ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

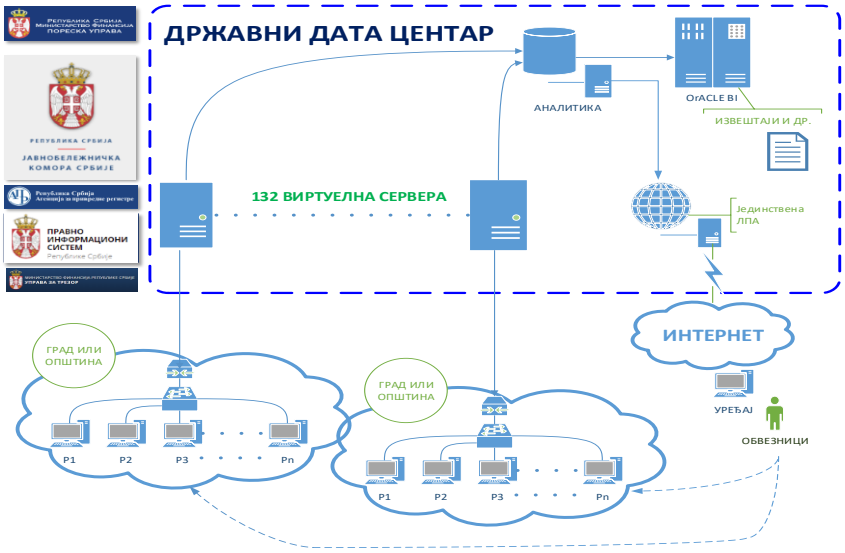
УПРАВЉАЊЕ ИНФОРМАЦИОНИМ СИСТЕМОМ ЛОКАЛНЕ ПОРЕСКЕ АДМИНИСТРАЦИЈЕ

Број: 400- 474/2021-03/43
Београд, 10. децембар 2021. године

ПОРЕД ЗНАЧАЈНОГ УНАПРЕЂЕЊА УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМОМ, НЕОПХОДНО ЈЕ УНАПРЕДИТИ КОМУНИКАЦИЈУ СА КОРИСНИЦИМА И УПРАВЉАЊЕ ПОДАЦИМА ПРЕУЗЕТИХ ИЗ ДРУГИХ ЕВИДЕНЦИЈА И РЕГИСТАРА

Реформа јавних финансија обухватила је и пореску децентрализацију са циљем обезбеђивања изворних прихода за сваки град и општину у Републици Србији. Институција је у својим извештајима констатовала многе недостатке у процесу евидентирања, обраде и извештавању о спорним и дубиозним потраживањима. У ревизији сврсисходности пословања „Ефикасност наплате изворних прихода ЈЛС“ установљено је да су многи проблеми изазвани неажурношћу евиденције у ИСЛПА. Проблеми у наплати изворних прихода ЈЛС могу бити последица неадекватног управљања информационим системом.

Јединице локалне самоуправе су преузеле део евиденције и један број запослених из Пореске управе, формирале организационе јединице да врше обрачун и наплату 14 изворних прихода, а најзначајнији од њих је порез на имовину. У систему се евидентирају порези на имовину правних и физичких лица, док се порез на поклон и пренос апсолутних права и даље води у Пореској управи. Формирањем јединственог информационог система ЛПА, обједињени су сви системи на једном месту, омогућен је увид у све обавезе једним упитом, дигитално подношење пријава за правна лица, као и друге могућности, а што може да доведе до повећаног ризика по интегритет, поверљивост и доступност информација у систему.
Желели смо да оценимо квалитет управљања ИСЛПА и утврдимо да ли је обезбеђена поверљивост, расположивост и интегритет информација, података, докумената и апликације у информационом систему.



Илустрација: Принципијелна шема система

Државни дата центар је повећао **доступност** ЛПА система корисницима и обвезницима, смањујући истовремено ризике услед хаварије. Потребно је да се успостави ефикасно управљање проблемима и инцидентима и по-бољша комуникација са крајњим корисницима. **Интегритет** се заснива на подацима из националних регистара који нису изграђени на стандардизован начин тако да очуваност изворног садржаја, комплетност и заштита података није потпуна. **Поверљивост** информација, података и докумената није обезбеђена у потпуности, јер подаци који се преузимају из других националних регистара и евиденција се чувају без криптозаштитних механизама.

Препоруке

Државна ревизорска институција дала је препоруке Канцеларији за ИТеУ да:

- унапреди контакт форму са тикетинг системом који омогућава кориснику који је пријавио проблем да прати промену статуса и коначну обраду пријаве;
- изради Споразум о нивоу оперативних услуга са свим ЈЛС и да садржајем уреде питања обраде података и питања информационе безбедности;
- донесе све потребне акте којима се уређују питања информационе безбедности, да обезбеде примену прописаних мера заштите и да у складу са проценом ризика обезбеде информационе ресурсе за успостављање резервне локације јединственог ЛПА система.

Препоруке Институту „Михајло Пупин“ да:

- обезбеди одговарајуће апликативне контроле на начин да се подаци који се преносе из других регистара означе (маркирају) ако нису комплетни како се не би наставила обрада без свих неопходних података.;
- обезбеди механизам за снимање ревизорског трага којим би се обезбедило хронолошко документовање и праћење промена података у оквиру пословних процеса, активности или операција од почетка до краја;
- обезбеди могућност ручног и аутоматског означавања обвезника са спорним и дубиозним пореским обавезама и обезбеде обуку корисника у вези ове функционалности.

Препоруке ЛПА Града Београда и Крагујевца, општинама Инђија, Ариље и Жагубица да:

- уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање;
- допуни постојеће акте којима уређује питања информационе безбедности тако што ће ближе уредити одговарајуће техничке, организационе и кадровске мере неопходне за безбеднији рад са ИСЛПА свих запослених у ОЈП;
- успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места.

Садржај

Скраћенице и термини

У прегледу су дате скраћенице које су коришћене у извештају:

Пун назив	**Скраћеница**
Јединице локалне самоуправе	ЈЛС
Орган за јавне приходе јединице локалне самоуправе	ОЈПЈЛС
Информациони систем локалне пореске администрације	ИСЛПА
Јединствени информациони систем локалне пореске администрације	ЈИСЛПА
Сервисна магистрала органа - је централизована софтверско-хардверска платформа за интеграцију и управљање електронским услугама органа.	СМО
Информационо-комуникациони систем	ИКТ систем
Оператор информационо-комуникационог система	Оператор ИКТ система
Информациони систем	ИС
Информационе технологије	ИТ
Дневник активности обраде података (енгл. Log за бележење ревизорског трага енгл. Audit trail)	Журнал
Закон о заштити података о личности	ЗЗПЛ
Закон о информационој безбедности	ЗИБ
Закон о пореском поступку и пореској администрацији	ЗППА
Орган за јавне приходе градске управе Београда	ОЈП Београд
Орган за јавне приходе градске управе Крагујевца	ОЈП Крагујевац
Орган за јавне приходе општинске управе Инђије	ОЈП Инђија
Орган за јавне приходе општинске управе Ариље	ОЈП Ариље
Орган за јавне приходе општинске управе Житорађе	ОЈП Житорађа

I Резиме и препоруке

Реформа јавних финансија обухватила је између осталог и пореску децентрализацију са циљем обезбеђивања изворних прихода за сваки град и општину у Републици Србији. Институција је у својим извештајима констатовала многе недостатке у процесу евидентирања, обраде и извештавању о спорним и дубиозним потраживањима. У ревизији сврсисходности пословања „Ефикасност наплате изворних прихода ЈЛС“ установљено је да су многи проблеми изазвани неажурношћу евиденције у ИСЛПА. Проблеми у наплати изворних прихода ЈЛС могу бити последица неадекватног управљања информационим системом.

Јединице локалне самоуправе су преузеле део евиденције и један број запослених из Пореске управе, формирале организационе јединице да врше обрачун и наплату 14 изворних прихода, а најзначајнији од њих је порез на имовину. У систем се евидентирају порези на имовину правних и физичких лица, док се порез на поклон и пренос апсолутних права и даље води у Пореској управи. Формирањем јединственог информационог система ЛПА, обједињени су сви системи на једном месту, омогућен је увид у све обавезе једним упитом, дигитално подношење пријава за правна лица, као и друге могућности, а што може да доведе до повећаног ризика по интегритет, поверљивост и доступност информација у систему.

Државна ревизорска институција је спровела ревизију сврсисходности пословања „Управљање информационим системима у локалној пореској администрацији“. Ревизијом су обухваћени субјекти ревизије који користе информациони систем ЛПА и то: Град Београд - Секретаријат за јавне приходе, Град Крагујевац - Градска пореска управа, Општина Инђија - Одељење за утврђивање и наплату јавних прихода, Општина Ариље - Служба ЛПА, Општина Житорађа - Служба за утврђивање и наплату локалних јавних прихода, испоручилац софтверског решења Институт "Михајло Пупин". и Државни дата центар - Канцеларија за информационе технологије и електронску управу. Након спроведене ревизије закључили смо да је:

ПОРЕД ЗНАЧАЈНОГ УНАПРЕЂЕЊА УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМОМ, НЕОПХОДНО ЈЕ УНАПРЕДИТИ КОМУНИКАЦИЈУ СА КОРИСНИЦИМА И УПРАВЉАЊЕ ПОДАЦИМА ПРЕУЗЕТИХ ИЗ ДРУГИХ ЕВИДЕНЦИЈА И РЕГИСТАРА

Наведено смо утврдили на основу закључака, које износимо у наставку, а закључци су донети на основу налаза, који су приказани испод сваког закључка.

ЗАКЉУЧАК 1: Доступност информација, података и докумената ИС ЛПА је повећана формирањем Јединственог система у Државном дата центру истовремено смањујући ризике који могу настати услед хаварије. Потребно је побољшати управљање проблемима, инцидентима и комуникацију са крајњим корисницима.

- Налаз 1.1: Канцеларија за ИТеУ није у потпуности успоставила адекватно управљање проблемима и инцидентима, јер постојећа контакт форма нема потврду о пријему и обради поруке у складу са темом поруке, отежавајући превенцију инцидената, стварајући ризик да евентуални проблеми и инциденти ескалирају, отежају или онемогуће доступност ЛПА апликације;
- Налаз 1.2: Канцеларија за ИТеУ није у потпуности успоставила адекватно управљање услугама, јер није закључила уговоре/споразуме са ЈЛС о нивоу пружених услуга и мерама информационе безбедности, чиме се ствара ризик да се приликом појаве

техничких проблема неадекватно реагује, отежа или онемогући доступност ЛПА апликације;

- Налаз 1.3: Канцеларија за ИТеУ није у потпуности успоставила адекватно управљање информационом безбедношћу, јер није уредила и применила процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система што за последицу има већи степен рањивости система и већи степен рањивости осетљивих података о личности који се налазе у систему.

ЗАКЉУЧАК 2: Интегритет информација, података и докумената ИС ЛПА није обезбеђен у потпуности, јер у већем делу се заснива на подацима преузетим из екстерних система и регистара без означавања извора података, што за последицу може имати немогућност утврђивања аутентичности, непорецивости и комплетности података.

- Налаз 2.1: Апликативне контроле дозвољавају преузимање ћириличних и латиничних података из екстерних система без означавања извора података, што ствара ризик од грешака у обради и за последицу може имати смањење ефикасности у раду;
- Налаз 2.2: ЛПА апликација обезбеђује снимак последње извршене радње над подацима и нема историјат промена што ствара ризик немогућности накнадног утврђивања узрока и извршиоца ненамерне грешке као и других потенцијалних радњи злоупотребе;
- Налаз 2.3: Извештавање о пореском дугу обвезника заснива се на појединачној анализи сваке пореске картице обвезника без које није могуће утврдити старост дуга нити да ли је дуг у спору, или да ли има дубиозан карактер (сумњиво – неизвесног износа и могућности наплате) што онемогућава увид у структуру пореског дуга на нивоу ОЈПЈЛС, стварајући ризик прецењивања износа потраживања, погрешног пословног извештавања и угрожавање финансирања рада ЈЛС.

ЗАКЉУЧАК 3: Поверљивост информација, података и докумената који се користе у ЛПА није обезбеђена у потпуности, јер подаци, документи и информације које се преузимају из других матичних евиденција и регистара се чувају без крипто-заштитних механизама.

- Налаз 3.1: ОЈП Београд, Крагујевац, Инђија, Ариље и Житорађа није у потпуности уредила поступак рада са документима, изворима и врстама података (лични подаци обвезника/грађана, подаци о некретнинама, финансијски подаци, тајни подаци итд.), стварајући ризик од настанка неправилне употребе података, информација и докумената, недозвољеног објављивања, или неке друге злоупотребе, што за последицу може створити непланиране судске трошкове;
- Налаз 3.2: ОЈП Београд и Ариље нису усвојили и ОЈП Крагујевац и Житорађа нису у потпуности успоставили адекватно управљање информационом безбедношћу ЛПА, јер нису уредили и применили процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система што за последицу има већи степен рањивости система и података о личности који се налазе у систему;
- Налаз 3.3: ОЈП Београд, Крагујевац, Инђија, Ариље и Житорађа није у потпуности успоставила механизам управљања овлашћењима у ИСЛПА, чиме се ствара ризик да због недостатка адекватног раздвајања дужности дође до ненамерних грешака, оштећења или губитка података и докумената, што за последицу може имати њихово неблаговремено откривање и отклањање.

У циљу побољшања управљања информационим системом локалне пореске администрације, Државна ревизорска институција даје следеће препоруке:

Граду Београду - Секретаријату за јавне приходе, да:

1. уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање. (Налаз 3.1.) – Приоритет 2[1].
2. донесе све потребне акте којима се уређују питања информационе безбедности, да обухвати све информационе ресурсе и обезбеди примену прописаних мера заштите информационог система. (Налаз 3.2.) – Приоритет 1[2].
3. успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места. (Налаз 3.3.) – Приоритет 1.

Граду Крагујевцу - Градској пореској управи, да:

1. уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање. (Налаз 3.1.) – Приоритет 2.
2. допуни постојеће акте којима уређује питања информационе безбедности тако што ће ближе уредити одговарајуће техничке, организационе и кадровске мере неопходне за безбеднији рад са ИСЛПА свих запослених у ОЈП. (Налаз 3.2.) – Приоритет 1.
3. успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места. (Налаз 3.3.) – Приоритет 1.

Општини Инђији - Одељењу за утврђивање и наплату јавних прихода, да:

1. успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места. (Налаз 3.3.) – Приоритет 1.

Општини Ариљу – Служби ЛПА, да:

1. уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање. (Налаз 3.1.) – Приоритет 2.
2. донесе све потребне акте којима се уређују питања информационе безбедности, да обухвати све информационе ресурсе и обезбеди примену прописаних мера заштите информационог система. (Налаз 3.2.) – Приоритет 1.
3. успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места. (Налаз 3.3.) – Приоритет 1.

Општини Житорађи – Локалној пореској администрацији, да:

1. уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање. (Налаз 3.1.) – Приоритет 2.
2. допуни постојеће акте којима уређује питања информационе безбедности тако што ће ближе уредити одговарајуће техничке, организационе и кадровске мере неопходне за безбеднији рад са ИСЛПА свих запослених у ОЈП. (Налаз 3.2.) – Приоритет 1.

[1] Приоритет 2 - Несврсисходности које је могуће отклонити у року до годину дана.
[2] Приоритет 1 - Несврсисходности које је могуће отклонити у року од 90 дана.

3. успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места. (Налаз 3.3.) – Приоритет 1.

Канцеларији за информационе технологије и електронску управу, да:

1. унапреди контакт форму са тикетинг системом који омогућава кориснику који је пријавио проблем да прати промену статуса и коначну обраду пријаве. (Налаз 1.1.) – Приоритет 2.
2. изради Споразум о нивоу оперативних услуга са свим ЈЛС и да садржајем уреде питања обраде података и питања информационе безбедности. (Налаз 1.2.) – Приоритет 2.
3. донесе све потребне акте којима се уређују питања информационе безбедности, да обезбеде примену прописаних мера заштите и да у складу са проценом ризика обезбеде информационе ресурсе за успостављање резервне локације јединственог ЛПА система. (Налаз 1.3.) – Приоритет 2.

Институту „Михајло Пупин“, да:

1. обезбеди одговарајуће апликативне контроле на начин да се подаци који се преносе из других регистара означе (маркирају) ако нису комплетни како се не би наставила обрада без свих неопходних података. (Налаз 2.1.) – Приоритет 3[3].
2. обезбеди механизам за снимање ревизорског трага којим би се обезбедило хронолошко документовање и праћење промена података у оквиру пословних процеса, активности или операција од почетка до краја. (Налаз 2.2.) – Приоритет 3.
3. обезбеди могућност ручног и аутоматског означавања обвезника са спорним и дубиозним пореским обавезама и обезбеде обуку корисника у вези ове функционалности. (Налаз 2.3.) – Приоритет 3.

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
10. децембар 2021. године

[3] Приоритет 3 - Несврсисходности које је могуће отклонити у року до три године.

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Управљање информационим системом локалне пореске администрације" у периоду од марта до септембра 2021. године[4]. Ревизија сврсисходности пословања је спроведена у складу са Законом о Државној ревизорској институцији[5], Пословником Државне ревизорске институције[6] и Програмом ревизије Државне ревизорске институције за 2021. годину.
Ревизија је обављена на начин и према поступцима утврђеним оквиром ревизорских стандарда Међународне организације врховних ревизорских институција (INTOSAI), Кодексом професионалне етике државних ревизора, принципима Међународних стандарда врховних ревизорских институција (ISSAI), Методолошким правилима и смерницама за ревизију сврсисходности пословања и Методолошким правилима и смерницама за ИТ ревизију Државне ревизорске институције.

1. Проблем

Реформа јавних финансија обухватила је и пореску децентрализацију са циљем обезбеђивања изворних прихода за сваки град и општину у Републици Србији. Институција је у својим извештајима констатовала многе недостатке у процесу евидентирања, обраде и извештавању о спорним и дубиозним потраживањима. У ревизији сврсисходности пословања „Ефикасност наплате изворних прихода ЈЛС" установљено је да су многи проблеми изазвани неажурношћу евиденције у ИСЛПА. Проблеми у наплати изворних прихода ЈЛС могу бити последица неадекватног управљања информационим системом.

Јединице локалне самоуправе су преузеле део евиденције и један број запослених из Пореске управе, формирале организационе јединице да врше обрачун и наплату 14 изворних прихода, а најзначајнији од њих је порез на имовину. У систем се евидентирају порези на имовину правних и физичких лица, док се порез на поклон и пренос апсолутних права и даље води у Пореској управи. Формирањем јединственог информационог система ЛПА, обједињени су сви системи на једном месту, омогућен је увид у све обавезе једним упитом, дигитално подношење пријава за правна лица, као и друге могућности, а што може да доведе до повећаног ризика по интегритет, поверљивост и доступност информација у систему.

Државна ревизорска институција је у ревизији сврсисходности пословања спроведену у 2020. години са темом „Ефикасност наплате изворних прихода у јединицама локалне самоуправе"[7] између осталог утврдила недостатке у евиденцијама, нередовно ажурирање података, неповезаност података о имовини и обвезнику, због чега постоји ризик да утврђена потраживања нису потпуна и да постоје обвезници којима потраживања неће бити утврђена благовремено.

2. Циљ ревизије

Изабрана тема је повезана са Циљем 2 из Стратешког плана ДРИ за период 2019-2023, где је одређено да ће ДРИ утврдити проблеме и предложити решења за међусекторске проблеме на свим нивоима, ради унапређивања одговорности и транспарентности. Односно у оквиру овог старешког циља реализоваће се два потциља и то потциљ 2.2: Унапредити финансијско планирање и евидентирање прихода и расхода и потциљ 2.5: Унапредити јавно управљање и коришћење информационих технологија (ИТ)[8].

[4] Број ревизије 400-1118/2019-03.
[5] „Службени гласник РС", бр. 101/05, 54/07, 36/10 и 44/18-др.закон.
[6] „Службени гласник РС", број 9/09.
[7] Извештај о ревизији сврсисходности пословања „Ефикасност наплате изворних прихода у јединицама локалне самоуправе" **http://www.dri.rs/php/document/download/3457/1**
[8] Стратешки план Државне ревизорске институције за период 2019-2023. године **http://www.dri.rs/upload/documents/Opsti_dokumenti/DRI%20Strateski%20plan2018-2023.pdf**

ИТ системи су од кључног значаја за пословање у оквиру јавног сектора и активности постају све скупље, сложеније као и степен осетљивости података које оне садрже. Осим тога, иницијативе е-управе у Србији имају за циљ унапређење коришћења ИТ и интернета широм јавне управе да би се обезбедиле информације грађанима и привредним друштвима. Циљ ДРИ је и да се помогне да се унапреди способност ИТ система да сви јавни програми постану ефикаснији, а да се при томе штите кључно пословање и осетљиве информације.

У складу са наведеним, кључни циљ ревизије је да оценимо квалитет управљања информационим системом локалне пореске администрације и утврдимо да ли је обезбеђена довољна доступност или расположивост система, да ли је обезбеђен интегритет и неопходна поверљивост информација, података, докумената и апликације у информационом систему.

3. Ревизијска питања

За остварење циља ревизије формулисали смо главно питање и три ревизорска питања. Имајући у виду значај који информациони систем локалне пореске администрације (даље ИС ЛПА) има за јединице локалне самоуправе (даље ЈЛС), Државна ревизорска институција се определила да главно питање ревизије буде:

Да ли се адекватно управља информационим системом локалне пореске администрације?

Примењујући Методолошка правила и смернице за ревизију сврсисходности пословања извршили смо декомпозицију главног питања на три ревизорска питања уважавајући сву сложеност информационог система локалне пореске администрације.

Посматрајући универзални информациони модел сваког система који подразумева прво да је успостављен (тј. да постоји, да је доступан свим заинтересованим странама, пројектантима, корисницима, обвезницима, грађанима, итд.) тако да смо у том смислу испитивали:

1. Да ли је на адекватан начин обезбеђена **расположивост** информација, података и докумената у информационом систему?

   Да би донели закључак о адекватности начина обезбеђења расположивости информационог система ЛПА и свега што он обухвата, испитивали смо:

   1. Да ли је успостављено адекватно управљање проблемима и инцидентима?
   2. Да ли је успостављено адекватно управљање услугама?
   3. Да ли је успостављено адекватно управљање информационом безбедношћу?

   као и друга питања која обезбеђују расположивост система и услуге.

2. Да ли је на адекватан начин обезбеђена **интегритет** информација, података и докумената у информационом систему?

   Да би донели закључак о адекватности начина обезбеђења интегритета информационог система ЛПА, информација, података, докумената и свега што обухвата, испитивали смо:

   1. Да ли ЛПА апликација има адекватне контроле валидности улазних података?
   2. Да ли ЛПА апликација обезбеђује интегритет снимак извршене радње (унос, измена, увид, штампа и др.) над подацима и документима?
   3. У којој мери ЛПА апликација обезбеђује израду прописаних извештаја пореских дужника?

   као и друга питања која обезбеђују интегритет система и услуге.

3. Да ли је на адекватан начин обезбеђена **поверљивост** информација, података и докумената у информационом систему?

Да би донели закључак о адекватности начина обезбеђења поверљивости информационог система ЛПА и свега што он обухвата, испитивали смо:

1. Да ли је успостављено адекватно управљање подацима?
2. Да ли је успостављено адекватно управљање информационом безбедношћу?
3. У којој мери су додељена овлашћења корисницима ЛПА апликације у складу са описом радних места?

као и друга питања која обезбеђују поверљивост овог система и услуге.

Одређивање најризичнијих аспеката главног ревизијског питања урађено је процењивањем ризика у складу са Методолошким правилама и смерницама за ИТ ревизију Државне ревизорске институције, која поставља квантитативне и квалитативне критеријуме, што је детаљније разрађено у Прилогу 1 - Методологија у поступку рада.

4. Обим и ограничења ревизије

Ревизијом смо обухватили четири ИТ области у седам субјеката и то градске управе Београд, Крагујевац, општинске управе Инђија, Ариље и Житорађа, Канцеларија за информационе технологије и електронску управу која управља државним дата центром и Института „Михајло Пупин“ који је у државном власништву добављача софтверског решења. Ревизија је обухватила период 2018-2020. година време најснажније трансформације државне управе кроз дигитализацију услуга пореског система, док за поједине анализе смо користили и податке из 2021. године.

Предмет испитивања је био:

- Опште ИТ контроле процеса управљања ИТ операцијама које треба да обезбеде правовремено препознавање системских проблема у експлоатацији софтверског решења и помоћ у отклањању као подршка преко 1500 корисника-службеницима локалних пореских администрација, 5,9 милиона обвезника, потенцијално штетним догађајима – безбедносних инцидената (догађаји са материјално значајним последицама по информациону имовину);
- Опште ИТ контроле процеса управљања уговорима са добављачима ИТ услуга које треба да обезбеде квалитетну испоруку услуга чувања података, реаговања у случају хаварије ради обезбеђења континуитета пословања у редовној и ванредној ситуацији (догађаји са материјално значајним последицама по информациону имовину);
- Опште ИТ контроле и активности у обезбеђивању информационе безбедности целокупног информационог система, посебно за информационе системе који размењују података са другим информационим системима;
- Процена адекватности и поузданости апликативних контрола рачунарске апликације која обухвата интерне акте (стратегије, планове, политике, процедуре, обрасце итд.) процесе, људе и системе сва три субјекта ревизије у складу са дефинисаним циљем.

