < 4$ ), средња вредност није једнака 4 ( $H_a: \mu \neq 4$ ), и средња вредност је већа од 4 ( $H_a: \mu > 4$ ), што је најважнија информација за ово истраживање. Коришћен је једностранни t-тест (енгл. *one-sample t-test*) са нивоом поузданости од 95% у софтверу Stata (в.13). У табели 18 приказани су резултати тестирања нулте хипотезе (3) за вредновање основних карактеристика eVCM модела.

---

<sup>2</sup> Потребно је обратити пажњу на негацију у закључивању: ако је  $H_0$  одбачена као погрешна хипотеза, прихвата се алтернативна хипотеза  $H_a$  као тачна – што представља негацију у односу на израз (3).

Табела 18 - Вредновање основних карактеристика еВСМ модела

Питање из Упитника	Средња вредност: $\mu$	Стд. девијација	95% интервал поверења		t-вредност	Вероватноћа одбацивања алтернативне хипотезе		
						$H_a: \mu < 4$	$H_a: \mu \neq 4$	$H_a: \mu > 4$
П1.1*	4.500	0.647	4.287	4.713	t = 4.762	Pr(T < t) = 1.0000	Pr(   T   >   t   ) = 0.0000	Pr(T > t) = <b>0.0000</b>
П1.2*	4.500	0.647	4.287	4.713	t = 4.762	Pr(T < t) = 1.0000	Pr(   T   >   t   ) = 0.0000	Pr(T > t) = <b>0.0000</b>
П1.3*	4.684	0.620	4.481	4.888	t = 6.805	Pr(T < t) = 1.0000	Pr(   T   >   t   ) = 0.0000	Pr(T > t) = <b>0.0000</b>
П1.4*	4.421	0.758	4.172	4.670	t = 3.423	Pr(T < t) = 0.9992	Pr(   T   >   t   ) = 0.0015	Pr(T > t) = <b>0.0008</b>
П1.5	4.132	1.119	3.764	4.499	t = 0.724	Pr(T < t) = 0.7634	Pr(   T   >   t   ) = 0.4732	Pr(T > t) = 0.2366

\*: Индикатори који су прошли t-тест у смислу да је вероватноћа одбацивања нулте хипотезе  $H_0$  испод нивоа значајности од 5%; подебљаним словима (енгл. *bold*) је означена вероватноћа с којом може да се одбаци нулта хипотеза о средњој вредности једнакој 4, у односу на алтернативну хипотезу да је средња вредност већа од 4.

За илустрацију примене теста статистичке значајности (t-теста) узет је први део Упитника (питања П1.1 - П1.5), а касније је цела анализа проширена и на остале одговоре из Упитника. Наведена питања односе се на вредновање основних карактеристика модела, тачније на вредновање основа адаптивног еВСМ-а, које уједно представљају и полазне хипотезе овог истраживања (видети поглавље 1.3). Питање П1.1 проверава да ли је модел јасно формулисан; питање П1.2 да ли је модел свеобухватан; питање П1.3 да ли је модел користан; питање П1.4 да ли је модел адаптиван и питање П1.5 да ли је модел подстицајан. Основна статистичка анализа показује да резултати евалуације подржавају ефикасност модела у имплементацији еВСМ-а, јер је просечна оцена за свако питање већа од 4 (видети колону „Средња вредност“ у табели 18).

Међутим, ова тврдња не узима у обзир неизвесност формирања узорка. Ако се неизвесност укључи у анализу, потребно је прво одредити интервал поузданости, а потом спровести тестирање нулте хипотезе о средњој вредности узорка. Поступак је за почетак илустрован на примеру одговора испитаника на питање П1.1.

Средња вредност за прву оцену П1.1 у узорку износи 4.5. Али да би се проценила хипотеза да је она заиста већа од 4.0, мора се узети у обзир неизвесност око те процене. Интервал поузданости од 95% креће се од 4.287 до 4.713, што укључује вредност 4.5, тако да постоје добри изгледи за одбијање нулте хипотезе да је средња вредност 4.0.

Формална процена нулте хипотезе ( $H_0$ ) да је средња вредност 4.0 упоређује се са једном од три алтернативне хипотезе ( $H_a$ ): да је средња вредност мања од 4.0, да средња вредност није једнака 4.0, али да може бити већа или мања, и да је средња вредност већа од 4.0.

Прво ће бити размотрен случај да је средња вредност мања од 4.0, тј.  $H_a$ : средња вредност  $< 4.0$ . Имајући у виду број опажања и њихову стандардну девијацију, постоји потпуна вероватноћа (1.0000) да се изабере узорак са средњом вредношћу 4 (видети колону  $H_a$ :  $\mu < 4$  у табели 18), у односу на узорак са средњом вредношћу мањом од 4.0. Та вероватноћа је већа од 0.05, па се прихвата нулта хипотеза да је средња вредност узорка 4.0 у корист алтернативне да је његова средња вредност мања од 4.0. Дакле, узорак са средњом вредношћу 4 је много вероватнији него узорак са средњом вредношћу мањом од 4.

Следећи случај је  $H_a$ : средња вредност  $\neq 4.0$ . Ако је просечна вредност целе популације 4.5, а стандардна девијација 0.647, вероватноћа извлачења узорка са средњом вредношћу 4.0 у односу на узорак са средњом вредношћу различитом од 4.0 износи 0,0000. Ова вероватноћа је нижа од 0.05, па се у овом случају одбацује нулта хипотеза да је средња вредност 4.0 у корист алтернативне хипотезе да је средња вредност различита од 4.0 (већа или мања од 4.0).

Дакле, средња вредност је различита од 4.0 али још увек није тестирана алтернативна хипотеза да је она већа од те вредности, тј.  $H_a$ : средња вредност  $> 4.0$ . Ако је просечна вредност целе популације 4.5, а стандардна девијација 0.647, онда вероватноћа избора узорка са средњом вредношћу 4.0 у односу на узорак са средњом вредношћу већом од 4.0 износи 0,0000. Ова вероватноћа је нижа од 0.05, па се у овом случају одбацује нулта хипотеза да је средња вредност 4.0, а прихвата алтернатива да је средња вредност већа од 4.0.

То значи да је тестирање нулте хипотезе доказало да је својство eVCM модела ефикасно са становишта постављеног питања П1.1, односно да је модел јасно формулисан. Другим речима, питање П1.1 је прошло тест статистичке значајности (t-тест). На основу информација из табеле 18, може се извести исти закључак и за следећа три питања: П1.2, П1.3 и П1.4.

Последње питање П1.5 захтева посебно образложење. Његова средња вредност је већа од 4.0 (4.132), али није могуће статистички доказати да би избор узорка увек био такав да гарантује средњу вредност већу од 4.0 имајући у виду неизвесност око избора узорка (која се огледа у знатно већој стандардној девијацији од 1.119 у односу на претходне случајеве). Вероватноћа да се одбаци нулта хипотеза ( $H_0$ : средња вредност = 4.0) у корист алтернативне хипотезе ( $H_a$ : средња вредност  $< 4.0$ ) јесте 0.7634. Како је она већа од 0.05, то говори да се нулта хипотеза налази у подручју прихватања и да је вероватније да би узорак пре имао средњу вредност 4.0 него мању од 4.0. На другој страни, вероватноћа да се одбаци нулта хипотеза ( $H_0$ : средња вредност = 4.0) у корист алтернативне хипотезе ( $H_a$ : средња вредност  $\neq 4.0$ ) јесте 0.4736. Како је то, такође, веће од 0.05, алтернативна хипотеза да је средња вредност различита од 4.0 (већа или мања) одбацује се у корист нулте хипотезе да средња вредност износи тачно 4.0. И у последњем случају, вероватноћа да се одбаци нулта хипотеза ( $H_0$ : средња вредност = 4.0) у корист алтернативне хипотезе ( $H_a$ : средња вредност  $> 4.0$ ) јесте 0.2366. Како је и то веће од 0.05, алтернативна хипотеза да је средња вредност већа од 4.0 одбацује се у корист нулте хипотезе да средња вредност износи тачно 4.0.

Дакле, узимајући у обзир неизвесност, није могуће поуздано закључити да је средња вредност одговора на питање П1.5 већа од референтне вредности коју смо одредили као ниво ефикасности. Тачније речено, нулта хипотеза да средња вредност овог питања одговара

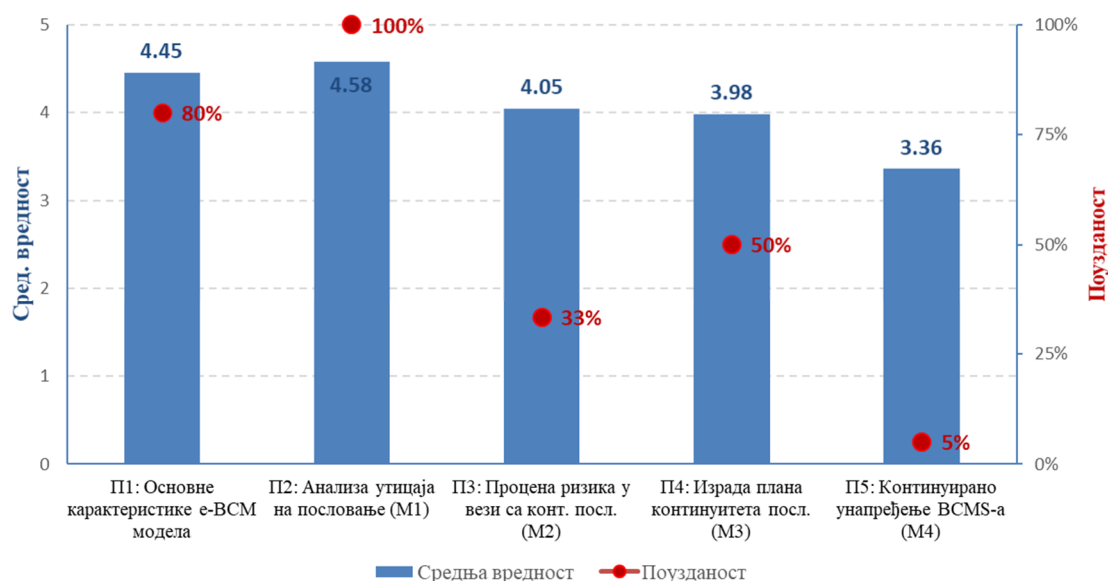


висини референтне вредности је потврђена у односу на све алтернативне хипотезе (мада са различитим процентима вероватноће). Међутим, наш критеријум ефикасности еVCM модела захтева да његова оцена прелази висину референтне вредности, што искључује случај када се поклапа са њом. У том смислу, прва четири питања о оцени ефикасности еVCM модела пролазе статистички тест поузданости, док последње питање не пролази, иако има средњу вредност већу од 4.0.

Остала делови Упитника односе се на ефикасност четири појединачна метода од којих се састоји еVCM модел. Метод за континуирано унапређење BCMS-а (M4) има најнижу просечну оцену, 3.36 (видети **Прилог 7**), јер укључује напредне активности из перспективе зрелости континуитета пословања, и његова успешна примена захтева одређено време и искуство. У оквиру њега, ниједан одговор није прошао тест алтернативне хипотезе да је средња вредност већа од 4. Континуитет пословања је процес који се развија [1], што доводи до закључка да је овом методу потребна континуирана пракса да би се постигао жељени ниво ефикасности.

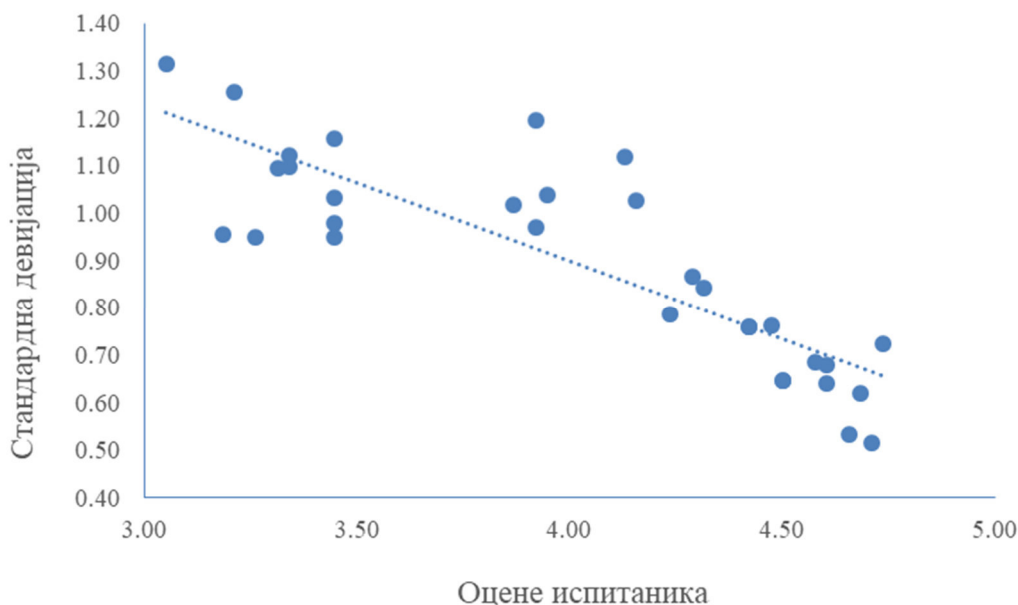
Остали методи модела имају просечне оцене веће од 4 или близу 4. Метод за спровођење анализе утицаја на пословање (M1) има просечну оцену 4.58 и сви одговори су прошли тест алтернативне хипотезе да је средња вредност већа од 4, што показује да је овај метод, од сва четири метода, најефикаснији у примени. Метод за процену ризика у вези са континуитетом е-пословања (M2) има просечну оцену 4.05, али је делимично прошао t-тест – само је једна трећина одговора задовољила тест алтернативне хипотезе да је средња вредност већа од 4. Слично, Метод за израду плана континуитета пословања (M3) има просечну оцену 3.98, али је такође само делимично прошао t-тест – половина одговора је задовољила тест алтернативне хипотезе да је средња вредност већа од 4. Ови резултати имплицирају да су методама M2 и M3 потребна додатна прилагођавања, посебно у областима сталног унапређења, како би се постигла пуна ефикасност у пракси.

Резултати анализе средње вредности узорка и поузданости узорка визуелно су приказани на слици 13, а комплетни резултати су дати у **Прилогу 7**. На слици 13 на левој скали се налази просечна вредност оцене за сваку групу питања (у форми стубова), а на десној скали је проценат питања који су прошли t-тест (у форми црвених тачака).



**Слика 13 - Средње вредности и проценат поуздања одговора из групе питања**

Постоји доста јака линеарна веза између варијабилитета оцена и висине самих оцена, што је приказано на слици 14. Испрекидана линија представља уклопљену линију линеарне регресије оцене испитаника и стандардних девијација. Што је већа оцена, то је мањи варијабилитет одговора. Међутим, код нижих оцена (између 3 и 3.5) тај варијабилитет озбиљно расте. Када испитаници оцењују неку компоненту модела као успешну, онда међу њима нема великих разлика у мишљењима. Међутим, када се оцене испитаника крећу око осредње ефикасности (између 3 и 3.5), онда се њихови одговори знатније разликују.

