Ревизија сврсисходности пословања

Управљање информационим системима у јавним предузећима за обједињену наплату

Разлози:

Претходне ревизије финансијских извештаја и правилности пословања утврдили су:

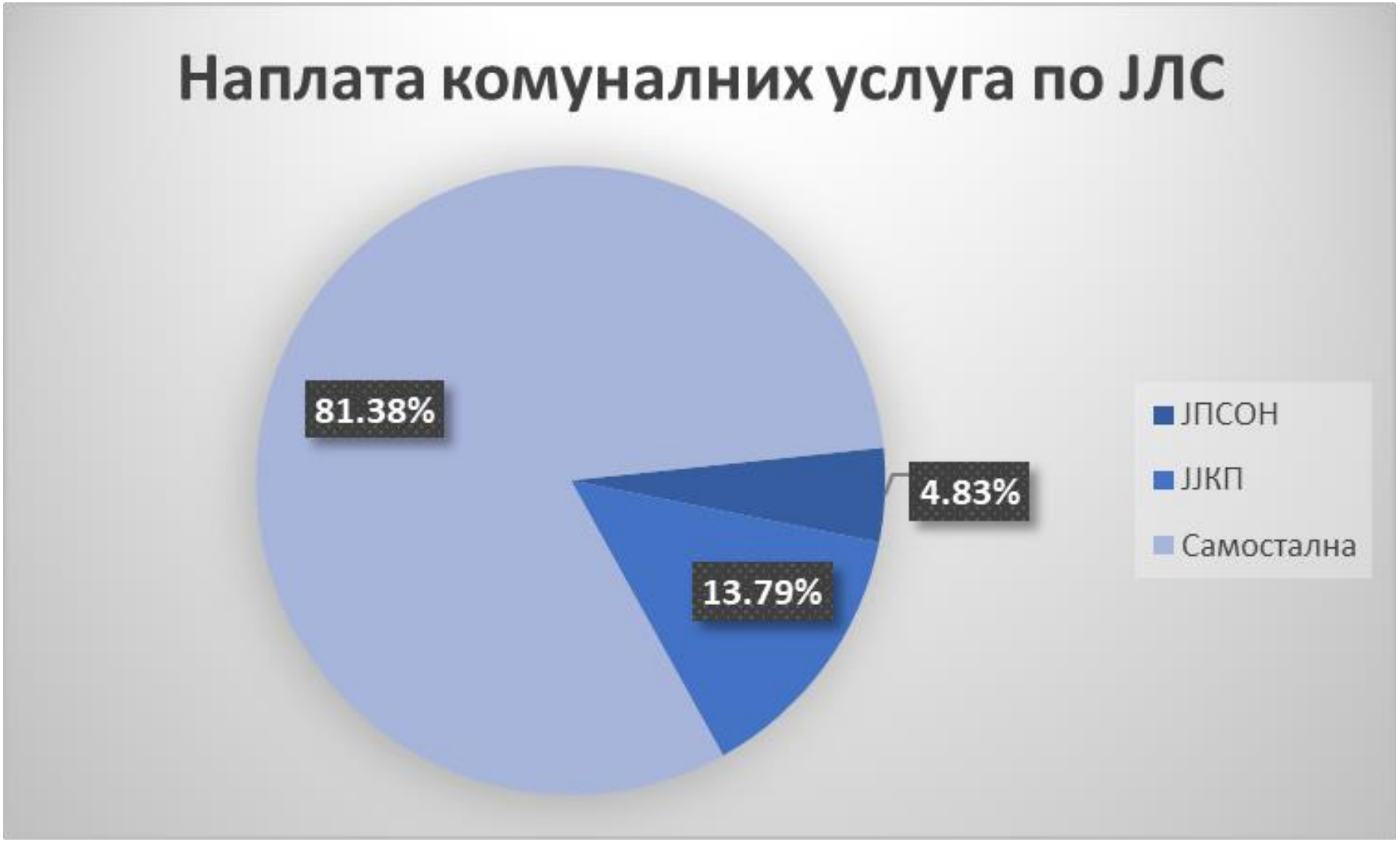
- Неусклађености евиденција пружалаца услуга и предузећа за обједињену наплату комуналних услуга;
- Недостатак организационих и техничких капацитета;
- Мањкавости рачунарске апликације;
- Малог броја обучених корисника, итд;