У поступку ревизије нисмо испитивали:

- Да ли финансијски извештаји субјеката ревизије истинито и објективно приказују њихово финансијско стање, резултате пословања и новчане токове, у складу са прихваћеним рачуноводственим начелима и стандардима;
- Финансијске трансакције и одлуке у вези са примањима и приходима и расходима и издацима, ради утврђивања да ли су односне трансакције извршене у складу са законом, другим прописима и за планиране сврхе;
- Међусобне обавезе и потраживања органа јавне управе која су обухваћена ревизијом.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе, послали упитнике субјектима ревизије.

Ревизијом нисмо обухватили анализу да ли сва правна и физичка лица плаћају обавезе, односно да ли постоје лица којима се не врши обрачун и наплата обавеза преко система локалне пореске администрације.

5. Методологија у поступку рада

Да бисмо остварили циљ ревизије и одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions), као и све податке добијене од субјеката ревизије. Анализирали смо податке и информације за период од 2018. до 2020. године. Такође смо за поједине анализе користили и податке из 2021. године.

Управљање информационим системом подразумева успостављање низа пословних процеса, посебно зато што је реч о техничко-технолошком систему који обухвата опрему, софтвер, комуникацију и друге погодности које се користе у сврху евидентирања, чувања, обраде, преноса података у било ком облику. Приликом оцењивања ИТ управљања примењена је скала од 1 до 5 са следећим ознакама: Оцена 1 - потпуно незадовољавајуће, Оцена 2 - делимично незадовољавајуће, Оцена 3 - делимично задовољавајуће, Оцена 4 - задовољавајуће и Оцена 5 - потпуно задовољавајуће.

Које пословне процесе треба да успостави организација чије пословање није могуће без употребе рачунарских система, дефинишу међународни стандарди чији се захтеви налазе и у основама наших прописа.

У фази планирања ревизије прикупљени су подаци и документација на основу које је извршена процена ризика у циљу одређивања обима ревизије.

У ревизији информационих система обим[9] се одређује из једног или више домена и то:

- Организациона политика за ИТ;
- Организациона управљачка структура за ИТ;
- Опште контроле у оквиру пословања које су аутоматизоване;
- Управљање имовином;
- Развој, набавка и одржавање информационих система, укључујући и мапирање пословних процеса и повезане програмске логике;
- Управљање ИТ операцијама;
- Управљање физичким окружењем;
- Управљању људским ресурсима;
- Управљање комуникацијама;
- Управљање информатичком безбедношћу;
- Управљање усклађеношћу са прописима;
- Пословни континуитет и управљање опоравком након елементарних непогода/хаварије;
- Управљање контролама апликација.

Приручником[10] је предвиђена оцена сложености информационог система и могућност избора области за испитивање и то: ИТ управљање, развој и набавка, ИТ операције, ангажовање добављача, планови континуитета пословања и опоравка од хаварије, информациона безбедност и апликативне контроле. Уважили смо сложеност ИС ЛПА и изабрали субјекте ревизије тако да обухватимо све елементе система.

Посматрајући универзални информациони модел сваког система чији први аспект је да је успостављен (тј. да постоји, да је расположив или доступан свим заинтересованим странама, пројектантима, корисницима, обвезницима, грађанима, итд.) у том смислу смо испитивали активности Канцеларије за ИТеУ, која је обавила значајан посао виртуелизације физичких сервера за све ЈЛС и њихово безбедно повезивање успостављањем сервисне магистрале органа.

[9] Методолошка правила и смернице за ИТ ревизију Државне ревизорске институције.
[10] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енгл. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).

Други аспект информационог модела је интегритет података и информација који се евидентирају, преузимају, обрађују и чувају у информационом систему. Обрада података и извештавање се врши употребом ЛПА апликације, од стране корисника/запослених на пословима ЛПА, а коју обезбеђује Институт „Михајло Пупин“. Преузимање података из других информационих система и регистара и повезивање у Јединствен информациони систем, омогућило је стандардизовање пореско правних процеса обраде података и миграцију података из 31 ЈЛС које нису биле обухваћене пре централизације ЛПА.

Трећим аспектом информационог модела, да ли су подаци, информације и документи доступни овлашћеним странама и недоступни неовлашћеним лицима, тј. Поверљивост информација испитивали смо путем упитника код свих ЈЛС које су биле извор информација у ревизији, и непосредно увидом код пет субјеката ревизије ЈЛС корисника ЛПА, два града Београд и Крагујевац и три општине Инђија, Ариље и Житорађа којима смо дали и препоруке да унапреде свој рад.

Специфичност код овако великог броја корисника система који су уједно руковаоци личних података обвезника је да процесе обраде података обављају два обрађивача Канцеларије за ИТеУ који управља радом Државног дата центра и добављача апликације и базе података Института „Михајло Пупин“.

Проценили смо ревизијски ризик и одабрали домене: ИТ операције, ангажовање добављача, информациона безбедност и апликативне контроле.

Табела 1. Преглед ризичних области

Област/домени	Ниво ризика	Напомена
ИТ управљање	Низак	У фази планирања утврђено да постоји стратешко планирање дигитализацијом државне управе, активности планиране акционим планом су у доброј мери реализоване.
Развој и набавка	Низак	Сопствени развој апликације од стране Института са најдужим искуством у примени информационих технлогија редовно самостално унапређење и усклађивање апликације са прописима и другим захтевима.
ИТ операције	Висок	Вишегодишње искуство у организованом решавању рекламација на основу управног поступка и физичке документације преспоро се трансформисала у дигитални облик комуникације и многи елементи оперативног управљања пате од недостатака.
Ангажовање добављача	Висок	Јединице локалне самоуправе свој континуитет пословања заснивају на оцени да је за њега задужен државни дата центар иако ни један проис или споразум не дефинише обавезе једне и друге стране што је веома висоо ризично у случају хаваријских догађаја.
Планови континуитета пословања и опоравка од хаварије	Средњи	Модернизација критичне информатичке инфраструктуре прилично је смањина ризик по континуитет пословања у ситуацијама нежељених догађаја или ванредних ситуација повећала је употребу информационих услуга и ставило под притисак мрежну инфраструктуру. Недостатак планова у ЈЛС који морају бити спроводљиви са расположивим ресурсима, периодично тестирани и сви недостаци документовани и отклоњени преставља и даље значајан ризик.
Информациона безбедност	Висок	Корисници информационих услуга поред правних лица, бројчано најзначајнија су физичка лица чији се лични подаци обрађују у информационом систему. Изложеност следећим ризицима: неовлашћено откривање информација; неовлашћена модификација или уништење информација; угроженост ИС од хакерског напада; уништавање инфраструктуре; ометање приступа; поремећај обраде података у ИС; и ризик да подаци буду украдени, поставља читав низ безбедносних захтева.
Апликативне контроле	Висок	Ризици су повезани са улазним подацима који се обрађују у апликацији и могу произвести значајно умањење ефикасности система или дати погрешан резултат иако постоје рекламације. Непостојање адекватних извештаја доводе до ризика стварања погрешних извештаја о финансијском стању пореског дуга.

Детаљнији опис коришћене методологије дат је у Прилогу 1.

III Опис предмета ревизије

1. Законодавни и институционални оквир

Законом о финансирању локалне самоуправе[11] прописано је да јединици локалне самоуправе (даље ЈЛС) припадају изворни приходи остварени на њеној територији и да стопе изворних прихода, као и начин и мерила за одређивање висине локалних такси и накнада утврђује скупштина ЈЛС у складу са законом.

ЈЛС припадају изворни приходи остварени на њеној територији по 14 различитих основа[12], а најважнији изворни приход јединице локалне самоуправе је приход од пореза на имовину. **Законом о порезима на имовину**[13] је уређено опорезивање имовине у РС и он прописује основне елементе пореза на имовину који администрирају локалне пореске администрације (даље ЛПА) као надлежни органи јединице локалне самоуправе применом **закона о пореском поступку и пореској администрацији**[14].

ЈЛС води податке који су од значаја за утврђивање износа изворних јавних прихода као и податке о њиховој наплати у јединственом информационом систему (даље ЈИС). Служба Владе надлежна за пројектовање, усклађивање, развој и функционисање система електронске управе успоставља и води ЈИС ЛПА и обезбеђује техничке услове за његову примену[15].

2. Информациони системи локалне пореске администрације

Информациони систем је сложен скуп технологије, процеса и људи који заједно функционишу ради процесирања, складиштења и преношења информација и података, како би се подржала мисија организације и њене пословне функције. ЈЛС води податке који су од значаја за утврђивање износа изворних јавних прихода као и податке о њиховој наплати у јединственом информационом систему (даље ЈИС). Служба Владе надлежна за пројектовање, усклађивање, развој и функционисање система електронске управе успоставља и води ЈИС ЛПА и обезбеђује техничке услове за његову примену[16].

Канцеларија за ИТеУ[17] је успоставила државни дата центар за смештај кључне информационо-комуникационе инфраструктуре Републике Србије. Како су навели представници Канцеларије центар испуњава Tier 3+ стандард, а услуге се пружају у складу са стандардом ИСО 27001, као и стандардима квалитета ИСО 9001 и квалитетом пружања услуга ИСО 20000. Државни дата центар поред смештања опреме државних органа пружа и услуге државног клауда – Government cloud[18].

---

[11] "Службени гласник РС", бр. 62/2006, 47/2011, 93/2012, 99/2013 - усклађени дин. изн., 125/2014 - усклађени дин. изн., 95/2015 - усклађени дин. изн., 83/2016, 91/2016 - усклађени дин. изн., 104/2016 - др. закон, 96/2017 - усклађени дин. изн., 89/2018 - усклађени дин. изн., 95/2018 - др. закон, 86/2019 - усклађени дин. изн. и 126/2020 - усклађени дин. изн.

[12] Ибид, члан 6.

[13] "Службени гласник РС", бр. 26/2001, "Сл. лист СРЈ", бр. 42/2002 - одлука СУС и "Сл. гласник РС", бр. 80/2002, 80/2002 - др. закон, 135/2004, 61/2007, 5/2009, 101/2010, 24/2011, 78/2011, 57/2012 - одлука УС, 47/2013, 68/2014 - др. закон, 95/2018, 99/2018 - одлука УС, 86/2019 и 144/2020.

[14] "Службени гласник РС", бр. 80/2002, 84/2002 - испр., 23/2003 - испр., 70/2003, 55/2004, 61/2005, 85/2005 - др. закон, 62/2006 - др. закон, 63/2006 - испр. др. закона, 61/2007, 20/2009, 72/2009 - др. закон, 53/2010, 101/2011, 2/2012 - испр., 93/2012, 47/2013, 108/2013, 68/2014, 105/2014, 91/2015 - аутентично тумачење, 112/2015, 15/2016, 108/2016, 30/2018, 95/2018, 86/2019 и 144/2020.

[15] Ибид, члан 159.

[16] Ибид, члан 159.

[17] Уредба о Канцеларији за информационе технологије и електронску управу „Службени гласник РС“, 73/2017, 8/2019.

[18] Државни клауд је модел за омогућавање свеобухватног, погодног мрежног приступа на захтев дељеним заједничким подесивим рачунарским ресурсима (мрежама, виртуелним машинама, складиштима података,

Слика број 1. Државни дата центар у Крагујевцу, панорамни снимак

Ресурси у дата центру се државним органима нуде по моделу IaaS (Инфраструктура као услуга - Infrastructure as a Service) односно, издају се виртуелни серверски ресурси према захтеву корисника. Овај модел подразумева да су све инфраструктурне, односно хардверске компоненте укључујући и слој виртуелизације[19] хостоване[20] у државном дата центру. На тај начин корисник ове услуге не мора да брине о обезбеђивању адекватног простора и одржавању опреме.

Подаци и опрема различитих државних институција су смештени у државни дата центар, међу којима су Министарство државне управе и локалне самоуправе, Централни регистар обавезног социјалног осигурања, Министарства пољопривреде и многих других. У центру се налази опрема и подаци Канцеларије за ИТеУ, државна Oracle cloud инфраструктура. Државни дата центар је изграђен у Крагујевцу и састоји се од 2 објекта површине око 14 хиљада квадратних метара.

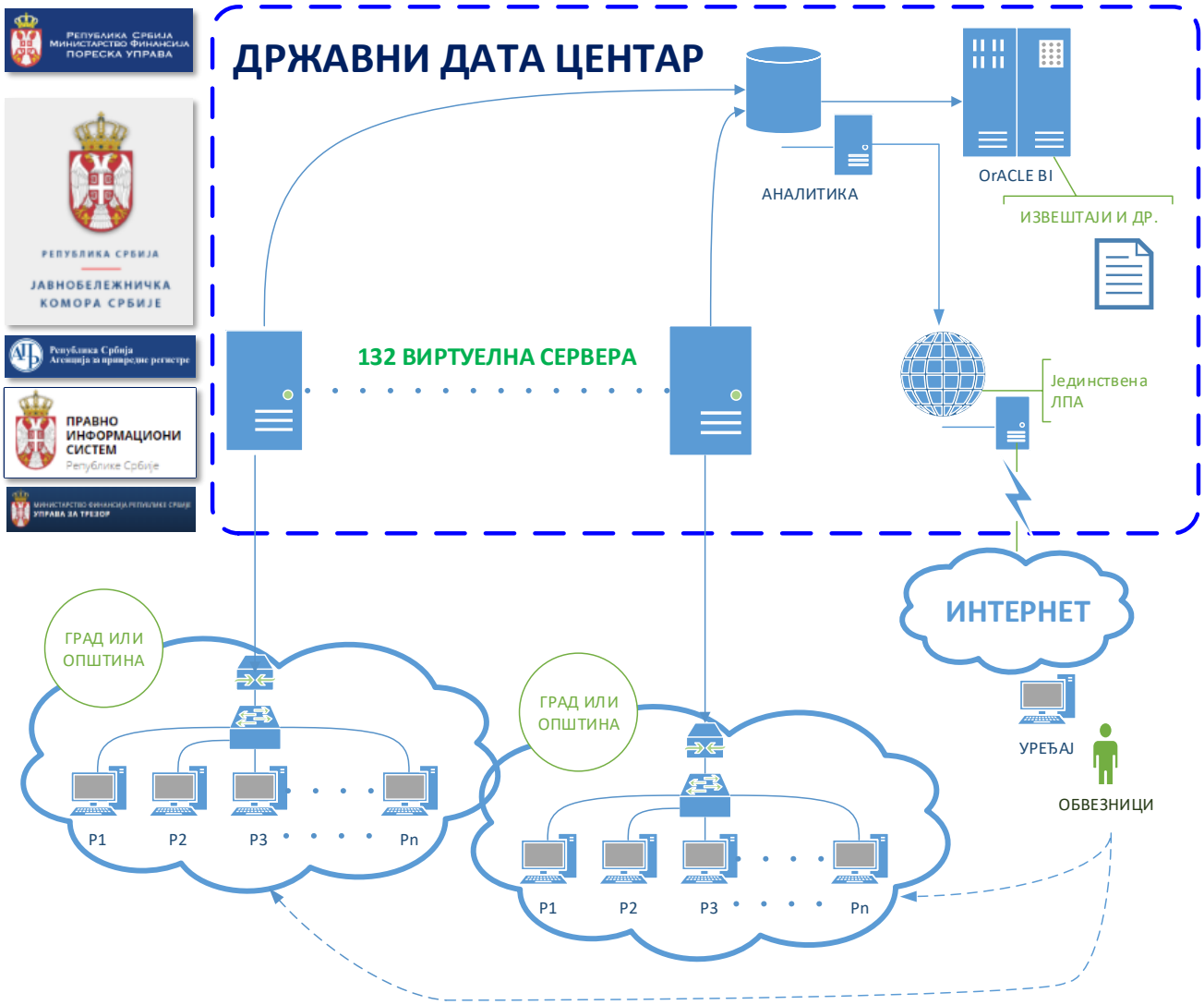
У продукцији је први објекат од 8.185 м^2, 640 рек ормана, са могућношћу допуне за још 320 рек ормана. Укупан капацитет 1080 рек ормана који је 5 пута већи од Државног дата центра у Београду, пружа услуге државним органима и комерцијалним корисницима.

апликацијама и услугама) који могу брзо да буду расположиви и употребљени, уз минималан напор управљања или активност понуђача услуге. (NIST800-145, **https://csrc.nist.gov/publications/detail/sp/800-145/final**)

[19] Виртуелизација је софтверска симулација хардвера на којем ради други софтвер. Другим речима, виртуелизација је поступак трансформисања физичких рачунарских система у софтверске рачунарске системе, који се извршавају на хардверу/опреми посебно намењеној за рад више софтверских рачунарских система истовремено. **https://csrc.nist.gov/publications/detail/sp/800-125/final**

[20] Хостовање је информатичка услуга коју пружа добављач, може обухватити давање меморијског простора на серверу за смештај апликације или веб презентације, базу података за смештај променљивог дела садржаја или података, може обухватати и регистрацију домене, јавну ИП адресу итд.

Испуњава стандард поузданости од 99,995% и сви системи су дуплирани – 2N редуданса[21]. Без напајања са оба енергетска вода систем може да ради 96 сати, без досипања горива у резервоаре. Максимална енергетска ефикасност – топлота коју ослобађа опреме користи се за грејање административног простора и тренутно је запослено 20 младих стручњака из Крагујевца који раде на пословима одржавања.



Слика број 2. Принципијелна шема система ЛПА

Државни дата центар у Београду је извршио виртуализацију свих серверских система у 132 ЈЛС инсталирајући их на једном месту где је успостављен и централни систем за пословно извештавање омогућујући нове значајне могућности фискалног система у целини. Успостављени ЈИС ЛПА преузима податке из изворних регистара, и то из: Регистра матичних књига, Регистра пребивалишта, Регистра привредних друштава, односно предузетника, Катастра непокретности и других регистара неопходних за његово вођење, у складу са законом којим се уређује електронска управа[22]. (Видети слику број 1. Принципијелна шема система ЛПА)

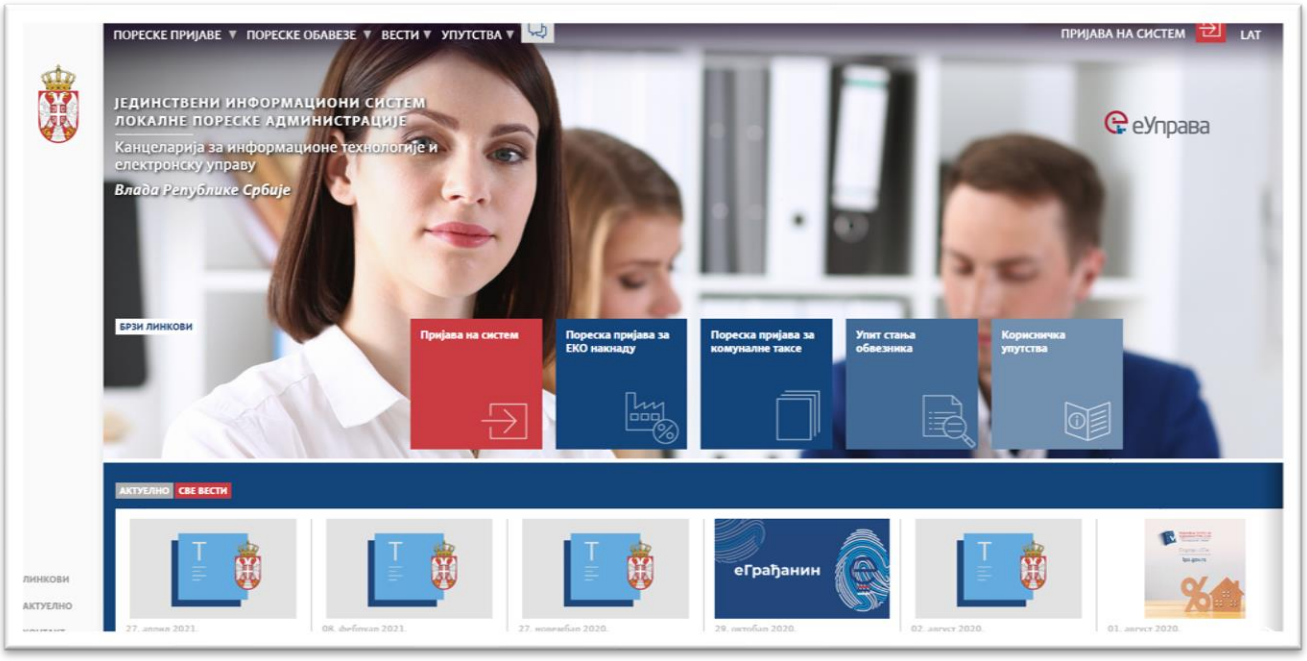
[21] 2N редундантни систем се састоји од два идентична независна система, и када један систем може преузети све оперативне потребе другог система, који може да откаже из било ког разлога. Овакав систем се сматра отпорним на грешке, јер се лако одржава и поправља један док је други у функцији.

[22] Ибид [4], члан 159.

Рачунарска апликација за локалну пореску администрацију

Апликативни слој ИСЛПА јединствен за све ЈЛС развијан је равноправно са решењима других произвођача али квалитетом решења обухватио је 80% ЈЛС. Захваљујући квалитетном решењу, имплементацији, обуци и подршци корисницима бољој од конкуренције, 2018. године постаје једино решење у процесу консолидације фискалног система ЈЛС. На нивоу структуре базе података реч је о дистрибуираном систему који истовремено решава добар део питања униформног и стандардизованог извештавања технологијом веб портала. Портал ЛПА је део ЈИС ЛПА који је намењен пореским обвезницима за контролу свог пореског дуга у ЛПА на територији Србије и подношење пореских пријава ППИ1 и ППИ2. Приступ Порталу је могућ електронском сертификационом картицом и тада обвезник може да користи обе функционалности.

Слика број 3. Интернет портал ЈИСЛПА



Отварањем корисничког налога обвезник само у једној ЛПА, добија налог за читаву територију Србије. Налог се односи на порески идентификациони број обвезника без обзира да ли се ради о ЈМБГ или ПИБ идентификацији.

Изменама и допунама ЗППА од 01.01.2019. године обавезно је подношење пореских пријава ППИ-1 електронским путем преко портала ЈИСЛПА на адреси **https://lpa.gov.rs**. На овај начин поред пријава за текућу годину подносе се и пореске пријаве ППИ-1 и не прихватају се скенирани папирни обрасци попуњени руком.

У оквиру ЛПА апликације избора Евиденција пријава – Утврђивање обавеза - Имовина правних лица-ППИ-1 налазе се табови: ППИ-1 Пријава, Пријем података - пријем података из XML фајла, таб Преглед е-ППИ-1 Пријава - преглед и пренос пореских пријава поднетих преко портала и Преглед објеката - преглед података о објектима за све поднете пореске пријаве. Преглед пореских пријава које су поднете преко портала е-управе могуће је у избору Преглед е-ППИ-1 Пријава. Издвајање скупа пријава поднетих преко портала ЈИС-а могуће је задавањем критеријума претраге *Извор података* – WEB.

1. Активности које је потребно спровести у фискалној години пре израде завршног рачуна

1. Евидентирање познатих каматних стопа;

2. Књижење задужења и сторно задужења на основу пријава ППИ-1, решења о задужењу, Р-налога, репрограма, ванбилансне евиденције и решења о принудној наплати. Пре књижења неопходно је евидентирати познате датуме уручења решења.;
3. Књижење камате и валоризације на доспеле рате репрограма;
4. Сторнирање несторнираних привремених аконтација;
5. Књижење уплата;
6. Превалутирање датума на први следећи радни дан уколико доспева нерадног дана.

2. Активности које је потребно спровести у фискалној години око израде завршног рачуна и формирања почетних стања, привремених задужења и репрограма у следећој години

1. Провера исправности књиговодствених налога;
2. Израда контролног упита стања са 31.12.20xx. за завршни рачун;
3. Књижење камате обрачунате упитом стања (у синтетици);
4. 4 Књижење временских разграничења;
5. Штампа образаца завршног рачуна;
6. Ажурирање шифарника за формирање привремених задужења у следећој години;
7. Формирање почетних стања, привремених задужења и рата репрограма у следећој години.

3. Завршни рачун – штампа образаца: упоредни преглед класе 2 И ГО-3/1

Акција *извоза* формира се датотека са упоредним прегледом стања на синтетичким рачунима у класи 2 (класа обвезника) из Бруто биланса и стања на аналитичким рачунима из обрасца ГО-3/1 (израчунатом на основу упита стања).