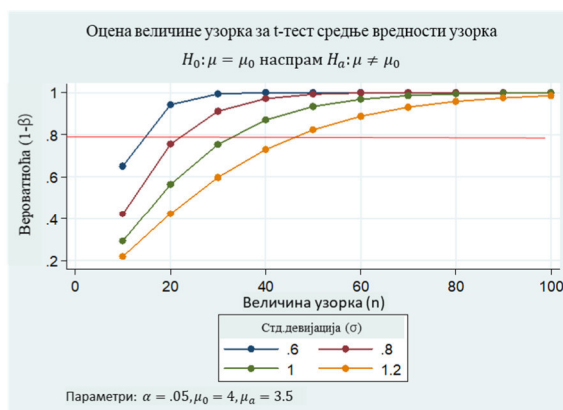
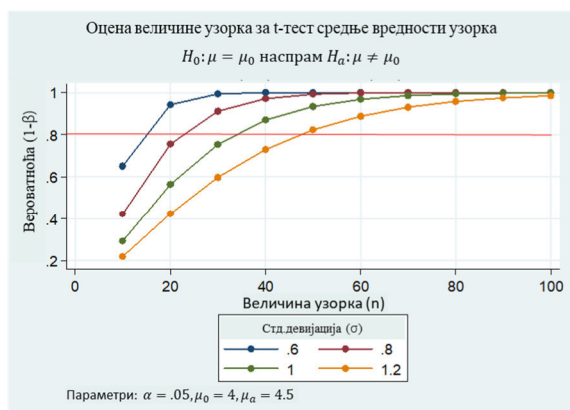


Слика 14 - Однос варијабилитета и појединачних оцена испитаника

Последње питање које је анализирано у оквиру првог корака вредновања ефикасности модела јесте величина узорка. Узорак у овом истраживању се састоји од 32 серије података (број питања из Упитника), свака са 38 тачака посматрања (број испитаника). То је мали узорак са становишта броја тачака посматрања, али богат узорак са становишта карактеристика анализираних модела. Ипак, поставља се питање да ли је он довољан за закључивање о ефикасности адаптивног eVSM модела на основу тестирања нулте хипотезе о средњој вредности оцена испитаника. Одговор је потврдан и заснива се на експерименту који је приказан на слици 15.

Циљ тестирања нулте хипотезе је да се процени ваљаност тврдње о односу неког параметра у популацији  $\mu$  према циљној вредности тог параметра у узорку  $\mu^*$ . Пошто се често циљни параметар изједначава са нулом  $\mu^* = 0$ , односно ставом да дата појава „нема утицаја“, хипотеза се назива нулта хипотеза  $H_0: \mu^* = 0$ . Затим се формира узорак, прикупе се подаци и тестира се алтернативна хипотеза  $H_a: \mu^* \neq 0$  да дата појава „има утицаја“.

У овом истраживању не тестира се нулта хипотеза „нема утицаја“ против алтернативне хипотезе „има утицаја“, него се тестира нулта хипотеза да је „средња вредност“ одговора испитаника на постављена питања „различита, већа или мања“ од референтне вредности код алтернативне хипотезе.



Слика 15 - Хипотетичко тестирање величине узорка

Тестирање хипотезе може да направи једну од две врсте грешака: грешка типа I због погрешног одбацивања нулте хипотезе и грешка типа II због погрешног прихватања нулте хипотезе. Вероватноћа за настанак грешке типа I је  $\Pr(\text{одбачено } X_0 \mid X_0 \text{ тачно})$ , а вероватноћа за настанак грешке типа II се обично означава као  $\beta = \Pr(\text{неуспешно одбачено } X_0 \mid X_0 \text{ нетачно})$ . Није могуће једновремено минимизирати обе врсте грешака. Зато се, по правилу, фиксира коефицијент  $\alpha$  који изражава прихватљиви ниво грешке типа I (5% или 1%), а потом се минимизира настанак грешке типа II  $\beta$ , односно максимизира вероватноћа одсуства те грешке:  $1 - \beta$ .

Што је  $\beta$  ближе нули, то је поузданост тестирања нулте хипотезе у односу на алтернативну хипотезу већа. Грешка тестирања хипотезе  $\beta$  је функција коефицијента  $\alpha$ , стандардне девијације, односно варијансе  $\sigma$  и величине узорка  $n$ . Код тестирања нулте хипотезе у табели 18, била је позната величина узорка ( $n$ ) и тестиране су три алтернативне хипотезе ( $H_a: \mu > 4$ ,  $H_a: \mu \neq 4$ ,  $H_a: \mu < 4$ ). Код експерименталног одређивања величине узорка постоје две алтернативне хипотезе ( $H_a: \mu < 4$  и  $H_a: \mu > 4$ ). Непозната варијабла је величина узорка. Ако се преузму вредности за коефицијенте  $\alpha$  и  $\sigma$  као унапред дате, могуће је симулирати потребну величину узорка као функцију вероватноће одсуства грешке у закључивању:  $1 - \beta$ .

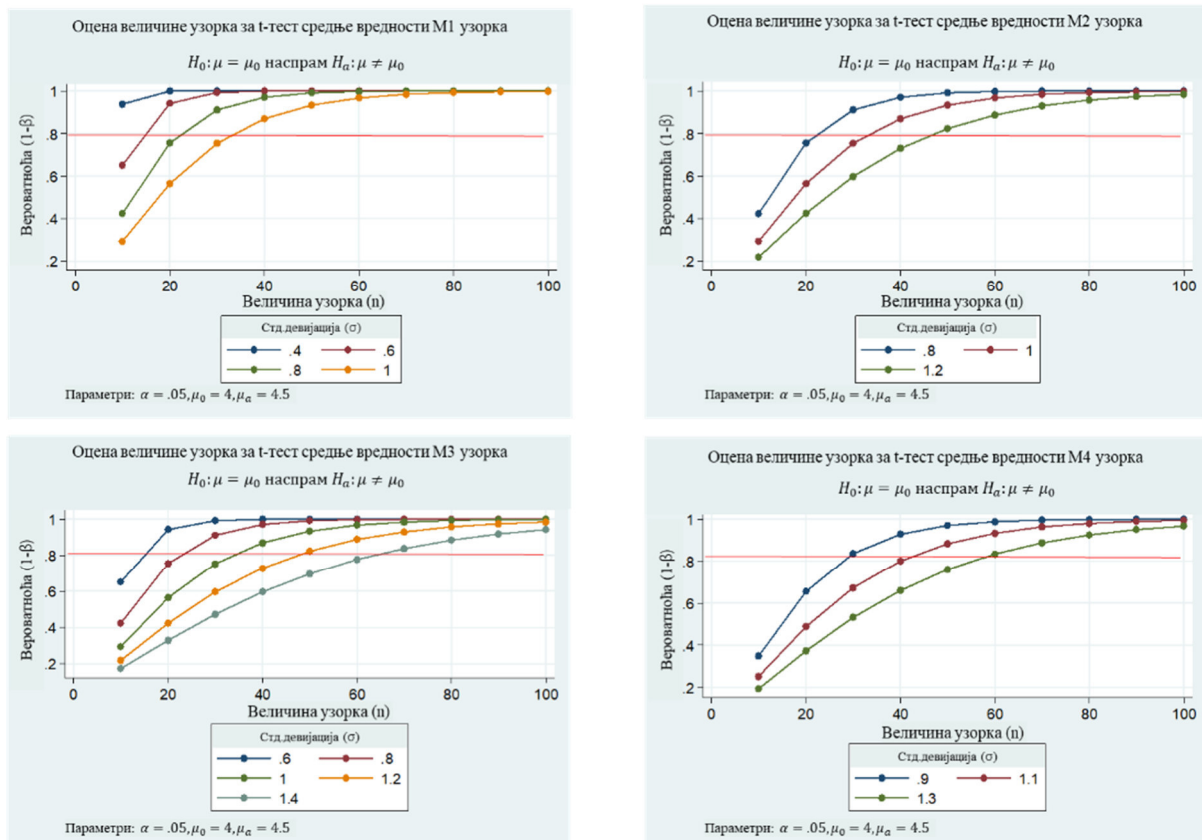
Као пример у експерименту анализирана је група питања П1 која се односи на вредновање основних карактеристика модела. За експеримент су важне њихове стандардне девијације, односно варијабилитет одговора испитаника. Оне се крећу од 0.620 код питања П1.3 до 1.119 код питања П1.5. У том распону је тестирана величина узорка (стандардне девијације 0.6, 0.8, 1.9 и 1.2). Тестирана су два екстремна случаја. У првом случају нулта хипотеза је  $H_0 = 4$  и она се тестира у односу на алтернативну хипотезу  $H_a=4.5$ . Овај случај одговара тврдњи да је модел добро постављен и одговара изјавама испитаника на питање П.1.1. Резултати су приказани на левој страни слике 15. У другом случају нулта хипотеза је такође  $H_0 = 4$ , али се она тестира у односу на алтернативну хипотезу  $H_a=3.5$ . То одговара тврдњи да је модел лош. Резултати су приказани на десној страни слике 15.

Вероватноћа да се избегне грешка типа II због погрешног прихватања нулте хипотезе је варијабла и представља решење спроведеног експеримента. Црвеном линијом обележена је вероватноћа 0.8 што се узима као висока вредност код ове врсте експеримента. За четири питања из групе П.1. (П1.1-П1.4) величина узорка од 40 је била потпуно прихватљива. Једино

је питање П.1.5 захтевало већи узорак (стандардна девијација 1.2 на слици 15). Оно, међутим, и иначе није прошло тест одбацивања нулте хипотезе сходно табели 18.

Исти тест је поновљен и са смањивањем маргине грешке са 5% на 1%, али су резултати били слични, тако да нема потребе да се наводе на овом месту. Промена алтернативне хипотезе (смањивање са 4.5 на 3.5), такође, није битније утицала на потребну величину узорка. Дакле, експеримент не потврђује нити одбацује претпоставку о ефикасности модела еVCM, него само говори о потребној величини узорка за поуздано закључивање, ако оцене испитаника имају варијабилитет као што произилази из Упитника. Закључак експеримента, примењеног на групу питања П1, потврђује да дата величина узорка не представља проблем за статистичко закључивање.

Како су стандардне девијације код осталих питања везаних за вредновање четири метода еVCM модела (групе питања П2-П5) блиске тестираном распону код основних карактеристика модела (група питања П1), може се закључити да величина узорка у целом овом истраживању не представља проблем у закључивању. Поновљен је експеримент са слике 15 (са алтернативном хипотезом  $H_a = 4.5$ ) за групе питања која се односе на вредновање четири метода еVCM модела и добијени резултати су приказани на слици 16.



Слика 16 - Хипотетичко тестирање величине узорка за четири метода модела

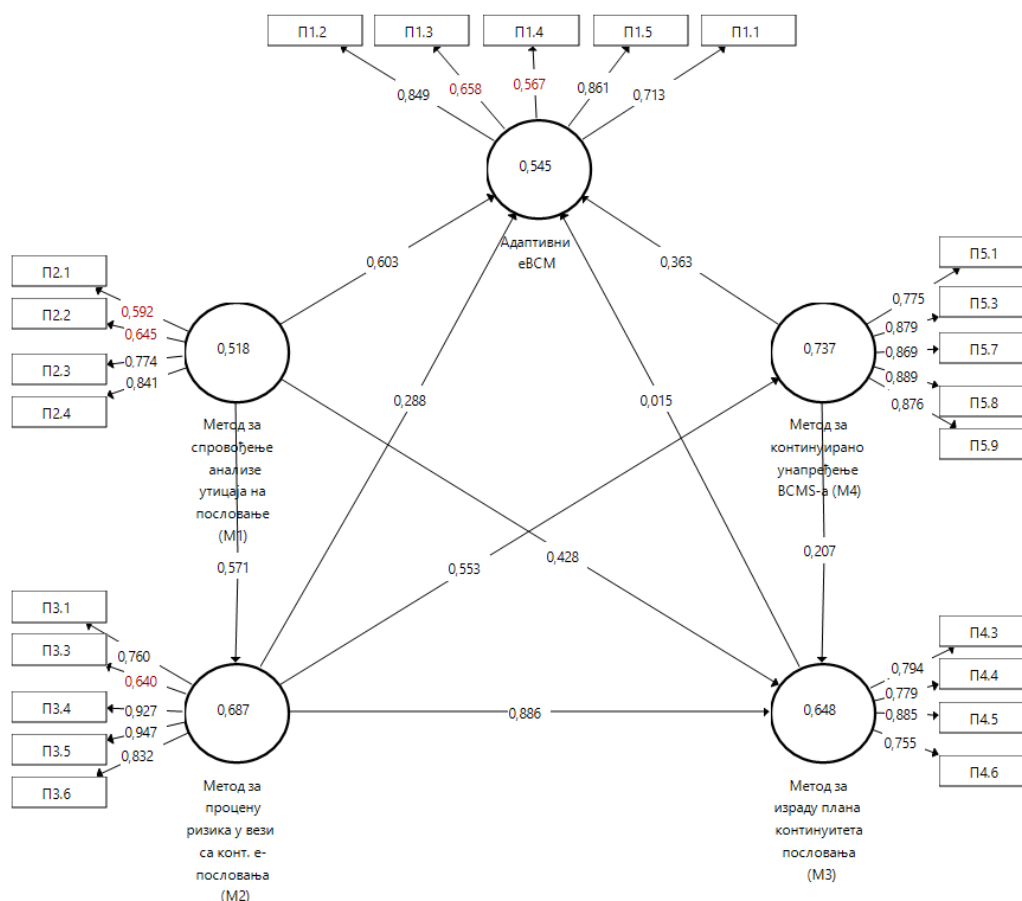
Код метода М1 ниједно питање не захтева повећање узорка. У случају метода М2 питање П3.5 захтева повећање узорка до величине 45 одговора јер има стандардну девијацију близу вредности од 1.2. Код метода М3, два питања захтевају узорак до величине 70 одговора: П4.5 и П4.6, јер је код њих стандардна девијација већа од 1.2. У случају метода М4 два питања имају стандардну девијацију већу од 1.1 због чега траже проширење узорка до величине од 60

одговора: П5.2 и П5.5. Иначе, сва питања која захтевају повећање узорка нису у претходној анализи прошла тест статистичке значајности (видети **Прилог 7**).

На основу наведене анализе може се потврдити раније изнета претпоставка да величина узорка није представљала ограничење за статистичку анализу тачности хипотеза истраживања (група питања П1) и ефикасности модела у имплементацији eVCM (групе питања П2-П5).

#### 4.5.2 Оцена PLS-SEM модела латентне варијабле

Након основних статистичких анализа резултата вредновања модела, извршена је детаљнија PLS-SEM анализа. Први део PLS-SEM анализе је оцена PLS-SEM модела латентне варијабле [151], [155], [159]–[161]. Модел латентне варијабле је представљен на слици 17 и он је рефлектујући: свака његова мера (индикатор) представља ефекат (или манифестацију) одговарајућег конструкта [151]. Сви конструкти су измерени са више индикатора. PLS-SEM модел латентне варијабле је дефинисан на основу Упитника за вредновање модела, тако да његовом оценом практично оцењујемо поузданост и валидност Упитника за вредновање модела. Анализа поузданости и валидности модела латентне варијабле спроведена је коришћењем PLS-SEM стандардног алгоритма. Резултати су приказани на слици 17 и у табели 19.



**Слика 17 - Резултати PLS алгоритма (унутрашњи модел: тотални ефекти; спољашњи модел: коефицијенти спољног оптерећења, конструкти: Average Variance Extracted - AVE)**

Прво је процењена **интерна доследност и поузданост** (енгл. *internal consistency reliability*), тј. да ли су предложени индикатори (питања из Упитника) валидне мере конструката. Као што тврди [151], композитна поузданост (енгл. *composite reliability*) јесте одговарајућа мера поузданости и интерне доследности. У поређењу са алтернативном мером - Cronbach's alpha, композитна поузданост узима у обзир варирање коефицијената спољног оптерећења самог индикатора, а не само међусобне корелације посматраних индикатора. Табела 19 показује да су вредности композитне поузданости за све конструкте између 0,80 и 0,95, демонстрирајући високу поузданост и интерну доследност [151], [159], [161].

Затим је испитано да ли је утврђена **конвергентна валидност** (енгл. *convergent validity*) мерењем поузданост индикатора и Average Variance Extracted (AVE) вредности свих конструката [151].

Индикатори повезани са истим конструктом, са великим вредностима коефицијената спољног оптерећења (енгл. *outer loadings*) имају много тога заједничког, што је уграђено у конструкт. Утврђено правило је да латентна варијабла (конструкт) треба да објасни значајан део варијансе сваког индикатора, обично најмање 50 процената. То значи да коефицијент спољног оптерећења индикатора треба да буде најмање 0,708 јер је тај број на квадрат једнак 0,50. Минимални прихватљиви ниво за коефицијент спољног оптерећења је 0,4. Сви индикатори су дефинисани у **Прилогу 5** (питања у Упитнику за вредновање модела), а њихови коефицијенти спољног оптерећења дати су у **Прилогу 7**.