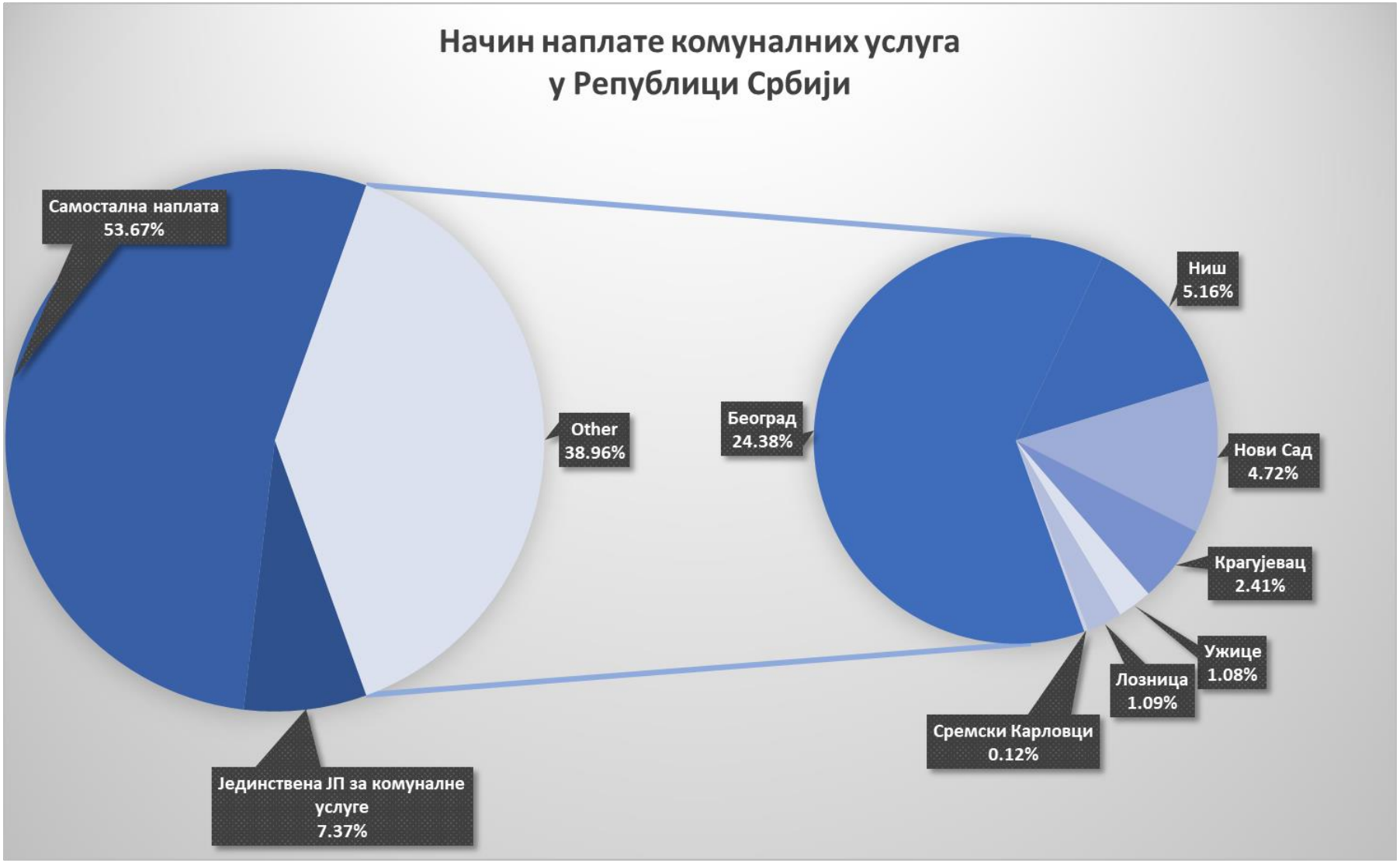
- Обавезе из Закона о информационој безбедности;
- Обавезе из Закона о заштити података о личности;

- Интерес грађана у многим градовима и општинама да обједине наплату.

