ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ПОСЛЕРЕВИЗИОНИ ИЗВЕШТАЈ О МЕРАМА ИСПРАВЉАЊА
ЈКП Шумадија Крагујевац
по ревизији сврсисходности пословања
„Информациони систем у јавном градском превозу у граду Крагујевцу“

Број: 400-488/2023-07/61
Београд, 22. мај 2024. године

САДРЖАЈ

1. УВОД 3

2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА 4

2.1. ЈКП Шумадија Крагујевац није у потпуности успоставило организацију ИТ безбедности 4

2.1.1. Опис несврсисходности 4

2.1.2. Исказане мере исправљања и њихово вредновање (препорука 1) 4

2.2. ЈКП Шумадија Крагујевац није успоставило процес приступа систему на задовољавајући начин. 5

2.2.1. Опис несврсисходности 5

2.2.2. Исказане мере исправљања (препорука 2) 5

2.3. ЈКП Шумадија Крагујевац није у плану континуитета пословања предвидело управљање резервним копијама 6

2.3.1. Опис несврсисходности 6

2.3.2. Исказане мере исправљања (препорука 3) 6

2.4. ЈКП Шумадија Крагујевац није у потпуности успоставило управљање ИТ ризицима 7

2.4.1. Опис несврсисходности 7

2.4.2. Исказане мере исправљања (препорука 4) 7

2.5. ЈКП Шумадија Крагујевац није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података 8

2.5.1. Опис несврсисходности 8

2.5.2. Исказане мере исправљања (препорука 5) 8

2.6. ЈКП Шумадија Крагујевац нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга 9

2.6.2. Исказане мере исправљања (препорука 6) 9

2.7. ЈКП Шумадија Крагујевац није у потпуности уредило процес наплате карата и механизам контроле тог процеса 10

2.7.1. Опис несврсисходности 10

2.7.2. Исказане мере исправљања (препорука 7) 10

2.8. ЈКП Шумадија Крагујевац није у потпуности уредило контролу пружених услуга од стране ангажованих превозника. 10

2.8.1. Опис несврсисходности 10

2.8.2. Исказане мере исправљања (препорука 7) 11

3. МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА 11

1. УВОД

Државна ревизорска институција издала је Извештај о ревизији сврсисходности пословања Информациони систем у јавном градском превозу у граду Крагујевцу, број: 400- 488/2023-07/41, 25. децембар 2023. године, у којем је навела закључке и налазе.

С обзиром да, све откривене несврсисходности нису биле отклоњене у току ревизије, Институција је од субјекта ревизије, ЈКП Шумадија Крагујевац, захтевала достављање одазивног извештаја.

Субјект ревизије је у остављеном року од 90 дана доставио одазивни извештај, потписан и оверен од стране одговорног лица 27. марта 2024. године. Документацију је доставио путем мејла 27. марта 2024. године, и допунска објашњења 22.05.2024. године

У одазивном извештају су приказане мере исправљања утврђених несврсисходности. У послеревизионом поступку смо прегледали одазивни извештај, оценили његову веродостојност и оценили да ли су мере исправљања задовољавајуће.

У овом извештају:

- приказујемо несврсисходности које су обелодањене у извештају о ревизији за које је захтевано предузимање мера исправљања,
- резимирамо предузете мере исправљања и
- дајемо мишљење о томе да ли су мере за исправљање стања, исказане у одазивном извештају, задовољавајуће.

2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА

ПРИОРИТЕТ 2 - Несврсисходности које је могуће отклонити у року до годину дана

2.1. ЈКП Шумадија Крагујевац није у потпуности успоставило организацију ИТ безбедности

2.1.1. Опис несврсисходности

Организација ИТ безбедности у ЈКП Шумадија Крагујевац, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата примену адекватних докумената која уређују ову област, управљање инцидентима и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

2.1.2. Исказане мере исправљања и њихово вредновање (препорука 1)

ЈКП Шумадија Крагујевац је препоручено да успостави организацију информационе безбедности која обухвата усвајање, ажурирање и имплементацију аката која уређују ову област – акта (правилника) о информационој безбедности, процедура које се односе на ИТ безбедност, управљање инцидентима, и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података.

Донет је Правилник о безбедности информационо-комуникационог система ЈКП Шумадија Крагујевац дана 13.11.2023.године. Како је наведено у Извештају о спровођењу препорука, најкасније до децембра 2024 ће бити имплементирана нова верзија Стандарда 27001-2022

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

Правилник о безбедности информационо-комуникационог система ЈКП Шумадија Крагујевац

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.2. ЈКП Шумадија Крагујевац није успоставило процес приступа систему на задовољавајући начин.