**Табела 19 - Резултати оцене модела латентне варијабле**

Конструкти	Композитна поузданост	AVE
Адаптивни eBСM	0.854	0.545
Метод за спровођење анализе утицаја на пословање (M1)	0.808	0.518
Метод за процену ризика у вези са континуитетом е-пословања (M2)	0.915	0.687
Метод за израду плана континуитета пословања (M3)	0.880	0.648
Метод за континуирано унапређење BСMS-а (M4)	0.933	0.737

Од почетног скупа индикатора, дванаест индикатора са коефицијентима између 0,40 и 0,70 разматрано је за уклањање из PLS-SEM модела, као што је предложено у [151]. Уклањање сваког од индикатора пажљиво је разматрано како не би утицало на композитну поузданост или AVE вредност одговарајућег конструкта, као што је предложено у [151]. Шест индикатора са ниским коефицијентима спољног оптерећења (испод 0,7) није укључено у даљу анализу: П2.5, П2.6, П3.2, П4.1, П4.2 и П5.6. На пример, велика већина испитаника се „потпуно сложила“ са питањима „П2.5 За све кључне пословне процесе организације утврђени су циљни параметри опоравка...“ и „П4.1 Дефинисани су циљеви и делокруг система управљања континуитетом пословања...“.

Поред тога, три индикатора са високим коефицијентима спољног оптерећења (од преко 0,95) такође су искључена из PLS-SEM модела: П5.2, П5.4 и П5.5, како је препоручено у [151], тако да композитна поузданост одговарајућих конструката буде испод горње границе од 0,95.

На слици 17 је приказано да сви преостали индикатори имају коефицијенте спољног оптерећења изнад жељеног нивоа од 0,708 или близу те вредности (довољно блиске вредности су означене црвеном бојом).

Резултати оцене модела латентне варијабле (видети табелу 19) показују да су све AVE вредности веће од прихватљивог прага 0,5 који предлаже [151], што значи да сваки од конструката у просеку објашњава више од половине варијансе својих индикатора.

На крају је испитана **дискриминаторна валидност**, односно, у којој мери се у пракси један конструкт заиста разликује од других конструката. Као што тврди [151], постоје две мере дискриминаторне валидности: унакрсна оптерећења индикатора, која се сматрају либералним приступом [164], и Fornell-Larcker критеријум, који је конзервативнији приступ [165]. Применом првог приступа, утврђена је дискриминаторна валидност за све конструкте. То значи да је код сваког индикатора коефицијент спољног оптерећење на припадајућем конструкту већи од свих њихових оптерећења над осталим конструктима (зато се ова метода назива „унакрсна оптерећења“).

Fornell-Larcker критеријум упоређује квадратни корен AVE вредности конструкта са вредностима корелација тог конструкта са осталим конструктима. Прецизније, квадратни корен AVE вредности конструкта треба да буде већи од његове највеће корелације са било којим другим конструктом [151]. Резултати примене овог критеријума за процену дискриминаторне валидности приказани су у табели 20.

**Табела 20 - Дискриминаторна валидност: Fornell-Larcker критеријум**

Конструкт	М1	Адапти вни еVCM	М4	М3	М2
Метод за спровођење анализе утицаја на пословање (М1)	0.720				
Адаптивни еVCM	0.619	0.738			
Метод за континуирано унапређење VCMС-а (М4)	0.359	0.569	0.859		
Метод за израду плана континуитета пословања (М3)	0.437	0.489	0.606	0.805	
Метод за процену ризика у вези са континуитетом е-пословања (М2)	0.571	0.538	0.553	0.841	0.829

На основу Fornell-Larcker критеријума дискриминаторна валидност није потврђена само између Метода за процену ризика у вези са континуитетом е-пословања (М2) и Метода за израду плана континуитета пословања (М3). Пошто је корелација између ова два конструкта само нешто већа од квадратног корена AVE вредности за конструкт М3 (приближно за 0,037), ово одступање се може сматрати прихватљивим.

Из свега наведеног, можемо закључити да су мерне карактеристике конструката прихватљиве, и да је PLS-SEM модел латентне варијабле прошао тест поузданости и валидности, а самим тим и Упитник за вредновање модела.

#### 4.5.3 Оцена PLS-SEM структурног модела и тестирање хипотеза евалуације

У трећем кораку вредновања Модела за адаптивно управљање континуитетом електронског пословања оцењен је PLS-SEM структурни модел. Спроведене су следеће процене [151], [155], [159]–[161]:

- колинеарност између конструката,
- предиктивна тачност модела,
- предиктивна релевантност модела и
- структурни односи унутар модела (тј. тестирање хипотеза евалуације).

Први корак у процени структуралног модела је **процена колинеарности**. Разлог је тај што се процена коефицијената путање у структурним моделима заснива на регресионој методи најмањих квадрата (енгл. *Ordinary least squares*, скраћено OLS) сваке ендogene латентне варијабле на основу претходних конструката (конструката претходника на путањи). У свим методама вишеструке регресије, у које спада и метода најмањих квадрата, коефицијенти путање могу бити пристрасни ако постоји значајан ниво колинеарности између конструката предиктора исте варијабле [151]. За процену колинеарности у PLS-SEM анализи се користи VIF фактор, односно фактор инфлације варијанце (енгл. *variance inflation factor*). Резултати примене овог критеријума показали су да дефинисани структурни модел нема проблем колинеарности, пошто су све вредности VIF фактора испод вредности 5, као што препоручује [151], [160].

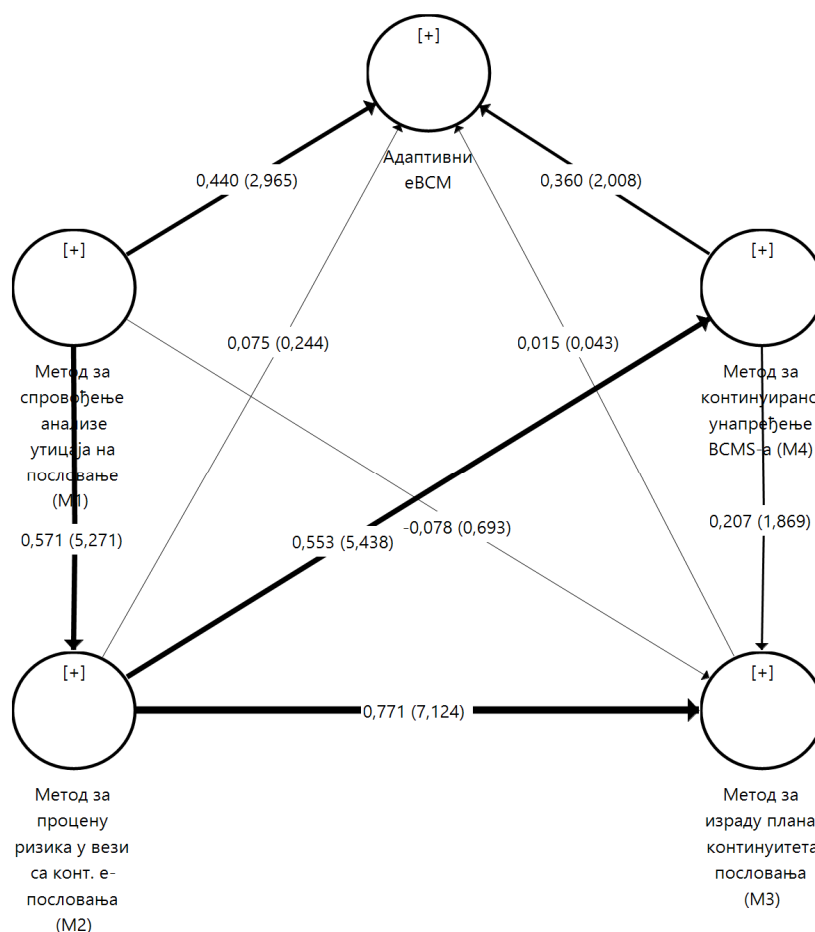
Основни критеријум за **процену предиктивне тачности SEM модела** је коефицијент детерминације ( $R^2$ ), који се израчунава као квадратна корелација стварних и предвиђених вредности одређеног ендogene конструкта [151]. Коефицијент представља комбиноване ефекте егзогенних латентних варијабли на ендogenous латентну варијаблу. Вредности  $R^2$  коефицијента за ендogene латентне варијабле су: Адаптивни eVCM ( $R^2 = 0,525$ ), М2 ( $R^2 = 0,326$ ), М3 ( $R^2 = 0,741$ ) и М4 ( $R^2 = 0,305$ ). Вредност  $R^2$  за М3 се сматра значајном, док се вредности  $R^2$  за остале ендogene латентне варијабле (Адаптивни eVCM, М2 и М4) сматрају умереним [164][166].

За **процену предиктивне релевантности SEM модела** коришћен је Stone-Geisser-ов параметар  $Q^2$  [167], [168]. Вредности  $Q^2$  веће од нуле за одређену рефлективну ендogenous латентну варијаблу указују на предиктивну релевантност структурног модела за овај одређени конструкт. Применом *blindfolding* процедуре са стандардном даљином изостављања од седам (енгл. *omission distance D=7*), у оквиру SmartPLS софтвера добијена је  $Q^2$  вредност од 0,427 за М3, што указује на велику предиктивну релевантност [151]. Остале ендogene латентне



променљиве имају средњу предиктивну релевантност: Адаптивни eVCM ( $Q^2 = 0,227$ ), M2 ( $Q^2 = 0,187$ ) и M4 ( $Q^2 = 0,175$ ).

**Структурни односи унутар PLS-SEM модела** који представљају хипотезе евалуације процењени су коришћењем коефицијената путање, који су добијени након покретања PLS алгоритма (видети слику 17). Коефицијенти путање који имају вредност близу +1 представљају снажне позитивне односе (и обрнуто за негативне вредности) који су готово увек статистички значајни. Што су ближе процењене вредности коефицијената путање вредности 0, то су слабији односи у моделу. Да ли је коефицијент путање значајан зависи од његове стандардне грешке која се добија помоћу методе реузорковања (енгл. *bootstrapping*). Стандардна грешка реузорковања омогућава израчунавање емпиријске t-вредности. Када је емпиријска t-вредност већа од унапред дефинисане критичне вредности, кажемо да је коефицијент значајан са одређеном вероватноћом грешке (тј. са одређеним нивоом значајности). У овом истраживању коришћена је критична вредност од 1,96 која одговара нивоу значајности од 5% [151]. Структурни модел је оцењен применом методе реузорковања са 10,000 узорака и поменути нивоом значајности од 5%. Резултати су приказани на слици 18 и у табели 21.



**Слика 18 - Резултати реузорковања (унутрашњи модел: коефицијенти путање и у заградама t-вредности)**

Резултати указују на позитиван и значајан утицај Метода за спровођење анализе утицаја на пословање (M1) и Метода за континуирано унапређење BCMS-а (M4) на Адаптивни eVCM, али нису потврдили значајан директни ефекат Метода за процену ризика у вези са

континуитетом е-пословања (М2) или Метода за израду плана континуитета пословања (М3). М1 има најјачи ефекат на Адаптивни еВСМ ( $\beta = 0,440$ ,  $t > 1,96$ ), а потом М4 ( $\beta = 0,360$ ,  $t > 1,96$ ). На основу ових резултата се може закључити да су хипотезе евалуације **H1a** и **H1d** потврђене. Однос између Метода за процену ризика у вези са континуитетом е-пословања (М2) и Адаптивног еВСМ није значајан ( $\beta = 0,075$ ,  $t < 1,96$ ), па хипотеза **H1b** није потврђена. На сличан начин, ни хипотеза **H1c** није потврђена, јер однос између Метода за израду плана континуитета пословања (М3) и Адаптивног еВСМ није значајан ( $\beta = 0,015$ ,  $t < 1,96$ ).

Метод за спровођење анализе утицаја на пословање (М1) има значајан утицај ( $\beta = 0,571$ ,  $t > 1,96$ ) на Метод за процену ризика у вези са континуитетом е-пословања (М2), па је хипотеза **H2a** потврђена. Са друге стране, М1 нема значајан утицај на М3 ( $\beta = -0,078$ ,  $t < 1,96$ ) па, према томе, хипотеза **H2b** није потврђена.

Метод за процену ризика у вези са континуитетом е-пословања (М2) има значајан утицај и на М3 ( $\beta = 0,771$ ,  $t > 1,96$ ) и на М4 ( $\beta = 0,553$ ,  $t > 1,96$ ), што потврђује хипотезе **H3a** и **H3b**.

И на крају, хипотеза **H4** није потврђена пошто однос између Метода за континуирано унапређење ВСМС-а (М4) и Метода за израду плана континуитета пословања (М3) није значајан ( $\beta = 0,207$ ,  $t < 1,96$ ).

**Табела 21 - Резултати реузорковања**

Хипотезе евалуације	Оригинални узорак	Средња вредност узорка	Стандардна девијација	t-вредност
H1a: M1 -> Адаптивни еВСМ	0.440	0.468	0.148	2.965***
H1b: M2 -> Адаптивни еВСМ	0.075	0.104	0.307	0.244
H1c: M3 -> Адаптивни еВСМ	0.015	0.009	0.359	0.043
H1d: M4 -> Адаптивни еВСМ	0.360	0.298	0.179	2.008***
H2a: M1 -> M2	0.571	0.598	0.108	5.438***
H2b: M1 -> M3	-0.078	-0.071	0.112	0.693
H3a: M2 -> M3	0.771	0.769	0.108	7.124***
H3b: M2 -> M4	0.553	0.564	0.102	5.438***
H4: M4 -> M3	0.207	0.204	0.111	1.869

\*\*\*  $t > 1,96$  (ниво значајности 5%)

## 4.6 Дискусија резултата

Основна статистичка анализа потврђује полазне хипотезе истраживања и ефикасност модела у имплементацији еВСМ-а. Метод за спровођење анализе утицаја на пословање (М1) најефикаснији је у пракси, док су за остала три метода потребна додатна прилагођавања модела да би се постигао жељени ниво ефикасности.

Хипотезе евалуације тестиране у PLS-SEM анализи могу се поделити у две групе: једна која испитује директан допринос модела у успостављању адаптивног еВСМ-а (Н1а, Н1б, Н1с, Н1д) и друга која испитује унутрашњу структуру модела, то јест, међузависности метода као компонената модела (Н2а, Н2б, Н3а, Н3б, Н4). Резултати тестирања хипотеза приказани су у табели 22.

Табела 22 - Резултати тестирања хипотеза евалуације

Хипотеза евалуације	Статус хипотезе
<b>Група 1: Директан допринос метода у успостављању адаптивног еВСМ-а</b>	
<b>Н1а:</b> Метод за спровођење анализе утицаја на пословање (М1) доприноси успостављању адаптивног еВСМ-а.	<b>Потврђена</b>
<b>Н1б:</b> Метод за процену ризика у вези са континуитетом електронског пословања (М2) доприноси успостављању адаптивног еВСМ-а.	Није потврђена
<b>Н1с:</b> Метод за израду плана континуитета пословања (М3) доприноси успостављању адаптивног еВСМ-а.	Није потврђена
<b>Н1д:</b> Метод за континуирано унапређење ВСМС-а (М4) доприноси успостављању адаптивног еВСМ-а.	<b>Потврђена</b>
<b>Група 2: Унутрашња структура модела</b>	
<b>Н2а:</b> Примена Метода за спровођење анализе утицаја на пословање (М1) доприноси примени Метода за процену ризика у вези са континуитетом е-пословања (М2).	<b>Потврђена</b>
<b>Н2б:</b> Примена Метода за спровођење анализе утицаја на пословање (М1) доприноси примени Метода за израду плана континуитета пословања (М3).	Није потврђена
<b>Н3а:</b> Примена Метода за процену ризика у вези са континуитетом е-пословања (М2) доприноси примени Метода за израду плана континуитета пословања (М3).	<b>Потврђена</b>

Хипотеза евалуације	Статус хипотезе
<b>H3b:</b> Примена Метода за процену ризика у вези са континуитетом е-пословања (M2) доприноси примени Метода за континуирано унапређење ВСМС-а (M4).	Потврђена
<b>H4:</b> Примена Метода за континуирано унапређење ВСМС-а (M4) доприноси примени Метода за израду плана континуитета пословања (M3).	Није потврђена

Адаптивни еВСМ, који обухвата полазне хипотезе истраживања, представља ефикасност модела у успостављању адаптивног еВСМ-а. Резултати показују да Метод за спровођење анализе утицаја на пословање (M1) и Метод за континуирано унапређење ВСМС-а (M4) имају позитиван и значајан утицај на успостављање адаптивног еВСМ-а, чиме су хипотезе **H1a** и **H1d** потврђене. За остала два метода, Метод за процену ризика у вези са континуитетом електронског пословања (M2) и Метод за израду плана континуитета пословања (M3), резултати PLS-SEM анализе нису показали значајне ефекте, тј. хипотезе **H1b** и **H1c** нису потврђене. То значи да су, у предложеном моделу, ВИА анализа и континуирано унапређења ВСМС-а фактори који су примарно одговорни за ефикасно успостављање адаптивног еВСМ-а. С друге стране, резултати евалуације показују да Метод за процену ризика у вези са континуитетом е-пословања (M2) има индиректни утицај на Адаптивни еВСМ, преко Метода за континуирано унапређење ВСМС-а (M4), јер су резултати процене ризика основа за третман ризика.

