ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

ИЗВЕШТАЈ

О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

ЕФЕКТИВНОСТ ИНФОРМАЦИОНОГ СИСТЕМА СОЦИЈАЛНА КАРТА У МИНИСТАРСТВУ ЗА РАД, ЗАПОШЉАВАЊЕ, БОРАЧКА И СОЦИЈАЛНА ПИТАЊА, БЕОГРАД

Број: 400-58/2024-07/21
Београд, 20. август 2024. године

ПОТРЕБНО ЈЕ ДА МИНИСТАРСТВО ИЗВРШИ ПУНУ ИМПЛЕМЕНТАЦИЈУ ИС СОЦИЈАЛНА КАРТА, УРЕДИ ОДНОС СА ПРУЖАОЦЕМ УСЛУГЕ И УЗ ЈАЧАЊЕ КАДРОВСКИХ КАПАЦИТЕТА У СЕКТОРУ ЗА ИТ, УНАПРЕДИ ИТ УПРАВЉАЊЕ, ОБЕЗБЕДИ ПЛАН КОНТИНУИТЕТА ПОСЛОВАЊА И ПОБОЉША ИТ БЕЗБЕДНОСТ

Циљ успостављања Социјалне карте је постојање јединствене и централизоване евиденције, у електронском облику која садржи тачне и ажурне податке о социјално-економском статусу појединца и са њим повезаних лица и која омогућава корисницима података да обављају послове обраде података ради утврђивања чињеница неопходних за остваривање права и услуга из области социјалне заштите. Најважнији проблеми у примени информационог система Социјална карта су: непотпуна имплементација, незавршена интеграција са Системом за заштиту и аутоматизацију инструмената социјалне заштите (СОЗИС), информациона безбедност и континуитет пословања у случају нежељених догађаја.

[1]

Министарство не управља информационим технологијама на одговарајући начин због непостојања плана развоја информационих технологија, недовољних кадровских капацитета и употребе великог броја информационих система. Информациони систем Социјална карта није у потпуности имплементиран, а поред недостатака у апликативним контролама, нису ни сви предвиђени корисници укључени у информациони систем Социјална карта.

Министарство није успоставило свеобухватне мере којима се обезбеђује континуитет пословања у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања информационог система Социјална карта, укључујући и управљање резервним копијама.

Министарство није успоставило управљање информационом безбедношћу на свеобухватан начин, јер није ускладило Акт о безбедности информационо-комуникационих система са прописима, као ни организационо и кадровски успоставило управљање информационом безбедношћу, док на нивоу информационог система Социјална карта не постоје правила и процедуре праћења и контроле записа о догађајима (логова) нити сарадње са пружаоцем услуге одржавања, што може довести до нарушавања безбедности ИС.

Препоруке

Државна ревизорска институција је субјекту ревизије (Министарству за рад, запошљавање, борачка и социјална питања) дала 11 препорука од којих су најважније следеће:

- да омогући приступ ИС Социјална карта и другим (предвиђеним) корисницима у складу са одредбама Закона о социјалној карти, потписаним Споразумом са Канцеларијом за ИТ и електронску управу, или на други адекватан начин;

- да отклоне уочене недостатке у апликативним контролама информационог система Социјална карта и да прецизно дефинишу активности надзора и контроле решавања нотификација у коришћењу ИС Социјална карта;

- да успостави свеобухватно управљање резервним копијама података што подразумева активности на обуци кадрова и проверу исправности резервних копија података у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације;

- да успостави механизам редовног праћења и контроле записа о догађајима (логова) на нивоу целокупног ИС Социјална карта;

- да уреди однос са пружаоцем услуге одржавања ИС Социјална карта у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

[1] Извор за слику: ДРИ.

Садржај

прописима, као ни организационо и кадровски успостављено управљање информационом безбедношћу, док на нивоу ИС Социјална карта не постоје правила и процедуре праћења и контроле записа о догађајима (логова) нити сарадње са пружаоцем услуге одржавања, што може довести до нарушавања безбедности ИС. 51

Скраћенице и термини

У прегледу су дате скраћенице које су коришћене у извештају:

Пун назив	Скраћеница
Министарство за рад, запошљавање, борачка и социјална питања	Министарство
Центри (Центар) за социјални рад	ЦСР
Државна ревизорска институција	ДРИ
Информациони систем	ИС
Информационо-комуникациони системи од посебног значаја	ИКТ системи
Јединствени регистар Социјална карта	ИС Социјална карта
Конкурсна документација	КД
Канцеларија за информационе технологије и електронску управу	Канцеларија за ИТ и електронску управу
Систем за заштиту и аутоматизацију инструмената социјалне заштите	ИС СОЗИС
Апликација за новчану социјалну помоћ (евиденција корисника, обрачун исплата)	ИС НСП
Апликативни софтвер за дечије и родитељске додатке и породиљско одсуство (подршка Закону о финансијској подршци породици са децом)	ИС ДД-РД
Апликација за помоћ и негу другог лица (евиденција корисника, обрачун исплата)	ИС ТНП
Апликација за смештај лица у хранитељске породице и установе (евиденција корисника, обрачун исплата)	ИС Смештај у установе
Апликација за посебну новчану накнаду	ИС ПНН
Софтвер за јединствену матичну евиденцију и исплату права корисника у области борачко-инвалидске заштите	ИС Борачке заштите
Јединствени матични број грађанина	ЈМБГ
Јединица локалне самоуправе	ЈЛС
Централни регистар обавезног социјалног осигурања	ЦРОСО
Пореска управа	ПУ
Аутономна покрајина	АП

I Резиме извештаја

1. Резиме и препоруке

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Ефективност информационог система Социјална карта у Министарству за рад, запошљавање, борачка и социјална питања“.

ИС Социјална карта представља јединствену и централизовану евиденцију у електронском облику која садржи тачне и ажурне податке о социјално-економском статусу појединца и са њим повезаних лица и која омогућава корисницима података да обављају послове обраде података ради утврђивања чињеница неопходних за остваривање права и услуга из области социјалне заштите[2].

Циљ ревизије је да се оцени ефективност ИС Социјална карта у Министарству.

Након спроведене ревизије сврсисходности пословања утврдили смо следеће:

Неопходно је да Министарство за рад, запошљавање, борачка и социјална питања унапреди ИТ управљање, обезбеди континуитет пословања (и у случају прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта) и обезбеди виши ниво информационе безбедности ИС Социјална карта.