2.2.1. Опис несврсисходности

Није успостављен процес приступа на задовољавајући начин, због тога што усвојене процедуре (политике) које уређују овај процес нису усклађене са начином рада у информационом систему за јавни градски превоз, а односе се на логички приступ, безбедан рад на даљину и мере физичке заштите, није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података.

2.2.2. Исказане мере исправљања (препорука 2)

ЈКП Шумадија Крагујевац је препоручено да уреди процес приступа систему, што подразумева измену и усвајање процедура које уређују овај процес и контролу тог процеса, а односи се на логички приступ, рад на даљину и физичку заштиту система.

Дана 01.02.2024. године закључен је нов Уговор о набавци услуга изнајмљивања и имплементације информационог система за контролу и управљање јавним превозом у реалном времену и изнајмљивање опреме за аутоматску наплату превоза и уоквиру техничке спецификације тачка 2.

"Пружалац услуга, на захтев овлашћеног лица ЈКП Шумадија Крагујевац:

- одобрава и укида права приступа корисницима система (корисник, шифра, ниво приступа),
- доставља активности корисника (лог фајлови) кроз претрагу и преглед записа,
- ажурира лозинке."

Додатно је наведено и да су менаџер за безбедност информација и систем администратор дужни су да редовно прате реализацију ових процеса и поштовање сигурносних политика и уговорених обавеза испоручилаца и да о свим инцидентима и нарушавању обавеза и правила информишу руководство, без одлагања). Управљање опремом прописано је упутствима ИУ.25.01 Безбедност преносивих компјутера и телефона, ИУ 25.03 Складистење података, ИУ 25.07 Поступање са медијумима и ИУ.25.12 Управљање опремом. Рад на даљину је регулисан са упутством ИУ.25.05 Одобравање права приступа базама података и ИУ.25.01 Безбедност преносивих компјутера и телефона.

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

Уговор о набавци услуга изнајмљивања и имплементације информационог система за контролу и управљање јавним превозом у реалном времену и изнајмљивање опреме за аутоматску наплату превоза од 01.02.2024.

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.3. ЈКП Шумадија Крагујевац није у плану континуитета пословања предвидело управљање резервним копијама

2.3.1. Опис несврсисходности

ЈКП Шумадија Крагујевац, због недовољно хардверских ресурса, недовољно искуства и стручног знања и обученог ИТ кадра, није у плану континуитета пословања предвидела управљање резервним копијама, што може за последицу имати губитак података.

2.3.2. Исказане мере исправљања (препорука 3)

ЈКП Шумадија Крагујевац је препоручено да успостави свеобухватан план континуитета пословања у ванредним околностима, што подразумева усвајање и имплементацију процедуре за управљање резервним копијама.

Дана 01.02.2024.године закључен је нов Уговор о набавци услуга изнајмљивања и имплементације информационог система за контролу и управљање јавним превозом у реалном времену и изнајмљивање опреме за аутоматску наплату превоза и уоквиру техничке спецификације тачка 2.

"Пружалац услуге је дужан да доставља резервне копије података, на недељном нивоу, које су читљиве у форматима (txt, csv) на локацију коју одреди Наручилац. "

Како је наведено у Извештају о спровођењу препорука, у току је јавна набавка рачунарске и сродне опреме. У јуну 2024.године план је имплементације хардвера за управљање резервним копијама од стране пружаоца услуге.

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

Уговор о набавци услуга изнајмљивања и имплементације информационог система за контролу и управљање јавним превозом у реалном времену и изнајмљивање опреме за аутоматску наплату превоза од 01.02.2024.

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.4. ЈКП Шумадија Крагујевац није у потпуности успоставило управљање ИТ ризицима

2.4.1. Опис несврсисходности

ЈКП Шумадија Крагујевац није у потпуности успоставила управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера. Нарочито када се документација налази у електронском облику.

2.4.2. Исказане мере исправљања (препорука 4)

ЈКП Шумадија Крагујевац је препоручено да успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

Донет је План третмана ризика у ЈКП Шумадија Крагујевац за период јануар – децембар 2024.године. У ЈКП Шумадија је успостављана процедура која третира управљање ризицима и дефинисана је са ИП.00.08 Управљање ризиком, а одговорност за њену примену поред директора и представника руководства – носилац појединачног процеса, у конкретном случају руководилац јавног транспорта путника. У наведеној процедури су дефинисани Анализа ризика, као систематски процес разумевања природе и нивоа ризика, као и Оцена ризика као процес који обухвата идентификацију, анализу и вредновање ризика.