У другој групи хипотеза евалуације које оцењују међузависности метода модела, две хипотезе нису потврђене: **H2b** (M1 -> M3) и **H4** (M4 -> M3).

План континуитета пословања (ВСР) јесте документовани скуп поступака који усмерава организацију да одговори, да се опорави и да настави са пословањем на унапред дефинисаном нивоу активности након инцидентног догађаја [1]. ВСР омогућава да се кључни пословни процеси опораве брзо и ефикасно, да се штета по пословање организације сведе на минимум и да се управља прекидом у пословању [111]. Планом континуитета пословања се успоставља функционисање кључних пословних процеса организације у оквиру циљних параметара опоравка, који су дефинисани ВИА анализом [137]. Из тих разлога је очекивано да постоји значајан директни утицај Метода за спровођење анализе утицаја на пословање (M1) на Методу за израду плана континуитета пословања (M3). Иако ова хипотеза није потврђена у поступку вредновања модела, потврђена је индиректна веза између метода M1 и M3 преко Метода за процену ризика у вези са континуитетом е-пословања (M2). Овакав резултат истиче важност редоследа у примени метода модела. Из свега наведеног можемо закључити да је неопходно спровести и ВИА анализу и процену ризика као основе за дефинисање плана континуитета пословања.

У оквиру Метода за континуирано унапређење ВСМС-а (M4) у планираним интервалима се тестира план континуитета пословања, којим се потврђује његов садржај и проверава могућност опоравка кључних пословних процеса у оквиру циљних параметара опоравка [1], [59]. Самим тим је веза између Метода за континуирано унапређење ВСМС-а (M4) и Метода за израду плана континуитета пословања (M3) неопходан део ефикасног управљања континуитета пословања. За хипотезу евалуације **H4**, која дефинише везу између ова два

метода, емпиријска t-вредност је нешто испод границе прихватања ( $t=1.869$ ), тј. хипотеза није потврђена али није у потпуности ни одбачена. За ефикасно управљање континуитетом пословања је потребно време, па је потребно урадити и додатно вредновање модела након неколико година од његовог увођења.

Модел би требало примењивати сваки пут када дође до промене било ког од параметара модела, што омогућава да еВСМ флексибилно одговори на промене у пословном окружењу организације. Корективне мере за унапређење ВСМС-а су дефинисане у оквиру Метода за континуирано унапређење ВСМС-а (М4). Прилагодљивост променама у пословном окружењу организације, заједно са корективним мерама за унапређење ВСМС-а, омогућава адаптивни еВСМ.

Како је већина хипотеза евалуације потврђена, можемо закључити да је у пракси потврђено да је модел ефикасан у успостављању адаптивног управљања континуитетом е-пословања, као и да поседује неопходну унутрашњу конзистентност и логичку структуру.

## 5 Научни и стручни доприноси

Основни научни допринос докторске дисертације је развој модела за адаптивно управљање континуитетом електронског пословања који је прилагодљив променама у окружењу у коме послује организација. Предложени модел дефинише општи оквир за успостављање и континуирано унапређење еВСМ-а, а посебно је прилагођен организацијама које користе савремене технологије е-пословања. Модел дефинише практичне кораке за дефинисање важних елемената система управљања континуитетом пословања (ВСМС): анализе утицаја на пословања, процене ризика и плана континуитета пословања. Осим тога, модел води организацију кроз континуирано унапређење ВСМС-а који је, као што је показано, један од главних покретача ефикасног успостављања адаптивног еВСМ-а.

Улога модела је да унапреди и побољша успостављање континуитета електронског пословања коришћењем техника које су посебно прилагођене специфичним карактеристикама организације, без обзира на величину и тип организације. Предложени модел адаптивног управљања континуитетом електронског пословања је примењен у пракси, у три организације које послују у финансијском сектору у Србији.

Научни доприноси дисертације огледају се у:

- Дефинисању новог концепта управљања континуитетом електронског пословања (еВСМ), чиме се уводи и нова област истраживања и одговарајући сет нових појмова;
- Дефинисању модела за адаптивно управљање континуитетом електронског пословања који је прилагодљив променама у окружењу у коме послује организација која користи савремене технологије е-пословања;
- Дефинисању метода за спровођење анализе утицаја на пословање;
- Дефинисању метода за процену ризика у вези са континуитетом е-пословања;
- Дефинисању метода за израду плана континуитета пословања;
- Дефинисању метода за континуирано унапређење ВСМС-а.

Стручни доприноси дисертације огледају се у:

- Систематизацији литературе из области управљање континуитетом пословања и развоја модела за адаптивно управљање континуитетом пословања;
- Дефинисању смерница за примену предложеног модела у пракси у било којој врсти организације;
- Анализи предложеног модела са аспекта ефикасности, корисности и применљивости у успостављању континуитета електронског пословања;
- Анализи предложеног модела са аспекта прилагодљивости променама у окружењу у коме послује организација.

## 6 Будућа истраживања

Мали узорак евалуације представља главно ограничење овог истраживања. Из тог разлога је одабрана PLS-SEM метода за вредновање модела, која је ефикасна са малим величинама узорка. Поред тога, анализом величине узорка методом нулте хипотезе, примењене на средње вредности узорка, показано је да величина узорка не утиче на статистичко закључивање које је спроведено у оквиру поступку вредновања модела – под датим емпиријским карактеристикама варијабилитета одговора испитаника. Уколико би стандардне девијације оцена испитаника биле веће у неком новом истраживању, потребно је, наравно, повећати величину узорка. Након додатних примена еВСМ модела у пракси, биће спроведено вредновање модела на већем узорку.

Модел је дефинисан као општи оквир који се може применити у било којој организацији која користи савремене технологије е-пословања, али је у пракси примењен само у организацијама из финансијског сектора. Како би се адресирало ово потенцијално питање валидности истраживања, додатни правац у будућем истраживању ће бити имплементација модела у организацијама које нису у финансијском сектору. Овај правац је делимично назначен применом модела у Народној банци Србије, у оквиру које послује и Завод за израду новчаница и кованог новца (ЗИН) као посебан привредни субјекат из области графичке индустрије.

Додатно, организације у којима је примењен модел имају карактеристике заједничке са другим организацијама које користе савремене технологије е-пословања и то: 1) коришћење електронских сервиса (е-услуга) које су кључне за пословање (нпр. продаја осигурања путем интернета, В2В услуге у НБС, итд.), 2) коришћење виртуалне инфраструктуре, 3) постојање пословних процеса који укључују више организационих јединица и 4) високи стандарди везани за безбедност информација и заштиту података.

Будућа истраживања ће обухватити додатну примену и вредновање модела у организацијама које користе савремене технологије е-пословања, како у финансијском сектору, тако и изван њега.

## 7 Закључак

Управљање континуитетом пословања (ВСМ) је интердисциплинарна област од широког и актуалног значаја у данашње време које се може окарактерисати растућим претњама од природних катастрофа, инцидената изазваних људским фактором и несрећа/технолошких инцидената [33]. У случају инцидентног догађаја, недостатак ВСМ-а може проузроковати озбиљан губитак прихода, а у најгорем случају, може довести и до престанка пословања [99]. Приликом успостављања ВСМ-а је потребно сагледати најгори могући сценарио који би се могао догодити и одредити колико брзо се кључни пословни процеси могу опоравити, као и колико брзо пословање може доћи до тачке са које нема повратка [99]. Главни циљ ВСМ-а је ублажавање губитака и припрема ефикасног реаговања у случају већих инцидентних догађаја.

Коришћење савремених технологија е-пословања и њихов убрзани развој, значајно је повећао ризике од потенцијалних претњи изазваних инцидентним догађајима којима су изложене организације и њихови информациони системи. Истраживање у оквиру ове докторске дисертације уводи нов концепт „Управљања континуитетом електронског пословања“ (еВСМ) које је погодно за модерна технолошка окружења, и које пружа организацијама адекватан одговор на поменуте претње. Истраживање је фокусирано на управљање континуитетом пословања у организацијама које користе савремене технологије електронског пословања: интернет, мобилно рачунарство, електронске сервисе и виртуалну инфраструктуру.

Основни циљ истраживања је дефинисање модела за адаптивно управљање континуитетом електронског пословања који је довољно општи и довољно флексибилан да може да се примени у успостављању еВСМ-а у било којој организацији. Модел је примењен у три финансијске организације различитих величина, и у оквиру истраживања процењена је његова ефикасност у успостављању адаптивног еВСМ-а. Резултати PLS-SEM анализе показали су да два од четири метода модела - ВІА анализа и континуирано побољшање ВСМ-а - имају статистички позитиван допринос ефикасном успостављању адаптивног еВСМ-а. Са друге стране, тестирање нулте хипотезе је показало да је модел у целости ефикасан у примени адаптивног еВСМ-а, као и сви методи модела изузев метода за континуирано побољшање ВСМ-а. Ови резултати су делимично потврђени и тестом статистичке значајности. За недвосмислену процену ефикасности модела у успостављању адаптивног еВСМ-а потребне су додатне примене и евалуације на додатним подацима.

Иако је узорак евалуације модела релативно мали, важно је истаћи да је једна од институција која је применила предложени модел централна банка, са комплексним пословним процесима и специфичним захтевима. Из тог разлога може се сматрати да су резултати евалуације релевантни, а посебно у околностима када у доступној литератури не постоје слична истраживања.

Будућа истраживања ће обухватити даљи развој модела и додатне његове примене како у финансијском сектору, тако и изван њега. Са новим променама у пракси биће спроведене и додатне евалуације модела са циљем да се докаже да сва четири метода модела имају важан допринос ефикасном успостављању адаптивног еВСМ-а.



## 8 Литература

- [1] *ISO 22301:2012 Societal security - Business continuity management systems - Requirements*. Geneva: International Organization for Standardization, 2012.
- [2] B. Radenković, M. Despotović Zrakić, Z. Bogdanović, D. Barać, and A. Labus, *Elektronsko poslovanje*. Beograd: Fakultet organizacionih nauka, 2015.
- [3] K. C. Laudon and C. Guercio Traver, *E-commerce 2012: business, technology, society*, 8th ed. Pearson Education, 2012.
- [4] D. Chaffey, “E-Business and E-Commerce Management - Strategy, Implementation and Practice,” 4th ed., Prentice Hall, 2009.
- [5] F. Arduini and V. Morabito, “Can banks protect themselves for the unthinkable? A Business Continuity Update,” *Commun. ACM*, vol. 53, no. 3, pp. 121–125, 2010.
- [6] J. Bergström, R. van Winsen, and E. Henriqson, “On the rationale of resilience in the domain of safety: A literature review,” *Reliab. Eng. Syst. Saf.*, vol. 141, pp. 131–141, Sep. 2015, doi: 10.1016/j.res.2015.03.008.
- [7] M. Smith and P.-A. Shields, “Strategies for IT and communications,” in *The Definitive Handbook of Business Continuity Management*, A. Hiles, Ed. John Wiley & Sons, Ltd, 2007, pp. 205–235.
- [8] W. Lewis, R. T. Watson, and A. Pickren, “An empirical assessment of IT disaster risk,” *Commun. ACM*, vol. 46, no. 9, p. 201, 2003, doi: 10.1145/903893.903938.
- [9] J. Cook, “A Six-Stage Business Continuity and Disaster Recovery Planning Cycle,” *SAM Adv. Manag. J.*, vol. 80, no. 3, pp. 23–68, 2015.
- [10] M. Rabbani, H. R. Soufi, and S. A. Torabi, “Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery,” *Saf. Sci.*, vol. 85, pp. 9–22, Jun. 2016, doi: 10.1016/j.ssci.2015.12.025.
- [11] B. Herbane, “The evolution of business continuity management: A historical review of practices and drivers,” *Bus. Hist.*, vol. 52, no. 6, pp. 978–1002, 2010, doi: 10.1080/00076791.2010.511185.
- [12] *Foreign Corrupt Practices Act (FCPA)*, Pub.L. 95-213. USA: Department of Justice, 1977.
- [13] *Expedited Funds Availability Act (Regulation CC)*. USA: National Credit Union Administration, 1987.
- [14] *Financial Services Modernization Act (“Gramm–Leach–Bliley Act”)*, Pub.L. 106-102. USA, 1999.

- [15] *Health Insurance Portability and Accountability Act (HIPAA)*, Pub.L. 104–191. USA, 1996.
- [16] *Telecommunications Act*, Pub.L. 104-104. USA, 1996.
- [17] *Enduring Constitutional Government and Continuity of Government Operations, Presidential Decision Directive 67 (PDD 67)*. USA, 1998.
- [18] *Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD 63)*. USA, 1998.
- [19] *Interagency paper on sound practices to strengthen the resilience of the U.S. financial system*. USA: Securities and Exchange Commission, 2002.
- [20] *Business continuity planning booklet*. USA: Federal Financial Institutions Examination Council (FFIEC), 2003.
- [21] *The Business Continuity Institute 10 standards of professional competence*. London: Business Continuity Institute, 2003.
- [22] *Good practice guidelines (1st ed.)*. London: Business Continuity Institute, 2002.
- [23] *Publicly available specification 56: Guide to business continuity management*. London: British Standards Institution, 2003.
- [24] *BH 221: Business continuity management, second edition*. Sydney: Standards Australia, 2004.
- [25] *SS507 Singapore standard for business continuity/disaster recovery service providers*. Singapore: The Standards, Productivity and Innovation Board (SPRING Singapore), 2004.
- [26] *ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management*. Geneva: International Organization for Standardization, 2007.
- [27] *BS 25999-2:2007 Specification for Business Continuity Management*. London: British Standards Institution, 2007.
- [28] *BS 25999-1:2006 Business Continuity Management. Code of Practice*, no. Nov. London: British Standards Institution, 2006, p. 42.
- [29] B. S. Butler and P. H. Gray, “Reliability, mindfulness, and information systems,” *MIS Q. Manag. Inf. Syst.*, vol. 30, no. 2, pp. 211–224, 2006, doi: 10.2307/25148728.
- [30] *ISO/IEC 25000:2014 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE*. Geneva: International Organization for Standardization, 2014.
- [31] E. Bauer, *Design for Reliability: Information and Computer-Based Systems*, 1st ed. Wiley-IEEE Press, 2010.