Извештавање из ЛПА апликације

У извештајном делу омогућени су сви прописани обрасци као и други извештаји о кумулативном и појединачном прегледу финансијских показатеља од интереса за рад ОЈП, као што су:

1) **Фискална анализа – Анализа пријава и утврђених обавеза** (по врсти јавног прихода) омогућава подршку пословног процеса Фискалне анализе улазних елемената за обрачун по врсти изворног јавног прихода, као и утврђених задужења по задатим критеријумима и за изабрани фискални период;
2) **Фискална анализа – Анализа пореског књиговодства**
   - **Решења** (утврђена обавеза) омогућава преглед и евидентирање података о обрачунатим, урученим и евидентираним решењима о задужењу по свим видовима јавних прихода;
   - **стање на аналитичким рачунима** омогућено је добијање извештаја о стању на рачунима обвезника и проценту наплате за задате критеријуме;
   - **стање на синтетичким рачунима** - омогућено је добијање извештаја о стању на рачунима јавних прихода - Бруто биланс, Биланс стања и Главна књига за задате критеријуме.
3) **Пореско књиговодство:**
   - **Преглед књиговодствених налога**
     - налози (преглед аналитичких и синтетичких ставки за одабрани налог);
     - аналитика - омогућен је увид у аналитичке ставке за изабрани налог - за конкретног обвезника или аналитика за одређени рачун јавног прихода и одређену шифру промета (увид у књиговодствене ставке на индивидуалним рачунима обвезника);
     - упоредни преглед - омогућава преглед синтетике и аналитике за изабрани налог или скуп налога.
   - **Књижење задужења** омогућава преглед и евидентирање података о обрачунатим, урученим и евидентираним решењима о задужењу по свим видовима јавних прихода.
     - **Књижење уплата** омогућава пријем, преглед и књижење извода рачуна јавних прихода локалне самоуправе које свакодневно доставља Трезор;

- **Измене књиговодствених налога** омогућава евидентирање налога за књижење којима је омогућена корекција стања на рачунима обвезника – ручни налози
- **Завршни рачун** омогућава израду Годишњег обрачуна за текућу фискалну годину и формирање почетних стања у наредној години. Основне функције у процесу израде Годишњег обрачуна су формирање Бруто биланса и Биланса стања на дан 31. децембар, као и књижење обрачунате камате у Главној књизи;
- **Сторнирање привремених аконтација** Преглед несторнираних привремених задужења омогућен је за изабраног обвезника, рачун или пореску обавезу;
- **Репрограм** у делу евиденције решења за репрограм омогућено је добијање извештаја по различитим критеријумима;
- **Ванбилансна евиденција о**могућено је вођење ванбилансног пореског рачуноводства. Ванбилансна аналитика даје преглед прекњижених износа дугова и камате са рачуна обвезника (аналитика) у ванбилансно пореско рачуноводство (ванбилансна аналитика). Преглед је омогућен по основима прекњижавања у ванбилансну евиденцију (брисање, застарелост, стечај).

Слика број 4. Преузимање података са уговора од нотара

4) **Редовна наплата – упит стања за више обвезника** где је омогућена израда упита стања за изабрани скуп обвезника (сви обвезници, физичка лица, правна лица, предузетници, ортачке радње, умрла лица) или учитавање обвезника према одговарајућим задатим критеријумима (у сврху контроле дужника са формираног списка обвезника или обвезника за које одобрено одлагање дугованог пореза, а све у сврху вођења поступка редовне наплате);
5) **Евиденција пријава – утврђивање обавеза** где је омогућено издвајање пријава и формирање извештаја по рачунима јавних прихода према изабраним критеријумима (статус пријаве, извору података и др.) као и преглед пријава које су примљене електронским путем;
6) **Поред извештаја у систему ЛПА формиран је и Аналитички систем ЈИС ЛПА** који обезбеђује приказ, чување и штампу предефинисаних извештаја који дају одговоре на уобичајена аналитичка питања. Групе аналитичких извештаја приказују се на посебним странама прегледа "ISLPA" аналитичког система. На свакој страни извештаја могућ је избор вредности параметара извештаја, којима се одређује обухват извештаја **(прилог – документ 22 – BI упутство за кориснике)**

За потребе пословног извештавања дефинисани су BI извештаји и груписани су у неколико целина: структура обвезника, пријаве, решења и задужења, решења по обвезнику и рачуну, аналитика, салдо, салдо дужника, дужници, највећи дужници, картон обвезника, дуговања, дуговања обвезника по рачуну, дуговања обвезника по општини, преплате обвезника по рачуну, уплате, уплате по шифри промета и упит стања.

IV Закључци

На основу анализе података и документације достављених од стране субјеката ревизије, као и обављених интервјуа (представници субјеката ревизије и извора информација), донели смо следећи закључак:

Поред значајног унапређења управљања информационим системом, неопходно је додатно унапредити управљање матичним евиденцијама јавних регистара и комуникацију са корисницима.

Закључак је донет на основу закључака о појединачним питањима уједно аспектима информационог модела и то:

1. **Доступност информација**, података и докумената ИС ЛПА је повећана формирањем Јединственог система у Државном дата центру истовремено смањујући ризике који могу настати услед хаварије. Потребно је побољшати управљање проблемима, инцидентима и комуникацију са крајњим корисницима.
2. **Интегритет информација**, података и докумената ИС ЛПА није обезбеђен у потпуности, јер у већем делу се заснива на подацима преузетим из екстерних система и регистара без означавања извора података, што за последицу може имати немогућност утврђивања аутентичности, непорецивости и комплетности података.
3. **Поверљивост информација**, података и докумената који се користе у ЛПА није обезбеђена у потпуности, јер подаци, документи и информације које се преузимају из других матичних евиденција и регистара се чувају без крипто-заштитних механизама.

ЗАКЉУЧАК 1: Доступност информација, података и докумената ИС ЛПА је повећана формирањем Јединственог система у Државном дата центру истовремено смањујући ризике који могу настати услед хаварије. Потребно је побољшати управљање проблемима, инцидентима и комуникацију са крајњим корисницима.

Наш циљ у овом делу извештаја, био је да одговоримо на прво ревизијско питање, односно да ли је на адекватан начин обезбеђена доступност информација, података и докумената у информационом систему.

Посматрајући универзални информациони модел сваког система који прво да је успостављен (тј. да постоји, да је расположив или доступан свим заинтересованим странама, пројектантима, корисницима, обвезницима, грађанима, итд.) у том смислу смо испитивали:

Да би донели закључак о адекватности начина обезбеђења расположивости информационог система ЛПА и свега што он обухвата, испитивали смо:

1. Да ли је успостављено адекватно управљање проблемима и инцидентима?
2. Да ли је успостављено адекватно управљање услугама?
3. Да ли је успостављено адекватно управљање информационом безбедношћу?

као и друга питања која обезбеђују расположивост система и услуге.

Законом о пореском поступку и пореској администрацији је дефинисано да успостављање и вођење ЈИС ЛПА обавља Канцеларија за ИТеУ, исто тако у наставку реченице је наведено и да обезбеђује техничке услове за његову примену. Оваква дефиниција је створила конфузију код корисника/пореских службеника ЈИС ЛПА, као и код пореских обвезника, тако да питања у вези примене прописа која су правне природе бивају упућивана у Канцеларију за ИТ. Додатан проблем у пракси ствара и нова измена обавезе објављена у „Службеном гласнику РС“ бр. 96/2021, где се у члану 32 дефинише да послове вођења ЈИС ЛПА преузима Министарство финансија – Пореска управа, најкасније до 1. јануара 2024. године.

Обавезе проистекле из Закона о финансирању локалне самоуправе[23] примењују ЈЛС и самим тим су они и надлежни да одређују све елементе за утврђивање и наплату појединачних износа пореских обавеза. Појам вођења[24] система у овом случају је реч о делу пореског система за финансирање активности локалне самоуправе подразумева управљање системом. Због погрешно прихваћеног појма вођења система, многи корисници-службеници ЛПА и порески обвезници са питањима у вези примене пореских прописа обраћају се Канцеларији за ИТеУ.

Управљање проблемима и инцидентима је процес који обезбеђује да се правовремено препознају у евидентирају сви потенцијални проблеми у употреби ЈИС ЛПА. Многи од тих проблема јављају се у раној фази коришћења, где у добром делу представљају проблеме усаглашености разних софтверских решења и/или оперативног система итд. и често проблеми у раду са ИС препознају као безбедоносни проблеми тј. Инциденти. Зато је потребно да корисници могу пријавити такве проблеме служби подршке, која их евидентира, а затим и да правовремено реагује и отклони разлог проблема. Како се инцидент може десити било где у систему, запослени који уочи настали проблем треба да обавесте надлежно лице, које ће предузети даље кораке, или дати инструкције. Како је прописана обавеза за операторе ИКТ система, они су дужни да инциденте пријављују на првој страни портала cert.rs. Процес почиње када корисник попуни контакт форму која га усмерава како да успешно пријави и прати такву комуникацију са

[23] Ибид [1], члан 6.

[24] Вођење у теорији менаџмента подразумева активности између руководилаца и сарадника које имају за циљ остварење заједничког циља кроз мотивисање, стил руковођења и комуницирање.

службама подршке за систем ЛПА. Обвезници, корисници, добављачи и пружалац услуге државног клауда имају интерес да постављају питања која се морају евидентирати у форми пријаве техничког проблема, или проблем у софтверу, могућег предлога унапређења корисничког интерфејса. Обвезници могу имати потребе и за пореско-правним питањем које се мора проследити надлежном органу за јавне приходе у ЈЛС према којој обвезник има неку обавезу, нпр. некретнину, седиште предузећа итд. Зато је неопходно успоставити потпуно контролисан процес комуникације по принципима управног поступка.

Управљање услугама подразумева процес који обезбеђује да се у продукционом окружењу морају надгледати, контролисати и прегледавати вршење услуга. Када ствари крену лоше, требало би да постоје робусни процеси на месту за чување, решавање и осигуравање да се оне више не понове. Циљ вршења услуге је да омогући функционисање окружења што је могуће равномерније и стандардније. Корисници директно комуницирају са оперативним службама и било какав проблем може имати директан утицај на њихову перцепцију рада пружаоца услуга и на крају и на репутацију. Зато је неопходно све обавезе које имају ЈЛС и пружалац услуге државног клауда да буду уређене Споразумом обзиром да се ради о органима јавне управе Републике Србије чије су обавезе, права и одговорности уређени прописима. Многе обавезе које произилазе из Закона о информационој безбедности заједно са повезаним ризицима преносе се на Канцеларију за ИТеУ која пружа услуге државног клауда.

Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица[25].

Укључује мере откривања, документовања и решавање проблема неовлашћеног приступа или измене података на серверима, обради и преносу података и омогућавању рада овлашћеним корисницима. Информациона безбедност обухвата безбедност система и безбедност комуникација.

Према одредбама члана 7 Закона о информационој безбедности оператор ИКТ система од посебног значаја (у нашем случају-Канцеларија за ИТеУ) одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидента, односно превенција и умањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима[26]. Мере заштите ИКТ система су у Закону о информационој безбедности подељене на 28 мера заштите[27]. Према одредбама члана 8 Закона о информационој безбедности оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система. Такође је дужан да самостално или уз ангажовање спољних експерата врши проверу усклађености примењених мера ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње и да о томе сачини извештај[28].

У оквиру мера информационе безбедности неопходно је донети и План континуитета пословања (Business Continuity Planning-BCP) подразумева активности које организација спроводи у циљу опоравка пословних процеса након појаве нежељених догађаја. Хаварије које се могу јавити у ЈИСЛПА треба уредити Планом опоравка од хаварије (енгл. Disaster Recovery Plan-DRP). У пракси је то план како организација наставља да послује након што се деси хаварија на систему.

[25] Члан 2 став 1 тачка 3 Закона о информационој безбедности.
[26] Члан 7 став 2 Закона о информационој безбедности.
[27] Члан 7 став 3 Закона о информационој безбедности.
[28] Члан 8 став 4 Закона о информационој безбедности.

Према одредбама Закона о информационој безбедности (члан 7) и према члану 29 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја[29] оператор ИКТ система[30] треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура.

Такође је прописано да оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације (члан 29 став 2 Уредбе)[31].

Задатак оператора ИКТ система је да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације (члан 29 став 3 Уредбе).

Налаз 1.1: Канцеларија за ИТеУ није у потпуности успоставила адекватно управљање проблемима и инцидентима, јер постојећа контакт форма нема потврду о пријему и обради поруке у складу са темом поруке, отежавајући превенцију инцидената, стварајући ризик да евентуални проблеми и инциденти ескалирају, отежају или онемогуће доступност ЛПА апликације.

Законом о информационој безбедности[32] се одређују мере заштите од безбедносних ризика у ИКТ системима и одговорностима правних лица приликом управљања и коришћење ИКТ система. Чланом 8 Закона прописана је обавеза да оператор ИКТ система донесе Акт о безбедности ИКТ система од посебног значаја којом се уређују мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја. Посебна Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја детаљније дефинише садржај акта који се мора редовно усклађивати с променама у окружењу и у самом ИКТ систему.

За процену доступности у погледу подршке корисницима ЛПА апликације послат је упитник на адресе 167 јединица локалне самоуправе према списку Министарства надлежног за послове државне управе и локалне самоуправе и пристигло је укупно 106 одговора.

На питање да ли сте имали ситуације да вам је ЛПА апликације била недоступна, 71 ЛПА је одговорила са да, односно 67% од укупног броја, 29 ЛПА је одговорило са не, односно 27% од укупног броја, 3 ЛПА је одговорило са не знам, односно 3% од укупног броја и преосталих 3 ЛПА је одговорило са остало, односно 3% од укупног броја.

На питање недоступност ЛПА апликације се десила, 65 ЛПА је одговорило са веома ретко, односно 61% од укупног броја, 9 ЛПА је одговорило са једном, не сећа се тачно када, односно 8% од укупног броја. 1 ЛПА је одговорила са више пута у последње две године, односно 1% од укупног броја, 5 ЛПА је одговорило са више пута у последњих годину дана, односно 5% од укупног броја, 3 ЛПА је одговорило са више пута у последњих пар месеци, односно 3% од укупног броја, 17 ЛПА је одговорило са никада, односно 16% од укупног броја, 1 ЛПА је одговорила са једном недељно, односно 1% од укупног броја и преостала 1 ЛПА је одговорила са остало, односно 1% од укупног броја.

[29] „Службени гласник РС“ бр. 94/2016.

[30] Оператор ИКТ система – правно лице, орган власти или организациона јединице органа власти који користи информационо-комуникациони систем у оквиру обављања своје делатности, односно послова из своје надлежности.

[31] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

[32] Члан 7 Закона о информационој безбедности.

На питање трајање недоступности ЛПА апликације је било колико дуго, 85 ЛПА је одговорило са краткотрајно, односно 80% од укупног броја, 2 ЛПА је одговорило са цео радни дан, односно 2% од укупног броја, 2 ЛПА је одговорило са више радних дана, односно 2% од укупног броја, 6 ЛПА је одговорило са не знам тачно, односно 6% од укупног броја и преосталих 11 је одговорило са остало, односно 10% од укупног броја.

Ретке и краткотрајне недоступности ЈИСЛПА запослене у ОЈП нису угрозиле њихов рад, а то се видело на основу њиховог одговора да у 4% ЛПА никоме нису пријављивали проблем јер имају искуство да су прекиди краткотрајни и повезани са прекидом интернета.

Слика број 5. Преглед пријаве проблема

На питање решавања техничких проблема у коришћењу ЛПА апликације коме су пријавили, 66 ЛПА је одговорило са Институту „Михајло Пупин“, односно 62% од укупног броја, 2 ЛПА је одговорило са Канцеларији за ИТеУ, односно 2% од укупног броја, 31 ЛПА је одговорила са Интерној ИТ служби, односно 29% од укупног броја, 4 ЛПА је одговорило са никоме нисам пријавио, односно 4% од укупног броја и преосталих 3 ЛПА је одговорило са остало, односно 3% од укупног броја.

Корисници још увек не препознају Канцеларију за ИТеУ као пружаоца услуге државног клауда, тј. Органа који управља државним дата центром.

На веб презентацији ЈИСЛПА **https://lpa.gov.rs/jisportal/homepage** постоји контакт форма „Будимо у контакту“ која позива обвезника да постави питање, коментар, сугестију или да пријави било какав проблем који је у оквиру надлежности Канцеларије за ИТеУ. Надлежности и послови Канцеларије су дефинисани[33] тако да она успоставља и води ЈИСЛПА и обезбеђује техничке услове за његову примену. Како је у два дела посебно наглашено да у првом делу Канцеларија „успоставља и води ЈИСЛПА“, а у другом делу она „обезбеђује техничке услове“, у пракси је направило ситуацију да се обвезници обраћају Канцеларији за сва питања, и да се та питања једноставно прослеђују добављачу софтверског решења. Природа обраћања путем ове

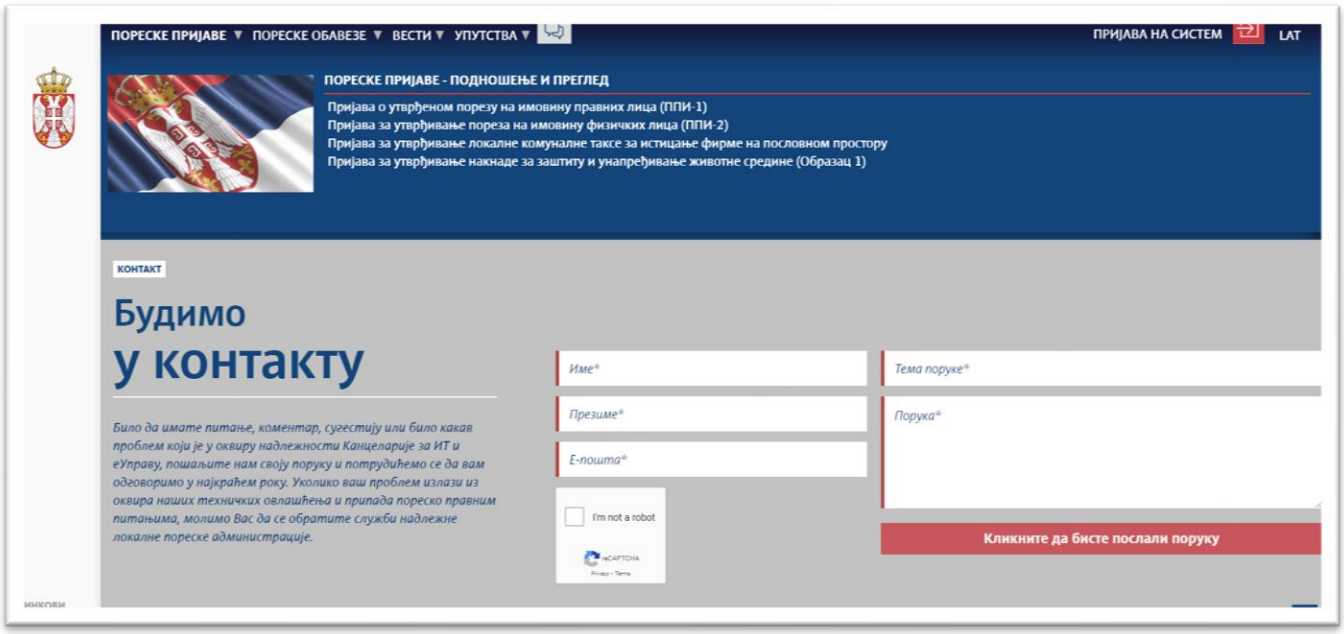
[33] Члан 159 Закона о пореском поступку и пореској администрацији

форме су различита и није мали број случајева да су пореско-правне природе, а она спадају у надлежности ОЈП ЈЛС.

Без потврде пријема поруке у којој се налази послати садржај, обвезник/корисник није сигуран да је порука испоручена на праву адресу и да ће добити одговор.

Постојећа контакт форма нема потврду пријема пријаве нити било какву класификацију проблема према типу, нпр. пореско-правно питање, технички проблем, проблем пријављивања са цертификатом, итд, чиме би се одредило преусмеравање поруке на адресу надлежног органа или запосленог у органу за тај тип питања.

Слика број 6. Интернет портал ЈИСЛПА



Циљ управљања проблемима и инцидентима је успостављање механизма којим се инциденти евидентирају, а потом и благовремено отклоне. Како се инцидент може десити било где у систему, запослени који уочи настали проблем треба да обавести надлежно лице, које ће предузети даље кораке, или дати инструкције. форма за пријаву на првој страни портала би се допунила са типом пријаве: захтев за информацију или пријава техничког проблема, проблем у софтверу, предлог унапређења корисничког интерфејса, пореско-правно питање итд. које ће одредити ко обрађује пријаву итд.

Препорука: Препоручује се Канцеларији за ИТеУ да унапреди контакт форму са тикетинг системом који омогућава кориснику који је пријавио проблем да прати промену статуса и коначну обраду пријаве.

Налаз 1.2: Канцеларија за ИТеУ није у потпуности успоставила адекватно управљање услугама, јер није закључила уговоре/споразуме са ЈЛС о нивоу пружених услуга и мерама информационе безбедности, чиме се ствара ризик да се приликом појаве техничких проблема неадекватно реагује, отежа или онемогући доступност ЛПА апликације.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене; утврдити поступак извештавања, праћења и поступања у складу са захтевима Канцеларије у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга.

Канцеларија успоставља механизме надзора над пружањем услуга тако што се са сваким испоручиоцем услуге треба да склопи посебан уговор (уговори), којим се дефинишу:

- Захтевани ниво услуге од пружаоца услуга (Service Level Agreement - SLA[34]);
- Услови везани за информациону безбедност и поверљивост података (Споразум о поверљивости);

Ови уговори се контролишу пре пријема услуге, као и пре продужетка уговора. Све промене уговора регулишу се анексима уговора или новим уговорима. Уговори морају да садрже недвосмислене и мерљиве критеријуме којима ће се утврдити да ли се уговорени нивои услуге поштују.

Канцеларија треба да одреди која лица су одговорна за надзор извршења уговора за сваког посматраног пружаоца услуга по том уговору. Ова лица управљају односима са пружаоцем услуга и редовно прате, анализирају, преиспитују и проверавају извршене услуге и усаглашеност са уговореним нивоом услуге. Приликом надзора над извршењем квалитета и саобразности уговорене услуге проверава се да ли пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама и могућностима Канцеларије.

У поступку објективне евалуације квалитета и обима пружене услуге у односу на уговорену, потребно је прикупити све релевантне чињенице, мере, податке и документацију у вези са извршењем услуге, као и прикупити податке од непосредних, крајњих, корисника у вези са предметом услуге.

Лица која врше надзор извршења уговора са испоручиоцем морају да предузму одговарајуће мере уколико се уоче недостаци у пружању услуге (захтев за исправком/унапређењем, опомена о раскиду уговора, предлог измена услова уговора). Када се уговор мења или прекида, морају се уклонити сва права приступа која су овим уговором додељена трећим лицима (запослени код пружаоца услуга). Надаље, мора се осигурати да у случају измене или прекида уговора, да ће сва опрема, софтвер и информације у електронском или папирном облику бити враћени.

Уговором са пружаоцем услуга треба обезбедити могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација.

Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи Канцеларија ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

Препорука: Препоручује се Канцеларији за ИТеУ да изради Споразум о нивоу оперативних услуга са свим ЈЛС и да садржајем уреде питања обраде података и питања информационе безбедности.

Налаз 1.3: Канцеларија за ИТеУ није у потпуности успоставила адекватно управљање информационом безбедношћу, јер није уредила и применила процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система што за последицу има већи степен рањивости система и већи степен рањивости осетљивих података о личности који се налазе у систему.

Законом о информационој безбедности[35] као прве мере заштите одређено је успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се

[34] Service Level Agreement - SLA је уговор између наручиоца и испоручиоца услуге којим се прецизира какву врсту подршке за пружање услуге је испоручилац услуге дужан да пружи.
[35] Члан 7 Закона о информационој безбедности.

остварује управљање информационом безбедношћу. У Уредби о ближем уређењу мера заштите информационо-комуникационих система[36] дефинише се да оператор ИКТ система треба да обезбеди да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност.

Све веће претње по безбедност информационог система долази из сајбер простора путем електронских порука са злонамерним садржајем. Зато је неопходно редовно обавештавати запослене о најновијим покушајима да буду преварени лажном поруком које нападачи користе како би преузели управљање над појединим деловима или целокупним системом. У том процесу унутрашње комуникације треба обухватити и друге такве догађаје као што су злоупотреба лозинке за приступ систему, итд.

Поред обавештавања потребно је и организовати интерно обучавање о новим обавезама, прописима и другим важним догађајима који утичу на безбедност информационог система.

Слика број 7. Највећих 15 претњи у сајбер (интернет) простору

Извор: Европска агенција за сајбер безбедност, https://www.enisa.europa.eu/

Законом о информационој безбедности[37] је инцидент дефинисан као сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система. Када је реч о клауд решењима све сајбер претње истовремено и претње за ЈИСПА.

Обавеза сваког оператора да о инцидентима у ИКТ систему обавештава надлежни орган и то је уређено Уредбом[38] којом су дефинисани сви неопходни елементи инцидената, који се достављају електронским путем.