Циљ:

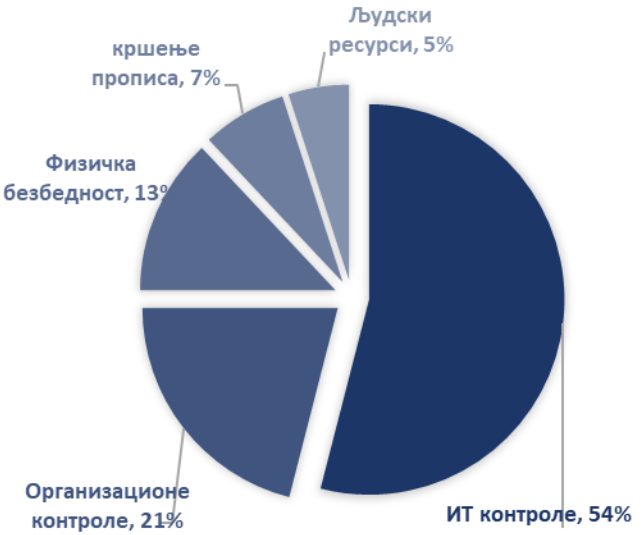
Оценити да ли опште ИТ контроле и апликативне контроле спречавају, откривају и отклањају неефикасности у управљању информационим системом јавног предузећа за обједињену наплату комуналних услуга.


Наплата комуналних услуга по ЈЛС
81.38%
4.83%
13.79%
ЈПСОН
ЈЈКП
Самостална

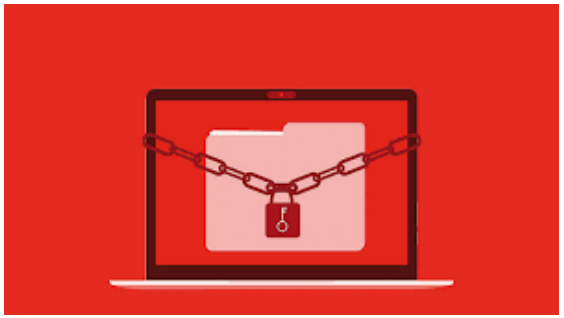

Начин наплате комуналних услуга
у Републици Србији
Самостална наплата
53.67%
Other
38.96%
Јединствена ЈП за комуналне услуге
7.37%
Београд
24.38%
Ниш
5.16%
Нови Сад
4.72%
Крагујевац
2.41%
Ужице
1.08%
Лозница
1.09%
Сремски Карловци
0.12%