ИТ ризици су препознати и у стандарду ИСО 27001. ИТ ризици су евидентирани , анализирани и класификовани кроз документе Методологија за процену ризика са записима СОА у коме су евидентирани сви записи предузећа, укључујући и записе јавног транспорта путника, у којој су форми сачињени, ко је задужен за њихово архивирање, на којој локацији се налазе, време чувања. За сваки запис је процењен значај информације у смислу поверљивости, расположивости и интегритета. Такође је за сваки запис евидентирана претња која је вреднована кроз ниво претње, евидентирана је потенцијална рањивост и вреднована кроз ниво рањивости и прорачунат је ризик у складу са Контролом из изјаве о применљивости (СОА). Поред тога ризици су евидентирани вредновани и квалификовани кроз запис Информациона имовина са власницима и оценом којом је евидентирана комплетна информациона имовина, укључујући процедуре, пословне процесе, информације (јавне, неповерљиве, интерне, поверљиве, строго поверљиве), хардвер, софтвер, интернет, места рада, неопходни технички сервиси, запослени и нематеријална имовина која је анализирана, вреднована и квалификована у смислу поверљивости, интегритета, доступности, као и вредности информационе имовине.

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

ИЗ.25.03 План третмана ризика 2024

ИП.00.08 Управљање ризиком

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.5. ЈКП Шумадија Крагујевац није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података

2.5.1. Опис несврсисходности

ЈКП Шумадија Крагујевац није у потпуности уредила сарадњу са пружаоцем услуга када је у питању заштита и обрада података, у смислу успостављања механизма којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи, начина на који се прати реализација извршења уговора и на начин прописан Законом о информационој безбедности и Законом о заштити података о личности што за последицу има смањени степен поузданости система.

2.5.2. Исказане мере исправљања (препорука 5)

ЈКП Шумадија Крагујевац је препоручено да уреди сарадњу са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о информационој безбедности и Законом о заштити података о личности.

Како је наведено у Извештају о спровођењу препорука, у току спровођења ревизије, ЈКП Шумадија Крагујевац је у септембру 2023. године са пружаоцем услуге Кенткарт потписао Уговорне клаузуле у вези са радњама обраде података о личности. Такође, како су навели из ЈКП Шумадија Крагујевац поред већ до сада да уређене сарадње са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о информационој безбедности и Законом о заштити података о личности, која се огледа у обавезној тачки уговора која регулише ово осетљиво питање, активноси лица за заштиту података о личности, план је да служба јавног транспорта путника у сарадњи са правном службом и лицем за заштиту података о личности сачини и додатну клаузулу о поверљивости са Апексом. Као модел може да послужи клаузула о поверљивости информација коју предузеће има са Сименсом.

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

Уговор о набавци услуга изнајмљивања и имплементације информационог система за контролу и управљање јавним превозом у реалном времену и изнајмљивање опреме за аутоматску наплату превоза од 01.02.2024.

04 Уговорне клаузуле у вези са радњама обраде података о лицности - кенткарт соутхеаст еуропе

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.6. ЈКП Шумадија Крагујевац нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга

2.6.1. Опис несврсисходности

ЈКП Шумадија Крагујевац нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга што за последицу може имати отежану наплату, отежану и/или онемогућену контролу месечних карата, онемогућено праћење ГПС сигнала возила, отежан обрачун за плаћање услуга превозницима и онемогућено пружање услуга грађанима у смислу информисања и допуне картица у дужем временском периоду.

2.6.2. Исказане мере исправљања (препорука 6)

ЈКП Шумадија Крагујевац је препоручено да успостави план континуитета пословања у случају раскида сарадње са пружаоцима услуга, у смислу усвајања плана, и његове имплементације након тога.

Дана 01.02.2024.године закључен је нов Уговор о набавци услуга изнајмљивања и имплементације информационог система за контролу и управљање јавним превозом у реалном времену и изнајмљивање опреме за аутоматску наплату превоза и уоквиру техничке спецификације тачка 15.став 3

"У случају раскида уговора од стране пружаоца услуга, пружалац услуга је у обавези да у периоду од наредних 90 дана омогући несметано функционисање имплементираног система, а све у складу са чланом 29. Уредбе о ближем уређењу мера заштите информационо комуникационих система од посебног значаја(„Службени гласник РС“ бр. 94 од 24. новембра 2016.г."