[36] "Сл. Гласник РС", бр. 94/2016.

[37] Члан 2 Закона о информационој безбедности.

[38] Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја ("Сл. гласник РС", бр. 11/2020) и претходна Уредба о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у ИКТ системима од посебног значаја („Сл. Гласник РС“ бр. 94/2016).

Тако је предвиђено да се о инцидентима у ИКТ системима од посебног значаја, а који могу да имају значајан утицај на нарушавање информационе безбедности у целом друштву, пријаве ЦЕРТ-у који је успоставило регулаторно тело РАТЕЛ.

Како Канцеларија за ИТеУ води Државни дата центар све више постаје значајно успостављање управљања клаудом, применом радног оквира за ИТ контроле клауд апликација. Алијанса за безбедност клауда[39] од 2008. године усавршава радни оквир којег су усвојиле готово све државе и институције које се баве информационом безбедношћу, а пре свега Национални институт за стандарде и технологију[40].

Контролни оквир за информациону безбедност у клауду[41] садржи 17 домена који покривају све кључне аспекте клауд технологије. Сваки домен је подељен на 197 контролна циља. Може се користити као алат за систематску процену имплементације у облаку, пружајући смернице о томе које безбедносне контроле треба да спроведе који актер у ланцу употребе клауд решења.

1. **Домен ревизије и уверавања** (A&A) састоји се од шест (6) контролних спецификација. Овај домен је осмишљен као подршка пружаоцима и корисницима клауд услуга у дефинисању и спровођењу процеса управљања ревизијом за подршку планирању ревизије, анализи ризика, процени безбедносне контроле, закључку, санирању, генерисању извештаја и прегледима прошлих извештаја и пратећих доказа.
2. **Домен безбедности апликација и интерфејса** (АИС) укључује седам (7) контролних спецификација које помажу организацијама у облаку да мигрирају ка сигурном дизајну, развоју, примени и раду апликација и њихових интерфејса у облаку.
3. **Домен континуитета пословања и оперативне отпорности** (БЦР) помаже пружаоцима и корисницима клауд услуга да осигурају услуге у облаку које пружају или користе буду поуздане. Домен води стратегије отпорности - укључујући развој планирања ублажавања и напора за имплементацију - како би се омогућило организацијама да наставе пословање када се суоче са предвиђеним и непредвиђеним поремећајима. Домен се састоји од једанаест (11) контролних спецификација.
4. **Домен контроле промена и управљања конфигурацијом садржи девет** (9) контрола. Ове контроле су осмишљене да умање ризике повезане са променама конфигурације имовине информационих технологија (ИТ) придржавањем робусног процеса управљања променама - без обзира на то да ли се ИТ имовином управља интерно или екстерно.
5. **Домен криптографије, шифровања и управљања кључевима** (ЦЕК) састоји се од двадесет и једне (21) контролне спецификације осмишљене да осигура да се подаци и кључеви користе за заштиту и правилну заштиту података.
6. **Домен безбедност центра података** је домен се састоји од петнаест (15) контролних спецификација које помажу организацијама које пружају услуге хостинга центара података, које се називају „пружаоци услуга у облаку“.
7. **Домен безбедност података и управљање животним циклусом приватности** је домен који садржи деветнаест (19) контрола приватности и сигурности података. Ове контроле нису специфичне за индустрију или сектор и нису фокусиране на одређену земљу или пропис.

[39] Cloud Security Alliance (CSA) је непрофитна организација са мисијом да „промовише употребу најбољих пракси за обезбеђивање сигурности у клауд рачунарству и да пружи образовање о употреби клауда како би се осигурали сви други облици рада на рачунару. ЦСА има преко 80.000 појединачних чланова широм света. ЦСА је стекла значајну репутацију 2011. године када је америчка председничка администрација изабрала ЦСА као место за објављивање стратегије рачунарства у облаку савезне владе.

[40] NIST - Национални институт за стандарде и технологију је физичко-научна лабораторија и регулаторна агенција Министарства трговине САД. Његова мисија је промовисање америчких иновација и индустријске конкурентности. Активности НИСТ-а су организоване у лабораторијске програме који укључују науку и нанотехнологију, инжењеринг, информациону технологију, истраживање неутрона, мерење материјала и физичко мерење. Од 1901. до 1988. године агенција се звала Национални завод за стандарде.

[41] Cloud Controls Matrix (CCM) https://cloudsecurityalliance.org/blog/2020/10/16/what-is-the-cloud-controls-matrix-ccm/

8. **Домен управљања, управљања ризицима и усклађености** (ГРЦ) користи осам (8) контролних спецификација за подршку, дефинисање и усмеравање напора у погледу безбедности и усклађености организације (посебно корпоративног и ИТ управљања).
9. **Домен људских ресурса** (ХРС) кључан је за успех структуре усклађености организације. Људски ресурси су канал између ИТ безбедности и особља и обухвата интеракцију особља са системима, технологијом, средствима и подацима. Домен користи тринаест (13) контрола за подршку организацији у осигуравању усклађености особља са сигурносним политикама осмишљеним за заштиту организације, клијената и радне снаге.
10. **Домен управљање идентитетом и приступом** (ИАМ) садржи шеснаест (16) контролних спецификација и решава критичну потребу за обезбеђивањем одговарајућег приступа ресурсима у све хетерогенијим технолошким облачним окружењима.
11. **Домен интероперабилности и преносивости** (ИПИ) ЦЦМ -а има четири (4) контролне спецификације које се односе на интероперабилност и преносивост у облачном окружењу.
12. **Домен безбедност инфраструктуре и виртуелизације** (ИВС) домен води девет (9) контрола који промовишу примену и одржавање политика и процедура за ефикасно планирање, обезбеђивање и побољшање отпорности инфраструктуре и коришћење технологија виртуелизације.
13. **Домен евидентирање и надгледање је критичан процес безбедносних операција**. Тринаест (13) контрола у овом домену наглашавају управљање и процесе за оснаживање организација са пословањем заснованим на облаку са средствима за остваривање ефикасног евидентирања и праћења.
14. **Домен за управљање безбедносним инцидентима, е-откривање и форензику у облаку** (СЕФ) има осам (8) контролних спецификација осмишљених да осигурају да се утврђене политике и тестиране процедуре доносе како би се на одговарајући начин одговорило на безбедносне инциденте ради ублажавања пословних ризика (укључујући све захтеве за безбедност обавештења о кршењу).
15. **Домен транспарентност и одговорност за управљање ланцем снабдевања** (СТА) описује широк скуп контрола управљања ризиком у ланцу снабдевања, садржи четрнаест (14) контролних спецификација.
16. **Домен управљања претњама и рањивостима** (ТВМ) састоји се од десет (10) контролних спецификација које решавају широк спектар забринутости које би могле прерасти у текућа питања сигурносне архитектуре и инжењеринга инфраструктуре организације.
17. **Домен универзалног управљања крајњим тачкама** (УЕМ) усредсређен је на примену контрола ради ублажавања ризика повезаних са коришћењем рачунара док је изван пословне канцеларије, укључујући мобилне уређаје и уређаје крајњих тачака уопште. УЕМ домен подржава организације у ефикасној примени четрнаест (14) контролних спецификација, као што је одржавање пописа свих крајњих тачака, одобравање услуга и апликација прихватљивих за коришћење од крајњих тачака, спровођење безбедносних мера као што су екрани за аутоматско закључавање, заштитни зидови и откривање злонамерног софтвера, и коришћење технологија за спречавање, шифровање складишта и технологија за спречавање губитка података.

Канцеларија за ИТеУ поседује Нацрт акта којим се уређује питања у вези информационе безбедности али још није усвојен и објављен како би се сви запослени упознали са својим правима, обавезама и одговорностима које су обавезни да примењују. Виртуелне машине ЛПА постоје само на једној локацији, а на резервној локацији у Крагујевцу нема инсталације што по процени ризика и не мора, нпр. можете одлучити да буде хладна резерва.

У постојећој структури запослених нема довољно компетентних људи за обављање послова управљања информационом безбедношћу. Нису спроведене прописане обавезе из ЗИБ.

Због недефинисаних елемената пословног односа може доћи до немогућности утврђивања одговорности и настанка судског спора.

Последице могу бити: непостојање исправних тестираних резервних копија података; непостојање спроводљивог плана опоравка у случају хаварије; непостојање резервних делова и других резервних ресурса; не организовање обука из информационе безбедности; губитак

корпоративне способности и знања губитком људског капитала; губитак података; неовлашћен приступ или недозвољено изношење/цурење података; одавање личних података обвезника; стварање непотребно великих трошкова у случају настанка нежељених догађаја ванредних ситуација; прекид континуитета пословања у дужем временском периоду са значајним финансијским губицима.

Препорука: Препоручује се Канцеларији за ИТеУ донесе све потребне акте којима се уређују питања информационе безбедности, да обезбеде примену прописаних мера заштите и да у складу са проценом ризика обезбеде информационе ресурсе за успостављање резервне локације јединственог ЛПА система.

ЗАКЉУЧАК 2: Интегритет информација, података и докумената ИС ЛПА није обезбеђен у потпуности, јер у већем делу се заснива на подацима преузетим из екстерних система и регистара без означавања извора података, што за последицу може имати немогућност утврђивања аутентичности, непорецивости и комплетности података.

Наш циљ у овом делу извештаја, био је да одговоримо на друго ревизијско питање, односно да у којој мери се примењују опште и апликативне контроле улаза, обрачуна и излаза података у информационом систему локалне пореске администрације.

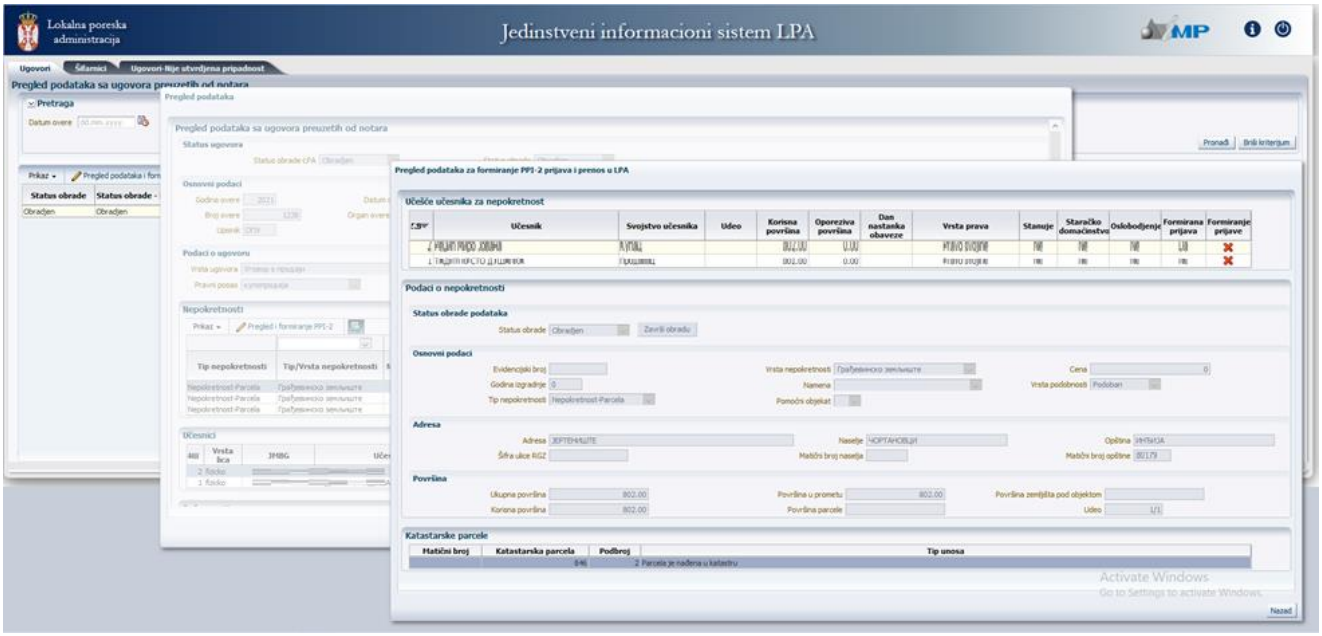
На основу постављеног питања, формулисали смо и следећа потпитања:

1. Да ли ЛПА апликација има адекватне контроле валидности улазних података?
2. Да ли ЛПА апликација обезбеђује интегритет и снимак извршене радње (унос, измена, увид, штампа и др.) над подацима и документима?
3. У којој мери ЛПА апликација обезбеђује израду прописаних извештаја пореских дужника?

Информациони системи су критични за многе пословне организације јер подржавају кључне процесе пословања. Са собом носе и значајне пословне ризике, погрешне одлуке због погрешне евиденције услед ненамерних или намерних грешака, губитак података, неовлашћено објављивање података, укључујући и повећане претње по сајбер безбедност услед све већег пословања преко интернета и на крају нерентабилног одржавања.

Прегледи апликативних контрола омогућавају руководству независну процену ефикасности и ефективности дизајна и деловања интерних контрола и процедура у информационом систему, а које се односе на аутоматизовање пословних процеса, идентификацију проблема који се односе на апликацију, а који заврђују додатну пажњу. [42]

Слика број 8. Преглед података за формирање ППИ-2 пријава и пренос у ЛПА у апликацији ЈИСЛПА



Апликативне контроле су уско повезане са појединачним трансакцијама, у овом случају обрачуна и наплате изворних прихода и њихово тестирање пружа ревизору уверавање о тачности одређених функционалности прецизније него тестирање општих контрола.

[42] Приручник за ИТ ревизију врховних ревизорских институција WGITA – IDI/INTOSAI, 2013.

Националним инвестиционим планом у периоду 2007-2009. године извршена је фискална децентрализација управљања јавним финансијама. Том приликом су дефинисани технички захтеви за реализацију информационог система ЛПА. Све до 2018. године од укупно 145 ЈЛС, информатичко решење Института „Михајло Пупин“ је поседовало њих 114, док је остатак од 31 користило софтверска решења других произвођача. У току 2019. године обављена је и миграција података са ИС ЛПА од других произвођача, чиме се комплетирао ЈИС ЛПА.

Тако су створени услови за примену Портала ЛПА као дела ЈИС ЛПА који је намењен пореским обвезницима за контролу свог пореског дуга у ЛПА на територији Србије и подношење електронских пореских пријава имовине правних лица, имовине физичких лица, комуналних, такси, ЕКО накнаде, и омогућена су електронска плаћања. Приступ Порталу је могућ пријавом помоћу квалификованог електронског сертификата[43] и двофакторском аутентикацијом[44] преко Портала за електронску идентификацију **https://eID.gov.rs**.

Подаци и информације које се евидентирају и обрађују у ИСЛПА се чувају у системима за управљање базама података (сервери базе података). Они омогућавају вишекорисnички рад значајног броја корисника, велики складишни простор за податке и обраду значајног броја трансакција. Питање интегритета тих података у суштини је питање поверења у такве евиденције, јер спровести контролу над свим подацима и процесима у том обиму је посебан изазов. Апликација омогућава администрацију свих изворних прихода који су поверени ЈЛС, на ограничен број пореских инспектора, праћење реализације и интерна контрола није могућа без праћења, броја трансакција, броја, обрачуна, броја измена свих врста.

ИСЛПА се заснива на Oracle RDBMS верзија 10g за коју је произвођач обуставио подршку и последње отклањање неусклађености је било јула 2013. године[45]. Унапређење система података на вишу новију верзију Oracle RDBMS базу података могуће је извести реинжењерингом целокупног система. За такав поступак је потребно дефинисати нове техничке захтеве.
Апликативни слој ИСЛПА јединствен за све ЈЛС развијан је равноправно са решењима других произвођача али квалитетом решења обухватио је 80% ЈЛС. Захваљујући квалитетном решењу, имплементацији, обуци и подршци корисницима бољој од конкуренције, 2018. године постаје једино решење у процесу консолидације фискалног система ЈЛС. На нивоу базе података реч је о дистрибуираном систему који решава питања униформног и стандардизованог извештавања. Портал ЛПА је део ЈИС ЛПА који је намењен пореским обвезницима за контролу свог пореског дуга у ЛПА на територији Србије и подношење пореских пријава ППИ1 и ППИ2. Приступ Порталу је могућ електронском сертификационом картицом и тада обвезник може да користи обе функционалности.

Налаз 2.1: Апликативне контроле дозвољавају преузимање ћириличних и латиничних података из екстерних система без означавања извора података, што ствара ризик од грешака у обради и за последицу може имати смањење ефикасности у раду.

Циљ контрола улазних података је провера да ли унос врше овлашћене особе, да ли врше унос из валидних извора података, да ли су подаци тачни и комплетни, а да када то нису апликација

[43] Пријава квалификованим електронским сертификатом представља највиши ниво поузданости и корисницима који се пријављују на овај начин доступне су све услуге. Корисници који се пријављују на овај начин могу самостално да генеришу ниже нивое поверења (основни и средњи ниво поузданости) као и да електронски потписују документа и захтеве.

44Пријава мобилним телефоном (двофакторска аутентикација) представља средњи ниво поузданости и корисницима који се пријављују на овај начин доступно је 98% услуга. Предност овог начина пријављивања јесте у томе што корисницима нису потребни квалификовани електронски сертификати, већ инсталирана апликација на њиховим паметним уређајима (мобилни телефон или таблет).

[45] https://support.oracle.com/knowledge/Oracle%20Database%20Products/742060_1.html

не изврши обраду таквих података, што се потврђује од стране интерне контроле валидацијом података.

Валидација је поступак утврђивања или проверавања ваљаности тј. утврђивања веродостојности[46], тачности[47] и комплетности[48] неког податка и/или документа из којег се подаци преузимају или преписују. Валидација може имати и за циљ испитивање законитости документа или податка. Циљ валидације је доказивање да неки податак нема само привидну ваљаност, нпр. податак постоји (унет је у евиденцију), него његова вредност припада очекиваном скупу вредности. Утврђивање да ли податак припада очекиваном скупу (законит, истинит и да ли се налази у дефинисаним границама, могућих вредности) изводи се на неколико различитих узорака, чиме се ствара могућност упоређивања резултата и извођења поузданих закључака о валидности унетог податка.[49]

Сви подаци који се уносе у информациони систем морају бити засновани на проверљивим изворним документима. Документи које корисник прилаже и даје на увид приликом уноса података су личне карте, уговор о купопродаји итд. Улазни подаци треба да се контролишу на могућност појаве грешке или омашке.

Корисници система ЈИСЛПА врше размену података са другим националним регистрима и евиденцијама, као и размену документације путем система еЗУП прибављајући податке, информације, документацију и друге чињенице у пореском поступку. Тако се пријаве од обвезника правних лица добијају путем електронске пријаве ППИ-1, а преузимањем података из уговора којег је евидентирао јавни бележник преузима из нотарског система из којег се формира ППИ-2 образац пријаве. Подаци о непокретности се преузимају из катастра Републичког геодетског завода, адреса обвезника из регистра којег води Министарство унутрашњих послова, као и други наведени извори у *налазу 3.1.* који служе за одређивање других околности за одобравање олакшица у складу са прописима.

Јавни бележник дужан је да пореску пријаву у року од 24 сата од тренутка извршења радње, односно правоснажну одлуку коју је донео у оквиру законом поверених јавних овлашћења у року од 24 сата од дана правоснажности, по службеној дужности, учини доступном, односно достави кроз електронски шалтер путем којег се достављају исправе и размењују подаци у поступку уписа у катастар непокретности и катастар водова републичком органу надлежном за послове катастра непокретности и катастра водова, односно преко е-шалтера и СМО надлежном пореском органу[50].

Приликом уноса података од стране јавног бележника први корак провере се односи на могућност уноса само непокретности које се налазе уписане у катастар непокретности. Законом прописан податак *година изградње непокретности* у апликацији није обавезан, што за последицу омогућава да се пријаве могу попунити без уноса године изградње непокретности што онемогућава утврђивање основице без накнадно ступања у контакт са обвезником. Тако је могуће формирати ППИ-2 образац који је некомплетан. Запослени који је ангажован на пословима преноса података у ЈИСЛПА врши проверу достављених података и да би коначну верификацију, обрачун пријаве и израду решења урадио запослени ангажован на обрачуну пријава.

Рачунарска апликација за ЛПА је у том погледу у складу са прописима и омогућава испуњавање свих захтева из Правилника, корисник врши преузимање података из уговора евидентираног

[46] **Веродостојност** подразумева да су трансакције истините и да се заснивају на оригиналним документима.
[47] **Тачност** подразумева да су трансакције исправне и у складу са изворним подацима који се евидентирају.
[48] **Комплетност, потпуност** – подразумева да ниједна исправна трансакција није изостављена из евиденција.
[49] ISSAI 5300 – Смернице за ИТ ревизију, INTOSAI 2016.
[50] Члан 33б. став 1. и 2. Закона о порезима на имовину,"Сл. гласник РС", бр. 26/01... 144/20.

апликацији који је у надлежости Министарства правде и Републичког геодетског завода. У *налазу 3.1.* су наведени извори података, корисничка искуства и задовољство ЛПА апликацијом.

Што се тиче пријема пореске пријаве за утврђивање пореза на имовину правних лица ППИ-1 које се подносе искључиво у електронском облику и по којима се врши самоопорезивање, постоји логичка и математичка контрола (валидација) при уносу података у пријави на самом порталу, а након пријема пријаве у ЈИС ЛПА запослени ангажован на обради ППИ-1 поново врши проверу података из пријаве, додељује јој одговарајући статус v врши њено књижење.

У апликацији еШалтер приликом евидентирања података о непокретности поље у бази за прихватање године изградње[51] предметне непокретности није означено као обавезно и могуће је попунити пријаву без њега.

Пријаве се могу попунити без уноса године изградње непокретности што онемогућава утврђивање основице без накнадно ступања у контакт са обвезником. Тако може настати грешка у утврђивању висине обавезе и умањење ефикасности рада ИСЛПА. Подаци у бази података се складиште у латиници и ћирилици чиме се може ометати поуздано претраживање података и створити ризик од дуплираних уноса.

Препорука: Препоручује се Институту „Михајло Пупин“ да обезбеди одговарајуће апликативне контроле на начин да се подаци који се преносе из других регистара означе (маркирају) ако нису комплетни како се не би наставила обрада без свих неопходних података.

Налаз 2.2: ЛПА апликација обезбеђује снимак последње извршене радње над подацима и нема историјат промена што ствара ризик немогућности накнадног утврђивања узрока и извршиоца ненамерне грешке као и других потенцијалних радњи злоупотребе.

Интегритет подразумева очуваност изворног садржаја и комплетност података[52], такви подаци, информације и процеси заштићени су од неовлашћеног или непредвиђеног мењања, односно да евентуалне такве промене не остају неопажене.

Код система за управљање базама података Oracle RDBMS постоје механизми да неовлашћени корисник не може вршити измене, као што постоји и механизам да ни овлашћени корисник не може вршити неовлашћене измене без документовања таквих активности. Интегритет ИСЛПА обухвата: оперативни систем, сервер за управљање базама података, табеле и колоне у базама и кориснички дефинисан интегритет.

Интегритет оперативног система у овој ревизији је испитиван у оквиру питања о адекватности управљања информационом безбедности ИСЛПА. Oracle RDBMS поседује команде за проверу и верификацију интегритета целокупног система и обезбеђен је софтверски алат за поправке оштећених датотека.

Интегритет података се у систему база података обично спроводи низом ограничења интегритета или правила. Три врсте ограничења интегритета су својствени део модела релационих података: интегритет ентитета, интегритет домена и референцијални интегритет. И посебну важност има кориснички дефинисани интегритет који се спроводи кроз апликативне контроле у самој апликацији.

- **Интегритет ентитета** односи се на концепт примарног кључа и огледа се у томе да свака табела мора имати примарни кључ и да колона примарног кључа треба бити јединствена, и не сме бити NULL дефиниције. На овај начин се спречавају дупликати на нивоу релационе базе података али не у потпуности без додатних механизама.

[51] Ибид.
[52] Закон о информационој безбедности ("Сл. гласник РС", бр. 6/2016, 94/2017 і 77/2019)

- **Интегритет домена** одређује да све колоне у релационој бази података морају бити декларисане по типу. Тако се спречавају погрешни уноси у којем није могуће унети текстуални опис у колони где су новчани износи или датум документа.
- **Референцијални интегритет** односи се на концепт страног кључа. Када су две или више табела повезане, морамо осигурати да вредност страног кључа у сваком тренутку одговара вредности примарног кључа. У противном када не постоји референцијално ограничење долази до појаве неповезаних редова тзв. Референтни интегритет ће спречити кориснике да: додају непокретности на рачун непостојећим корисницима и исто тако неће дозволити брисање корисника са списка ако постоје евидентиране његове обавезе у повезаној табели.
- **Кориснички дефинисани интегритет** односи се на скуп правила која је одредио дизајнер апликације, а која не спадају ју претходно наведеним врстама интегритета. Када се врши обрада рачуна по појединачним аналитичким ставкама укупни збирови по новчаним износима се евидентирају у повезаној табели заглавља рачуна. Кориснички дефинисан интегритет подразумева да било која исправка или измена износа појединачне ставке се аутоматски обрачунава и у повезаној табели заглавља рачуна. Ова врста интегритета се може постићи и програмирањем тригера над табелом или покретањем складиштене процедуре за обрачун. Интегритет података мора бити обухваћен целом обрадом трансакције узимајући у обзир и евидентирање заставица за контролу/верификацију евидентираних података.