Наведено заснивамо на закључцима и налазима који су изложени у наставку текста:

1. Министарство не управља информационим технологијама на одговарајући начин због непостојања плана развоја ИТ, недовољних кадровских капацитета и употребе великог броја ИС.
   - ✓ Министарство није успоставило адекватну организациону структуру за ИТ управљање, како у смислу кадровских капацитета тако и нивоа стручног знања запослених на тим пословима.
   - ✓ Министарство није успоставило стратешко ИТ планирање, јер није донело план развоја ИТ и управљање ризицима, а нарочито имајући у виду значај ИС Социјална карта.
   - ✓ Министарство није извршило пуну имплементацију ИС Социјална карта, јер поред недостатака у апликативним контролама, није омогућило да сви предвиђени корисници буду укључени у ИС Социјална карта.
2. Министарство није успоставило свеобухватне мере којима се обезбеђује континуитет пословања, у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта, укључујући и управљање резервним копијама.
   - ✓ Министарство није успоставило план континуитета пословања у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта.
   - ✓ Министарство не врши свеобухватно управљање резервним копијама зато што није обезбедило обуку запослених и тестирање резервних копија података.
3. Министарство није успоставило управљање информационом безбедношћу на свеобухватан начин, јер није ускладило Акт о безбедности са прописима, као ни организационо и кадровски успоставило управљање информационом безбедношћу, док на нивоу ИС Социјална карта не постоје правила и процедуре праћења и контроле

[2] Део члана 3 Закона о социјалној карти.

записа о догађајима (логова) нити сарадње са пружаоцем услуге одржавања, што може довести до нарушавања безбедности ИС.

- ✓ Акт о безбедности ИКТ система Министарства није усклађен са Законом о информационој безбедности, променама у окружењу и са ИКТ системом Социјална карта.
- ✓ Министарство није у потпуности успоставило организацију ИТ безбедности у смислу обезбеђивања одговарајућих организационих и кадровских капацитета.
- ✓ Министарство није успоставило механизам за редовно праћење и контролу записа о догађајима (логова) на нивоу целокупног ИС Социјална карта.
- ✓ Министарство није уредило управљање ИТ пословима (администрирање система) на начин да те послове обављају искључиво државни службеници.
- ✓ Министарство није успоставило (уредило) однос са пружаоцем услуге одржавања ИС Социјална карта у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

Након спроведене ревизије „Ефективност информационог система Социјална карта у Министарству за рад, запошљавање, борачка и социјална питања", Државна ревизорска институција даје следеће препоруке:

Министарству за рад, запошљавање, борачка и социјална питања:

1. да успостави адекватну организациону структуру за ИТ управљање, укључујући јачање кадровских капацитета и/или стручних знања запослених (приоритет 3[3]) – Налаз 1.1.
2. да одреди приоритете развоја ИТ и успоставе управљање ИТ ризицима што подразумева евидентирање, класификацију, анализу свих ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика (приоритет 2[4]) – Налаз 1.2.
3. да омогући приступ ИС Социјална карта и другим (предвиђеним) корисницима у складу са одредбама Закона о социјалној карти, потписаним Споразумом са Канцеларијом за ИТ и електронску управу, или на други адекватан начин (приоритет 2) – Налаз 1.3.
4. да отклоне уочене недостатке у апликативним контролама информационог система Социјална карта и да прецизно дефинишу активности надзора и контроле решавања нотификација у коришћењу ИС Социјална карта (приоритет 2) – Налаз 1.3.
5. да успостави план континуитета пословања што подразумева усвајање и имплементацију правила и процедура континуитета пословања у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта (приоритет 2) – Налаз 2.1.
6. да успостави свеобухватно управљање резервним копијама података што подразумева активности на обуци кадрова и проверу исправности резервних копија података у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације (приоритет 2) – Налаз 2.2.

[3] Приоритет 3 - Несврсисходности које је могуће отклонити у року до три године.
[4] Приоритет 2 - Несврсисходности које је могуће отклонити у року до годину дана.

7. да Акт о безбедности ИКТ система усклади са одредбама Закона о информационој безбедности и да усвоји и имплементира процедуре постизања и одржавања адекватног нивоа безбедности ИС Социјална карта (приоритет 2) – Налаз 3.1.
8. да предузме мере на организационом и кадровском успостављању информационе безбедности, кроз јачање кадровских капацитета и обуку запослених у циљу обављања послова заштите безбедности информационих система (приоритет 2) – Налаз 3.2.
9. да успостави механизам редовног праћења и контроле записа о догађајима (логова) на нивоу целокупног ИС Социјална карта (приоритет 3) – Налаз 3.3.
10. да за послове из делокруга органа државне управе, односно администраторе система ИС Социјална карта именује искључиво лица запослена у Министарству за рад, запошљавање, борачка и социјална питања (приоритет 1[5]) – Налаз 3.4.
11. да уреди однос са пружаоцем услуге одржавања ИС Социјална карта у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом (приоритет 2) – Налаз 3.5.

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

Захтев за достављање одазивног извештаја

Министарство за рад, запошљавање, борачка и социјална питања је, на основу члана 40 став 1 Закона о Државној ревизорској институцији, дужно да поднесе 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.

Субјект ревизије је обавезан 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 Министарство за рад, запошљавање, борачка и социјална питања је дужно 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 Министарство за рад, запошљавање, борачка и социјална питања је 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, и трећег приоритета, односно које је могуће отклонити у року до три године, Министарство за рад, запошљавање, борачка и социјална питања је обавезно да достави 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 истинитости навода о мерама исправљања, предузетим од стране субјекта ревизије, подносиоца одазивног извештаја. У случају потребе извршиће се и провера веродостојности 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.

Генерални државни ревизор

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
20. август 2024. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Ефективност информационог система Социјална карта у Министарству за рад, запошљавање, борачка и социјална питања" у периоду од 3. јануара до 20. августа 2024. године.[6] Ревизија сврсисходности пословања је спроведена у складу са Законом о Државној ревизорској институцији[7], Пословником Државне ревизорске институције[8] и Програмом ревизије Државне ревизорске институције за 2024. 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

Министарство је на основу Програма о раду Владе из 2017.[9] и 2020.[10] године, Програма развоја електронске управе у Републици Србији 2020-2022. године са припадајућим акционим планом[11], Програма развоја електронске управе у Републици Србији 2023-2025. године са припадајућим акционим планом[12], Закона о социјалној карти[13] и Правилника о ближим техничким условима успостављања и вођења Социјалне карте[14], успоставило Јединствени регистар Социјалне карте.