- [32] E. Bauer and R. Adams, *Reliability and Availability of Cloud Computing*, 1st ed. Wiley-IEEE Press, 2012.
- [33] M. Labus, M. Despotović-Zrakić, and Z. Bogdanović, “Introducing adaptive E-business continuity management,” *Adv. Intell. Syst. Comput.*, vol. 569, 2017, doi: 10.1007/978-3-319-56535-4\_62.
- [34] M. Turoff, S. R. Hiltz, V. A. Bañuls, and G. Van Den Eede, “Multiple perspectives on planning for emergencies: An introduction to the special issue on planning and foresight for emergency preparedness and management,” *Technol. Forecast. Soc. Change*, vol. 80, no. 9, pp. 1647–1656, 2013, doi: 10.1016/j.techfore.2013.07.014.
- [35] J. Hall, *Information Technology Auditing*, Internatio. Mason, OH, United States: Cengage Learning, Inc, 2010.
- [36] S. Snedaker and C. Rima, *Business Continuity and Disaster Recovery Planning for IT Professionals*, Second Edi. Elsevier Inc., 2014.
- [37] *Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*. Brussels: Commission of the European Communities, 2006, p. 28.
- [38] *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Brussels: The Council of the European Union, 2008, pp. 75–82.
- [39] *Directive 2009/138/EC (Solvency II)*, vol. L335. Brussels: European Parliament and European Council, 2009, p. L335/1-129.
- [40] *High-level principles for business continuity*. Basel: Bank for International Settlements, Basel Committee on Banking Supervision, 2006.
- [41] *Basel II: International Convergence of Capital Measurement and Capital Standards*. Basel: Basel Committee on Banking Supervision, 2004.
- [42] *Basel - 1: International Convergence of Capital Measurement and Capital Standards*. Basel: Basel Committee on Banking Supervision, 1988.
- [43] *Basel III: A global regulatory framework for more resilient banks and banking systems December 2010 (rev June 2011)*. Basel: Basel Committee on Banking Supervision, 2011.
- [44] *Implementing Recommendations of the 9/11 Commission Act of 2007, Pub.L. 110–53*. USA, 2007, pp. 1–286.
- [45] *Sarbanes-Oxley Act, Pub.L 107-204*. USA, 2002.
- [46] *Consumer Credit Protection Act, Pub.L. 90-321*. USA, 2018, pp. 1–292.

- [47] *E-Government Act of 2002, Pub.L. 107-347*. USA, 2002.
- [48] *Emergency Management and Civil Protection Act, R.S.O. 1990, CHAPTER E.9*. Canada, 1990.
- [49] *Civil Contingencies Act 2004, 2004 CHAPTER 36*. United Kingdom, 2004.
- [50] R. Marshall, A. Isaac, and J. Ryan, "Integration of Operational Risk Management and the Sarbanes-Oxley Act Section 404," in *Risk Management: A Modern Perspective*, 2005.
- [51] *Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije*, „Službeni glasnik RS“, br. 23/2013, 113/2013, 2/2017 i 88/2019. Republika Srbija: NBS, 2019.
- [52] *Odluka o izmenama i dopunama Odluke o minimalnim standardima upravljanja informacionim sistemom finansijske institucije*, „Službeni glasnik RS“, br. 88/2019. Republika Srbija: NBS, 2019.
- [53] *Zakon o sustavu civilne zaštite, NN 82/15, 118/18*. Republika Hrvatska, 2015.
- [54] *Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika*. Republika Hrvatska: Hrvatska narodna banka, 2006.
- [55] *Одлука о управљању информационим системима у банкама*. Република Српска: Агенције за банкарство Републике Српске, 2017.
- [56] *Odluka o upravljanju informacionim sistemom u banci*. BiH: Agencije za bankarstvo Federacije BiH, 2017.
- [57] *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*. Geneva: International Organization for Standardization, 2019.
- [58] International Organization for Standardization, "ISO 22301 - Business Continuity." ISO, Geneva, 2019, [Online]. Available: <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100442.pdf>.
- [59] B. Zawada and G. Marbais, "Implementing ISO 22301," *Avalution Consulting*. 2015.
- [60] *ISO 22300:2018 Security and resilience — Vocabulary*. Geneva: International Organization for Standardization, 2018.
- [61] *ISO 22311:2012 Societal security — Video-surveillance — Export interoperability*. Geneva: International Organization for Standardization, 2012.
- [62] *ISO/TR 22312:2011 Societal security — Technological capabilities*. Geneva: International Organization for Standardization, 2011.

- [63] *ISO 22313:2012 Societal security — Business continuity management systems — Guidance*. Geneva: International Organization for Standardization, 2012.
- [64] *ISO 22315:2014 Societal security — Mass evacuation — Guidelines for planning*. Geneva: International Organization for Standardization, 2014.
- [65] *ISO/TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*. Geneva: International Organization for Standardization, 2015.
- [66] *ISO/TS 22318:2015 Societal security — Business continuity management systems — Guidelines for supply chain continuity*. Geneva: International Organization for Standardization, 2015.
- [67] *ISO 22320:2018 Security and resilience — Emergency management — Guidelines for incident management*. Geneva: International Organization for Standardization, 2018.
- [68] *ISO 22322:2015 Societal security — Emergency management — Guidelines for public warning*. Geneva: International Organization for Standardization, 2015.
- [69] *ISO 22324:2015 Societal security — Emergency management — Guidelines for colour-coded alerts*. Geneva: International Organization for Standardization, 2015.
- [70] *ISO 22397:2014 Societal security — Guidelines for establishing partnering arrangements*. Geneva: International Organization for Standardization, 2014.
- [71] *ISO 22398:2013 Societal security — Guidelines for exercises*. Geneva: International Organization for Standardization, 2013.
- [72] *Good Practice Guidelines*. London: Business Continuity Institute, 2018.
- [73] *BSI-Standard 100-4: Business Continuity Management*. Bonn, Germany: Federal Office for Information Security (BSI), 2009.
- [74] *COBIT 5 – Control Objectives for Information & Related Technology 5*. USA: ISACA, IT Governance Institute Standards, 2014.
- [75] S. Lacy and I. Macfarlane, *ITIL: Service Transition*. London: The Stationery Office, 2007.
- [76] Majid Iqbal and M. Nieves, *ITIL: Service Strategy*. London: The Stationery Office, 2007.
- [77] Office of Government Commerce, *ITIL: Service Operation*. London: The Stationery Office, 2007.
- [78] C. Rudd and V. Lloyd, *ITIL: Service Design*. London: The Stationery Office, 2007.

- [79] G. Spalding, *ITIL: Continual Service Improvement*. London: The Stationery Office, 2007.
- [80] *ISO 9001:2015 Quality management systems — Requirements*. Geneva: International Organization for Standardization, 2015.
- [81] *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Geneva: International Organization for Standardization, 2013.
- [82] *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*. Geneva: International Organization for Standardization, 2013.
- [83] *ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance*. Geneva: International Organization for Standardization, 2017.
- [84] *ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*. Geneva: International Organization for Standardization, 2016.
- [85] *ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. Geneva: International Organization for Standardization, 2016.
- [86] *ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*. Geneva: International Organization for Standardization, 2016.
- [87] *ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*. Geneva: International Organization for Standardization, 2014.
- [88] *ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements*. Geneva: International Organization for Standardization, 2014.
- [89] *ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*. Geneva: International Organization for Standardization, 2013.
- [90] *ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*. Geneva: International Organization for Standardization, 2011.
- [91] *NIST SP 800-34 Contingency Planning Guide for Federal Information Systems*. USA: National Institute of Standards and Technology, 2010.

- [92] *ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements*. Geneva: International Organization for Standardization, 2018.
- [93] *ISO/IEC TS 17021-6:2014 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems*. Geneva: International Organization for Standardization, 2014.
- [94] *ISO 31000:2018 Risk management — Guidelines*. Geneva: International Organization for Standardization, 2018.
- [95] *ISO GUIDE 73:2009 Risk management — Vocabulary*. Geneva: International Organization for Standardization, 2009.
- [96] *IEC 61508:2010 Functional Safety of Electrical, Electronic and Programmable Electronic Safety Related Systems*. Geneva: International Electrotechnical Commission, 2010.
- [97] *IEC 60300-1:2014 Dependability management - Part 1: Guidance for management and application*. Geneva: International Electrotechnical Commission, 2014.
- [98] D. Faertes, “Reliability of supply chains and business continuity management,” *Procedia Comput. Sci.*, vol. 55, no. Itqm, pp. 1400–1409, 2015, doi: 10.1016/j.procs.2015.07.130.
- [99] F. Gibb and S. Buchanan, “A framework for business continuity management,” *Int. J. Inf. Manage.*, vol. 26, no. 2, pp. 128–141, 2006, doi: 10.1016/j.ijinfomgt.2005.11.008.
- [100] S. M. Hawkins, D. C. Yen, and D. C. Chou, “Disaster recovery planning: a strategy for data security,” *Inf. Manag. Comput. Secur.*, vol. 8, no. 5, pp. 222–230, 2000, doi: 10.1108/09685220010353150.
- [101] C. W. Zobel, “Representing perceived tradeoffs in defining disaster resilience,” *Decis. Support Syst.*, vol. 50, no. 2, pp. 394–403, 2011, doi: 10.1016/j.dss.2010.10.001.
- [102] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*. CRC Press, 2006.
- [103] J. Järveläinen, “IT incidents and business impacts: Validating a framework for continuity management in information systems,” *Int. J. Inf. Manage.*, vol. 33, no. 3, pp. 583–590, 2013, doi: 10.1016/j.ijinfomgt.2013.03.001.
- [104] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, “Integrated business continuity and disaster recovery planning: Towards organizational resilience,” *Eur. J. Oper. Res.*, vol. 242, no. 1, pp. 261–273, 2015, doi: 10.1016/j.ejor.2014.09.055.
- [105] B. Herbane, D. Elliott, and E. M. Swartz, “Business Continuity Management: Time for a strategic role?,” *Long Range Plann.*, vol. 37, no. 5, pp. 435–457, 2004, doi:

10.1016/j.lrp.2004.07.010.

- [106] M. Niemimaa, J. Järveläinen, M. Heikkilä, and J. Heikkilä, “Business continuity of business models: Evaluating the resilience of business models for contingencies,” *Int. J. Inf. Manage.*, vol. 49, no. April, pp. 208–216, 2019, doi: 10.1016/j.ijinfomgt.2019.04.010.
- [107] Bajgoric Nijaz, “Business continuity management: a systemic framework for implementation,” *Kybernetes*, vol. 43, no. 2, pp. 156–177, 2014, doi: 10.1108/K-11-2013-0252.
- [108] A. P. Sanchez Dominguez, “Business Continuity Management: A Holistic Framework for Implementation,” *Culminating Proj. Inf. Assur.*, no. 5–2016, 2016.
- [109] W. N. Z. Wong, “Transforming corporate performance: A business continuity management approach,” *Organ. Dyn.*, 2018, doi: <https://doi.org/10.1016/j.orgdyn.2018.08.004>.
- [110] J. Lindström, S. Samuelsson, and A. Hägerfors, “Business continuity planning methodology,” *Disaster Prev. Manag.*, vol. 19, no. 2, pp. 243–255, 2010, doi: 10.1108/09653561011038039.
- [111] M. Savage, “Business continuity planning,” *Work Study*, vol. 51, no. 5, pp. 254–261, 2002, doi: 10.1108/00438020210437277.
- [112] R. L. Tammineedi, “Business Continuity Management: A Standards-Based Approach,” *Inf. Secur. J. A Glob. Perspect.*, vol. 19, no. 1, pp. 36–50, 2010, doi: 10.1080/19393550903551843.
- [113] J. Botha and R. Von Solms, “A cyclic approach to business continuity planning,” *Inf. Manag. Comput. Secur.*, vol. 12, no. 4, pp. 328–337, 2004, doi: 10.1108/09685220410553541.
- [114] V. Cerullo and M. J. Cerullo, “Business continuity planning: A comprehensive approach,” *Inf. Syst. Manag.*, vol. 21, no. 3, pp. 70–78, 2004, doi: 10.1201/1078/44432.21.3.20040601/82480.11.
- [115] S. A. Torabi, H. Rezaei Soufi, and N. Sahebjamnia, “A new framework for business impact analysis in business continuity management (with a case study),” *Saf. Sci.*, vol. 68, pp. 309–323, 2014, doi: 10.1016/j.ssci.2014.04.017.
- [116] Z. Zeng and E. Zio, “An integrated modeling framework for quantitative business continuity assessment,” *Process Saf. Environ. Prot.*, vol. 106, pp. 76–88, 2017, doi: <https://doi.org/10.1016/j.psep.2016.12.002>.
- [117] K.-M. (Noel) Bryson, H. Millar, A. Joseph, and A. Mobolurin, “Using formal MS/OR modeling to support disaster recovery planning,” *Eur. J. Oper. Res.*, vol. 141, no. 3, pp. 679–688, 2002, doi: 10.1016/S0377-2217(01)00275-2.
- [118] B. Van de Walle and A. F. Rutkowski, “A fuzzy decision support system for IT Service Continuity threat assessment,” *Decis. Support Syst.*, vol. 42, no. 3, pp. 1931–1943, 2006, doi: 10.1016/j.dss.2006.05.002.



- [119] A. Montshiwa, A. Nagahira, and S. Ishida, “Modifying Business Continuity Plan (BCP) Towards an Effective Auto-Mobile Business Continuity Management (BCM): A Quantitative Approach,” *J. Disaster Res.*, vol. 11, pp. 691–698, 2016, doi: 10.20965/jdr.2016.p0691.
- [120] M. F. Blos, S. L. Hoeflich, and P. E. Miyagi, “A general supply chain continuity management framework,” *Procedia Comput. Sci.*, vol. 55, no. Itqm, pp. 1160–1164, 2015, doi: 10.1016/j.procs.2015.07.087.
- [121] H. Baba, T. Watanabe, M. Nagaishi, and H. Matsumoto, “Area Business Continuity Management, a New Opportunity for Building Economic Resilience,” *Procedia Econ. Financ.*, vol. 18, no. September, pp. 296–303, 2014, doi: 10.1016/S2212-5671(14)00943-5.
- [122] V. Lozupone, “Disaster recovery plan for medical records company,” *Int. J. Inf. Manage.*, vol. 37, no. 6, pp. 622–626, 2017, doi: <https://doi.org/10.1016/j.ijinfomgt.2017.05.015>.
- [123] S. A. Torabi, R. Giah, and N. Sahebjamnia, “An enhanced risk assessment framework for business continuity management systems,” *Saf. Sci.*, vol. 89, pp. 201–218, 2016, doi: <https://doi.org/10.1016/j.ssci.2016.06.015>.
- [124] L. Jingye and T. Takehiro, “Practical Process for Introducing Smart Business Continuity Management of Smart City in Japan,” *Procedia Eng.*, vol. 146, pp. 288–295, 2016, doi: <https://doi.org/10.1016/j.proeng.2016.06.390>.
- [125] M. Kato and T. Charoenrat, “Business continuity management of small and medium sized enterprises: Evidence from Thailand,” *Int. J. Disaster Risk Reduct.*, vol. 27, pp. 577–587, 2018, doi: <https://doi.org/10.1016/j.ijdr.2017.10.002>.
- [126] M. Labus, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, and S. Popović, “Adaptive E-Business Continuity Management: Evidence from the Financial Sector,” *Comput. Sci. Inf. Syst.*, 2019, [Online]. Available: <http://www.comsis.org/archive.php?show=ppr691-1902>.
- [127] “Virtual Corporation’s Business Continuity Maturity Model,” *Virtual Corporation*, 2003. <https://www.virtual-corp.com/bcmm>.
- [128] K. Randeree, A. Mahal, and A. Narwani, “A business continuity management maturity model for the UAE banking sector,” *Bus. Process Manag. J.*, vol. 18, no. 03, pp. 472–492, 2012, doi: 10.1108/14637151211232650.
- [129] M.-A. Kaufhold *et al.*, “Business Continuity Management in Micro Enterprises: Perception, Strategies, and Use of ICT,” *Int. J. Inf. Syst. Cris. Response Manag.*, 2018, doi: 10.4018/ijiscram.2018010101.
- [130] B. Zawada, “The practical application of ISO 22301,” *J. Bus. Contin. Emer. Plan.*, 2014.
- [131] R. B. Pojasek, “Organizations and their contexts: Where risk management meets sustainability performance,” *Environ. Qual. Manag.*, vol. 22, no. 3, pp. 81–93, 2013, doi: 10.1002/tqem.21338.