Модел базе података је обухватио механизме који обезбеђују све наведене врсте интегритета, док се директно из сваког записа може очитати ко и када је креирао запис и индиректно из журнала базе података измене појединих ентитета записа. Колоне са датумима су правилно декларисане као и постојање релација између повезаних табела.

Недостаје механизам хеш заштите[53] који обезбеђује комплетност преузетих података од других регистара и евиденција. Механизам спречава да апликација обрађује некомплетне податке или податке који су мењани од стране администратора базе. Ко је извршио последње измене ових података могуће је очитати индиректно у журналу базе података.

Контрола пореско-правног процеса треба да обезбеди достизање циља процеса и избегавање негативних догађаја путем превенције, детекције и исправке. Код ЛПА са малим бројем запослених примењују се компензационе контроле.

У компензационе контроле спадају журнали активности корисника у систему (рад са датотекама, фолдерима и другим системским ресурсима), системски журнали приступања корисника (пријављивање, идентификација и ауторизација корисника), ревизорски траг или историјат промена у бази података, итд. Механизми аутоматског генерисања журнала активности представљају способност оперативног система, рачунарске апликације или система за управљање базом података да евидентира све промене или активности корисника у бази података, на информационом систему или рачунарској апликацији. Опште контроле информационог система треба да обезбеде да ови механизми буду укључени у оперативном систему и серверу базе података, а функционални захтеви у софтверској апликацији треба да обезбеде механизам аутоматског журнала у апликацији и да функционишу апликативне контроле.

Журнал рачунарске апликације евидентира активности корисника апликације, а журнали оперативног система и система базе података евидентирају активности администратора ових система, на тај начин документују се све обраде података које настају у процесу рада корисника.

Руководилац корисника јавних средстава (руководилац ОЈП) одговоран је за документовање свих пословних промена, врши обезбеђење ревизорског трага унутар корисника јавних средстава. Ревизорски траг је запис који обезбеђује хронолошко документовање и праћење

[53]Смернице за ревизију информационог система јавног дуга (GUID 5259 Public Debt Information Systems)

пословних промена у оквиру пословних процеса, активности или операција од почетка до краја, као и могућу реконструкцију тока.

Не постоји апликативна контрола која обезбеђује снимање свих врста обрада од стране корисника ЛПА апликације као што су: унос, измена, увид, штампа, прорачуни и друге обраде података.

Ревизорски траг је снимак који покрива целокупну документацију и приказује пословне промене у свим фазама и пружа могућност да се прате документовани докази од збирних до појединачних износа и обрнуто.

Сви могући исходи у процесу утврђивања обавезе доводе до процеса допуњавања и измене података, тако да је недостатак извора података и хронологија измене неопходна у процесу интерне контроле руководиоца ОЈП.

Недовољно унапређење постојеће апликације и усклађивање за обавезама из Закона о буџетском систему, Правилником о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему финансијског управљања и контроле у јавном сектору и Закону о информационој безбедности довела је до овог недостатка.

Неблаговремено откривање неовлашћене промене података која може довести до погрешног обрачуна и наплате, додатних трошкова рекламација због нетачности, и на крају немогућности утврђивања разлога настанка грешке и личне одговорности може створити негативне последице на резултате пословања.

Препорука: Препоручује се Институту „Михајло Пупин“ да обезбеди механизам за снимање ревизорског трага којим би се обезбедило хронолошко документовање и праћење промена података у оквиру пословних процеса, активности или операција од почетка до краја.

Налаз 2.3: Извештавање о пореском дугу обвезника заснива се на појединачној анализи сваке пореске картице обвезника без које није могуће утврдити старост дуга нити да ли је дуг у спору, или да ли има дубиозан карактер (сумњиво – неизвесног износа и могућности наплате) што онемогућава увид у структуру пореског дуга на нивоу ОЈПЈЛС, стварајући ризик прецењивања износа потраживања, погрешног пословног извештавања и угрожавање финансирања рада ЈЛС.

Излазне контроле пружају уверавање да ће подаци који се достављају обвезницима бити тачни, презентовани, форматирани и испоручени на доследан и сигуран начин.

Излазне контроле укључују:

- **Евидентирање и чување израђених решења, других докумената и рачуна на сигурном месту**;
- **Рачунарски генерисана документа и/или рачуни** – Сва документа овог типа треба архивирати и третирати као и физичка (папирна) документа;
- **Дистрибуција рачуна и других излазних докумената** - Излазни документи и рачуни дистрибуирају се преко масовне штампе и ЈП Поште Србије;
- **Билансирање и усаглашавање излаза** обавља се у процесу фискалне анализе;
- **Руковање излазним грешкама** – обавља се у поступку жалбе на решење;
- **Чување записа о грешкама у решењима и другим излазним документима** – хронолошка евиденција свих насталих грешака и отклањање истих;
- **Верификација пријема решења и других излазних докумената** – Уређен поступак који спроводи ЈП Пошта Србије.

У претходним ревизијама је утврђено да се одлучивање о третману пореског дуга (отпис, умањење, одлагање итд.) пореских обвезника вршило на основу података који нису

евидентирани у систему. Утврђено је да не постоје извештаји о спорним и дубиозним пореским обавезама (образац ЕСДПО), извештаји о застарелим обавезама (образац ЕЗПО), извештаји о отпису пореских обавеза (образац ЕОПО) и извештај о пореском дугу (образац ИПД) чиме је битно угрожен процес пословног извештавања, планирања прихода, као и процес доношења одлука.

На систему ЈИС ЛПА омогућено је издвајање дугова по рочности у циљу утврђивања износа обавеза за које је наступила релативна или апсолутна застарелост, као и спорних и дубиозних потраживања. Да би се пореска обавеза прогласила спорним или дубиозним потраживањем неопходан услов је да је обвезник брисан из регистра пореских обвезника и да је за његове обавезе наступила застарелост прописана законом.

Књижење спорних и дубиозних пореских обавеза врши се на основу решења о утврђивању износа спорних или дубиозних обавеза пореских обвезника, а по спроведеној процедури.

Процедура подразумева да се странка, правно или физичко лице обвезник локалних јавних прихода обрати захтевом за отпис дуговања по основу застарелости потраживања.

ОЈП утврђује чињенице од значаја за поступање у управној ствари, на основу доказа. Као доказ у пореском поступку могу се употребити пореска пријава, порески биланс, пословне књиге и евиденције, рачуноводствени искази, пословна документација и друге исправе и информације којима располаже пореска управа, прикупљене од пореског обвезника или трећих лица, исказ сведока, налаз вештака, увиђај и свако друго средство којим се чињенице могу утврдити. Чињенице и докази су већином већ евидентирани у ЈИСЛПА или се прибављају по службеној дужности преко СМО.

Проверава се оправданост захева и доноси решење којим одлучује о поднетом захтеву. Тек тада су створени услови да се обвезник стави на један од извештаја ЕСДПО, ЕЗПО или ЕОПО, већ према захтеву обвезника.

Обвезник локалних јавних прихода (између осталог и пореза на имовину) може својој ЛПА поднети и следеће захтеве:

- Захтев за отпис дуговања по основу застарелости потраживања;
- Захтев за отпис плаћања дугованог пореза;
- Захтев за отпис камате по основу неуредне доставе;
- Захтев за одлагање плаћања дугованог пореза на рате;
- Захтев за издавање пореског уверења;
- Захтев за повраћај више или погрешно наплаћеног пореза;
- Захтев за прекњижење више или погрешно наплаћеног пореза, итд.

Када се захтев реши отписом, створени су услови да се обвезник нађе на једном од захтеваних евиденција. Уважавајући све специфичности поступака за утврђивање спорних и дубиозних пореских обавеза, Правилник о пореском рачуноводству је дефинисао и поступак чувања у ванкњиговодственој (ванбилансној) евиденцији организационе јединице пореског органа у року прописаном чланом 134 који одредио време трајног чувања документације и апликације, док је за штампани облик на папиру за Дневник 10 година, за изворну, пратећу документацију и исправе платног промета 5 година, а за помоћне обрасце и радну документацију запослених 2 године.

Евиденција о спорним и дубиозним пореским обавезама саставља се са стањем на дан 31. децембра, уз порески завршни извештај, на Обрасцу ЕСДПО, који обухвата податке о броју ПИБ/ЈМБГ пореског обвезника, име и презиме (назив), број и датум решења, рачун и износ обавезе (дуг и камата).

У периоду пре формирања ЈИСЛПА софтверско решење Института „Михајло Пупин“ имплементирано је у 114 ЈЛС, док је формирањем извршена миграција података и за 31 ЈЛС.

Миграција података са других информационих система на ЈИСЛПА је обухватило само податке једне пословне године, а за израду извештаја о дуговањима за ове 31 ЈЛС неопходно је извршити миграцију и претходних година како би се обухватио најмање период од последњих 10 година.

Омогућено је доношење и књижење решења о преносу обавезе из књиговодствене у ванбилансне евиденцију и то у случајевима:

- брисања обвезника из прописаног регистра (АПР);
- застарелости права на наплату пореза;
- у поступку стечаја након куповине пореског обвезника;
- након окончања стечаја банкротством.

Пренос обавеза из књиговодствене у ванбилансну евиденцију спроводи се како за дугове тако и за преплату. Увид у ванбилансну евиденцију подржан је кроз систем ЈИС ЛПА.

Преглед евиденције о застарелим пореским обавезама омогућен је у форми прописаног извештаја ЕЗПО. У истој апликацији предвиђен је и преглед евиденције о спорним и дубиозним пореским обавезама у форми прописаног извештаја ЕСДПО.

Рачунарска апликација за ЛПА је у том погледу у складу са прописима и омогућава испуњавање свих захтева из Правилника док прекњижавање спорних и дубиозних обавеза директно зависи од рокова. С обзиром да се рокови прерачунавају од сваке нове радње[54] коју је предузела ОЈП или обвезник, а за које није прописана и не води се евиденција у ЈИС ЛПА, већ се доноси решење у посебном пореском поступку и евидентира у ЕСДПО.

У том смислу, унапређење рачунарске апликације код евидентирања спорних и дубиозних пореских обавеза може бити обезбеђивањем поља за означавање (штиклирање/маркирање) обвезника чији дуг се евидентира у ЕСДПО и на тај начин се омогућава да у складу са прописаном шемом књижи у ванбилансној евиденцији.

Препорука: Препоручује се Институту „Михајло Пупин“ да обезбеди могућност ручног и аутоматског означавања обвезника са спорним и дубиозним пореским обавезама и обезбеде обуку корисника у вези ове функционалности.

[54] Члан 114д ЗПППА.

ЗАКЉУЧАК 3: Поверљивост информација, података и докумената који се користе у ЛПА није обезбеђена у потпуности, јер подаци, документи и информације које се преузимају из других матичних евиденција и регистара се чувају без крипто-заштитних механизама.

Циљ у овом делу извештаја, био је да одговоримо на треће ревизијско питање, односно да ли је на адекватан начин обезбеђена поверљивост информација, података и докумената у информационом систему. Веома важан део ЈИСЛПА припада ЈЛС који за послове прикупљања изворних прихода употребљавају десктоп рачунаре у својим месним канцеларијама. Сваки рачунар повезан у локалну рачунарску мрежу, која је повезана попречном везом Л3ВПН на магистралу државних органа.

Да би донели закључак о адекватности начина обезбеђења поверљивости информационог система ЛПА и свега што он обухвата, испитивали смо:

1. Да ли је успостављено адекватно управљање подацима?
2. Да ли је успостављено адекватно управљање информационом безбедношћу?
3. У којој мери су додељена овлашћења корисницима ЛПА апликације у складу са описом радних места?

Реформа јавних финансија обухватила је и пореску децентрализацију са циљем обезбеђивања изворних прихода за сваки град и општину у Републици Србији. Институција је у својим извештајима констатовала многе недостатке у процесу евидентирања, обраде и извештавању о спорним и дубиозним потраживањима. У ревизији сврсисходности пословања „Ефикасност наплате изворних прихода ЈЛС“ установљено је да су многи проблеми изазвани неажурношћу евиденције у ИСЛПА. Проблеми у наплати изворних прихода ЈЛС могу бити последица неадекватног управљања информационим системом.

Јединице локалне самоуправе су преузеле део евиденције и један број запослених из Пореске управе, формирале организационе јединице да врше обрачун и наплату 14 изворних прихода, а најзначајнији од њих је порез на имовину. У систем се евидентирају порези на имовину правних и физичких лица, док се порез на поклон и пренос апсолутних права и даље води у Пореској управи. Формирањем јединственог информационог система ЛПА, обједињени су сви системи на једном месту, омогућен је увид у све обавезе једним упитом, дигитално подношење пријава за правна лица, као и друге могућности, а што може да доведе до повећаног ризика по интегритет, поверљивост и доступност информација у систему.

Налаз 3.1: ОЈП Београд, Крагујевац, Инђија, Ариље и Житорађа није у потпуности уредила поступак рада са документима, изворима и врстама података (лични подаци обвезника/грађана, подаци о некретнинама, финансијски подаци, тајни подаци итд.), стварајући ризик од настанка неправилне употребе података, информација и докумената, недозвољеног објављивања, или неке друге злоупотребе, што за последицу може створити непланиране судске трошкове.

ОЈП обављају послове утврђивања, контроле и наплате изворних јавних прихода буџета ЈЛС за које су надлежни у складу са прописима као и друге послове прописане Законом о пореском поступку и пореској администрацији.[55] Поред финансијских података насталих у пореском поступку утврђивањем износа пореза на основу одлука надлежних органа о ценама, неопходних података о непокретности из катастра, решења се доносе на лично име власника непокретности

[55] Члан 11, Закона о пореском поступку и пореској администрацији ("Сл. гласник РС", бр. 80/2002, 84/2002 - испр., 23/2003 - испр., 70/2003, 55/2004, 61/2005, 85/2005 - др. закон, 62/2006 - др. закон, 63/2006 - испр. др. закона, 61/2007, 20/2009, 72/2009 - др. закон, 53/2010, 101/2011, 2/2012 - испр., 93/2012, 47/2013, 108/2013, 68/2014, 105/2014, 91/2015 - аутентично тумачење, 112/2015, 15/2016, 108/2016, 30/2018, 95/2018, 86/2019 и 144/2020)

или на правно лице, чиме се морају спроводити и обавезе из Закона о заштити података о личности.

Како је и сам ЗПППА предвидео, сваки документ, информација, податак или друга чињеница о пореском обвезнику до којих су службена лица и сва друга лица која учествују у пореском поступку дошла у пореском, прекршајном, предистражном или судском поступку морају третирати као тајни подаци. Како је то уређено Законом о тајности података[56] и припадајућим уредбама[57], сам начин поступања[58], значи да службеник мора спроводити обавезе из више закона који уређују та питања.

ЗПППА[59] прописује да се у ЈИСЛПА воде подаци о пореском обвезнику, и то: назив, односно лично име, ПИБ, као и подаци из пореских пријава и других аката и регистара, који су од значаја за утврђивање изворних јавних прихода ЈЛС, подаци о утврђеним изворним јавним приходима, као и подаци о наплати тих јавних прихода.

Преузимање податке из изворних регистара[60] и то из: Регистра матичних књига, Регистра пребивалишта, Регистра привредних друштава, односно предузетника, Катастра непокретности и других регистара неопходних за његово вођење, у складу са законом којим се уређује електронска управа[61].

ОЈП размењује податке са:

1. Јавним бележницима - оверене исправе које достављају преко СМО[62];
2. Републички геодетски завод омогућио је и сервис за проверу улице у РГЗ регистру у оквиру ЈИС ЛПА, као приступ директно на свом порталу, а могу се вршити и појединачне провере преко портала еУправа - еЗУП;
3. Агенција за привредне регистре - по писаном захтеву Секретаријата, добијени подаци о оствареном приходу и разврставању правних лица и предузетника се учитавају у систем ЛПА;
4. Министарство унутрашњих послова - сервис за тренутно пребивалиште у оквиру ЈИС ЛПА као и појединачне провере кретања пребивалишта преко портала еУправа - еЗУП;
5. Министарство финансија – Управа за трезор, изводи о плаћању;
6. ЈП “ПТТ Србија" од кога се преузима адресни шифарник и подаци о датуму достављених масовно донетих решења и опомена;
7. Министарство финансија - Пореска управа - од које се преузима ПИБ регистар;
8. Министарство за државну управу и локалну самоуправу, подаци из МКУ у базу пореских обвезника, а преко портала еУправа - еЗУП врши се појединачни увид у изводе из МКУ;
9. РФ ПИО - појединачне провере о корисницима и висини пензија преко портала еУправа - еЗУП;
10. Локални судски органи;
11. Канцеларија за ИТеУ - подаци о достављању пореских решења за порез на имовину физичких лица у електронске сандучиће на порталу еУправа;

[56] Закон о тајности података, „Службени гласник РС“ број 104 од 16. децембра 2009.

[57] Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у органима јавне власти: 79/2014-3
Уредба о посебним мерама физичко-техничке заштите тајних података: 97/2011-5
Уредба о посебним мерама заштите тајних података у ИКТ системима: 53/2011-5
Уредба о начину и поступку означавања тајности података, односно докумената: 8/2011-4
Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима: 89/2010-3

[58] Руководиоци органа јавне власти у чијем раду настају тајни подаци, односно који чува или користи тајне податке, донеће акт, односно одлуку, којим се уређује чување и руковање тајним подацима, у року од годину дана од дана ступања на снагу ове уредбе, односно до 29. децембра 2012. године.

[59] Члан 159. став 3, (Сл. гласник РС, бр. 80/02...144/20)

[60] Ибид став 4. и 5.

[61] Закон о електронској управи, "Службени гласник РС", број 27 од 6. априла 2018.

[62] Сервисна магистрала органа уређена законом о Електронској управи.

12. Друге ЛПА;
13. Централни регистар обавезног социјалног осигурања - појединачне провере осигураних лица преко портала еУправа - еЗУП;
14. РФЗО као извор података за пореске олакшице;
15. НСЗ као извор података за пореске олакшице, итд.

Правом приступа ЈИСЛПА од стране других органа, у складу са наведеним одредбама Закона, располаже Канцеларија за ИТеУ у складу са Уредбом о начину вођења Метарегистра, начину одобравања, суспендовања и укидања приступа сервисној магистрали органа и начину рада на Порталу еУправа[63].

Зашто је важно успоставити адекватно управљање подацима?

Да би ОЈП остварила законом прописане циљеве потребно је да успостави и одржава ефикасно управљање подацима и документима током читавог животног циклуса од креирања до уручивања или испоруке, њиховог ажурирања и на крају архивирања.

Поред наведених прописа које уређују послове ОЈП неопходно је уредити рад са подацима, појединачним (личним) документима без обзира да ли су у физичкој или дигиталној форми, одредити из којих извора се преузимају који подаци и ко је за валидност података одговоран[64] или начин на који се врши провера и потврђивање исправности.

Финансијско управљање и контрола је систем политика, процедура и активности које успоставља, одржава и редовно ажурира руководилац организације, а којим се управљајући ризицима обезбеђује уверавање у разумној мери да ће се циљеви организације остварити на правилан, економичан, ефикасан и ефективан начин[65].

У том уређеном пословном процесу обухваћен финансијским управљањем и контролом неопходно је одредити и одговорности запослених који га спроводе као и начин вршења контроле исправности, како би омогућили боље координиран и ефикаснији приступ употребе података и докумената. Притом треба описати све поступке који треба да обезбеде чување приватности странака у поступку, спроводећи одредбе о заштити података о личности, на начин који спречава недозвољен приступ подацима и документима.

У свом раду поред ЈИСЛПА апликације и базе података које се налазе код обрађивача тј. у државном дата центру, порески службеници своје помоћне и друге датотеке чувају на рачунарима у ОЈП, где информациону безбедност треба да осигура ИТ служба градске или општинске управе. У супротном, повећава се ризик од судских спорова, или доношења лоших пословних одлука[66] које могу довести до погрешне примене законских одредби или пропуштених могућности.

Шта је у ревизији утврђено?

На упитник који је послат на адресе 167 јединица локалне самоуправе према списку Министарства надлежног за послове државне управе и локалне самоуправе пристигло је укупно 106 одговора.

[63] "Службени гласник РС", број 104 од 28. децембра 2018.

[64] Који орган управља регистром или у чијој је надлежности издавање документа који се користи у пореском поступку.

[65] Члан 81, Закон о буџетском систему, "Сл. гласник РС", бр. 54/2009, 73/2010, 101/2010, 101/2011, 93/2012, 62/2013, 63/2013 - испр., 108/2013, 142/2014, 68/2015 - др. закон, 103/2015, 99/2016, 113/2017, 95/2018, 31/2019, 72/2019 и 149/2020.

[66] Мишљење министарства финансија, бр. 07-00-372/2019-04 од 11.12.2019.године, Непостојање права на отпис камате обрачунате за дуговани порез.

Обученост и компетентност запослених

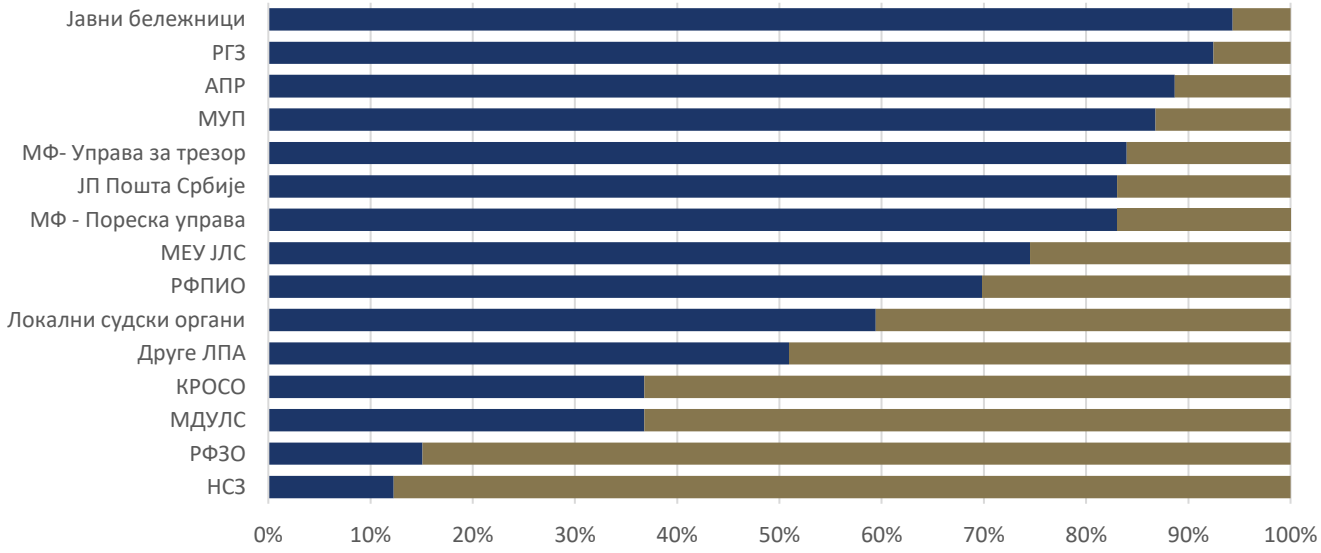
На питање када сте последњи пут имали обуку за рад у ЛПА апликацији, 2 ЛПА је одговорило са био сам на обуци у претходних годину дана, односно 2% од укупног броја, 50 ЛПА је одговорило са био сам на обуци у претходних пет и више година, односно 48% од укупног броја, 25 ЛПА је одговорило са све сам научио од колега и колегиница, односно 24% од укупног броја, 23 ЛПА је одговорило са остало, односно 22% од укупног броја и преосталих 5 ЛПА је одговорило да су самоуки, односно 5% од укупног броја. Међу ЛПА које су одговориле са остало превладава одговор да је део запослених био на обуци пре пет и више година, а део запослених учи од колега/колегиница. Постоји велика потреба за организовањем обука за рад у ЛПА апликацији.