Циљ успостављања Социјалне карте је постојање јединствене и централизоване евиденције, у електронском облику која садржи тачне и ажурне податке о социјално-економском статусу појединца и са њим повезаних лица и која омогућава корисницима података да обављају послове обраде података ради утврђивања чињеница неопходних за остваривање права и услуга из области социјалне заштите, а посебно ради ефикаснијег остваривања права и услуга социјалне заштите, праведније расподеле социјалне помоћи, унапређења ефикасности и проактивности рада органа у области социјалне заштите, обезбеђивања подршке у дефинисању и обликовању социјалне политике и праћења укупних ефеката мера социјалне заштите, као и обезбеђивање ажурних података о корисницима за случај ванредне ситуације.[15]

Повезивање Социјалне карте са регистрима и евиденцијама из члана 15 Закона о социјалној карти извршена је до 1. јануара 2022. године, а примена Јединственог регистра Социјалне карте отпочела је 4. априла 2022. године.

---

[6] Број ревизије: 400-58/2024-07.
[7] „Службени гласник РС", бр. 101/05, 54/07, 36/10 и 44/18-др. закон.
[8] „Службени гласник РС", број 9/09.
[9] https://media.srbija.gov.rs/medsrp/dokumenti/ekspoze-mandatarke-ane-brnabic280617_cyr.pdf, страна 61, поднаслов: „Боље таргетирана социјална заштита".
10 https://rsjp.gov.rs/wp-content/uploads/Ekspoze-2020.pdf, страна 41, наслов: „3.7.3. Социјална политика".
[11] „Службени гласник РС", бр. 85/20.
[12] „Службени гласник РС", бр. 33/23.
[13] „Службени гласник РС", бр. 14/21.
[14] „Службени гласник РС", бр. 67/21.
[15] Члан 3 Закона о социјалној карти.

Најважнији проблеми у досадашњој примени ИС Социјална карта су следећи:

1) *недовршена примена ИС Социјална карта*, која је тренутно у фаза интеграције са ИС СОЗИС , ИС ДД-РД и ИС Борачка и инвалидска заштита.

2) *велики број корисника ИС Социјална карта*
Администратори и корисници су ЦСР, јединице локалне самоуправе које обављају поверене послове, надлежни органи аутономне покрајине за спровођење социјалне заштите, надлежни републички орган за спровођење активности унапређења социјалне заштите и други органи државне управе и институције[16].

3) *завршена имплементација само I фазе ИС СОЗИС*[17], која се односи на електронску архиву и процесе рада у ЦСР. Друга фаза још није завршена и односи се на финансијски модул, извештавање и повезивање са исплатама права (Банком Поштанска штедионица и Управом за трезор)[18].

4) *синхронизација података са софтверским (под)системима којима управља Министарство*.

5) *Подаци се воде у различитим информационим подсистемима (за различита права)* и не постоје на нивоу Министарства укрштени упоредиви подаци за сваког појединца о свим новчаним примањима и услугама из области социјалне заштите које остварује, начину на који их остварује, па самим тим ни о укупним новчаним средствима и услугама које остварује[19].

6) *поузданост ИС*
Информациона безбедност (физички и логички приступ систему од стране запослених у Министарству и ЦСР, приступ систему и базама података од стране пружаоца услуга одржавања система, управљање лог фајловима и инцидентима, посебно у делу личних података корисника права).

7) *континуитет пословања у случају нежељених догађаја*
Како се провера социо-економског статуса појединца врши употребом информационих система, неопходно је обезбедити функционисање система увек, а то значи и у случају нежељених догађаја.

2. Циљ ревизије

Циљ ревизије је да се оцени ефективност ИС Социјална карта у Министарству.

3. Ревизорска питања

За остварење циља ревизије формулисали смо главно питање и ревизорска питања. Имајући у виду значај који ИС Социјална карта има у оквиру система социјалне заштите, ДРИ се определила да главно питање ревизије буде:

Да ли се на адекватан начин управља ИС Социјална карта Министарства за рад, запошљавање, борачка и социјална питања?

[16] члан 11 Закона о социјалној карти.
[17] Који треба да обједини све обрачуне и исплате права из социјалне заштите.
[18] Белешка са састанка са представником Министарства за рад, запошљавање, борачка и социјална питања.
[19] Образложење Закона о социјалној карти.

Примењујући Методолошка правила и смернице за ревизију сврсисходности пословања извршили смо декомпозицију главног питања на три аспекта и три ревизорска питања. 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.

Да бисмо одговорили на главно питање, испитивали смо:

1. На који начин се управља информационим технологијама у Министарству за рад, запошљавање, борачка и социјална питања?
2. У којој мери је успостављено управљање континуитетом пословања ИС Социјална карта у случају ванредних околности, хаварија и евентуалног раскида уговора са пружаоцем услуге развоја и одржавања ИС?
3. Да ли успостављене мере информационе безбедности обезбеђују поузданост ИС Социјална карта?

4. Обим и ограничења ревизије

Ревизијом смо обухватили три ИТ области у Министарству за период од 1. јануара 2022. године до 31. децембра 2023. године.

Предмет испитивања је било:

1) ИТ управљање - подразумева ИТ операције у организацији како би се обезбедило да организација задовољава потребе пословања у садашњости и да укључује планове за будуће потребе и развој. Основна улога ИТ управљања је да обезбеди: да ИТ систем одговара пословним потребама; да планира будуће промене на систему; да обезбеди неопходан ниво интерних контрола; да има одговарајућу организациону структуру и прецизно дефинисане описе послова запослених на ИТ пословима; и да примењује неопходне политике и процедуре који се односе на ИТ систем;[20]

2) Сарадња са пружаоцем услуге подразумева сарадњу са добављачем услуга развоја и одржавања ИС. Главна питања су ИТ безбедност у делу сарадње са пружаоцем услуге одржавања ИС Социјална карта, заштита и поверљивост података и ризик од непродужења/отказа уговора од стране пружаоца услуге. План континуитета пословања (енг. business continuity plan – BCP) и План опоравка од хаварије (енг. disaster recovery - DRP). BCP је процес који организација користи за планирање и тестирање опоравка својих пословних процеса након поремећаја. Такође описује како ће организација наставити да функционише у неповољним условима који могу настати (на пример, природне или друге несреће).[21]

3) 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[22].