- [132] A. L. Mendelow, “Environmental Scanning--The Impact of the Stakeholder Concept,” *Int. Conf. Inf. Syst.*, pp. 407–417, 1981.
- [133] M. Slabá, “Stakeholder Power-Interest Matrix and Stakeholder-Responsibility Matrix in Corporate Social Responsibility,” pp. 1366–1374, 2014.
- [134] G. Vancoppenolle, “What are we planning for?,” in *The Definitive Handbook of Business Continuity Management*, Second Edi., Andrew Hiles, Ed. John Wiley & Sons, Ltd, 2007, pp. 3–25.
- [135] M. O’Hehir, “What is a business continuity planning (BCP) strategy?,” in *The Definitive Handbook of Business Continuity Management*, Second Edi., A. Hiles, Ed. John Wiley & Sons, Ltd, 2007, pp. 27–45.
- [136] J. Watters, *Disaster Recovery, Crisis Response, and Business Continuity A Management Desk Reference*, 1st ed. Apress, 2013.
- [137] P. Sikdar, “Alternate Approaches to Business Impact Analysis,” *Inf. Secur. J. A Glob. Perspect.*, vol. 20, no. December 2014, pp. 128–134, 2011, doi: 10.1080/19393555.2010.551274.
- [138] C. Bertrand, “Business continuity and mission critical applications,” *Netw. Secur.*, vol. Vol. 20, no. No. 8, pp. 9–11, 2005.
- [139] R. Jones, “Building a Business Impact Analysis: The Keystone to Effective Business Continuity Planning,” *Burt. Res.*, 2008.
- [140] J. D. Nosworthy, “A Practical Risk Analysis Approach: Managing BCM Risk,” *Comput. Secur.*, vol. 19, no. 7, pp. 596–614, 2000, doi: 10.1016/S0167-4048(00)07020-6.
- [141] T. Aven, “Risk assessment and risk management: Review of recent advances on their foundation,” *Eur. J. Oper. Res.*, vol. 253, no. 1, pp. 1–13, 2016, doi: 10.1016/j.ejor.2015.12.023.
- [142] S.-C. Cha, P.-W. Juo, L.-T. Liu, and W.-N. Chen, “Duplicate Work Reduction in Business Continuity and Risk Management Processes,” *Res. Conf. Pap.*, vol. 9, no. Apr, pp. 25–40, 2010, doi: 10.1007/978-1-4419-1325-8.
- [143] *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. Geneva: International Organization for Standardization, 2018.
- [144] B. Suh and I. Han, “The IS risk analysis based on a business model,” *Inf. Manag.*, vol. 41, no. 2, pp. 149–158, 2003, doi: 10.1016/S0378-7206(03)00044-2.
- [145] ISACA, *CISA Review Manual 2014*. ISACA, 2013.
- [146] A. C. Cameron and P. K. Trivedi, *Microeconometrics: Methods and Applications*. Cambridge,

UK: Cambridge University Press, 2005.

- [147] J. H. Stock and M. W. Watson, *Introduction to Econometrics, Third Edition*. Pearson, 2017.
- [148] G. Casella and R. L. Berger, *Statistical Inference, Second Edition*. Duxbury-Thomson Learning, 2002.
- [149] StataCorp., “Stata Statistical Software.” StataCorp LP., College Station, TX, 2013, [Online]. Available: <https://www.stata.com/>.
- [150] L. C. Hamilton, *Statistics with STATA: Version 12*, Eighth Edi. Cengage Learning, Inc, 2013.
- [151] J. F. J. Hair, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, vol. 46, no. 1–2. 2014.
- [152] K. A. Bollen, *Structural Equations with Latent Variables*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 1989.
- [153] P. M. Bentler and D. G. Weeks, “Linear structural equations with latent variables,” *Psychometrika*, 1980, doi: 10.1007/BF02293905.
- [154] R. B. Kline, *Principles and practice of structural equation modeling*, 3rd ed. Guilford Press, 2011.
- [155] J. F. Hair, C. M. Ringle, and M. Sarstedt, “Partial Least Squares: The Better Approach to Structural Equation Modeling?,” *Long Range Plann.*, vol. 45, no. 5–6, pp. 312–319, 2012, doi: 10.1016/j.lrp.2012.09.011.
- [156] J. F. Hair and M. Sarstedt, “Innovative and established research methods in family business: Description, illustration and application guidelines,” *J. Fam. Bus. Strateg.*, vol. 5, no. 1, pp. 1–3, 2014, doi: 10.1016/j.jfbs.2014.01.010.
- [157] C. M. Ringle, S. Wende, and J.-M. Becker, “SmartPLS 3.” Boenningstedt: SmartPLS GmbH, 2015, [Online]. Available: [www.smartpls.com](http://www.smartpls.com).
- [158] S. P. Gudergan, C. M. Ringle, S. Wende, and A. Will, “Confirmatory tetrad analysis in PLS path modeling,” *J. Bus. Res.*, vol. 61, no. 12, pp. 1238–1249, 2008, doi: 10.1016/j.jbusres.2008.01.012.
- [159] J. F. Hair, M. Sarstedt, C. M. Ringle, and J. A. Mena, “An assessment of the use of partial least squares structural equation modeling in marketing research,” *J. Acad. Mark. Sci.*, vol. 40, no. 3, pp. 414–433, 2012, doi: 10.1007/s11747-011-0261-6.
- [160] J. F. Hair, C. M. Ringle, and M. Sarstedt, “Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance,” *Long Range Plann.*, vol. 46, no. 1–2, pp. 1–12, 2013, doi: 10.1016/j.lrp.2013.01.001.

- [161] M. Sarstedt, C. M. Ringle, D. Smith, R. Reams, and J. F. Hair, "Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers," *J. Fam. Bus. Strateg.*, vol. 5, no. 1, pp. 105–115, 2014, doi: 10.1016/j.jfbs.2014.01.002.
- [162] M. Reimann, O. Schilke, and J. S. Thomas, "Customer relationship management and firm performance: the mediating role of business strategy," *J. Acad. Mark. Sci.*, vol. 38, no. 3, pp. 326–346, 2010, doi: 10.1007/s11747-009-0164-y.
- [163] W. H. Greene, *Econometric Analysis*, 4th ed. Prentice Hall, 1999.
- [164] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a Silver Bullet," *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, Apr. 2011, doi: 10.2753/MTP1069-6679190202.
- [165] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.," *J. Mark. Res. (JMR). Feb1981*, vol. 18, no. 1, pp. 39-50. 12p. 1 Diagram, 1981, doi: 10.2307/3151312.
- [166] J. Henseler, "A New and Simple Approach to Multi-group Analysis in Partial Least Squares Path Modeling," *PLS'07 fifth Int. Symp. PLS Relat. methods*, pp. 104–107, 2007.
- [167] S. Geisser, "A Predictive Approach to the Random Effect Model," *Biometrika*, vol. 61, no. 1, p. 101, Apr. 1974, doi: 10.2307/2334290.
- [168] M. Stone, "Cross-Validatory Choice and Assessment of Statistical Predictions," *J. R. Stat. Soc.*, vol. 36, no. 2, pp. 111–147, 1974, doi: 10.2307/2984809.
- [169] *SRPS ISO 22301:2014 Друштвена bezbednost - Sistemi menadzmenta kontinuitetom poslovanja - Zahtevi*. Београд: Институт за стандардизацију Србије, 2014.

## 9 Прилози

### 9.1 Прилог 1 – Упитник за спровођење анализе утицаја на пословање (ВИА упитник)

Организациона јединица: \_\_\_\_\_

#### 1. Улога и основни циљеви организационе јединице

Описати укратко основну улогу и циљеве организационе јединице:

Основна улога	Основни циљеви

## 2. Идентификација кључних пословних процеса

Идентификовати кључне пословне процесе Ваше организационе јединице (ОЈ). Кључни пословни процеси у оквиру једне ОЈ су они пословни процеси који су најзначајнији за остваривање улоге и основних циљева ОЈ. Идентификација кључних пословних процеса се спроводи на основу анализе излаза из пословних процеса ка важним заинтересованим странама.

За сваки од кључних пословних процеса дефинисати циљни ниво активности (енгл. *Service Delivery Objective*, скраћено SDO) којим се дефинише одговарајући ниво опоравка пословног процеса који треба да буде постигнут током циљног времена опоравка.

Уколико постоји, описати могући алтернативни сценарио како би се пословни процес одржао на неком нивоу рада, чак ако је то испод жељеног нивоа услуге. На пример, издавање радног налога у папиру или наруџбенице у папиру уместо електронске верзије документа, могућност рада од куће и сл.

Код процеса	Назив процеса	Организациона јединица	Опис процеса	Циљни ниво активности (SDO)	Опис алтернативног сценарија (уколико постоји)

### 3. Анализа кључних пословних процеса

#### 3.1 Основне карактеристике кључних процеса

За сваки од кључних пословних процеса идентификованих у тачки 2:

- Дефинисати **операциону учесталост**: константно, по потреби, дневно, недељно, месечно, квартално
- Навести да ли пословни процес обрађује **критичне податке** (да/не). Уколико обрађује критичне податке попуњава се табела из тачке 3.3
- Навести да ли пословни процес има обавезу регулаторног или неког другог **важног извештавања** (да/не). Уколико постоји важно извештавање попуњава се табела из тачке 3.4
- Дефинисати **зависност** (мала, средња, велика) пословног процеса **од губитка комуникационих веза**, као што су телефони, имејл, интернет, итд.
- Уколико постоји, описати **временску зависност** (на пример, почиње сваког понедељка у 23 часа) или остале рокове везане за пословни процес.

Код процеса	Кључни пословни процес	Операциона учесталост	Обрада критичних података (да/не)	Важно извештавање (да/не)	Зависност од комуникационих веза (мала/средња/велика)	Рокови / временска зависност	Коментар

### 3.2 Неопходни ресурси кључних пословних процеса

За све кључне пословне процесе из тачке 2, идентификовати ресурсе који су неопходни да би процес функционисао (улазне ресурсе, ресурсе неопходне за одвијање процеса и ресурсе којима се излаз из процеса доставља до заинтересоване стране).

Код процеса	Кључни пословни процес	Назив ресурса	Испоручилац ресурса	Власништво ресурса	Период набавке ресурса

### 3.3 Обрада критичних података (енгл. *Critical Record Management*)

За све кључне пословне процесе за које сте у тачки 3.1 навели да обрађују критичне пословне податке, идентификовати критичне пословне податке, алтернативне изворе података (уколико постоје), постојање резервне копије и потребну фреквенцију израде резервних копија. Потребна фреквенција израде резервних копија је процена најдужег прихватљивог периода за који не постоји резервна копија података тј. периода за који подаци могу бити изгубљени.

Код процеса	Кључни пословни процес	Критични подаци	Назив апликације, базе података, фолдера, документа...	Постојање резервне копије (да/не)	Алтернативни извор података	Потребна фреквенција израде резервне копије	Коментар



### 3.4 Важно извештавање

За све кључне пословне процесе за које сте у тачки 3.1 навели да имају обавезу регулаторног или неког другог важног извештавања, навести називе извештаја, листу прималаца, фреквенцију извештавања, варијанте извештаја и врсту казне (новчани износ) уколико постоји.

Код процеса	Кључни пословни процес	Назив извештаја	Листа прималаца	Фреквенција извештавања	Варијанте извештаја (уколико постоје)	Врста казне (уколико постоји)	Коментар

## 4. Анализа међузависности процеса

### 4.1 Зависност од других процеса (енгл. *Upstream Dependencies*)

Навести зависности кључних пословних процеса од других пословних процеса у Вашој или другој организационој јединици. Одредити ниво зависности (низак, средњи, висок) и описати зависности укључујући и могуће алтернативе.

Код процеса	Кључни пословни процес	Пословни процес од кога зависи	Ниво зависности (низак/средњи/висок)	Опис зависности

Код процеса	Кључни пословни процес	Пословни процес од кога зависи	Ниво зависности (низак/средњи/висок)	Опис зависности

#### 4.2 Утицај на друге процесе (енгл. *Downstream Dependencies*)

Навести све пословне процесе у организацији који зависе од кључних пословних процеса у Вашој организационој јединици. Одредити ниво зависности (низак, средњи, висок) и описати зависности укључујући и могуће алтернативе.

Код процеса	Кључни пословни процес	Пословни процес на који утиче	Ниво зависности (низак/средњи/висок)	Опис зависности

## 5. Анализа последица прекида кључних пословних процеси

### 5.1 Директни финансијски утицај

Према најгорем могућем сценарију, за сваки од идентификованих кључних пословних процеса из тачке 2, проценити финансијски утицај у случају немогућности обављања пословне функције, тј. у случају прекида у раду пословног процеса.

Вредности прекида рада мање од 12 сати се односе на период у радним данима од 7 до 19 часова. Све вредности прекида рада у трајању мањем од 7 дана укључују искључиво радне дане.

*Напомена:* Скала за дефинисање трајање прекида у раду је параметар модела и овде је дата искључиво као пример.

Код процеса	Кључни пословни процес	Трајање прекида у раду												Коментар
		1 мин	5 мин	30 мин	1 сат	2 сата	4 сата	8 сати	24 сата	48 сати	72 сата	7 дана	14 дана	

## 5.2 Оперативни утицаји

Према најгорем могућем сценарију, за сваки од идентификованих кључних пословних процеса из тачке 2, проценити оперативне утицаје на целокупно пословање организације у случају немогућности обављања пословне функције, тј. у случају прекида у раду пословног процеса. Оперативни утицаји се оцењују на скали од 0 до 4, где 0 = нема утицаја, 4 = велики утицај.

Уколико нема разлике у оперативним утицајима услед прекида у раду појединачних пословних процеса, могуће је оценити заједно оперативне утицаје у случају прекида у раду групе процеса или целокупне Организационе јединице.

*Напомена:* Оперативни утицаји су параметар модела и овде су дати искључиво као пример.

Кључни пословни процес или група процеса														
Р.бр.	Оперативни утицај	Трајање прекида у раду												Коментар
		1 мин	5 мин	30 мин	1 сат	2 сата	4 сата	8 сати	24 сата	48 сати	72 сата	7 дана	14 дана	
1	Репутација организације													
2	Поверење грађана													
3	Поверење уговорних страна													
4	Новчани токови													
5	Законске обавезе													

6	Повећање расхода													
...	...													

### 5.3 Опоравак кључних пословних процеса

Описати процедуре за опоравак кључних пословних процеса након инцидентне ситуације која је проузроковала прекид у пословању, а након што су неопходни ресурси за подршку идентификованих кључних пословних процеса оспособљени.

Опоравак процеса може обухватити опоравак изгубљених критичних података и обраду заосталог посла. Време потребно за опоравак процеса описати у функцији трајања отказа система:

Код процеса	Кључни пословни процес	Опоравак изгубљених критичних података (да/не)	Обрада заосталог посла (да/не)	Опис опоравка	Потребно време	Процена потребних ресурса приликом опоравка (опрема и радна снага)	Коментар

## 6. Иницијално утврђивање циљних параметара опоравка

На основу свих прикупљених података иницијално утврдити циљне параметре опоравка кључних пословних процеса.