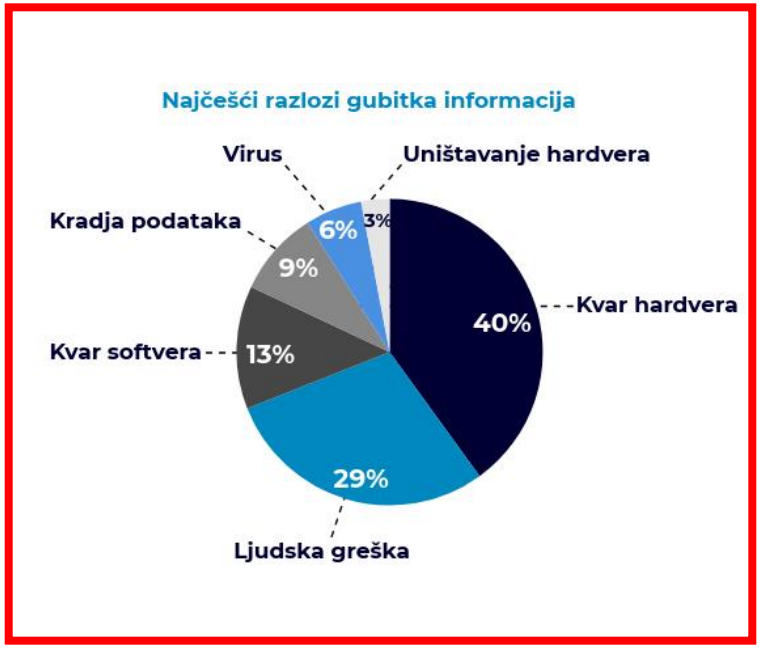
Преглед ИТ области

Област/домени	Ниво ризика	Напомена
ИТ управљање	Средњи	У фази планирања утврђено непостојање стратешких планова остварења пословних циљева и излагању ризику за безбедност информација.
Развој и набавка	Низак	Самостални развој апликације дуже од 40 година, унапређење и усклађивање апликације са прописима и другим захтевима.
ИТ операције	Средњи	Вишегодишње искуство у организованом решавању рекламација из облигационог домена довело је до недостатка процене утицаја на пословање и многи елементи оперативног управљања пате од недостатака.
Ангажовање добављача	Низак	Кључне процесе организују ангажовањем запослених у предузећу и пословно знање остаје у пословној организацији са обавезом подмлађивања развојног тима.
Планови континуитета пословања и опоравка од хаварије	Висок	Учестали **прекиди у пословању** услед дејства природних узрока и више силе погубно делује на пословне резултате. Услуге обрачуна и наплате су оне које се морају испоручити како би се осигурао континуитет пословања, избегло изазивање губитка и испуњавање законских или других обавеза. Ако ове услуге буду прекинуте у дужем временском периоду, то ће довести до финансијских и других губитака. Ако је опоравак од хаварије критичних функција компромитован, континуитет пословања ће бити угрожен. Ако улоге и одговорности нису јасне и разумљиве од стране одговарајућег кадра, добар план такође може постати неефикасан. Планови морају бити спроводљиви са расположивим ресурсима, периодично тестирани и сви недостаци документовани и отклоњени.
Информациона безбедност	Висок	Корисници комуналних 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 довести недозвољеног **модификовања/брисања** података и дати **погрешан резултат** без обзира што постоји обрада рекламација. Непостојање контрола обраде настају услед **погрешног мапирања** пословних правила, неадекватних **тестирања кода** програма, или **лоших контрола** над различитим верзијама програма за враћање интегритета обраде након неочекиваног прекида. Непостојање контрола излазних података доводе до ризика стварања **погрешних извештаја** о управљању и кршења поверљивости података. Стални **грешке у подацима** имају далекосежне последице по апликацију, с обзиром да подаци могу да се користе за велики обим трансакција у апликацији.