[20] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).
[21] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).
[22] Члан 7 став 3 Закона о информационој безбедности.

У поступку ревизије нисмо испитивали:

- Да ли финансијски извештаји Министарства истинито и објективно приказују њихово финансијско стање, резултате пословања и новчане токове, у складу са прихваћеним рачуноводственим начелима и стандардима;
- Финансијске трансакције и одлуке Министарства 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.

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[23]), као и све податке добијене од Министарства. Анализирали смо податке и информације за период од 2022. до 2023. године.

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

Приручником[24] је предвиђена оцена сложености ИС и могућност избора области за испитивање (ревизију) и то: ИТ управљање; развој и набавка; ИТ операције; Сарадња са пружаоцима услуга; Планови континуитета пословања и опоравка од хаварије; Информациона безбедност и Апликативне контроле.

Проценили смо ревизијски ризик и одабрали области за ревизију: ИТ управљање, Сарадња са пружаоцима услуга и Информациона безбедност.

III Опис предмета ревизије

ИС Социјална карта представља јединствену и централизовану евиденцију у електронском облику која садржи тачне и ажурне податке о социјално-економском статусу појединца и са њим повезаних лица. Омогућава корисницима података да обављају послове обраде података ради утврђивања чињеница неопходних за остваривање права и услуга из области социјалне заштите, ефикасније остваривање права, праведнију расподелу социјалне помоћи и унапређење рада органа у области социјалне заштите. Служи ефикаснијем остваривању права и услуга социјалне заштите, праведнијој расподели социјалне помоћи, унапређења ефикасности и проактивности рада органа у области социјалне заштите, обезбеђивању подршке у дефинисању и обликовању социјалне политике и праћењу укупних ефеката мера социјалне заштите, као и обезбеђивања ажурних података о корисницима за случај ванредне ситуације.[25]

[23] INTOSAI Радна група за ИТ ревизију.
[24] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).
[25] Члан 3 Закона о социјалној карти.

1) Законодавни и институционални оквир

Законодавни оквир

Закон о социјалној карти

Закон о социјалној карти је најновији закон из области социјалне заштити који је донет 2021. године, док је његова примена започела 2022. године. Овим Законом се уређује успостављање и вођење јединственог регистра Социјална карта, односно садржина, начин приступања, обрада и чување података у оквиру Социјалне карте, као и друга питања од значаја за његово успостављање и вођење[26].

ИС Социјална карта садржи базу података у којој су обједињени подаци од значаја за социјално-економски статус појединца и породице којој припада, али садржи и алате који треба да омогуће праћење тог статуса на основу података којима се располаже.[27]

У Социјалној карти воде се и обрађују подаци о појединцу и са њим повезаним лицима, у складу са законом којим се уређује заштита података о личности, који су неопходни за утврђивање социјално-економског статуса, односно за остваривање права и услуга из социјалне заштите у складу са законом, као и подаци о оствареним правима и услугама из социјалне заштите које лице користи или је користило, подаци о правима и услугама које су у поступку остваривања и подаци о одбаченим и одбијеним захтевима (неостварена права).[28]

Податке који се обрађују у Социјалној карти користе корисници података у органима надлежним за спровођење социјалне заштите, и то у ЦСР, јединицама локалне самоуправе које обављају поверене послове, Министарству, надлежном органу аутономне покрајине за спровођење социјалне заштите, надлежном републичком органу за спровођење активности унапређења социјалне заштите и другим органима државне управе и институцијама, у складу са законом.

Према одредбама Закона о социјалној карти корисници података обрађују податке о личности у складу са законом којим се уређује заштита података о личности.

Корисници података, у складу са својим надлежностима, приступају и користе Социјалну карту ауторизацијом приступа Социјалној карти или коришћењем података из Социјалне карте преко софтверског решења корисника података на Сервисној магистрали органа или преко Система за размену података. Министарство ће податке из Социјалне карте користити и за редовно ажурирање службених евиденција, које се воде као регистри из надлежности Министарства, као и ради обраде, анализе података и израде извештаја потребних за обављање послова из своје надлежности. [29]

Закон о социјалној заштити

Област социјалне заштите уређена је Законом о социјалној заштити[30] и подзаконским актима донетим од стране министарства надлежног за послове социјалне заштите. Право на социјалну заштиту има сваки појединац и породица којима је неопходна друштвена

[26] Члан 1 Закона о социјалној карти „Службени гласник РС“, бр. 14/21.
[27] Образложење Закона о социјалној карти.
[28] Члан 6 Закона о социјалној карти.
[29] Члан 14 Закона о социјалној карти.
[30] „Службени гласник РС“, бр. 24/11 и 117/22 - одлука УС.

помоћ и подршка ради савладавања социјалних и животних тешкоћа и стварања услова за задовољење основних животних потреба[31].

Одредбама члана 23 ст. 1-3 Закона о социјалној заштити прописано је да се о корисницима, правима која су остварили и услугама које су им пружене води евиденција, у електронском а може и у папирном облику, као и да су установе социјалне заштите и други пружаоци услуга социјалне заштите дужни да чувају документацију корисника, у изворном, а ако је могућно и у електронском облику, као и да је обезбеде од неовлашћеног приступа, умножавања и злоупотребе, независно од облика у коме су подаци из документације сачувани.

Закон о финансијској подршци породици са децом

Законом о финансијској подршци породици са децом[32] прописано је право на накнаду зараде, односно накнаду плате за време породиљског одсуства, одсуства са рада ради неге детета и одсуства са рада ради посебне неге детета, остале накнаде по основу рођења и неге детета и посебне неге детета и родитељски додатак. Одредбом члана 46 став 1 истог закона уређено је да, у циљу аутоматизације обрачуна износа за исплате које корисницима права врши Министарство[33] по основу тог закона, Министарство успоставља Информациони систем за исплату права. На основу унетих података, путем ИС-а води се евиденција поднетих захтева, донетих решења, евиденција доказа прибављених по службеној дужности електронским путем посредством ИС-а, као и подносилаца захтева и чланова њихових домаћинстава.

Закон о правима бораца, војних инвалида, цивилних инвалида рата и чланова њихових породица

Одредбом члана 32 став 1 Законом о правима бораца, војних инвалида, цивилних инвалида рата и чланова њихових породица[34] прописана су права бораца, војних инвалида, цивилних инвалида рата и чланова њихових породица, док је одредбом члана 177 став 1 истог закона прописано да јединствену евиденцију података у електронском облику води Министарство, те да унос података врши првостепени орган, који је одговоран за тачност података. Јединствена евиденција садржи податке о корисницима, остварeним правима, члановима корисниковог домаћинства, приходима корисника и чланова његовог домаћинства (члан 177 став 2 истог закона).