Код процеса	Кључни пословни процес	Циљна тачка опоравка (RPO)	Циљно време опоравка (RTO)	Најдужи прихватљиви прекид (MAO)	Коментар

## 9.2 Прилог 2 - Садржај документа Анализа утицаја на пословање

- 1 Сврха, подручје примене и корисници документа
- 2 Референтна документација
- 3 Дефиниције важних појмова
  - 3.1 Појмови
  - 3.2 Скраћенице
- 4 Увод
  - 4.1 Циљеви
  - 4.2 Делокруг
  - 4.3 Приступ и методологија
  - 4.4 Организација документа
- 5 Подаци из Упитника за спровођење анализе утицаја на пословање (попуњава се за сваку организациону јединицу из делокруга ВСMS-а)
  - 5.1 Назив организационе јединице
    - 5.1.1 Основна улога
    - 5.1.2 Кључни пословни процеси
    - 5.1.3 Неопходни ресурси кључних пословних процеса
    - 5.1.4 Извештавање у вези са кључним пословним процесима
    - 5.1.5 Најважније чињенице и запажања
- 6 Резултати анализе
  - 6.1 Најважније заинтересоване стране

- 6.2 Директни финансијски утицаји
  - 6.3 Оперативни утицаји
  - 6.4 Међузависности пословних процеса
  - 6.5 Циљни параметри опоравка
  - 6.6 Нивои критичности пословних процеса
  - 6.7 Приоритети приликом опоравка пословних процеса
- 7 Закључак и препоруке

## Прилози

Прилог 1: Листа учесника ВИА интервјуа

Прилог 2: Процене директних финансијских утицаја

Прилог 3: Оцене оперативних утицаја

Прилог 4: Матрица зависности пословних процеса

Прилог 5: Циљни параметри опоравка кључних пословних процеса

Прилог 6: Испуњени Упитници за спровођење анализе утицаја на пословање за све организационе јединице



### **9.3 Прилог 3 - Садржај документа Стратегија управљања континуитетом пословања**

- 1 Сврха, подручје примене и корисници документа
- 2 Референтна документација
- 3 Дефиниције важних појмова
  - 3.1 Појмови
  - 3.2 Скраћенице
- 4 Стратегија управљања континуитетом пословања
  - 4.1 Улазни подаци за стратегију
    - 4.1.1 Анализа утицаја на пословање
    - 4.1.2 Процена ризика у вези са континуитетом пословања
  - 4.2 Одговор на инцидент
    - 4.2.1 Кризни тимови
    - 4.2.2 Командни центар
    - 4.2.3 Извештавање и доношење одлука
    - 4.2.4 Сарадња са органима власти и хитним службама
    - 4.2.5 Зборна места евакуисаних
    - 4.2.6 Средства за комуникацију
    - 4.2.7 Превоз до алтернативних локација
    - 4.2.8 Комуникација са заинтересованим странама
  - 4.3 Стратегија обезбеђења неопходних ресурса
    - 4.3.1 Алтернативне локације и инфраструктура

4.3.2 Неопходни ресурси

4.3.3 Сарадња са партнерима и испоручиоцима

4.3.4 Избегавање јединствених тачака прекида

4.3.5 План припремних активности и финансијски ресурси

Прилози

Прилог 1: Циљни параметри опоравка пословних процеса

Прилог 2: Идентификоване претње

## 9.4 Прилог 4 - Садржај документа План континуитета пословања

- 1 Сврха, подручје примене и корисници документа
- 2 Референтна документација
- 3 Дефиниције важних појмова
  - 3.1 Појмови
  - 3.2 Скраћенице
- 4 План континуитета пословања
  - 4.1 Опште информације
    - 4.1.1 Делокруг плана континуитета пословања
    - 4.1.2 Саставни делови плана континуитета пословања
    - 4.1.3 Кризни штаб
    - 4.1.4 Доношење одлука у кризној ситуацији
  - 4.2 Активирање плана континуитета пословања
    - 4.2.1 План комуникације са заинтересованим странама
    - 4.2.2 Средства за комуникацију
  - 4.3 Опоравак пословања
    - 4.3.1 Планови опоравка пословања организационих делова
    - 4.3.2 Алтернативне локације
    - 4.3.3 Неопходни ресурси за спровођење плана
  - 4.4 Деактивирање плана континуитета пословања
  - 4.5 План припремних активности

## Прилози

Прилог 1: Кључни пословни процеси

Прилог 2: План комуникације са заинтересованим странама

Прилог 3: План припремних активности

Прилог 4: План одговора на инциденте

Прилог 5: План опоравка пословања (за сваку појединачну пословну функцију/организациону јединицу/локацију)

Прилог 6: План опоравка информационог система (DR план)

## 9.5 Прилог 5 - Упитник за вредновање модела

### УПИТНИК ЗА ВРЕДНОВАЊЕ МОДЕЛА

**Напомена:** Одговор се даје уписивањем ознаке x у одговарајући квадратић. Квадратић се активира дуплим кликом миша. За свако питање потребно је изабрати само један одговор

		Уопште се не слажем	Донекле се не слажем	Немам мишљење	Делимично се слажем	Потпуно се слажем
<b>I. Вредновање основних карактеристика модела</b>						
П1.1	Модел дефинише јасан и ефикасан поступак за успостављање континуитета пословања у организацији која користи савремене технологије електронског пословања.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П1.2	Модел свеобухватно сагледава специфичности пословања организације, а посебно употребу савремених технологија електронског пословања.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П1.3	Модел олакшава успостављање континуитета пословања у организацији која користи савремене технологије електронског пословања.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П1.4	Модел омогућава адаптивно управљање континуитетом електронског пословања у складу са променама у окружењу у коме послује организација.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П1.5	Модел доприноси повећању позитивног става према управљању континуитетом електронског пословања у организацији.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>II. Вредновање Метода за спровођење анализе утицаја на пословање</b>						
П2.1	Анализа утицаја на пословање је важна пословна активност у чије спровођење је укључено руководство организације.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П2.2	У склопу анализе утицаја на пословање идентификовани су кључни пословни процеси организације и њихове међузависности.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		Уопште се не слажем	Донекле се не слажем	Немам мишљење	Делимично се слажем	Потпуно се слажем
П2.3	У склопу анализе утицаја на пословање утврђени су неопходни ресурси за одвијање кључних пословних процеса организације.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П2.4	За све кључне пословне процесе процењени су финансијски и/или оперативни утицаји на целокупно пословање организације у случају прекида у њиховом раду.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П2.5	За све кључне пословне процесе организације утврђени су циљни параметри опоравка: најдужи прихватљив прекид (енгл. <i>Maximum Acceptable Outage - MAO</i> ), циљна тачка опоравка (енгл. <i>Recovery Point Objective - RPO</i> ) и циљно време опоравка (енгл. <i>Recovery Time Objective -RTO</i> ).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П2.6	На основу циљних параметара опоравка и међузависности процеса, за све кључне пословне процесе организације утврђени су нивои критичности са становишта континуитета пословања и дефинисани су приоритети приликом њиховог опоравка, тј. поновног успостављања након инцидентног догађаја.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>III. Вредновање Метода за процену ризика у вези са континуитетом е-пословања</b>						
П3.1	У оквиру организације успостављена је процена ризика у вези са континуитетом електронског пословања која свеобухватно сагледава специфичности пословања организације, а посебно употребу савремених технологија електронског пословања, и која се примењује над кључним пословним процесима организације и њиховим неопходним ресурсима.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П3.2	Ризици у вези са континуитетом пословања су идентификовани, процењени и документовани у регистру ризика.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П3.3	Процена ризика у вези са континуитетом електронског пословања се спроводи по потреби, минимум једном годишње или приликом већих промена у пословном окружењу организације.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П3.4	Организација има успостављен третман ризика са циљем превентивног деловања на узроке појављивања ризичног догађаја и његов могући утицај на целокупно пословање организације.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		Уопште се не слажем	Донекле се не слажем	Немам мишљење	Делимично се слажем	Потпуно се слажем
П3.5	Организација има дефинисане начине третмана ризика који обухватају умањење, избегавање, преношење и прихватање ризика.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П3.6	Организација има успостављен план обраде ризика у вези са континуитетом пословања којим се дефинишу додатне (нове) контроле за све ризике за које није изабрано прихватање ризика као начин третмана, као и потребне информација за праћење примене додатних контроле.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>IV. Вредновање Метода за израду плана континуитета пословања</b>						
П4.1	Дефинисани су циљеви и делокруг система управљања континуитетом пословања (енгл. <i>Business Continuity Management System - BCMS</i> ), као и одговорности за његово спровођење.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П4.2	Стратегија управљања континуитетом пословања је базирана на резултатима анализе утицаја на пословање и процене ризика у вези са континуитетом електронског пословања.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П4.3	Стратегијом су дефинисани и обезбеђени сви неопходни ресурси у случају кризне ситуације.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П4.4	План континуитета пословања садржи план комуникације, одговорности, алтернативне локације, потребне ресурсе у случају кризне ситуације, као и јасне поступке активирања и деактивирања.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П4.5	Сви запослени у организацији, спољни сарадници и остале заинтересоване стране које имају улогу у плану континуитета пословања су прошли одговарајућу обуку.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П4.6	Тестирање плана континуитета пословања се редовно спроводи на годишњем нивоу и по потреби у случају значајних промена у пословном окружењу организације.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>V. Вредновање Метода за континуирано унапређење BCMS-а</b>						

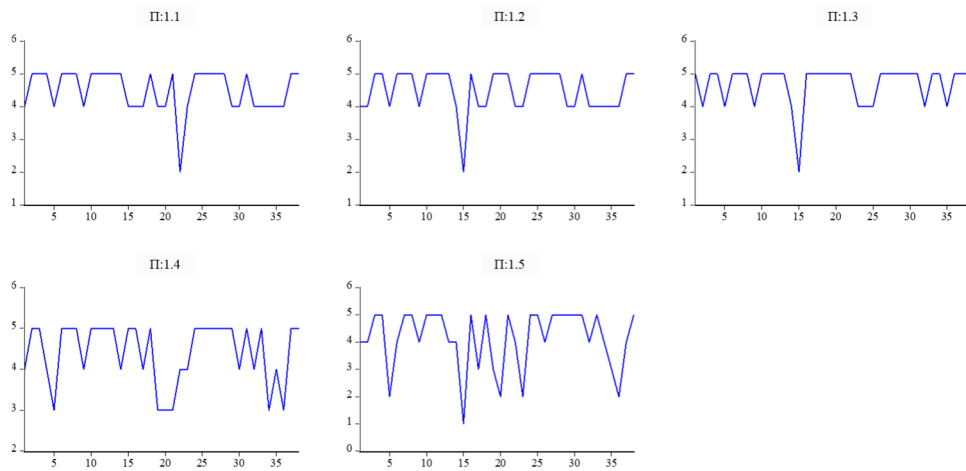
		Уопште се не слажем	Донекле се не слажем	Немам мишљење	Делимично се слажем	Потпуно се слажем
П5.1	Организација има успостављену метрику вредновања перформанси BCMS-а која између осталог обухвата вредновање ефикасности и ефективности, усклађеност са пословном стратегијом организације, интегрисаност у основне процесе управљања у организацији и прилагодљивост променама у окружењу у коме послује организација.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П5.2	Оцена перформанси BCMS-а се спроводи у планираним интервалима као и када настану значајне промене у окружењу организације, а посебно након сваког инцидента који је проузроковао активирање плана континуитета пословања.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П5.3	Резултати оцене перформанси BCMS-а се документују у форми извештаја који обавезно садржи предлоге корективних мера за унапређење BCMS-а.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П5.4	Организација има успостављено адекватно преиспитивање BCMS-а од стране руководства са циљем утврђивања потреба за променама у BCMS-у и идентификовања могућности за унапређење BCMS-а.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П5.5	Преиспитивање BCMS-а од стране руководства се спроводи у планираним интервалима као и када настану значајне промене у организацији и њеном окружењу, а посебно након сваког инцидента који је проузроковао активирање плана континуитета пословања.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П5.6	Преиспитивање BCMS-а од стране руководства обезбеђује доношење одлука о имплементацији корективних мера за унапређење BCMS-а и адекватно се документује.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П5.7	Организација има дефинисан план унапређења BCMS-а који садржи корективне мера за унапређење BCMS-а са приоритетима и детаљима имплементације.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
П5.8	План унапређења BCMS-а је ажуран и обухвата корективне мере у складу са резултатима тестирања плана континуитета пословања, оцене перформанси BCMS-а, резултата преиспитивања BCMS-а од стране руководства и осталих релевантних информација.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



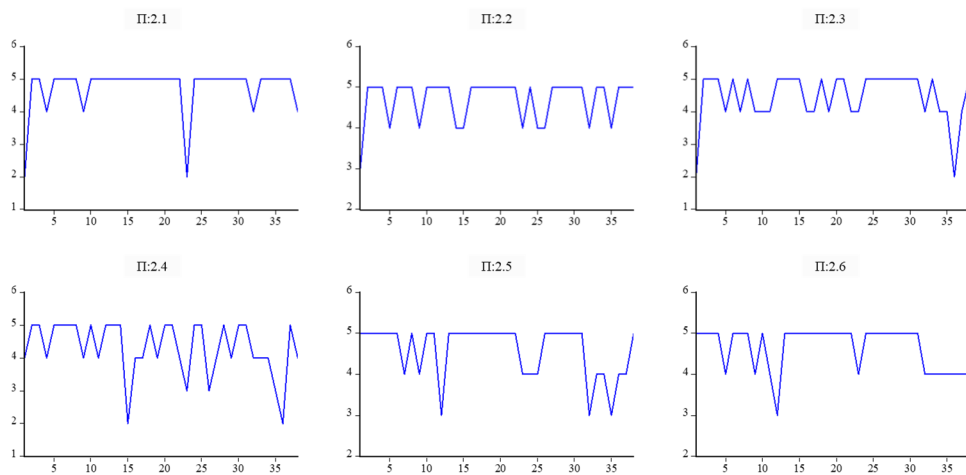
		Уопште се не слажем	Донекле се не слажем	Немам мишљење	Делимично се слажем	Потпуно се слажем
П5.9	Праћење напретка и извештавање руководства о статусу корективних мера дефинисаних планом унапређења ВСМС-а се спроводи у планираним временским интервалима и обавезно пре сваког преиспитивања ВСМС-а од стране руководства.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Изнети предлоге за унапређење модела:

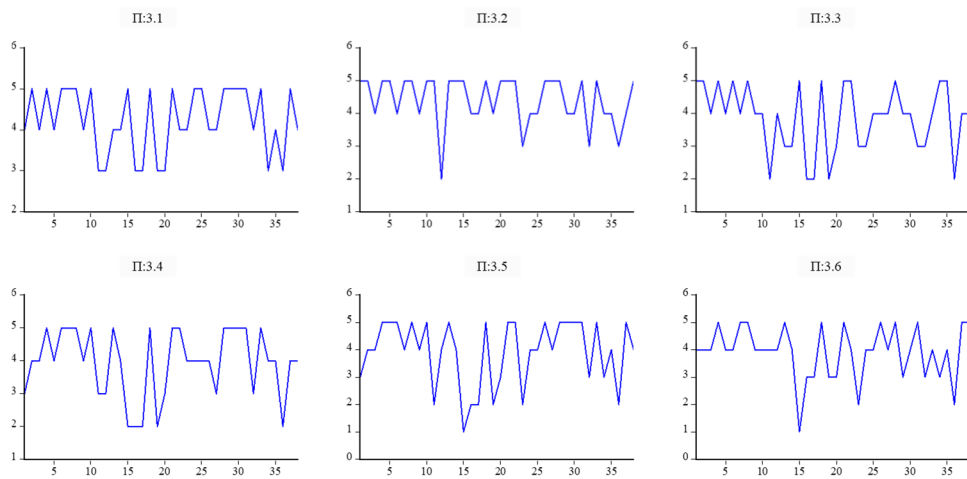
## 9.6 Прилог 6 - Одговори испитаника



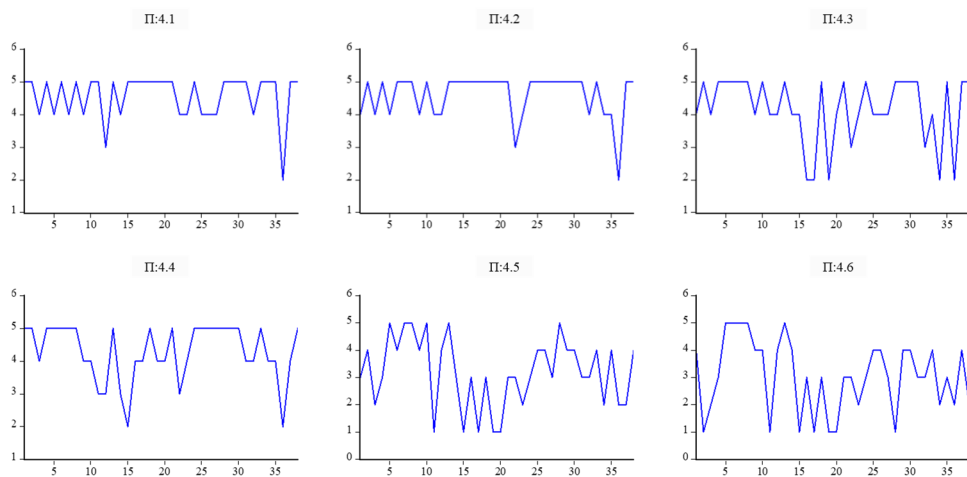
Слика 19 - Део I: Вредновање основних карактеристика модела