1. *Скупови података у систему обједињене наплате*



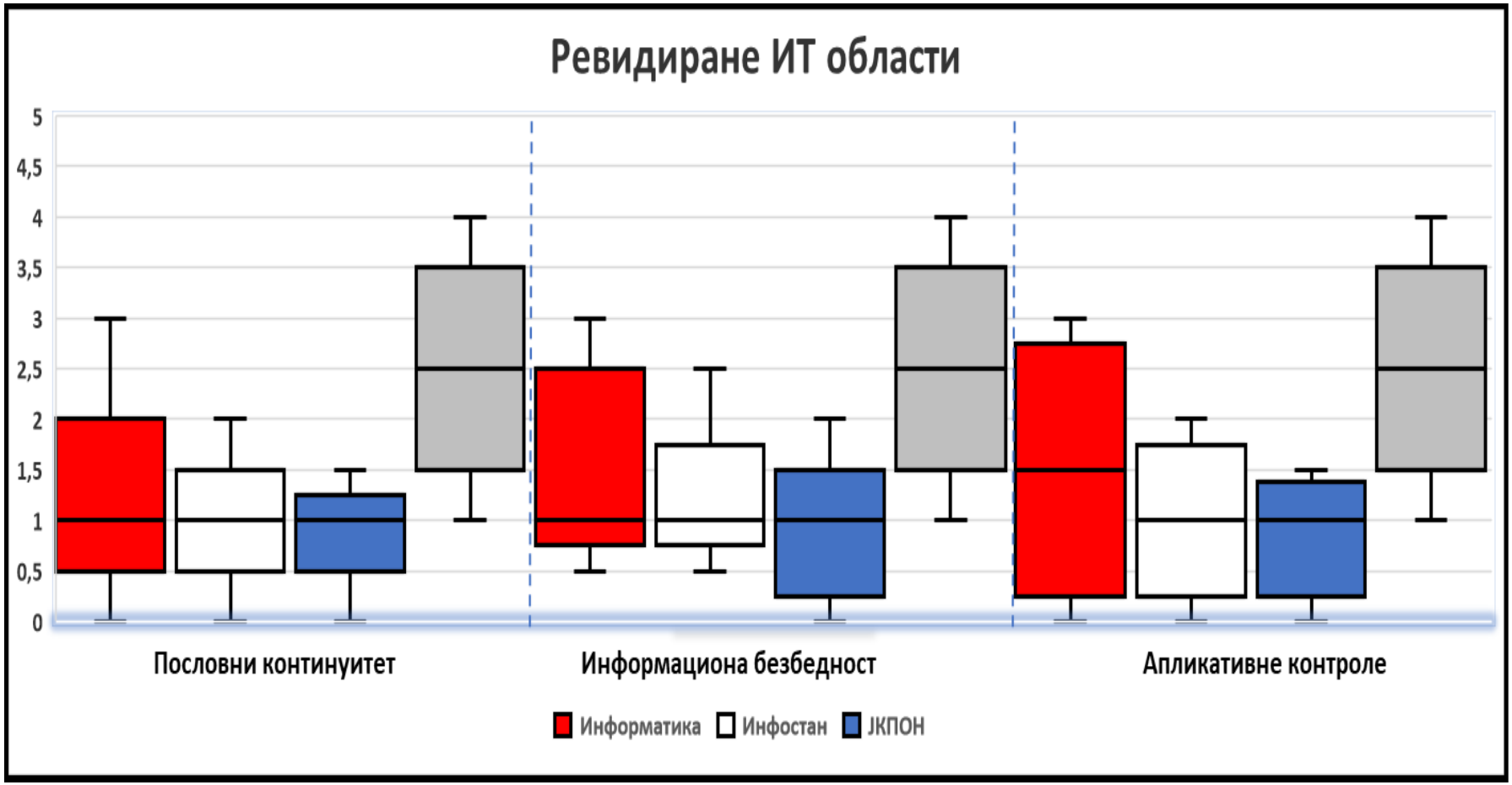


ЈКП „Инфостан технологије“ Београд [1977]

ЈКП „Информатика“ Нови Сад [1994/1971]

ЈКП „Обједињена наплата“ Ниш [2003/1983]

НЕОПХОДНО УНАПРЕЂЕЊЕ УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМИМА У ЈКП ЗА ОБЈЕДИЊЕНУ НАПЛАТУ РАДИ СПРЕЧАВАЊА ПОСЛЕДИЦА НЕЖЕЉНИХ ДОГАЂАЈА



ЗАКЉУЧАК 1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису успоставили ефективан план континуитета пословања и план опоравка од хаварије.