Институционални оквир

Чланом 5 став 1 Закона о социјалној карти уређено је да Министарство успоставља и води Социјалну карту, док је ставом 2 истог члана прописано да послове техничке подршке Министарству у успостављању и одржавању Социјалне карте, односно послове који се односе на чување, спровођење мера заштите и обезбеђивање сигурности и безбедности података у оквиру Социјалне карте, обавља служба Владе која је надлежна за пројектовање, усклађивање, развој и функционисање система електронске управе (Канцеларија за информационе технологије и електронску управу[35]).

[31] Члан 4 став 1 Закона о социјалној заштити.
[32] „Службени гласник РС“, бр. 113/17, 50/18, 46/21 - одлука УС, 51/21 - одлука УС, 53/21 - одлука УС, 66/21, 130/21, 43/23 - одлука УС и 62/23
[33] Надлежно за финансијску подршку породици са децом.
[34] „Службени гласник РС“, бр. 18/20.
[35] Члан 28 тачка 11) Закона о министарствима („Службени гласник РС“, бр. 128/20, 116/22 и 92/23 – др. закон)

Слика број 1: Приказ повезивања Јединственог регистра Социјална карта са софтверским решењима којима управља Министарство и са регистрима/евиденцијама које воде други надлежни органи[36]

Набавка ИС Социјална карта је започета 2018. године, а примена ИС је почела 4. априла 2022. године, на основу Одлуке министра о увођењу Регистра Социјална карта у оперативну употребу[37]. Према информацији добијеној од субјекта ревизије, ИС Социјална карта није у пуној примени (80%), јер је у току интеграција са ИС Борци Србије, ИС ДД РД и ИС СОЗИС.

До сада је у набавку, модификацију и доградњу ИС Социјална карта уложено 656.679.550 динара (погледати Табела број 3).

2) Информациони систем Социјална карта

Дефиниција

ИС Социјална карта представља ИС у коме се, сагласно одредби члана 6 став 1 Закона о социјалној карти, воде и обрађују подаци о појединцу и са њим повезаним лицима, у складу са законом којим се уређује заштита података о личности, који су неопходни за утврђивање социјално-економског статуса, односно за остваривање права и услуга из социјалне заштите у складу са законом, као и подаци о остварeним правима и услугама из социјалне заштите које лице користи или је користило, подаци о правима и услугама које су у поступку остваривања и подаци о одбаченим и одбијеним захтевима (неостварена права).

ИС Социјална карта је намењен да пружи што потпунију слику о социјално-економском статусу појединца, породице (домаћинства) и различитих социјалних група, као и да

[36] Члан 15 Закона о социјалној карти.
[37] Број: 021-01-00021/144/2022-14 од 29. марта 2022. године.

подржи, олакша и делимично аутоматизује поступке и процесе везане за поступање различитих субјеката у области социјалне заштите.[38]

ИС Социјална карта је имплементиран на инфраструктури високих перформанси која је смештена у Државном центру за управљање и чување података у Београду и повезан је на Јединствену информационо-комуникациону мрежу електронске управе.[39]

Слика број 2: Приказ корисничког интерфејса „Подаци о лицу“

ИС Социјална карта приступа се уз претходну електронску идентификацију на Порталу за електронску идентификацију еУправе (еИД), којим управља Канцеларија за ИТ и електронску управу.

ИС Социјална карта се приступа искључиво из Јединствене информационо-комуникационе мреже којом управља Канцеларија за ИТ и из VPN мреже Министарства која је опсегом IP адреса повезана са Јединственом комуникационом мрежом, тако да је искључена могућност приступа са интернета ИС Социјална карта.

Сви корисници ИС Социјална карта морају бити претходно регистровани у ИС Социјална карта.[40]

[38] преузето из КД ЈН 26/2018 - „Набавка Информационог система Социјална карта – I фаза“, стр. 7/125
[39] преузето из КД ЈН 12/2021 – „Набавка регистра Социјална карта – 2.фаза“, стр. 11/74
[40] објашњење преузето из одговора Министарства на тачку 23. Захтева за доставу података, који гласи „23. Извештај (обавештење) администратора Службе Владе у вези са покушајима неовлашћеног приступа ИС Социјална карта – члан 20 став 5 Правилника о ближим техничким условима успостављања и вођења Социјалне карте“.

Слика број 3: Кориснички интерфејс ИС Социјална карта

IV Закључци

У овом поглављу износимо закључке до којих смо дошли спроводећи ревизију сврсисходности на тему „Ефективност информационог система Социјална карта у Министарству за рад, запошљавање, борачка и социјална питања", код субјекта ревизије Министарства за рад, запошљавање, борачка и социјална питања.

Донети закључци представљају одговоре на постављена ревизијска питања, дефинисана у делу извештаја II Увод – 3. Ревизорска питања. Закључци су донети на основу утврђених налаза – сваки закључак је изведен на основу припадајућих налаза.

На основу анализе података и документације достављених од стране субјекта ревизије, као и обављених интервјуа (представници субјекта ревизије и извора информација), донели смо следеће закључке:

1. Министарство не управља информационим технологијама на одговарајући начин због непостојања плана развоја ИТ, недовољних кадровских капацитета и употребе великог броја ИС.
2. Министарство није успоставило свеобухватне мере којима се обезбеђује континутитет пословања, у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта, укључујући и управљање резервним копијама.
3. Министарство није успоставило управљање информационом безбедношћу на свеобухватан начин, јер није ускладило Акт о безбедности са прописима, као ни организационо и кадровски успоставило управљање информационом безбедношћу, док на нивоу ИС Социјална карта не постоје правила и процедуре праћења и контроле записа о догађајима (логова) нити сарадње са пружаоцем услуге одржавања, што може довести до нарушавања безбедности ИС.

У наставку извештаја наводимо закључке са одговарајућим налазима.

ЗАКЉУЧАК 1: Министарство не управља информационим технологијама на одговарајући начин због непостојања плана развоја ИТ, недовољних кадровских капацитета и употребе великог броја ИС.

Циљ овог дела извештаја је да одговоримо на прво ревизијско питање, односно на који начин се управља информационим технологијама у Министарству за рад, запошљавање, борачка и социјална питања.