Такође, наведено је да је ЈКП Шумадија Крагујевац успоставила план континуитета пословања и он је документован у оквиру процедуре ИП.25.06 План пословног континуитета, ако и припадајућим записима ИЗ.25.05 - Извештај о инциденту и ИЗ.25.55 – Одлука о именовању Тима за ванредне ситуације

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

Уговор о набавци услуга изнајмљивања и имплементације информационог система за контролу и управљање јавним превозом у реалном времену и изнајмљивање опреме за аутоматску наплату превоза од 01.02.2024.

ИП.25.06 План пословног континуитета

ИЗ.25.05 - Извештај о инциденту

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.7. ЈКП Шумадија Крагујевац није у потпуности уредило процес наплате карата и механизам контроле тог процеса

2.7.1. Опис несврсисходности

ЈКП Шумадија Крагујевац није у потпуности процедурама и другим актима уредила процес наплате карата и механизам контроле тог процеса, што за последицу може имати неусклађеност података о броју продатих карата које приказује апликација са подацима превозника, који врше продају карата.

2.7.2. Исказане мере исправљања (препорука 7)

ЈКП Шумадија Крагујевац је препоручено да процедурама и другим актима уреди процес наплате карата и механизам контроле тог процеса.

Како је наведено у Извештају о спровођењу препорука, у плану је припрема нове процедуре у систему финансијског управљања и контроле (ФУК) ЈКП Шумадија Крагујевац , и усвајање процедуре од Радне групе за ажурирање и развој система Фук-а.

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.8. ЈКП Шумадија Крагујевац није у потпуности уредило контролу пружених услуга од стране ангажованих превозника.

2.8.1. Опис несврсисходности

ЈКП Шумадија Крагујевац није у потпуности процедурама и другим актима уредила контролу пружених услуга од стране ангажованих превозника, што за последицу може имати плаћање услуга у износу вишем од износа који је заснован на стварно реализованим услугама.

2.8.2. Исказане мере исправљања (препорука 7)

ЈКП Шумадија Крагујевац је препоручено да процедурама и другим актима уреди контролу пружених услуга од стране ангажованих превозника.

Дана 01.12.2023.године закључен је нов Уговор о јавно-приватном партнерству за обављање комуналне делатности јавног градског и приградског превоза путника на територији Града Крагујевца између Града Крагујевца и превозника, на десет година.

Уговор о пружању услуге праћења и контроле јавног градског и приградског превоза путника поверен је ЈКП Шумадија Крагујевац.

Како је наведено у Извештају о спровођењу препорука, у плану је усвајање новеажуриране процедуре за праћење извршења уговорених обавеза од Радне групе за ажурирање и развој система Фук-а.

***Докази**:*

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији од 27. марта 2024. године

Уговор о пружању услуге праћења и контроле јавног градског и приградског превоза путника између Града Крагујевца и ЈКП Шумадија Крагујевац

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

3. МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА

Прегледали смо одазивни извештај, који је поднео субјект ревизије. Оценили смо да је одазивни извештај, који је потписало и печатом оверило одговорно лице субјекта ревизије, веродостојан.

Вредновање мера исправљања смо оценили на основу њиховог описа и достављене документације (акционог плана субјекта ревизије којим су планиране активности на отклањању откривених неправилности/несврсисходности). Сматрамо да смо добили довољне и одговарајуће доказе да можемо изрећи мишљење да ли су мере исправљања задовољавајуће.

Оцењујемо, да су планиране мере исправљања, наведене у акционом плану и описане у одазивном извештају који је поднео Субјект ревизије задовољавајуће.

Напомена:

У складу са одредбама члана 37. Закона о Државној ревизорској институцији, потребно је да, до истека рока за спровођење препорука, обавештавате Државну

ревизорску институцију о предузетим мерама и активностима на отклањању откривених несврсисходности и доставите одговарајуће доказе.

По истеку три године Државна ревизорска институција ће утврђивати ефекте остварене након спровођења препорука и отклањања откривених несврсисходности. У ове ефекте укључиће се и ефекти које сте исказали предузетим мерама и активностима из одазивног извештаја.

Генерални државни ревизор

_____

Др Душко Пејовић

Државна ревизорска институција

Макензијева 41

11000 Београд, Србија

22. мај 2024. године