Слика број 9. Обучавање запослених за рад у ЛПА апликацији

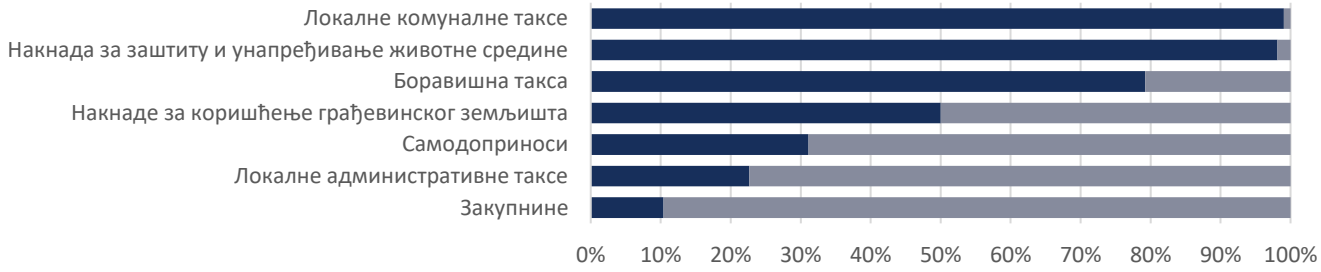
Размена података и Национални регистри

У току спровођења ревизије, прикупили смо податке од ЈЛС који се односе на размену података са другим државним органима и националним регистрима. На упитник који је послат на адресе 167 ЈЛС према списку Министарства надлежног за послове државне управе и локалне самоуправе пристигло је укупно 106 одговора. Имајмо у виду да правна лица самостално достављају попуњене обрасце преко портала, док физичка лица немају ту годишњу обавезу која постоји само приликом промета непокретности, онда није изненађујуће да запослени у ОЈП јавне бележнике препознају као своје најважније партнере. Иако се ти подаци преузимају из система еШалтер који је у Републичком геодетском заводу (РГЗ) постоји 5% ОЈП које не преузимају податке из апликације еШалтер. Сам увид у податке је обезбеђен у ЛПА апликацији као и неспорна корисност података за израду пријаве пореза за имовину ППИ-2 доводи нас до закључка да поједине ОЈП у свом раду не користе све постојеће функционалности ЛПА апликације. Ако прихватимо да корисници ЛПА апликације до података долазе преко апликације еШалтер и даље постоји 3% ОЈП који немају адекватна сазнања о овим функционалностима.

Слика број 10. Преглед броја ЈЛС које преузимају податке из других регистара и органа јавне управе



Слика број 11. Преглед употребе ЛПА апликације за обрачун и наплату других изворних прихода



ЗППА прописује да се у ЈИСЛПА воде подаци о пореском обвезнику, и то: назив, односно лично име, ПИБ, као и подаци из пореских пријава и других аката и регистара, који су од значаја за утврђивање изворних јавних прихода ЈЛС, подаци о утврђеним изворним јавним приходима, као и подаци о наплати тих јавних прихода.

Преузимају се подаци из изворних регистара као што је: Регистра матичних књига, Регистра пребивалишта, Регистра привредних друштава, односно предузетника, Катастра непокретности и других регистара неопходних за његово вођење, све у складу са законом којим се уређује електронска управа.

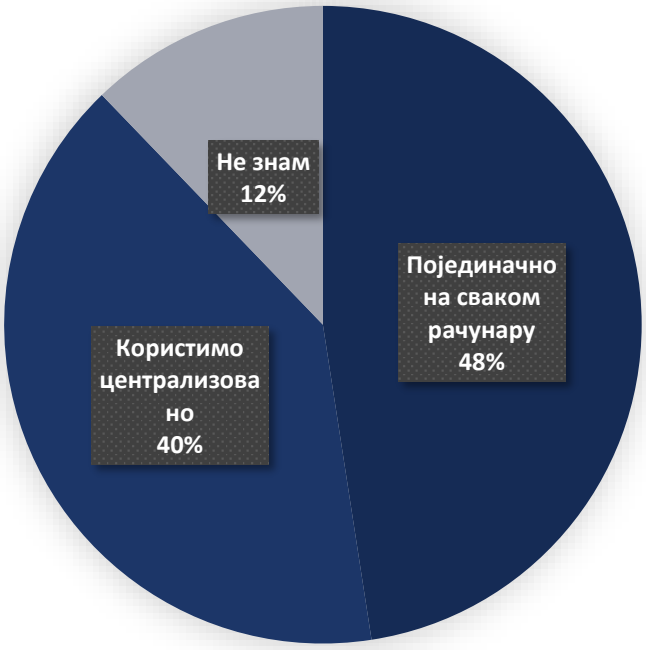
Ток утврђивања и извори података нису уређени интерним актима и препуштено је тумачењу пореског службеника, чиме се отежава контрола у поступању. Тако је утврђено да се непотпуне пријаве јавних бележника без прописаних података о години изградње непокретности обрађују у пореском поступку. Недостатак података о преузимању пореског дуга у процесу наслеђивања онемогућава ефикасно утврђивање износа и изискује накнадно прибављање тих података.

У члану 7 одређено је да се сви подаци, информације и документи или друга чињеница о пореском обвезнику до којих дођу службена лица сматрају тајним податком и притом су издвојени подаци о техничким проналасцима и патентима јер се у том случају штете по економском интересу Републике Србије не могу проценити.

Такође је речено да повреда тајности угрожава интерес Републике Србије и самог обвезника, чиме се подразумева да је таквим подацима и документима могуће одредити степен тајности „ПОВЕРЉИВО“ или „ИНТЕРНО“.
Када је реч о физичком приступу рачунарима у ОЈП, они су обезбеђени физичко-техничком заштитом у периоду ван радног времена, али када је реч о радном времену када обвезници и

други грађани се могу кретати радним простором неопходна је заштита и корисничких рачунара од неовлашћеног приступа.
Кориснички рачунари који се користе за приступ ЛПА апликацији у 92% ЈЛС имају контролу корисничког имена и лозинке, док 8% нема што ствара ризик приступања подацима, информацијама и документима који су снимљени на тим рачунарима без контролисаног логичког приступа.

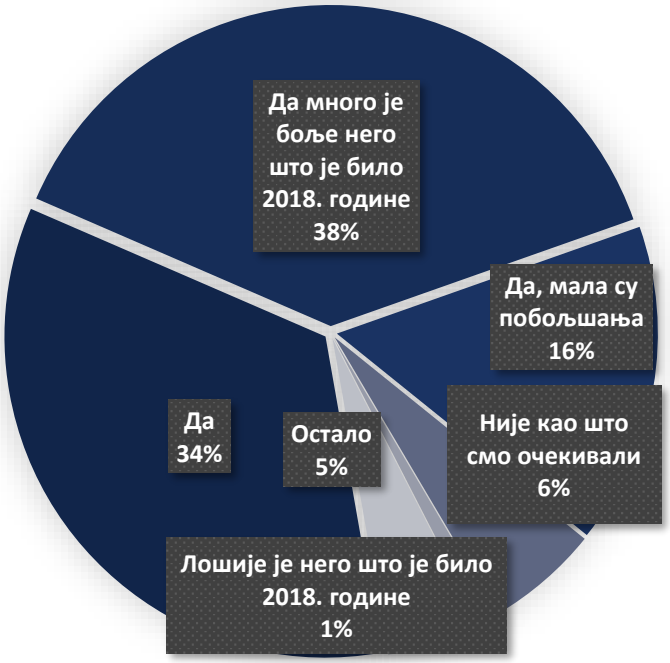
Слика број 12. Преглед управљања лозинкама



Када је реч о централизованом управљању и контроли промене лозинке 40% ЈЛС има централизовано управљање, што представља професионално особље које брине о информационој безбедности без обзира да ли је непосредно запослено у ОЈП, на нивоу ЈЛС, или предузеће ангажовано за те послове, како је и законом предвиђена могућност.

Поред ове врсте контроле приступа неопходно је успоставити и друге мере заштите како је предвиђено ЗИБ.

Слика број 13. Корисничко задовољство ЛПА апликацијом



Упитником су прикупљени одговори о задовољству корисника ЛПА апликације након обављене миграције у Државни дата центар и 38% ОЈП је изразило мишљење да је сада много боље него што је било пре 2018. године и 16% је приметио мања побољшања, што са 34% задовољних чини 88% задовољних корисника.

С обзиром да се у пореском поступку употребљава значајан број различитих извора података, информација и докумената, неопходно је донети интерни акт којим би се уредио избор

докумената и начин обраде што је уједно и законска обавеза евидентирања у Регистар административних поступака[67]. У свом раду спроводе административне поступке као што су:

1. Поступак утврђивања и контроле пореза на имовину физичких лица;
2. Поступак утврђивања локалне комуналне таксе;
3. Поступак утврђивања боравишне таксе за физичка лица која поседују решење о категоризацији и пружају услуге смештаја у објектима домаће радиности (кућа, апартман, соба) и сеоском туристичком домаћинству;
4. Поступак утврђивања самодоприноса;
5. Поступак одлагања плаћања дугованог пореза;
6. Поступак редовне наплате изворних јавних прихода;
7. Поступак принудне наплате изворних јавних прихода, итд.

Како је Закон којим се успоставља Регистар административних поступака као јавно доступна електронска база свих административних поступака ступио на снагу 7.5.2021. године за привреду, док ће за грађане бити доступан априла 2022. године, неопходно је да се сви поступци, документација и подаци[68] уреде интерним актима и евидентирају у Регистар. Свакако да рад са класификованим документима треба уредити у складу са предвиђеним мерама како је то дефинисано у Уредби о посебним мерама заштите тајних података у информационо-телекомуникационим системима.

Неопходно је успоставити и применити процедуре које уређују безбедност свих података, неовлашћени приступ и смањити ризике од недозвољеног објављивања личних података корисника и обвезника, што на крају за последицу може имати нарушавање поверљивости података. Резервне копије података и докумената са корисничких рачунара треба третирати посебним мерама заштите закључавања копија заштитним лозинкама.

ОЈП Београд

Обавља послове који се односе на: утврђивање, контролу и наплату изворних јавних прихода буџета Града и буџета градских општина за које је надлежан у складу са прописима. Употребљавајући ЛПА апликацију када врше измене и допуне функционалности, или је користе приликом обучавања запослених, користе се испоруке. Испоруке су инструкције, тј. кратка упутства од стране добављача апликације, чија обавештења стижу преко уграђене странице у самој апликацији.

Израђеном мапом пословних процеса уређени су процеси рада, али није уређен начин рада са изворним документима, који извори и која документа преко ког електронског система од ког надлежног органа се прибављају чињенице у пореском поступку и у ком периоду ажурирају. Време прибављања података и контрола исправности могу довести до грешака приликом израде решења и појаве накнадних рекламација обвезника, чиме се смањује укупна ефикасност ОЈП и ЈИСЛПА. Поред тога сва документа, податке и друге чињенице треба класификовати, одредити мере заштите у складу са прописима и дефинисати у Акту о информационој безбедности, припреме и доставе поступке у форми потребној за Регистар административних поступака.

Препорука: Препоручује се ОЈП Београд да уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање.

ОЈП Крагујевац

Обавља послове за које је надлежан у складу са прописима. Израђује сопствена упутства за рад запослених. Употребљавајући ЛПА апликацију када врше измене и допуне функционалности, или је користе приликом обучавања запослених, користе се испоруке. Испоруке су инструкције,

[67] Закон о регистру административних поступака ("Сл. гласник РС", бр. 44/2021)
[68] Ибид, члан 7 – подаци који се уписују у Регистар.

тј. кратка упутства од стране добављача апликације, чија обавештења стижу преко уграђене странице у самој апликацији.

Иако не поседује обједињено у једном документу рад са свим упутствима и другим инструкцијама, подаци се чувају на одвојеном месту заштићени од неовлашћеног приступа. Сва документа, податке и друге чињенице треба класификовати и у складу са тим одредити мере заштите, а поступке уредити и доставити у форми потребној за Регистар административних поступака.

Препорука: Препоручује се ОЈП Крагујевац да уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање.

ОЈП Инђија

Обавља послове за које је надлежан у складу са прописима. Израђује сопствена упутства за рад запослених. Употребу ЛПА апликације у ревидираном периоду, код измена или допуна функционалности, и/или приликом обучавања запослених користи испоруке од стране добављача апликације која су у облику инструкција, кратка упутства за обављање активности у пореско правним поступцима. Подаци се чувају на одвојеном месту заштићени од неовлашћеног приступа.

ОЈП Ариље

Обавља послове за које је надлежан у складу са прописима. Употребу ЛПА апликације у ревидираном периоду, код измена или допуна функционалности, и/или приликом обучавања запослених користи испоруке од стране добављача апликације која су у облику инструкција, кратка упутства за обављање активности у пореско правним поступцима. Сва документа, податке и друге чињенице треба класификовати и у складу са тим одредити мере заштите, а поступке уредити и дефинисати интерним актима, доставити у форми потребној за Регистар административних поступака.

Препорука: Препоручује се ОЈП Ариље да уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање.

ОЈП Житорађа

Обавља послове за које је надлежан у складу са прописима. Употребљавајући ЛПА апликацију када врше измене и допуне функционалности, или је користе приликом обучавања запослених, користе се испоруке. Испоруке су инструкције, тј. кратка упутства од стране добављача апликације, чија обавештења стижу преко уграђене странице у самој апликацији. Сва документа, податке и друге чињенице треба класификовати и у складу са тим одредити мере заштите, а поступке уредити и доставити у форми потребној за Регистар административних поступака.

Препорука: Препоручује се ОЈП Житорађа да уреди поступак рада и начин чувања података и докумената са корисничких рачунара, који се користе у пореском поступку, како би се онемогућила неовлашћена употреба и неовлашћено објављивање.

Налаз 3.2: ОЈП Београд и Ариље нису усвојили и ОЈП Крагујевац и Житорађа нису у потпуности успоставили адекватно управљање информационом безбедношћу ЛПА, јер нису уредили и применили процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система што за последицу има већи степен рањивости система и података о личности који се налазе у систему.

Циљ је био да испитамо да ли је донет и да ли се примењује Акт о информационој безбедности којим се уређују и питања заштите ИС ЛПА. Како је предвиђено Законом[69], сваки оператор ИКТ система од посебног значаја у обавези је да донесе Акт о информационој безбедности.

Актом се одређују мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја, и редовно мора да се ажурира како би био усклађен са променама у окружењу и самом ИКТ систему.

Ако не располаже са довољно компетентних лица запослених на ИТ пословима, дужан је да ангажује спољне експерте који ће вршити проверу усклађености примењених мера заштите и најмање једном годишње мора да сачини извештај.

Организација ИТ безбедности обухвата више послова које треба уредити, у смислу успостављања управљачке и организационе структуре, обученог и стручног ИТ кадра, процене ИТ ризика, обезбеђивања континуитета пословања у случају ванредних ситуација и у склопу тога управљања резервним копијама података, усвајања и имплементације правила и процедура за све ИТ послове, уређивање обавеза пружаоца услуга у складу са законом и подзаконским актима, контроле логичког и физичког приступа систему, управљања улазним и излазним подацима итд, укупно 28 мера заштите.

Анализирали смо да ли су усвојена одговарајућа документа која се односе на информациону безбедност, што је обавеза оператора ИКТ система од посебног значаја (значи градске и општинске управе), да ли су имплементирана и да ли је успостављена организациона ИТ структура са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу, а чији запослени су оспособљени за посао који раде и разумеју своју одговорност. Без успостављања адекватне организације ИТ безбедности није могуће управљати подацима на начин прописан законима.

Да би одабрали адекватне мере заштите неопходно је идентификовати сва информациона добра[70] и одредити одговорност за њихову заштиту; што значи обухватити опрему, оперативне системе, софтвер и запослене у ОЈП који раде на тим пословима и приступају ЈИСЛПА.

Адекватност одабраних мера зависи пре свега од тога колико планирани циљеви организације зависе од доступности ИКТ система, тј. његове доступности корисницима и другим заинтересованим странама (обвезницима, запосленима у ОЈП, руководству, министарствима који надгледају и контролишу рад, итд).

Доступност ИКТ система је однос времена рада и застоја, тако да финансијска вредност уложена у одабрану меру заштите треба да буде адекватна губитку који настаје за време застоја.

[69] Члан 6а, Закон о информационој безбедности "Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019.

[70] Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично, по Закону о информационој безбедности.

Табела 2. Прорачун времена трајања застоја на основу доступности ИКТ система

Доступност %	Застоји годишње	Застоји по кварталу	Застоји месечно	Застоји недељно	Застој у току 24 сата
90% („једна деветка“)	**36,53 дана**	**9,13 дана**	**73,05 сати**	**16.80 сати**	**2.40 сати**
95% („једна и по деветка“)	18,26 дана	4,56 дана	36,53 сати	8.40 сати	1.20 сати
97%	10,96 дана	2,74 дана	21,92 сати	5,04 сати	43,20 min
98%	7,31 дана	43,86 сати	14.61 сати	3.36 сати	28.80 min
99% („две деветке“)	**3,65 дана**	**21,9 сати**	**7.31 сати**	**1,68 сати**	**14.40 min**
99,5% ("две и по деветке")	1,83 дана	10.98 сати	3,65 сати	50,40 min	7.20 min
99,8%	17.53 сати	4,38 сати	87,66 min	20,16 min	2,88 min
99,9% („три деветке“)	**8,77 сати**	**2,19 сати**	**43,83 min**	**10.08 min**	**1,44 min**
99,95% ("три и по деветке")	4,38 сати	65,7 min	21,92 min	5,04 min	43,20 s
99,99% ("четири деветке")	**52.60 min**	**13.15 min**	**4,38 min**	**1,01 min**	**8,64 s**
99.995% ("четири и по деветке")	26.30 min	6,57 min	2,19 min	30.24 s	4,32 s
99.999% ("пет деветки")	**5,26 min**	**1.31 min**	**26,30 s**	**6,05 s**	**864,00** ms
99.9999% ("шест деветки")	**31,56 s**	**7.89 s**	**2,63 s**	**604,80 ms**	**86.40 ms**
99.99999% ("седам деветки")	**3,16 s**	**0,79 s**	**262,98 ms**	**60,48 ms**	**8,64 ms**
99.999999% ("осам деветки")	**315,58 ms**	**78,89 ms**	**26,30 ms**	**6,05 ms**	**864,00 µs**
99.9999999% ("девет деветки")	**31,56 ms**	**7,89 ms**	**2,63 ms**	**604,80 µs**	**86.40 µs**

Одабрана мера заштите је повезана са ризичним догађајем који може настати, као и са тим повезане негативне финансијске последице по пословање. Зато је неопходно да надлежни орган (градска, општинска управа, министарство финансија) донесе стратегију управљања ризиком и успостави Регистар ризика. Регистар ризика мора обухватити и ИТ ризике, обзиром да се пословање ОЈП не може ни замислити без ИС ЛПА.

Ризик представља вероватноћу да ће се десити одређени догађај који би могао имати негативан утицај на остваривање циљева корисника јавних средстава. Ризик се мери кроз његове последице и вероватноћу дешавања. Руководилац ЈЛС сноси одговорност за управљање ризицима. [71]

Проценом утицаја ризика на пословање утврђују су активности у пословању које су критичне по остварење циљева, од којих ресурса зависи постизање резултата, тако ће се обавити и избор примењених мера, које треба да обезбеде отпорност према ризику и јачање континуитета пословања.

Ако се комуникација између запослених, додела радних задатака, извештавање итд. обавља употребом електронске поште, онда је веома важно да сервер електронске поште (Mail server) функционише без прекида. Ако се процени да је рад сервера електронске поште пресудан за функционисање, неопходно је документовати:

- Попис свих пословних активности и ресурса како би се утврдило шта треба заштитити и/или опоравити након појаве поремећаја у пословању;
- Одредити приоритете процесима и услугама, који морају бити заштићени од последица поремећаја у пословању;
- Одредити времена опоравка (РТО) и тачку опоравка (РПО), колико брзо се мора наставити пословање након поремећаја и колику штету (нпр. губитак података итд.) можемо дозволити;
- Утврдити мере које треба применити за умањење ризика и последица поремећаја пословања у складу са претходним захтевима.

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у члану 29. уређује мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

[71] Правилник о о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему финансијског управљања и контроле у јавном сектору, "Сл. гласник РС", бр. 89/2019.

- Оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура.
- Оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације.
- Оператор ИКТ система треба да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.
- Оператор ИКТ система треба да идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система.

Дакле, поред обавезе да успостави континуитет пословања у случајевима ванредних ситуација, оператор ИКТ система има обавезу и да све те процесе и верификује, тј. тестира..

Кључни елементи континуитета пословања су: план и политика континуитета пословања, организација функције континуитета пословања, процена утицаја на пословање, управљање ризицима, превентивне контроле, план опоравка у случају хаварије, документација за план континуитета пословања, план тренинга и тестирања, информациона безбедност и резервне копије и план опоравка када су послови додељени добављачу услуга[72] тј. Канцеларији за ИТеУ.

План опоравка од хаварије[73] услед техничког квара ИС ЛПА подразумева процес планирања и тестирања опоравка информационог система (хардвера и софтвера) након што се деси хаварија[74].

План опоравка од хаварије треба да садржи:

- процедуре за опоравак информационог система кад наступе нежељени догађаји;
- приоритете опоравка ресурса информационог система;
- податке о тимовима и члановима тимова који ће бити одговорни за опоравак информационог система, њихове дужности и одговорности;
- резервни рачунски центар са свим компонентама за опоравак информационог система.

План опоравка од хаварије омогућава ОЈП да настави да функционише након што се деси хаварија. Обзиром да је ЈИСЛПА у надлежности Канцеларије ИТеУ ове послове треба уредити и Споразумом о нивоу пружене услуге, где ће се јасно одредити, опрема, софтвер, активности и раздвојити одговорност ОЈП и Канцеларије за ИТеУ.

План опоравка од хаварије ЈЛС треба да одреди приоритете тако да се обухвате рачунари запослених обзиром на значај наплате изворних прихода за пословање ЈЛС и времена враћања ОЈП у функционално стање.

ЈЛС је руковалац личних података грађана тако да Споразумом са Канцеларијом за ИТеУ мора уредити и управљање резервним копијама података.

Управљање резервним копијама података треба да обухвати поступке израде, чувања и тестирања ових копија, као и опоравка података и софтверских компонената, како би се омогућило поновно успостављање пословних процеса у оквиру циљног времена опоравка.

72 WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.
73 Енгл. Disaster Recovery Planning-DRP.
74 Хаварија је поремећај у техничко-технолошком систему који доводи до потпуног отказа у дужем временском периоду.

Неопходно је дефинисати ко треба да обезбеди да су резервне копије података ажурне и адекватно заштићене, а поступци опоравка тестирани и успешни.

Да би се уредила сва ова питања која претходе доношењу Акта о информационој безбедности ЈЛС треба да претходно уреди следеће: Стратегију/План развоја за период од 3-5 година, Стратегију управљања ризицима, Регистар ризика који обухвата ИТ ризике, потом донети План континуитета пословања, План мера и активности у ванредној ситуацији[75], План опоравка од хаварије, План израде резервних копија, полисе, процедуре, одлуке, као и друга општа акта којима се уређују питања примене информационих технологија.

Законом о информационој безбедности[76] се одређују мере заштите од безбедносних ризика у ИКТ системима и одговорностима правних лица приликом управљања и коришћење ИКТ система. Под редним бројем 28 се одређује мера која обезбеђује континуитет обављања посла у ванредним околностима. У уредби о ближем уређењу мера заштите информационо-комуникационих система[77] од посебног значаја се одређује да ЈКП треба да:

- предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура;
- успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације;
- верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације;
- идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система.

Законом о смањењу ризика од катастрофа и управљању ванредним ситуацијама[78] су утврђене бројне обавезе органа локалне самоуправе, са циљем да се, уз њихов незаменљив допринос и кроз сарадњу са другим субјектима, смањи ризик од катастрофа и делотворније управља ванредним ситуацијама у Републици Србији.

Омогућено је да привредни субјекти који су овлашћени да се баве израдом Процене угрожености од катастрофа и Плана заштите и спасавања, могу бити ангажовани на изради планова, и дефинисати задатке које и како треба да обезбеде континуитет пословања у ванредним ситуацијама.

Орган локалне самоуправе треба да се побрине да организује свој рад и да као оснивач ЈКП одреди степен безбедности и отпорности свих ЈКП, према ризицима који прете услед природних или техничко - технолошких несрећа.

Шта је у ревизији утврђено?

Да би утврдили репрезентативност изабраних ЈЛС послат је упитник на адресе 167 ЈЛС према списку Министарства надлежног за послове државне управе и локалне самоуправе, од којих је пристигло је укупно 106 одговора.

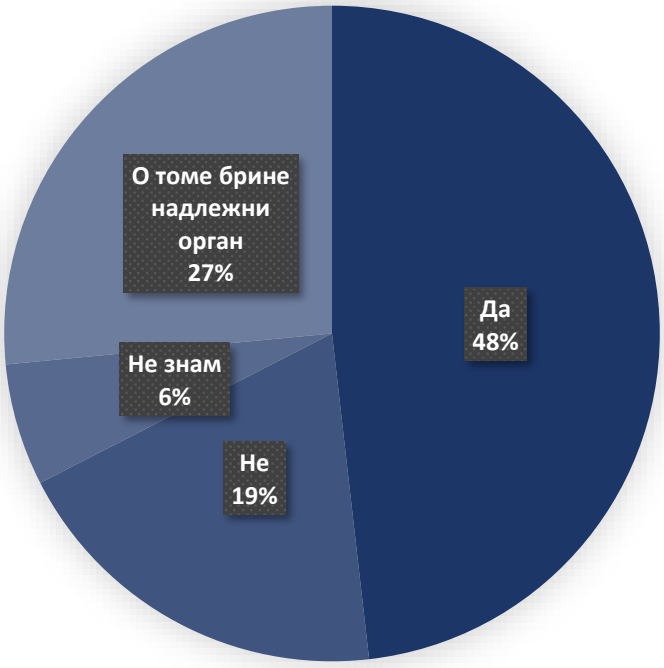
[75] Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, члан 13, "Сл. гласник РС", бр. 87/2018.
[76] Члан 7 Закона о информационој безбедности.
[77] "Сл. Гласник РС", бр. 94/2016.
[78] "Сл. гласник РС", бр. 87/2018.