На основу анализе законских и подзаконских аката, документације субјекта ревизије и одржаних интервјуа, донели смо закључак који темељимо на следећим налазима.

Налаз 1.1: Министарство није успоставило адекватну организациону структуру за ИТ управљање, како у смислу кадровских капацитета тако и нивоа стручног знања запослених на тим пословима.

Организациона структура је кључан део ИТ управљања у дефинисању улога руководства у циљу управљања и доношења одлука. Организациона структура мора јасно и прецизно да дефинише поделу дужности, одговорности, права и обавезе запослених у складу са пословним процесима, задацима организације и праћења резултата рада[41].

У оквиру Министарства организован је Сектор за информационе технологије који је подељен на два одељења. Радна места начелника оба одељења нису попуњена. У Сектору за ИТ запослено је 26 лица (21 на неодређено време и пет лица ангажовано је ван радног односа[42]). Од тога 14 лица (54%) не обављају послове који су по природи (описима посла) ИТ послови. Министарство није успоставило адекватну организациону структуру за ИТ управљање, како у смислу кадровских капацитета тако и нивоа стручног знања запослених на тим пословима.

Министарство није препознало значај Сектора за ИТ и потребу јачања стручних знања запослених ради постизања циљева организације, а нарочито због велико броја запослених којима се управља као и велики број ИС у употреби. Значајно ограничење у развоју ИТ у Министарству је недовољан број стручно запослених лица у Сектору за ИТ, смањена могућност запошљавања нових кадрова и претежно ослањање на пружаоце услуга (добављаче).

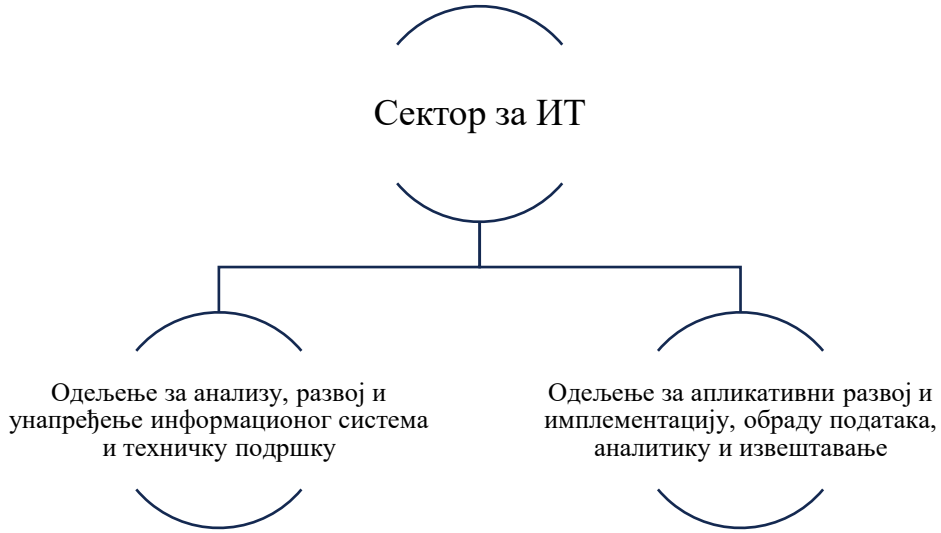
Последице недостатка кадровских капацитета (мањка руководећег и оперативног ИТ кадра), непостојање плана развоја ИТ и некординације између сектора у Министарству, су кашњења у спровођењу ИТ пројеката, неадовољној ИТ безбедности и значајној зависности од пружаоца услуге (добављача).

Кадровски капацитети Сектора за информационе технологије

Министарство је организационо подељено на девет сектора, Инспекторат за рад и Управу за безбедност и здравље на раду. Један од сектора Министарства је Сектор за информационе технологије. У оквиру Сектора за ИТ образована су два одељења: „Одељење за анализу, развој и унапређење информационог система и техничку подршку“ и „Одељење за апликативни развој и имплементацију, обраду података, аналитику и извештавање“[43].

[41] WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions).
[42] Уговор о привременим и повременим пословима.
[43] Правилник о организацији и систематизацији послова у Министарству за рад, запошљавање, борачка и социјална питања број: 011-00-490/1/2020-05 од 23. децембра 2020. године (важећи у 2022. години) и број:

Слика број 4: Приказ организационе структуре Сектора за ИТ[44]



Радна места начелника оба одељења у оквиру Сектора за ИТ нису попуњена. Радно место Начелника одељења за апликативни развој, имплементацију, обраду података, аналитику и извештавање је било попуњено до 1. маја 2023. године, односно до одласка начелнице у старосну пензију.

У Сектору за ИТ од систематизованих 26 радних места, попуњено је 21 радно место[45], 17 запослених поседују средњу стручну спрему, а четворо високу школу или факултет. Од тога 11 запослених (52%) обавља послове оператера и контролора података[46], пет запослених обавља послове администратора мреже и мрежних сервиса[47]. Остала попуњена радна места су помоћник министра, млађи саветник за планирање, анализу и извештавање, референт за канцеларијске и административне послове, систем администратор информационих система и администратор обраде података и техничке подршке.

011-00-281/1/2023-05 од 11. јула 2023. године, са изменама и допунама број: 011-00-281/2/2023-05 од 20. новембра 2023. године (важећи у 2023. години).

[44] Извор: ДРИ.

[45] 81% попуњености кадровских капацитета.

[46] Унос података у базе података према оперативним програмским решењима и контрола и пренос података из локалних база у централну базу Министарства; контрола и обрада података неопходних за реализацију права из области социјалне и дечије заштите и борачко-инвалидске заштите за кориснике на територији Републике Србије; пружа први ниво техничке подршке корисницима ИС и учествује у обукама за коришћење модула ИС. .

[47] Анализира рад система, конфигурише, надгледа и одржава мрежну инфраструктуру и сервисе , сарађује са корисницима ИС у циљу прилагођавања техничких захтева за унапређење ИТ решења и координише поступке решавања инцидената и захтева за променама; спроводи активности на развоју и унапређењу мрежне инфраструктуре и сервиса у складу са развојем нових технологија; прати нова хардверска и софтверска достигнућа у технолошкој области мрежне инфраструктуре.