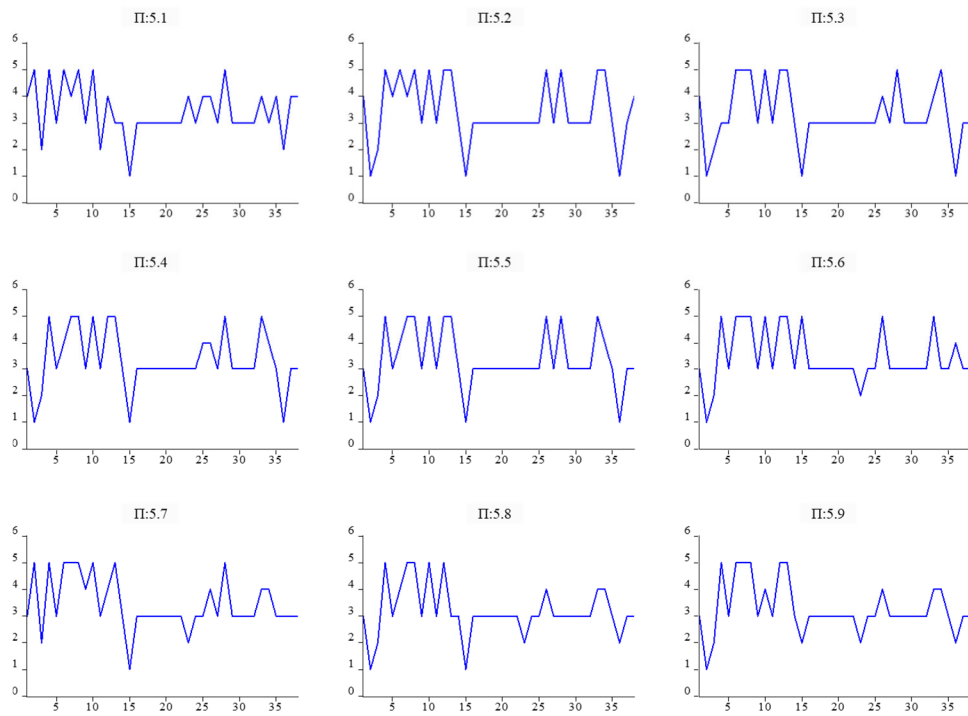
Слика 20 - Део II: Вредновање Метода за спровођење анализе утицаја на пословање



**Слика 21 - Део III: Вредновање Метода за процену ризика у вези са континуитетом е-пословања**



**Слика 22 - Део IV: Вредновање Метода за израду плана континуитета пословања**



**Слика 23 - Део V: Вредновање Метода за континуирано унапређење ВСМС-а**

## 9.7 Прилог 7 - Статистичка анализа питања из Упитника за вредновање модела

Табела 23 - Статистичка анализа питања из Упитника за вредновање модела (индикатори за рефлективно мерење конструката PLS-SEM модела)

Питање из Упитника (индикатор PLS-SEM модела)	Средња вредност $\mu$	Стандардна девијација	95% интервал поверења		t-вредност	Вероватноћа одбацивања алтернативне хипотезе			Коефицијент спољног оптерећења (енгл. Outer Loadings)
						$H_a: \mu < 4$	$H_a: \mu \neq 4$	$H_a: \mu > 4$	
<b>Део I: Вредновање основних карактеристика модела (просечна средња вредност 4.45)</b>									
П1.1*	4.500	0.647	4.287	4.713	t = 4.7621	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.707**
П1.2*	4.500	0.647	4.287	4.713	t = 4.7621	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.85**
П1.3*	4.684	0.620	4.481	4.888	t = 6.8058	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.665**
П1.4*	4.421	0.758	4.172	4.670	t = 3.4239	Pr(T < t) = 0.9992	Pr( T  >  t ) = 0.0015	Pr(T > t) = 0.0008	0.565**
П1.5	4.132	1.119	3.764	4.499	t = 0.7248	Pr(T < t) = 0.7634	Pr( T  >  t ) = 0.4732	Pr(T > t) = 0.2366	0.861**

---

**Део II: Вредновање Метода за спровођење анализе утицаја на пословање (просечна средња вредност 4.58)**

---

П2.1*	4.737	0.724	4.499	4.975	t = 6.2780	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.559**
П2.2*	4.711	0.515	4.541	4.880	t = 8.5037	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.600**
П2.3*	4.474	0.762	4.223	4.724	t = 3.8329	Pr(T < t) = 0.9998	Pr( T  >  t ) = 0.0005	Pr(T > t) = 0.0002	0.76**
П2.4*	4.316	0.842	4.039	4.592	t = 2.3129	Pr(T < t) = 0.9868	Pr( T  >  t ) = 0.0264	Pr(T > t) = 0.0132	0.787**
П2.5*	4.605	0.638	4.395	4.815	t = 5.8446	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.516
П2.6*	4.658	0.534	4.482	4.833	t = 7.5940	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.564

---

**Део III: Вредновање Метода за процену ризика у вези са континуитетом е-пословања (просечна средња вредност 4.05)**

---

П3.1*	4.237	0.786	3.978	4.495	t = 1.8571	Pr(T < t) = 0.9644	Pr( T  >  t ) = 0.0713	Pr(T > t) = 0.0356	0.765**
П3.2*	4.421	0.758	4.172	4.670	t = 3.4239	Pr(T < t) = 0.9992	Pr( T  >  t ) = 0.0015	Pr(T > t) = 0.0008	0.549
П3.3	3.868	1.018	3.534	4.203	t = -0.7968	Pr(T < t) = 0.2153	Pr( T  >  t ) = 0.4307	Pr(T > t) = 0.7847	0.640**
П3.4	3.947	1.038	3.606	4.289	t = -0.3125	Pr(T < t) = 0.3782	Pr( T  >  t ) = 0.7565	Pr(T > t) = 0.6218	0.915**

---

ПЗ.5	3.921	1.194	3.529	4.314	t = -0.4075	Pr(T < t) = 0.3430	Pr( T  >  t ) = 0.6860	Pr(T > t) = 0.6570	0.927**
ПЗ.6	3.921	0.969	3.602	4.240	t = -0.5021	Pr(T < t) = 0.3093	Pr( T  >  t ) = 0.6186	Pr(T > t) = 0.6907	0.835**

**Део IV: Вредновање Метода за израду плана континуитета пословања (просечна средња вредност 3.98)**

П4.1*	4.579	0.683	4.354	4.803	t = 5.2248	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.461
П4.2*	4.605	0.679	4.382	4.829	t = 5.4917	Pr(T < t) = 1.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 0.0000	0.661
П4.3	4.158	1.027	3.820	4.496	t = 0.9474	Pr(T < t) = 0.8252	Pr( T  >  t ) = 0.3496	Pr(T > t) = 0.1748	0.805**
П4.4*	4.289	0.867	4.004	4.574	t = 2.0581	Pr(T < t) = 0.9767	Pr( T  >  t ) = 0.0467	Pr(T > t) = 0.0233	0.838**
П4.5	3.211	1.255	2.798	3.623	t = -3.8765	Pr(T < t) = 0.0002	Pr( T  >  t ) = 0.0004	Pr(T > t) = 0.9998	0.773**
П4.6	3.053	1.314	2.621	3.485	t = -4.4441	Pr(T < t) = 0.0000	Pr( T  >  t ) = 0.0001	Pr(T > t) = 1.0000	0.629**

**Део V: Вредновање Метода за континуирано унапређење BCMS-а (просечна средња вредност 3.36)**

П5.1	3.447	0.950	3.135	3.760	t = -3.5858	Pr(T < t) = 0.0005	Pr( T  >  t ) = 0.0010	Pr(T > t) = 0.9995	0.705**
П5.2	3.447	1.155	3.068	3.827	t = -2.9484	Pr(T < t) = 0.0028	Pr( T  >  t ) = 0.0055	Pr(T > t) = 0.9972	0.942

П5.3	3.316	1.093	2.956	3.675	t = -3.8585	Pr(T < t) = 0.0002	Pr( T  >  t ) = 0.0004	Pr(T > t) = 0.9998	0.912**
П5.4	3.342	1.097	2.981	3.703	t = -3.6958	Pr(T < t) = 0.0004	Pr( T  >  t ) = 0.0007	Pr(T > t) = 0.9996	0.959
П5.5	3.342	1.122	2.973	3.711	t = -3.6156	Pr(T < t) = 0.0004	Pr( T  >  t ) = 0.0009	Pr(T > t) = 0.9996	0.965
П5.6	3.447	1.032	3.108	3.787	t = -3.3015	Pr(T < t) = 0.0011	Pr( T  >  t ) = 0.0021	Pr(T > t) = 0.9989	0.648
П5.7	3.447	0.978	3.126	3.769	t = -3.4830	Pr(T < t) = 0.0006	Pr( T  >  t ) = 0.0013	Pr(T > t) = 0.9994	0.806**
П5.8	3.184	0.955	2.870	3.498	t = -5.2685	Pr(T < t) = 0.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 1.0000	0.904**
П5.9	3.263	0.950	2.951	3.575	t = -4.7830	Pr(T < t) = 0.0000	Pr( T  >  t ) = 0.0000	Pr(T > t) = 1.0000	0.908**

**Индикатор\*:** индикатори који су прошли t-тест у смислу да је вероватноћа одбацивања нулте хипотезе  $H_0$  у корист алтернативе ( $H_a: \mu > 4$ ) испод нивоа значајности (5%).

**Коефицијент спољног оптерећења\*\*:** индикатори који су укључени у PLS-SEM модел



## 10 Биографија аутора

Милица Лабус рођена је 1976. године у Београду. Дипломирала је на Математичком факултету у Београду, смер Рачунарство и информатика, 2000. године, са просечном оценом 9.61. Магистарске студије из Рачунарства (*Computer Science*) завршила је на *Stanford* универзитету у Америци, 2001. године, а магистарске студије из Пословне администрације (*Master of Business Administration - MBA*) у COTRUGLI пословној школи у Београду, 2011. године.

Докторске студије, студијски програм Информациони системи и квантитативни менаџмент (изборно подручје Електронско пословање) уписала је 2014. године на Факултету организационих наука у Београду. Положила је свих девет, програмом предвиђених испита на докторским студијама са просечном оценом 10.

Милица Лабус има преко 18 година радног искуства у области информационих технологија. Радила је на многим пројектима у финансијском и јавном сектору. Запослена је у компанији Enetel Solutions, на позицији менаџера за развој пословања. Последњих осам године се интензивно бави пројектима из области управљања континуитетом пословања.

Од маја 2015. године поседује међународно признат сертификат за ИТ ревизора: *Certified Information Systems Auditor (CISA)*.

Списак изабраних пројеката:

- Спровођење анализе утицаја на пословање и дефинисање плана континуитета пословања, Народна банка Србије (септембар 2015 – април 2016), вођа консултантског тима
- Ревизија усаглашености информационог система са „Одлуком НБС о минималним стандардима управљања информационом системом финансијске институције“ („Службени гласник РС“, бр. 23/2013 и 113/2013), АМС осигурање (септембар 2014), ИТ ревизор
- Дефинисање стратегије развоја информационог система, АМС осигурање (јул 2014 – август 2014), ИТ консултант
- Усаглашавање са „Одлуком НБС о минималним стандардима управљања информационом системом финансијске институције“, Миленијум осигурање (фебруар 2014 – јун 2014), ИТ консултант
- Израда анализе утицаја на пословања, стратегије развоја информационог система, политике безбедности информација и плана континуитета пословања, Удружење осигуравача Србије (септембар 2012 - септембар 2013), ИТ консултант.

Радови објављени у часопису међународног значаја на SCI листи:

1. **Labus, M.,** Despotović-Zrakić, M., Bogdanović, Z., Barać, D., & Popović, S. (2019). Adaptive E-Business Continuity Management: Evidence from the Financial Sector. *Computer Science and Information Systems*. <http://www.comsis.org/archive.php?show=ppr691-1902>, ISSN: 1820-0214 (Print) 2406-1018 (Online), IF(2019)=0.927, M23

2. Barac, D., Ratkovic-Živanovic, V., **Labus, M.**, Milinovic, S., & Labus, A. (2017). Fostering partner relationship management in B2B ecosystems of electronic media. *Journal of Business and Industrial Marketing*, 32(8). <https://doi.org/10.1108/JBIM-02-2016-0025>, ISSN: 0885-8624, IF(2018)=1.961, M22
3. Labus, M., & **Labus, M.** (2017). Monetary Transmission Channels in DSGE Models: Decomposition of Impulse Response Functions Approach. *Computational Economics*. <https://doi.org/10.1007/s10614-017-9717-1>, ISSN: 0927-7099, IF(2018)=1.185, M22

Часописи међународног значаја (M24):

1. Đurić, I., Ratković-Živanović, V., **Labus, M.**, Groj D., Milanović, N. (2016) Designing an intelligent home media center, *Facta Universitatis, series Electronics and Energetics*, Vol. 29, No.3, pp. 475-487, ISSN:0353-3670 (Print) ISSN: 2217-5997 (Online), M24
2. Labus, M., **Labus, M.** (2016) From Fiscal Consolidation to Fiscal Optimization, *Ekonomika preduzeća*, No. 1-2, pp. 37-52, ISSN: 0353-443x, M24
3. Labus, M., **Labus, M.** (2015) Policy Mix for Fiscal Consolidation in Serbia: Conditional Forecast Approach, *Ekonomika preduzeća*, No. 1-2, pp. 17-31, ISSN: 0353-443x, M24

Зборници међународних научних скупова (M30):

1. **Labus, M.**, Despotović-Zrakić, M., & Bogdanović, Z. (2017). Introducing adaptive E-business continuity management. In *Advances in Intelligent Systems and Computing* (Vol. 569). [https://doi.org/10.1007/978-3-319-56535-4\\_62](https://doi.org/10.1007/978-3-319-56535-4_62), ISSN: 2194-5357, M33
2. **Labus, M.** (2017). E-business Continuity Management in Insurance Sector. In M. Zdravković, M., Konjović, Z., Trajanović (Ed.), *ICIST 2017 Proceedings* (Vol. 1, pp. 235–240), ISBN: 978-86-85525-19-3, M33
3. M. Despotović-Zrakić, A. Labus, Z. Bogdanović, **M. Labus**, S. Milinović (2015) A Virtual Laboratory for Teaching Internet of Things, *International conference on virtual learning ICVL 2015*, Timisoara, 31.10.2015, M33

Монографска студија/поглавље у књизи M12 или рад у тематском зборнику међународног значаја:

1. Vojinović, I., Barac, D., Jezdović, I., **Labus, M.**, & Jovanović, F. (2017). An Approach to Designing IoT-Based Business Models. In *Emerging Trends and Applications of the Internet of Things* (pp. 43-70). DOI: 10.4018/978-1-5225-2437-3.ch002, IGI Global.

## Изјава о ауторству

Име и презиме аутора Милица Лабус

Број индекса 5007/2014

### Изјављујем

да је докторска дисертација под насловом

Модел адаптивног управљања континуитетом електронског пословања

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, 15.07.2020



## Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Милица Лабус

Број индекса 5007/2014

Студијски програм Информациони системи и квантитативни менаџмент

Наслов рада Модел адаптивног управљања континуитетом електронског пословања

Ментор др Маријана Деспотовић-Зракић, ред. проф. Факултета организационих наука Универзитета у Београду

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањена у **Дигиталном репозиторијуму Универзитета у Београду**.

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, 15.07.2020



## Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Модел адаптивног управљања континуитетом електронског пословања

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)
2. Ауторство – некомерцијално (CC BY-NC)
3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)
4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)
5. Ауторство – без прерада (CC BY-ND)
6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.  
Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, 15.07.2020



1. **Ауторство.** Дозвољавање умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. **Ауторство – некомерцијално.** Дозвољавање умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. **Ауторство – некомерцијално – без прерада.** Дозвољавање умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. **Ауторство – некомерцијално – делити под истим условима.** Дозвољавање умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. **Ауторство – без прерада.** Дозвољавање умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. **Ауторство – делити под истим условима.** Дозвољавање умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.