Акт о информационој безбедности

У току спровођења ревизије, прикупили смо податке од ЈЛС који се односе на активност доношења Акта о информационој безбедности и имплементације мера информационе безбедности. Доношење Акта је законска обавеза оператера ИКТ система, значи и ЈЛС. Закон о информационој безбедности ступио на снагу 5. фебруара 2016. године, док су уредбе које ближе уређују примену закона донете 17. новембра 2016. године. У року од 90 дана требало је донети Акт о безбедности ИКТ система што значи да је последњи рок за то је био 17. фебруар 2017. године.

Надлежно Министарство, РАТЕЛ, СКГО је сачинило модел акта који је јавно доступан, али више од половине није донело акт нити је искористило законску могућност да ангажује спољне стручњаке за тај посао. Код 27% ЈЛС постоји свест о значају овог питања, али да ништа не предузимају очекујући да о њиховим обавезама брине неко други.

Слика број 14. Да ли је усвојен Акт о информационој безбедности?



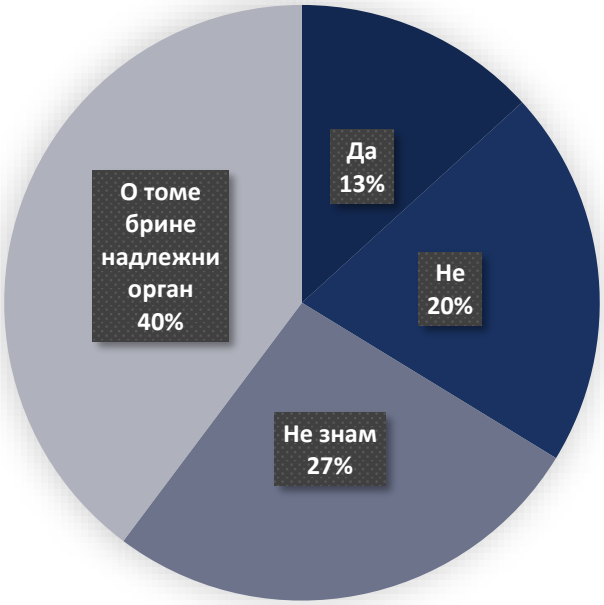
План континуитета пословања у ванредним ситуацијама

У току спровођења ревизије, прикупили смо податке од ЈЛС који се односе на План континуитета пословања у ванредним ситуацијама. Утврђено је да План континуитета пословања у ванредним ситуацијама поседује 13% ЈЛС, док код 40% ЈЛС постоји свест о значају овог питања, али план није донет, очекујући да о томе се побрине неко други. У претходним годинама догађаји који су произвели ванредне ситуације, људске жртве и материјалне штете у многим ЈЛС, проузроковане природним катастрофама, поплаве, земљотреси, пандемија корона вируса итд. изгледа да нису довољни разлог да се овом послу приступи озбиљније.

Планирање континуитета пословања у ванредним ситуацијама је део Плана континуитета пословања у којем се конкретно дефинишу активности и одговорна лица за одређени ризик. Како је 2020. године проглашено ванредно стање пандемије корона вируса, 81% ЈЛС су због недостатка плана за ванредно стање дочекале неопремљене преносним рачунарима и практично обуставиле свој рад.

Сви планови могу бити обједињени у један документ као План пословног континуитета или да сваки буде појединачни документ, што највише зависи од величине ЈЛС и процене ризика.

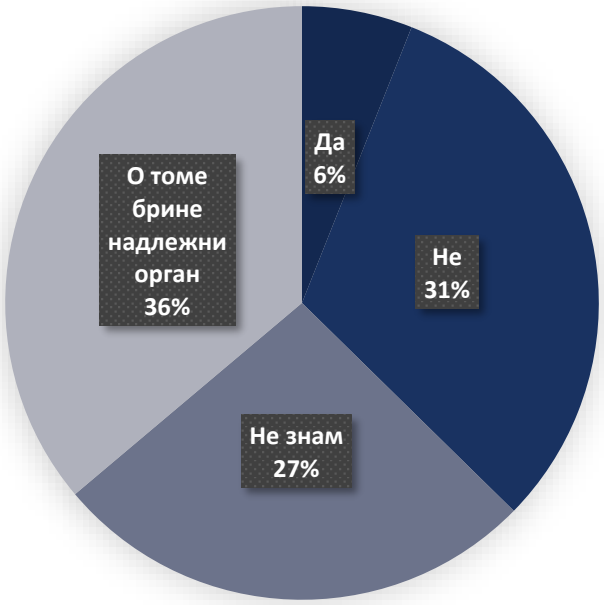
Слика број 15. Да ли је донет План континуитета пословања у ванредним ситуацијама?



План опоравка од хаварије

Анализом достављених одговора утврђено је да План опоравка од хаварије такође поседује 6% ЈЛС, док код 36% ЈЛС постоји свест о значају овог питања, али план није донет, очекујући да о томе се побрине надлежни орган. На основу Стратегије управљања ризиком и оцењеном приоритету рада информационе инфраструктуре неопходно је одредити, приоритет и редослед опоравка информационих система које користи ЈЛС.

Слика број 16. Да ли је донет План опоравка од хаварије?



Слика број 17.

План израде резервних копија

Када је реч о Плану израде резервних копија ситуација је нешто боља, поседује га 17% ЈЛС, док код 43% ЈЛС постоји свест о значају овог питања, али план није донет, очекујући да се о томе побрине надлежни орган.

Слика број 18. Да ли је донет План опоравка од хаварије?

Израда резервних копија података

Иако не постоје планови, постоји свест о значају резервних копија података, и у 45% се она обавља аутоматизовано на системима за резервне копије, корисници раде повремено на УСБ меморију или диску у 17% ЈЛС (иако су питања безбедности тог садржаја под знаком питања), али и даље постоји 7% ЈЛС који не воде бригу о том веома значајном питању.

Слика број 19. Да ли редовно израђујете резервне копије података са ЛПА рачунара?

Непостојање исправних тестираних резервних копија података, непостојање спроводљивог плана опоравка у случају хаварије, непостојање резервних делова и других резервних ресурса, не организовање обука из информационе безбедности, губитак корпоративне способности и знања губитком људског капитала, губитак података, неовлашћен приступ или недозвољено изношење/цурење података, одавање личних података обвезника, стварање непотребно великих

трошкова у случају настанка нежељених догађаја ванредних ситуација, прекид континуитета пословања у дужем временском периоду са значајним финансијским губицима.

ОЈП Београд

Када је у питању Стратегија управљања ризицима Града Београда, донета је још 2015. године којом је у начелу дефинисане обавезе руководилаца и запослених у органима и дефинисан је Образац Регистра ризика. Секретаријат за јавне приходе редовно израђује годишње извештаје о управљању ризицима, и редовно ажурира Регистар ризика.
У Регистру ризика нису обухваћени ИТ ризици који могу изазвати делимичне, краткотрајне као и дуже прекиде у раду ОЈП. Поред тога, недостаје процена утицаја на пословање и припадајуће мере које требају да избегну или умање негативни утицај на пословање. Процена пословног утицаја је поступак утврђивања које су активности у пословању су критичне по остварење циљева, од којих ресурса зависе постизање резултата, зависи и избор примењених мера које треба да обезбеде отпорност према ризику и јачање континуитета пословања. Које мере ће ОЈП применити зависи од процењеног значаја и утицаја критичног процеса и/или ресурса. Колико једна информациона услуга, електронска пошта, интернет презентација, ЛПА портал, систем за обрачун, интернет веза, итд. је важна за рад ОЈП одредиће избор начина обезбеђења наставка рада у случају остварења ризика.
Град Београд није донео Акт о информационој безбедности и није уредио мере заштите за постизање и одржавање адекватног нивоа информационе безбедности Секретаријата за јавне приходе, што за последицу може имати већу осетљивост на ризике од злоупотребе, оштећења или губитка података и докумената.
Град Београд није донео документа или потписао Споразум са Канцеларијом ИТеУ о разграничењу одговорности за обавезе: План пословног континуитета; План пословног континуитета у ванредним ситуацијама; План опоравка од хаварије; и План израде резервних копија којим би били обухваћени кориснички рачунари и друга информациона добра у Секретаријату за јавне приходе.

Препорука: Препоручује се ОЈП Београд да донесе све потребне акте којима се уређују питања информационе безбедности, да обухвати све информационе ресурсе и обезбеди примену прописаних мера заштите информационог система.

ОЈП Крагујевац

Град Крагујевац је донео Акт о информационој безбедности али није разрадио мере заштите података, информација и докумената са становишта примене мера заштите тајности података на корисничким рачунарима у ЛПА, имајући у виду обим послова и задатака и недовољног кадровског капацитета.

Препорука: Препоручује се ОЈП Крагујевац да допуни постојеће акте којима уређује питања информационе безбедности тако што ће ближе уредити одговарајуће техничке, организационе и кадровске мере неопходне за безбеднији рад са ИСЛПА свих запослених у ОЈП.

ОЈП Инђија

Општина Инђија је донела Акт о информационој безбедности у којем је детаљно уредила мере заштите информационих технологија и мере заштите података, информација и докумената.

ОЈП Ариље

Општина Ариље није донела Акт о информационој безбедности и није уредила мере заштите за постизање и одржавање адекватног нивоа информационе безбедности ОЈП, што за последицу може имати већу осетљивост на ризике од злоупотребе, оштећења или губитка података и докумената на корисничким рачунарима или ако оцени да не располажу са адекватним ИТ кадровима ангажује добављача услуге у складу са Законом о информационој безбедности.

Препорука: Препоручује се ОЈП Ариље да донесе све потребне акте којима се уређују питања информационе безбедности, да обухвати све информационе ресурсе и обезбеди примену прописаних мера заштите информационог система.

ОЈП Житорађа

Општина Житорађа је донела Акт о информационој безбедности али није обухватила информациона добра ОЈП и није одредила мере заштите података, информација и докумената поготово са становишта примене мера заштите тајности података на корисничким рачунарима или ако оцени да не располажу са адекватним ИТ кадровима ангажује добављача услуге у складу са Законом о информационој безбедности.

Препорука: Препоручује се ОЈП Житорађа да допуни постојеће акте којима уређује питања информационе безбедности тако што ће ближе уредити одговарајуће техничке, организационе и кадровске мере неопходне за безбеднији рад са ИСЛПА свих запослених у ОЈП.

Налаз 3.3: ОЈП Београд, Крагујевац, Инђија, Ариље и Житорађа није у потпуности успоставила механизам управљања овлашћењима у ИСЛПА, чиме се ствара ризик да због недостатка адекватног раздвајања дужности дође до ненамерних грешака, оштећења или губитка података и докумената, што за последицу може имати њихово неблаговремено откривање и отклањање.

Правилно раздвајање дужности је кључна превентивна контрола у систему финансијског управљања и контроле корисника буџетских средстава, јер смањује ризик од грешака и неодговарајућих акција. Она помаже у правовременом откривању грешака, отклањању последица грешке и свакако утврђивању разлога настанка грешке како би се унапредио систем интерне контроле. Никако не треба умањити ни значај смањења ризика од преваре, где треба да се обезбеди да једна особа не може да направи и сакрије грешке или неправилности у току обављања свакодневних активности.

Руководство треба да расподели одговорности, да би обезбедило унакрсну проверу поделе дужности[79]. Структура организације несме омогућити да одговорност за све аспекте обраде података лежи на једном запосленом. Функције **покретања, одобравања, уноса, обраде** и **провере** података требају бити раздвојене како би се осигурало да ниједно лице не може направити грешку, пропусте или друге неправилности и прећутати или прикрити доказе.

Раздвајање дужности у апликацијама спроводи се давањем права приступа у складу са захтевима за обрадом и приступом информацијама. Традиционално раздвајање дужности у ИТ окружењу је подељено на два дела: развој система и продукционо окружење. Служба ИТ подршке треба да буде одговорно за вођење продукционог система - осим за спровођење промена - и требало би да имају малу (помоћ у дефинисању техничких захтева) или никакву одговорност у процесу развоја. Ова контрола укључује ограни- чавање добављача везано за приступ или мењање продукционих програма, система или података. Слично томе, особље за развој система треба да има минималан контакт са продукционим системима.

Када је у питању мали број запослених где се дужности не могу употпуности раздвојити, морају се установити додатне – компензационе контроле како би се ублажили или смањили ризици од грешака или неправилности. Главна компензациона контрола у таквом случају су журнали апликација, сервера базе података и оперативног система.

Налози за приступ као што су Aministrator group, Super User итд, могу модификовати улазе лога, приступ датотекама, права као било који корисник или у било која улога морају се персоналозовати или доделити једном запосленом. У случајевима када то није могуће, број

[79] Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, COSO, September 2012, pp. 95-96.

запослених са овим налозима треба свести на минимум уз додатне контроле. Такве контроле у виду разних софтверских алата су такође на располагању и треба да буду размотерни да би се ограничило овлашћење и да се прате активности појединаца са администраторским налозима.[80]

Слика број 20. Додела послова по радним местима

	Фискална Анализа	Издавање Уверења	унос ППИ2	упит ППИ2	Наплата ППИ2	Наплата ППИ1	Одлагање ППИ2	Референт	књиговођа	Књижење	пореска контрола	попис	кориснички налог	Масовна стампа	Супернадзор
начелник пореске управе за јавне приходе	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
начелник одељења за пореску контролу -главни инспектор			■								■				
инспектор пореске контроле 1					■				■		■				
инспектор пореске контроле 2											■				
инспектор пореске контроле 3			■		■						■				
начелник одељења за наплату јавних прихода						■		■			■				
шеф службе за редовну наплату						■					■				
шеф службе за принудну наплату						■		■							
инспектор наплате 1			■	■		■					■				
инспектор наплате 2	■		■		■					■					
послови наплате			■	■	■										
послови принудне наплате			■	■	■	■						■			
инспектор принудне наплате		■			■	■	■								
инспектор принудне наплате							■								
инспектор принудне наплате					■	■	■								
начелник одељења за пореско правне и нормативне послове			■	■	■		■	■							
шеф службе за процену тржишне вредности непокретности				■		■					■				
начелник одељења за утврђивање јавних прихода				■	■	■		■			■				
шеф службе за утврђивање јавних прихода			■	■		■		■							■
шеф службе за евиденцију јавних прихода		■	■	■	■										
инспектор за послове утврђивања јавних прихода 1			■		■	■		■			■				
инспектор за послове утврђивања јавних прихода 1			■	■	■			■			■				
инспектор за послове утврђивања јавних прихода 2			■	■	■	■		■			■			■	
инспектор за процену тржишне вредности непокретности				■		■					■				
послови издавања уверења 1		■	■	■											
послови издавања уверења 2		■	■	■											
послови издавања уверења 2		■	■	■											
послови уноса пријава		■	⊠												
послови уноса пријава и утврђивање јавних прихода				■	■	■									
послови уноса пријава и утврђивање јавних прихода					■	■					■	■			
послови уноса пријава и утврђивање јавних прихода					■	■						■			
послови уноса пријава и утврђивање јавних прихода					■	■						■		■	
послови уноса пријава и утврђивање јавних прихода			■	■	■	■									
послови уноса пријава и утврђивање јавних прихода			■	■	■	■						■			
послови уноса пријава и утврђивање јавних прихода		■	■	■	■										
начелник одељења за пореско рачуноводство				■		■	■		■	■	■				
порески рачуновођа	■		■						■	■					
порески рачуновођа	■		■						■						
оперативни послови			■				■	■					■		
административни послови		■													

[80] Удружење интерних ревизора Србије по одобрењу IIA, на српском језику 2018. године, Ризици и контроле информационих технологија, МОПП – Водич за праксу 2.издање, The Institute of Internal Auditors (IIA), USA, March 2012, стр. 19.

Подела дужности треба да обезбеди унакрсну проверу одговорности да би се избегле некомпатибилности. Законом о информационој безбедности[81] се одређују мере заштите од безбедносних ризика у ИКТ системима и одговорностима правних лица приликом управљања и коришћење ИКТ система. Поједини послови у овој области треба да су уређени одговарајућим процедурама, то је и законска обавеза, зато што акт о безбедности као општи акт обично не садржи детаљне инструкције како се неки процес спроводи, и ко је за то одговоран.

Спровођење мера је посао добро обучених, стручних ИТ кадрова. Организацијски треба да буду уређени тако да омогућавају јасну поделу дужности и одговорности, али и контролу свих тих послова. Обим послова које обавља ОЈП се разликује и специфичан је за сваку ЈЛС, проблем раздвајања дужности није једноставан за решавање, али не би смело да се догоди да запослени на пословима уноса пријава нема права да уноси пријаве (знак X, на слици број 20).

На другој страни је да у једној доброј организацији неби смело бити дозвољено да иста службеничка звања често подразумева и плату за исте послове имају лица са другим правима и обимом радних задатака.
Уколико неке послове обавља пружалац услуге, то је потребно дефинисати уговором. Између осталог обавезно је дефинисати све обавезе пружаоца услуга када је у питању информациона безбедност.

Посебну пажњу треба посветити питањима приступа систему: физичком и логичком приступу. И то најпре одговарајућим процедурама, упутствима, евиденцијама, а затим и практичном имплементацијом тих докумената и контролом.

Треба обезбедити максималну могућу заштиту података грађана/обвезника, у складу са домаћим законодавством, почевши од тренутка приступа подацима (уз употребу електронског потписа или на начин који осигурава да се подацима обвезника не приступа без ревизорског трага евидентираног у журналу), али и успоставити мере контроле и заштите излазних података.

Све то, у посматраном периоду ревизије 2018-2020. година, није на адекватан начин препознато од стране ЈЛС које користе ИСЛПА. ЈЛС су различито и несвеобухватно уредиле ову област, занемарујући законске обавезе, док Министарство финансија – Пореска управа је једноставно предала део послова без икаквог надзора и контроле из своје надлежности да ове процесе испрате, најпре кроз редовно прикупљање података о овим питањима, а затим и предузимањем одговарајућих активности како би унапредиле информациону безбедност и обезбедиле поуздану основу за извештавање.

Управљање логичким приступом

Чланом 10. Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, у прописује одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа и то:

- Оператор ИКТ система је у обавези да предвиди процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, тако што предвиђа услове за одобравање и укидање овлашћеног приступа, проверу адекватности одобреног нивоа приступа и доделу јединствене идентификационе ознаке лицу којем се одобрава приступ (став 1);
- Оператор ИКТ система води евиденцију о додељеним и одузетим ознакама, утврђује услове за коришћење заједничке идентификационе ознаке у случајевима када је то неопходно, дефинише начин и услове онемогућавања и уклањања јединствених идентификационих ознака, као и услове за доделу и коришћење администраторских права (став 2);

[81] Члан 7 Закона о информационој безбедности.

- Лицима којима се одобрава овлашћени приступ омогућује се приступ на основу података за аутентификацију (лозинке, криптографски кључеви, подаци складиштени на токенима и сл.) (став 3);
- Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (став 4);
- Оператор ИКТ система дужан је да обезбеди механизам за укидање права приступа у случајевима промене радног места, престанка радног односа и, по потреби, у другим случајевима (став 5).

Сви оператори ИКТ система треба да овај процес уреде поштујући управо наведене одредбе Закона. Не значи само да се свим корисницима система доделе параметри приступа и улоге у систему. Потребно је и обезбедити механизам контроле тог процеса како би се у сваком тренутку могло установити да ли листа корисника одговара тренутној листи корисника система, са одговарајућим улогама.

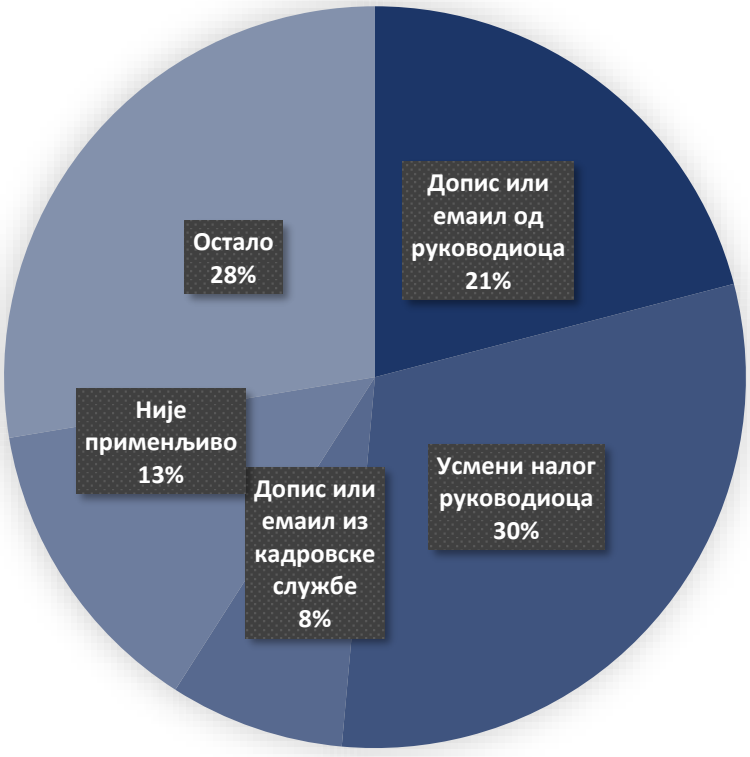
Само на такав, свеобухватан начин управљања логичким приступом се може обезбедити неопходан степен безбедности система и података.

На сличним принципима се уређује и физички приступ, дакле обухвата одређивање лица која могу да приступе сервер собама, разлоге за то, тј. улоге тих лица, и механизам контроле тог процеса.

Управљање логичким приступом

На питање као администратор ЛПА апликације додавање и брисање налога вршим, 22 ЛПА је одговорило са на основу дописа или емаил-а од шефа, односно 21% од укупног броја, 32 ЛПА је одговорило са на основу усменог налога шефа, односно 30% од укупног броја, 8 ЛПА је одговорило са на основу дописа кадровске или емаил-а, односно 8% од укупног броја, 14 ЛПА је одговорило да није применљиво, односно 13% од укупног броја и преосталих 30 ЛПА је одговорило са остало, односно 29% од укупног броја.

Слика број 21. Администратор ЛПА апликације додаје и укида налоге на основу?



Међу ЛПА које су одговориле са остало издвајају се објашњења да је администратор на нивоу града. Постоји простор да се донесу интерна акта на нивоу локалних пореских администрација којима ће уредити поступак доделе и одузимања функционалности, односно овлашћења за рад у апликацији ЛПА, нарочито са акцентом на ситуације пријема новог запосленог лица, замене привремено одсутног лица и трајног престанка рада у апликацији од стране претходно ангажованог лица. Доделе и одузимања овлашћења за рад у апликацији морају да буду ажурна и правовремена, као би се избегао потенцијални ризик он неовлашћеног приступа који може да доведе до нарушавања поверљивости.

Подела дужности је значајна за ефикасну интерну контролу зато што смањује ризик од грешака и неодговарајућих радњи. Уопштено, следеће функције треба распоредити на различите особе: одобрење, рачуноводство/усаглашавање, чување средства. Захтева се детаљан супервизорски преглед одговарајућих активности као активност компензационе контроле уколико се ове функције не могу поделити мањим одељењима. Када је једна особа ангажована на контролама приступа, на пример, та особа не треба да буде у могућности да себи додели права, а затим обави активност. Слично томе, она не треба да буде у могућности да обави трансакцију а затим да избрише логове (листинге) који представљају траг те активности. Уместо тога треба извршити правилан преглед процеса и раздвојити их да би се смањили ризици везани за одређени процес који буде угрожен злонамерно или кроз људску грешку.

Утврђивање да ли постоји табела за раздвајање дужности и провера адекватног раздвајања кључних задатака/ радних функција и дозвољених трансакција, затим, контрола листе корисника и привилегија приступа за кориснике. Процена да ли разграничење обавеза осигурава да особа која укуцава податке није одговорна и за верификацију документа. Провера да ли су усвојене компензационе контроле у случајевима када раздвајање дужности није изводљиво.

ОЈП Београд

Секретаријат обавља послове који се односе на: утврђивање, контролу и наплату изворних јавних прихода буџета Града и буџета градских општина за које је надлежан у складу са прописима и на процену тржишне вредности непокретности у складу са Законом о јавној својини, у поступцима принудне наплате пореског дуга, као и процену непокретности које су у својини града Београда.