Табела број 1. Приказ систематизованих радних места у оквиру Сектора за ИТ у 2023. години[48]

Редни број	Систематизована радна места у 2023. години	Број извршилаца	Попуњено	Степен стручне спреме који запослени имају
1	*2*	*3*	*4*	*5*
1.	Помоћник министра - Сектор за ИТ	1	1	VII
2.	Млађи саветник за планирање, анализу и извештавање	1	1	VII
Одељење за анализу, развој и унапређење информационог система и техничку подршку				
3.	Начелник Одељења за анализу, развој и унапређење информационог система и техничку подршку	1	0	/
4.	Аналитичар информационих система	1	0	/
5.	Референт за канцеларијске и административне послове	1	1	IV
6.	Систем администратор информационих система	1	1	VI
7.	Администратор мреже и мрежних сервиса	6	5	IV
Одељење за апликативни развој, обраду података, аналитику и извештавање				
8.	Начелник Одељења за апликативни развој, обраду података, аналитику и извештавање	1	0	/
9.	Администратор обраде података и техничке подршке	1	1	VI
10.	Оператер и контролор података	12	11	IV
	Укупно	26	21	/

Увидом у Правилник о организацији и систематизацији послова у Министарству из описа послова 11 запослених на пословима оператера и контролора података закључујемо да они не обављају ИТ послове, већ послове уноса података са решења и контроле унетих података.

У оквиру Сектора за ИТ, није систематизовано радно место које би у свом опису посла искључиво имало послове који се односе на информациону безбедност ИКТ система Министарства и контролу примене мера ИТ безбедности, што је за организацију ове величине и специфичног подручја рада неопходно.

У оквиру Сектора за ИТ ангажовано је пет лица на привременим и повременим пословима[49]. Од пет ангажованих лица, троје ангажованих лица према наведеним пословима не обављају послове везане за ИТ, док два лица обављају послове који су по природи ИТ послови.

Министарство није препознало значај Сектора за ИТ и потребу запошљавања/јачања стручних знања запослених. Значајно ограничење у развоју ИТ у Министарству је недовољан број стручно запослених лица у Сектору за ИТ, смањена могућност запошљавања нових кадрова и претежно ослањање на пружаоце услуга (добављаче). Последице недостатка кадровских капацитета (мањка руководећег и оперативног ИТ кадра), непостојање плана развоја ИТ и некоординације између сектора у Министарству,

[48] Извод из Правилника о унутрашњем уређењу и систематизацији радних места у Министарству за рад, запошљавање, борачка и социјална питања број: 011-00-281/1/2023-05 од 11. јула 2023. године, са изменама и допунама број: 011-00-281/2/2023-05 од 20. новембра 2023. године.
[49] Период обухвата ревизије је 2022. и 2023. година.

су кашњења у спровођењу ИТ пројеката, недовољној ИТ безбедности и значајној зависности од пружаоца услуге (добављача).

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да успостави адекватну организациону структуру за ИТ управљање, укључујући јачање кадровских капацитета и/или стручних знања запослених.

Налаз 1.2: Министарство није успоставило стратешко ИТ планирање, јер није донело план развоја ИТ и управљање ризицима, а нарочито имајући у виду значај ИС Социјална карта.

ИТ управљање представља целокупни оквир који води ИТ операције у организацији како би се обезбедило да организација задовољава потребе пословања данас и да укључује планове за будуће потребе и раст. ИТ управљање је интегрални део управљања организацијом и обухвата организационо вођење, институционалне структуре и процесе и друге механизме (извештавање и повратне информације, спровођење, ресурсе итд.) који обезбеђују да ИТ системи подржавају организационе циљеве и стратегију, док балансирају ризике и ефективно управљају ресурсима. ИТ управљање има кључну улогу у одређивању контролног окружења и поставља темеље за успостављање најбољих пракси интерне контроле и извештавања.[50]

Корисници јавних средстава успостављају финансијско управљање и контролу у складу са одредбама Закона о буџетском систему[51]. Према одредбама Закона о информационој безбедности[52], приликом планирања и примене мера заштите ИКТ система треба се руководити начелом управљања ризиком. Управљање ризицима обухвата идентификовање, процену и контролу над потенцијалним догађајима и ситуацијама које могу утицати на остварење циљева корисника јавних средстава, обезбеђујући разумно уверавање да ће ти циљеви бити остварени (члан 7 став 1 Правилника о заједничким критеријумима и стандардима за успостављање, функционисање и извештавање о систему финансијског управљања и контроле у јавном сектору).

Министарство је организационо успоставило Сектор за ИТ[53].

Министарство у свом раду користи 13 различитих ИС, два ИС су стављена ван употребе, („DMS“ и Регистар повреда на раду су набављени 2020. године), а два најважнија ИС (Социјална карта и СОЗИС) нису у потпуности имплементирана.

Такође, у оквиру Министарства не постоји усвојен стратешки или оперативни (акциони) план развоја ИТ. Иако Министарство (Сектор за ИТ) има могућност да искаже потребе приликом планирања буџета и кроз План јавних набавки, за сваку од јавних набавки преко два милиона динара потребна је сагласност Министарства финансија ради покретања поступка јавне набавке.

Министарство није препознало ИТ ризике кроз регистар ризика, нити кроз Методологију управљања ризицима.

Министарство није препознало значај стратешког и оперативног управљања ИТ и ризицима повезаним са ИТ. Разлог су мањак ИТ кадрова, велики број ИС који се

[50] IDI WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.
[51] „Службени гласник РС“ бр. 54/09, 73/10, 101/10, ….. 118/21, 138/22, 118/21 - др. закон и 92/23.
[52] члан 3 став 1 тачка 1).
[53] Више видети тачка 1.1.

тренутно користе и значајна зависност од добављача. Број и географска разуђеност индиректних корисника Министарства су такође узроци неадекватног управљања ИТ у Министарству.