- Налаз 1.1: Субјекти ревизије нису препознали и дефинисали значајне **ИТ ризике**, а што може негативно утицати на управљање информационим системима;
- Налаз 1.2: Субјекти ревизије нису вршили процену **утицаја на пословање** ни за препознате ризике, а што може негативно утицати на управљање информационим системима;
- Налаз 1.3: Субјекти ревизије немају планове за **ванредне ситуације**, јер оснивач није својим планом дефинисао задатке и обавезе за ове ЈКП, што може довести до штете и губитака;
- Налаз 1.4: Субјекти ревизије немају свеобухватне **планове опоравка** од хаварије информационог система којим би дефинисали тај процес, иако поседују знање и искуство у превазилажењу хаваријских догађаја;
- Налаз 1.5: ЈКПОН-Ниш није интерним актом уредила успостављени процес израде **резервних копија** података што може довести до неадекватног поступања у случају кадровске промене.

ЗАКЉУЧАК 2: Управљање безбедношћу информационих система није потпуно адекватно, јер није успостављено управљање инцидентима.

- Налаз 2.1: Субјекти ревизије поседују **Акт** којим уређују питања у вези информационе безбедности;
- Налаз 2.2: Субјекти ревизије нису успоставили **управљање инцидентима**;
- Налаз 2.3: Субјекти ревизије нису донели и спровели план комуникације у вези **сајбер претњи**;
- Налаз 2.4: У ЈКПОН-Ниш нису документоване **изјаве** запослених у вези преузимања одговорности;
- Налаз 2.5: Иако субјекти ревизије поседују минималну потребну опрему за онемогућавање неовлашћеног мрежног приступа они не врше редовно **преглед** покушаја упада у мрежу;

ЗАКЉУЧАК 3: Поред постојећих општих и апликативних контрола улаза, обрачуна и излаза података, неопходно је обезбедити аутоматизовано усаглашавање, као и додатне заштитне механизме.

- Налаз 3.1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису обезбедили усаглашавање података на **аутоматизован** начин;
- Налаз 3.2: Субјекти ревизије нису применили **заштитни механизам** који обезбеђује обраду података унетих само употребом апликације;
- Налаз 3.3: ЈКП „Инфостан технологије“ Београд није обезбедио избор датума **последње измене** као критеријум за извештавање;
- Налаз 3.4: Структура базе података није у довољној мери усклађена са прописаним обавезама мера заштите (**псеудонимизације**) личних података корисника у информационом систему.

Државна ревизорска институција дала је 34 препоруке ЈКП „Информатика“ Нови Сад, ЈКП „Инфостан технологије“ Београд и ЈКП „Обједињена наплата“ Ниш да:

Препорука	Пр.	Субјект
донесу План пословног континуитета	2	БГ, НИ
ИТ ризике уврсте у Регистар	1	НС, БГ, НИ
врше процену утицаја ризика на пословање	2	НС, БГ, НИ
израде План за ванредне ситуације (ПОКРЕТАЊЕ ИНИЦИЈАТИВЕ)	1	НС, БГ, НИ
израде Планове опоравка од хаварије	2	НС, БГ, НИ
израде свеобухватни План израде резервних копија података	1	НИ
успоставе процес управљања инцидентима	2	НС, БГ, НИ
успоставе процес обавештавања и обучавања запослених о сајбер претњама	1	НС, БГ
обезбеди да сви запослени потпишу изјаву да су упознати са обавезама у вези налога	1	НИ
превентивно врше редовни преглед журнала на опреми ИС	2	НС, БГ
обезбеде системе за аутоматско усклађивање евиденција са пружаоцима комуналних услуга	3	БГ, НИ
обезбеде заштитне механизме за податке који се преносе кроз комуникационе канале	3	БГ, НИ
обезбеде заштитне механизме који ће осигурати да апликација обрађује само податке унетих употребом апликације	3	НС, БГ, НИ
да приликом израде извештаја омогуће избор датума последње измене из претходног извештајног периода	3	БГ
израде Процену утицаја обраде на личне податке и план имплементације псеудонимизације личних података корисника	3	НС, БГ, НИ

ХВАЛА НА ПАЖЊИ!

kancelarija@dri.rs

www.dri.rs