Послови утврђивања, контроле и наплате годишњег пореза на имовину, локалних комуналних такси, накнаде за заштиту и унапређивање животне средине и других изворних јавних прихода за које је Секретаријат надлежан у складу са посебним прописом, врше се у оквиру одељења на подручју свих градских општина. Број запослених у одељењима за подручја градских општина су: Барајево, 6; Вождовац, 18; Врачар, 12; Гроцка, 8; Звездара, 17; Земун, 17; Лазаревац, 8; Младеновац, 8; Нови Београд, 26; Обреновац, 9; Палилула, 17; Раковица, 13; Савски венац, 12; Сопот, 6; Стари град, 13; Сурчин, 7 и Чукарица, 17.

Секретаријат са 62 запослена лица обавља послове координације рада одељења за подручја градских општина, пореског рачуноводства, редовне и принудне наплате, подношења захтева за покретање пореско прекршајног поступка, процене тржишне вредности непокретности.

Достављени преглед корисничких налога по радним местима у систематизацији за запослена лица и лица ангажованих по уговору о привременим и повременим пословима са прегледом послова/рола у ЈИС ЛПА показује да 14 налога који имају улогу контроле не обављају све неопходне контроле за 17 градских општина, јер поред послова контроле обављају и послове књижења. То обавезује одговорне руководиоце да контролу и преглед морају обављати и на основу допуњеног журнала апликације.

Препорука: Препоручује се ОЈП Београд да успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места.

ОЈП Крагујевац

Достављени преглед корисничких налога по радним местима у систематизацији за запослена лица и лица ангажованих по уговору о привременим и повременим пословима са прегледом послова/рола у ЈИС ЛПА показује да поједини налози немају све дозвољене улоге према организационој припадности и исти налози имају могућност обављања наплате и послова књижења, а што је последица недовољних кадровских капацитета. То обавезује одговорне руководиоце да контролу и преглед морају обављати и на основу допуњеног журнала апликације.

Препорука: Препоручује се ОЈП Крагујевац успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места.

ОЈП Инђија

У прегледу корисничких налога по радним местима у систематизацији за запослена лица и лица ангажованих по уговору о привременим и повременим пословима са прегледом послова/рола у ЈИС ЛПА показује да поједини налози имају могућност наплате и послове књижења. То обавезује одговорне руководиоце да контролу и преглед морају обављати и на основу допуњеног журнала апликације.

Препорука: Препоручује се ОЈП Инђија успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места.

ОЈП Ариље

Број лица на пословима ОЈП онемогућава правилно раздвајање дужности и то обавезује одговорне руководиоце да контролу и преглед морају обављати и на основу допуњеног журнала апликације.

Препорука: Препоручује се ОЈП Ариље успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места.

ОЈП Житорађа

Број лица на пословима ОЈП онемогућава правилно раздвајање дужности и то обавезује одговорне руководиоце да контролу и преглед морају обављати и на основу допуњеног журнала апликације.

Препорука: Препоручује се ОЈП Житорађа успостави процедуру за управљање корисничким налозима како би се обезбедило да свако лице које приступа ИС ЛПА има овлашћења у складу са описом свог радног места.

V Захтев за доставу одазивног извештаја

Субјекти ревизије су, на основу члана 40. став 1. Закона о Државној ревизорској институцији, дужни да поднесу Државној ревизорској институцији писани извештај о отклањању откривених несврсисходности (одазивни извештај) у року од 90 дана почев од наредног дана од дана уручења овог извештаја.

Одазивни извештај мора да садржи:

1) навођење ревизије, на коју се он односи;

2) кратак опис несврсисходности у пословању, које су откривене ревизијом;

3) приказивање мера исправљања.

Мере исправљања су мере које субјект ревизије предузима да би отклонио несврсисходности у свом пословању или мере умањење ризика од појављивања одређене несврсисходности у свом будућем пословању за чије предузимање субјект ревизије мора поднети уз одазивни извештај одговарајуће доказе.

Субјекти ревизије су обавезни да у одазивном извештају искажу мере исправљања по основу откривених несврсисходности односно свих закључака и налаза датих у Извештају о ревизији сврсисходности пословања, као и да поступи по датим препорукама. За мере исправљања је дужан да уз одазивни извештај достави доказе према следећем:

1. За налазе, односно несврсисходности првог приоритета, односно које је могуће отклонити у року од 90 дана субјекти ревизије су у обавези да доставе доказе о отклањању несврсисходности односно предузимању мера исправљања;
2. За налазе, односно несврсисходности другог приоритета, односно које је могуће отклонити у року до годину дана субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице;
3. За налазе, односно несврсисходности трећег приоритета, односно које је могуће отклонити у року до три године субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице.

На основу члана 40. став 2. Закона о Државној ревизорској институцији одазивни извештај је јавна исправа која је потписана и оверена печатом од стране одговорног лица субјекта ревизије.

Државна ревизорска институција ће оценити веродостојност одазивног извештаја, тј. провериће истинитост навода о мерама исправљања, предузетим од стране субјекта ревизије, подносиоца одазивног извештаја. У случају потребе извршиће се и ревизија одазивног извештаја. Такође, извршиће се и оцена да ли су мере исправљања исказане у одазивном извештају задовољавајуће.

Сагласно члану 57. став 1. тачка 3) Закона о Државној ревизорској институцији, ако субјекат ревизије у чијем су пословању откривене несврсисходности, не подносе у прописаном року Институцији одазивни извештај, против одговорног лица субјекта ревизије поднеће се захтев за покретање прекршајног поступка.

Ако се оцени да одазивни извештај не указује да су откривене несврсисходности отклоњене на задовољавајући начин, сматра се да субјект ревизије крши обавезу доброг пословања. Ако се ради о незадовољавајућем отклањању значајне несврсисходности, сматра се да постоји тежи облик кршења обавезе доброг пословања. У овим случајевима Државна ревизорска институције је овлашћена да предузима мере сагласно члану 40. ст 7. до 13. Закона о Државној ревизорској институцији.

ПРИЛОЗИ

1. Прилог 1 – Пример добре праксе односа према локалним изворним приходима

Општина Инђија је у сарадњи са друштвом Gisdata доо, 2008. године основала Агенцију за ИТ, ГИС и комуникације општине Инђија која од 2009. године наступа самостално на тржишту, нудећи више од 20 самостално осмишљених и развијених ИТ решења, међу којима је и Систем 48.

Систем 48 представља јединствени информациони систем у Европи којим се у року од само 48 сати решавају комунални проблеми грађана. Грађани имају могућност да различитим каналима који укључују email, web, SMS или позив пријаве проблем који оператери заводе кроз софтвер и прослеђују надлежној локалној служби која кроз највише 48 сати упућује одговор. У оквиру овог система општина Инђија је успоставила јединствени систем извештавања којим је обухваћено и одељење за утврђивање и наплату јавних прихода. Наиме, поменуто одељење током целе године на сваке две недеље израђује извештаје који обухватају анализе тренутног стања у обрачуну и наплати изворних прихода и доставља их одговорним лицима општине на разматрање. Поменути извештаји обухватају анализу тренда наплате по недељама за сваки изворни приход понаособ, поткрепљену одговарајућим табеларним и графичким приказима и упоредним прегледима укупне наплате по врсти јавних прихода. Овакав начин пословног извештавања обезбеђује непосредан увид у стање локалних изворних прихода и омогућава континуирано праћење стања наплате по врсти изворних прихода чиме се осигурава правовремено предузимање активности и доношење одлука којима се може утицати на одржавање постојећег нивоа наплате или његово побољшање.

Слика број 22. Насловна страна двонедељног извештаја одељења за утврђивање и наплату јавних прихода општине Инђија


ОПШТИНА ИНЂИЈА

СИСТЕМ 48

ИЗВЕШТАЈ

Одељења за утврђивање и наплату јавних прихода

за 14.05.2021. године

Извештајни период

19.04.2021. године – 09.05.2021. године

САДРЖАЈ:

1. ПОРЕЗ НА ИМОВИНУ
   - ПОРЕЗ НА ИМОВИНУ ОБВЕЗНИКА КОЈИ НЕ ВОДЕ ПОСЛОВНЕ КЊИГЕ
   - ПОРЕЗ НА ИМОВИНУ ОБВЕЗНИКА КОЈИ ВОДЕ ПОСЛОВНЕ КЊИГЕ
   * са упоредним прегледом наплате по месецима за период 2012-2021 (са 09.05.2021. год.)
2. КОМУНАЛНА ТАКСА ЗА ИСТИЦАЊЕ ФИРМЕ НА ПОСЛОВНОМ ПРОСТОРУ
   * са упоредним прегледом наплате по месецима за период 2013-2021 (са 09.05.2021. год.)
3. КОМУНАЛНА ТАКСА ЗА КОРИШЋЕЊЕ ПРОСТОРА НА ЈАВНИМ ПОВРШИНАМА
   * са упоредним прегледом наплате по месецима за период 2013-2021 (са 09.05.2021. год.)
4. ПОСЕБНА НАКНАДА ЗА ЗАШТИТУ И УНАПРЕЂЕЊЕ ЖИВОТНЕ СРЕДИНЕ
   * са упоредним прегледом наплате по месецима за период 2013-2021 (са 09.05.2021. год.)
5. КОМУНАЛНА ТАКСА ЗА КОРИШЋЕЊЕ РЕКЛАМНИХ ПАНОА
   * са упоредним прегледом наплате по месецима за период 2013-2021 (са 09.05.2021. год.)
6. ОСТАЛИ ЈАВНИ ПРИХОДИ
   * преглед наплате у извештајном периоду (са 09.05.2021. год.)
7. УПОРЕДНИ ПРЕГЛЕД УКУПНЕ НАПЛАТЕ ПО ВРСТИ ЈАВНИХ ПРИХОДА

Извор: Одељење за утврђивање и наплату јавних прихода општине Инђија

Лица запослена у одељењу за утврђивање и наплату јавних прихода која раде у информационом систему локалне пореске администрације имају континуирану стручну подршку ИТ стручњака из Агенције за ИТ, ГИС и комуникације општине Инђија у делу администрирања рачунара и рачунарске опреме чиме се обезбеђује додатна заштита у делу приступа систему, заштите од злонамерних софтвера, неовлашћеног приступа и хаварије рачунара и рачунарске опреме.

2. Прилог 2 – Методологија у поступку рада

У ревизији су коришћене технике прикупљање података и докумената у електронском облику (папирна документа ће се дигитализовати), анализа прикупљених података, анализе тренда и учешћа, интервјуи са одговорним лицима и друге технике.

Да би се извршила провера постојања и функционисања општих и апликативних контрола и квалитета ИТ система, а у складу с наведеном методологијом управљања ризицима, руководство субјекта ревизије треба да успостави континуиране контролне активности: контролу управљања заштитом ИТ система, контролу логичког и физичког приступа програмима и апликацијама, контролу управљања конфигурацијама и изменама програма и контролу поделе дужности и одговорности корисника. Правилно дефинисаним (програмираним) контролним поступцима у оквиру апликација, база података и оперативних система могуће је остварити ефективно раздвајање дужности и одговорности запослених у свакодневним пословним активностима. У овом случају, контролне активности представљају комбинацију мануелних и аутоматских (програмских) контролних поступака, с тим да врста контролних поступака зависи од природе, сложености и квалитета ИТ система.

Слика број 23. Ревизорско разумевање ИТ окружења и идентификовање општих контрола ИТ[82]

Примена Приручника за ИТ ревизију IDI/INTOSAI[83] обухвата следеће области:

- ИТ управљање,
- Развој и набавка,
- ИТ операције,
- Апликативне контроле,
  - Контроле улаза података у систем,
  - Контроле обраде података,
  - Контроле излаза података из система,
  - Безбедносне контроле,

[82] Међународне стандарде врховних ревизорских институција, ISSAI 1315, издаје INTOSAI, Међународна организација врховних ревизорских институција. **www.issai.org**

[83] Приручник усвојен на XXI Конгресу INTOSAI одржаном у Пекингу, Кина, октобар 2013. године

- Контроле за обезбеђење интегритета, аутентичности и непорецивости.
- Екстернализација услуга,
- План континуитета пословања (БЦП) и План опоравка од хаварије (ДРП),
- Информациона безбедност.

Методологија подразумева процену ризика по областима и подобластима и детаљно је обрађена у Приручнику.

Очекивани резултати ревизије

Приликом оцењивања ИТ управљања применићемо скалу од 1 до 5 са следећим ознакама:

1) Оцена 1 - потпуно незадовољавајуће,
2) Оцена 2 - делимично незадовољавајуће,
3) Оцена 3 - делимично задовољавајуће,
4) Оцена 4 - задовољавајуће и
5) Оцена 5 - потпуно задовољавајуће.

Да бисмо одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, стручну литературу, као и документацију и информације добијене од субјеката ревизије. Анализирали смо податке и информације за период од 2018. до 2020. године. Такође смо за поједине анализе користили и податке из 2021. године.

Састанци са представницима ОЈП

У циљу планирања ревизије и упознавањем са темом, идентификацијом потенцијалних проблема и ради прикупљање релевантних података, ревизорски тим је обавио разговор са одговорним и надлежним лицима из области информационих технологија у одређеним ОЈП и на састанку поставили унапред припремљена питања из следећих области:

- ИТ управљања;
- Развоја и набавке ИТ;
- ИТ операције;
- Уговори са добављачима ИТ услуга;
- Планови континуитета пословања и опоравка од хаварије;
- Информациона безбедност;
- Апликативне контроле.

Због ограниченог времена трајања састанака и опширности питања иста смо послали и на е-мејл адресе и уз питања затражили и одговарајућу документацију која се односи на постављена питања.

Захтев за доставу документације од субјеката ревизије

Обављени су састанци са субјектима ревизије, примљена су документа од субјеката ревизије путем електронске поште и интранет портала ДРИ, прикупљена су документа из јавно доступних извора

На овај начин, до саме израде извештаја, прикупљене су све четири категорије ревизијских доказа:

- Нематеријални докази (интервјуи, упитници и анкете) од субјеката;

- Документарни докази као писани документи – документација прикупљена од субјеката ревизије, евиденције, статистички подаци, и други извештаји;
- Физички докази – прикупљени обиласком субјеката ревизије;
- Аналитички докази – анализе рађења на бази добијених одговора на анкете и упитнике, анализе информационих система и база података ЈЛС – субјеката ревизије.

Извршена је квантитативна и квалитативна анализа и након тога се приступило изради извештаја.

Анкета за јединице локалне самоуправе

У циљу планирања ревизије и упознавањем са темом, идентификацијом потенцијалних проблема и ради прикупљање релевантних података, ревизорски тим је послао анкету на е-мејл адресе свих јединица локалне самоуправе које су извор информација у овој ревизији.
ЈЛС у Републици Србији су путем мејла добила питања из два упитника, један за кориснике апликације, а други упитник за ИТ подршку без обзира како је организована.
Упитник за кориснике апликације има пет група питања, прва се тиче броја запослених на пословима ЛПА, друга је број обвезника у ревидираним годинама ради оцењивања индикатора оптерећености запослених, трећа група је у вези функционалности саме апликације, четврта група питања је о начину приступања и пета група питања је о подршци корисницима у случајевима техничких тешкоћа приликом употребе.

Упитник: Управљање ИС ЛПА - питања за кориснике

За кориснике ЛПА апликације

Наведите укупан број запослених на **неодређено време** (стално запослени по систематизацији, урачунати и све руководиоце)

- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Наведите укупан број запослених на **одређено време** (привремено ангажовани, по уговору, на замени итд.)

- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Наведите укупан **број корисника** ЛПА апликације дана 31.12.

- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Број обвезника пореза на имовину

Наведите укупан број ФИЗИЧКИХ ЛИЦА - обвезника пореза на имовину

- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Наведите укупан број ПРАВНИХ ЛИЦА - обвезника пореза на имовину

- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Наведите укупан број ПРЕДУЗЕТНИКА - обвезника пореза на имовину

- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Наведите укупан број неуручених решења за порез на имовину:
- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Овде унесите број решења пре него их означите у апликацији да су уручена, приликом завршног књижења, прелаза на нову пословну годину.

Наведите претежни разлог за неуручена решења за порез на имовину:
- Непозната адреса
- Обвезник не станује на адреси
- Обвезник је преминуо
- Неће да прими решење
- Остало:

Наведите укупан број решења за порез на имовину у:
- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Наведите укупан број рекламација (усвојених жалби) на решење за порез на имовину у:
- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Овај податак може бити из било које друге евиденције. Унесите број решених жалби у првом степену.

Наведите претежни разлог за рекламацију на решење за порез на имовину:
- Непозната адреса
- Обвезник не станује на адреси
- Обвезник је преминуо
- Неће да прими решење
- Остало:

Апликација за ЛПА

Које друге изворне приходе обрачунавате и наплаћујете:
- Локалне административне таксе
- Локалне комуналне таксе
- Боравишна такса
- Накнаде за коришћење грађевинског земљишта
- Накнада за заштиту и унапређивање животне средине
- Концесионе накнаде
- Новчане казне из прекршајног поступка
- Закупнине
- Приходи од продаје услуга
- Приходи од камата на финансијска средства
- Приходи од донација
- Самодоприноси
- Остало:

Да ли би сте користили ЛПА апликацију и за оне изворне приходе које сада не користити те:
- Да
- Не-Мали број трансакција на годишњем нивоу.
- Не-Наплата је једнократна.
- Не-Приходи се евидентирају у другој апликацији.
- Не-Није применљиво.
- Не знам.
- Остало:

Изаберите све регистре и/или државне органе са којима размењујете податке у вези ЛПА:

- Министарство унутрашњих послова
- Министарство финансија - Пореска управа
- Министарство финансија - Управа за трезор
- Министарство за државну управу и локалну самоуправу
- Агенција за привредне регистре
- Републички геодетски завод
- Јавни бележници
- Републички фонд за ПИО
- Републички фонд за здравствено осигурање
- Централни регистар за обавезно социјално осигурање
- Локални судски органи
- Националну службу за запошљавање
- ЈП Пошта Србије - хибридна пошта
- Матична евиденција умрлих јединице локалне самоуправе
- Друге ЛПА
- Остало:

Изаберите извештаје које користите у ЛПА апликацији:

- Извештај по обрачунатим пријавама
- Извештај о измењеним ППИ-1
- Извештај о обвезницима са највећим задужењима
- Извештај о објектима имовине физичких лица
- Извештај о објектима опорезивања – комуналне таксе
- Извештај о објектима опорезивања – накнаде за коришћење јавних површина
- Извештај о обрађеним ППИ-1
- Извештај о предатим ППИ-1
- Извештај о пријавама боравишне таксе по насељима и категоријама објеката
- Извештај о стањима на рачуна обвезника по рачунима
- Извештај о стању на рачунима јавних прихода – Бруто биланс
- Извештај о стању на рачунима јавних прихода – Главна књига
- Извештај о утврђеним задужењима по пореским облицима
- Извештај одељења за утврђивање и наплату јавних прихода Порески бруто годишњи извештај
- Извештај по објектима и врстама непокретности
- Извештај о спорним и дубиозним потраживањима
- Извештај о застарелим обавезама
- Извештај о отпису пореских обавеза
- Извештај о пореском дугу
- Евиденција о неурученим решењима
- Евиденција о уручених решењима
- Евиденција о одобреном одлагању плаћања на почек или на рате
- Евиденција броја дуплираних решења
- Порески бруто годишњи извештај
- Порески нето годишњи извештај
- Преглед стања на рачунима по контима
- Преглед стања на рачунима пореских обвезника
- Неки други
- Остало:

Да ли знате шта је шифра -94?

- Активан ПИБ
- Привремено одузет ПИБ
- Трајно поништен ПИБ
- Угашен ПИБ
- Не знам.
- Остало:

Као администратор ЛПА апликације доделу функционалности у апликацији корисницима вршим:
- На основу распореда на радно место и радним задацима (систематизација)
- На основу дописа или мејл поруке од шефа
- На основу усменог налога шефа.
- Није применљиво.
- Остало:

Као администратор ЛПА апликације додавање и брисање налога вршим:
- На основу дописа или мејла од кадровске јединице
- На основу дописа или мејл поруке од шефа
- На основу усменог налога шефа
- Није применљиво.
- Остало:

Обуку за рад у ЛПА апликацији:
- Све потребно научио сам од колегиница/колега.
- Био/ла сам на обуци пре 5 и више година
- Био/ла сам на обуци последњих годину дана.
- Самоук/а.
- Остало:

Да ли сте задовољни са ЛПА апликацијом:
- Да, много боље је него што је било 2018. године
- Да, али су мала побољшања
- Да
- Не, није као што смо очекивали
- Не, сада је лошије него што је било 2018. године
- Остало:

Приступ ЛПА апликацији

Након укључења рачунара да ли уносите име и лозинку:
- Да
- Не
- Не знам.
- Остало:

Промену лозинке вршим:
- Сваки дан
- Једном недељно
- Једном месечно
- Једном годишње
- Није потребно често мењати
- Никада
- Остало:

Моју лозинку:
- Никада не дајем колегама
- Повремено дајем колегама на замени (боловање, одмор, итд.)
- Никада, никоме
- Не знам
- Остало:

Одржавање ЛПА апликације

Одржавање рачунара и другу ИТ подршку претежно врши:
- Запослено лице у ЛПА
- Запослени у јединици локалне самоуправе на неодређено време
- Запослени у јединици локалне самоуправе на одређено време

- Лице ангажовано по уговору о делу
- Лице ангажовано на основу уговора са фирмом/правним лицем
- Не знам
- Нико
- Остало:

Да ли сте имали ситуације када вам је ЛПА апликација била недоступна?
- Да
- Не
- Не знам
- Остало:

Недоступност ЛПА апликације се десила (колико се ја сећам):
- Једном, не сећам се тачно када.
- Више пута у последњих годину дана.
- Више пута у последње две године.
- Више пута у последњих месеци.
- Отприлике, једном недељно.
- Веома ретко.
- Никада.
- Остало:

Трајање недоступности ЛПА апликације је било:
- Краткотрајно.
- Цео радни дан.
- Више радних дана.
- Не знам тачно.
- Не знам тачно, информација о прекиду нам је накнадно достављена.
- Остало:

Техничке проблеме у коришћењу ЛПА апликације сте:
- Пријавили смо ИТ служби, интерно.
- Пријавили Канцеларији за ИТЕУ
- Пријавили Институту Михајло Пупин
- Пријавили Пореској управи и/или Министарству финансија.
- Ником нисам пријавио, сачекао сам да поново проради.
- Остало:

Да ли имате било какав предлог за побољшања?
- Да
- Не
- Остало:

У другом упитнику су питања намењена ИТ подршци која обезбеђује техничке услове у ОЈП, где су питања подељена у две групе, једна се односи на стање опремљености а друга група питања се тичу обезбеђивања информационе безбедности корисничких рачунара.

Упитник: Управљање ИС ЛПА - питања за ИТ особље

Опрема

Број рачунара са којих се приступа ЛПА апликацији
- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Број рачунара у ЛПА са оперативним системом који је:
- Старији од Windows 7: [унети број]
- Windows 7 или 8: [унети број]
- Windows 10: [унети број]

- Линукс: [унети број]
- Неки други: [унети број]

Број рачунара у ЛПА са ажурном заштитом од злонамерног софтвера (лиценциран антивирусни програм)
- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Број рачунара у ЛПА који су:
- Старији од 5 година: [унети број]
- Стари од 2 до 5 година: [унети број]
- Набављени у последњих годину дана: [унети број]

Након укључења рачунара запослени морају унети име и лозинку
- Да
- Не
- Не знам

Контролу промене лозинке врши се:
- Појединачно на сваком рачунару.
- Користимо централизовано (Активни директорић, домен контролер, итд.)
- Не знам
- Само једном

Колики су вам годишњи телекомуникациони трошкови за ЛПА апликацију били:
- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Колики су вам годишњи трошкови одржавања за ЛПА апликацију били:
- У 2018: [унети број]
- У 2019: [унети број]
- У 2020: [унети број]

Подршка корисницима

Резервну копија података са рачунара у ЛПА:
- Никада се не прави
- Корисници раде повремено на USB меморији или диску
- Врши се аутоматизовано на систем за резервне копије (Државног дата центра-Канцеларије за ИТЕУ)
- Не знам

Да ли сте пружали корисницима ЛПА апликације подршку код куће:
- Да
- Не
- Не знам

Да ли је донет Акт/Правилник о информационој безбедности:
- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли је донет План континуитета пословања (Шта се ради у случају природних непогода):
- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли је донет План опоравка од хаварије (шта се ради у случају техничког квара):

- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли је донет План израде резервних копија (Ко и када се врши израду резервних копија података и где се чувају):

- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли је донет План за ванредне ситуације (Мере које треба спровести по захтеву оснивача у ванредним околностима):

- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли сте до сада имали неки безбедносни инцидент (недозвољен приступ, лажни мејлови, рансомвер напад итд):

- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли сте неки инцидент пријавили надлежном органу:

- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли сте сачинили годишњи извештај о провери усклађености примењених мера заштите ИКТ система:

- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли сте именовали лице за заштиту података о личности:

- Да
- Не
- Не знам
- О томе брине надлежни орган.

Да ли имате неки предлог за унапређење начина рада:

- Да
- Не
- Не знам
- О томе брине надлежни орган.