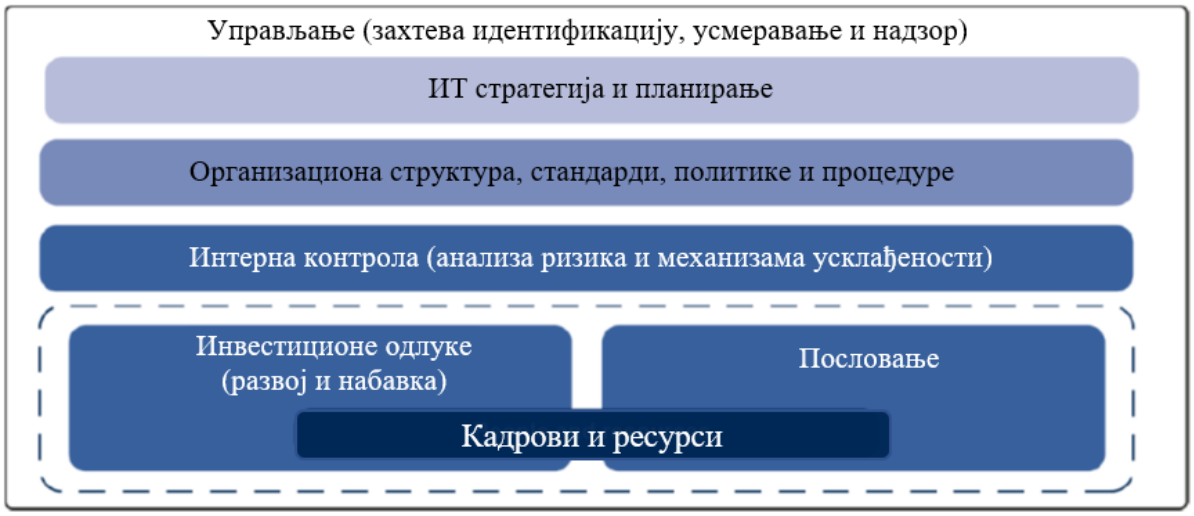
Последице великог броја ИС у употреби уз мањак стручног кадра су неадекватно ИТ управљање, непрепознавање ИТ ризика, могућих инцидената, а тиме се онемогућава правовремено реаговање што даље имплицира потенцијалне финансијске и нефинансијске губитке.

Стратешко и оперативно планирање

ИТ стратегија представља усклађивање ИТ стратегије и стратешких пословних циљева. Стратешки ИТ циљеви би требали да размотре тренутне и будуће потребе пословања, тренутне ИТ капацитете за пружање услуга, потребне ресурсе као и постојећу ИТ инфраструктуру и архитектуру, инвестиције, модел имплементације, кадрове и представе план који интегрише поменуто у заједнички приступ који подржава циљеве пословања.

Без ИТ стратегије, већи је ризик да организација неће одредити како ИТ могу пружити подршку постојећим и будућим потребама пословања. Затим, без ажурираног ИТ стратешког плана (акционог плана) – који се ослања на свеукупни стратешки план организације који укључује циљеве, мере перформанси, стратегију и међузависност између пројеката-организације ризикују се изостанак јасне дефиниције шта желе да постигну са ИТ.[54]

Слика број 5: Генерички оквир управљања ИТ[55]



Управљање ИТ ризицима

Према одредбама члана 3 став 1 тачка 1) Закона о информационој безбедности, приликом планирања и примене мера заштите ИКТ система треба се руководити начелом управљања ризиком. Избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности.

[54] IDI WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.
[55] IDI WGITA – IDI Приручник за ИТ ревизију врховних ревизорских институција (енг. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.

Сва питања разматрана у овој ревизији у основи имају процену одређених ризика (ИТ управљање, континуитет пословања, ИТ безбедност, итд.). Процена самих ризика посматра се кроз термине утицај и вероватноћа док се њихово рангирање изводи укрштањем утицаја и вероватноће. Процена утицаја обухвата процену ефекта који би неповољан догађај имао на организацију уколико би се остварио. Код процене вероватноће дешавања процењује се колика је вероватноћа настанка одређеног ризика унутар неког периода (нпр. годину дана). Из процене утицаја и вероватноће произилази процена укупне изложености ризику коју је неопходно извршити како би се утврдили приоритети, односно како треба управљати најзначајнијим ризицима[56].

У Уредби о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја[57], у члану 2 прописано је да оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности.

Методологија управљања ризицима (део Акта о безбедности ИКТ система Министарства усвојеног 2019. године)

Као саставни део Акта о безбедности информационо-комуникационог система Министарства за рад, запошљавање, борачка и социјална питања[58], Министарство је усвојило и Методологију управљања ризицима, како би помогло реализацији процене и третмана ризика.

Сагласно поменутој методологији, одговорност за процену ризика има Менаџер безбедности информација, заједно са тимом који је назначен од стране највишег менаџмента. Менаџер безбедности информација заједно са тимом је одговоран да спроведе процену и да изнесе предлог за третман ризика.

Према Методологији управљања ризицима, Министарство је предвидело следеће:

„У првој фази процене ризика, сврха је одредити ризике организације, да се дају предлози у односу на њихов третман, било да је то трансфер, смањивање, избегавање или прихватање постојећих ризика. Процесом спровођења процене ризика информационе безбедности управља и координира Менаџер безбедности информација, заједно са тимом који је одређен тим документом. Тим за управљање ризицима информационе безбедности укључује:

- Менаџера безбедности информација;
- Информатичара;
- Представника Секретаријата Министарства.

Завршни документ, Резултат процене и третмана ризика ће садржати препоруке везане за управљање ризицима (укључујући имплементације одређених контрола) само за средства која су рангирана као ризична високим оценама.

Методологија управљања ризиком је подељена на следеће фазе:

- Контекст;

[56] Смернице за управљање ризицима, Министарство финансија.
[57] „Службени гласник РС“, бр. 94/16.
[58] бр. 030-03-25/2020-01 од 9. октобра 2020. године.

- Идентификација информационих средстава и ризика;
- Класификација информационих средстава;
- Анализа релевантних претњи и ризика;
- Вероватноћа појаве претњи;
- Отворена дискусија са корисницима за сва средства о својим рањивостима;
- Оцена ризика;
- Процена података и припрема појединачних и збирних извештаја;
- Третман ризика (уклањање, смањење прихватања или трансфер).

Идентификација средстава је заправо регистар информационе имовине организације. Њихов опис и класификација је доступна у Регистру информационе имовине.

Третман ризика је последњи корак у процесу управљања ризицима. Завршна табела третмана ризика као сумарна процена се доставља руководству и на заједничком састанку се презентују сви резултати процеса процене и третмана ризика.

Коначна табела коју Тим за управљање ризицима информационе безбедности и Менаџер безбедности информација креирају може бити извршна, или се користи као информација и препоруке које користи руководство у доношењу своје одлуке у вези наредних активности у третману ризика. Руководство може у потпуности прихватити табелу третмана ризика и прогласити је Акционим планом за третман ризика у организацији.

Процена и третман ризика за информациона средства организације вршиће се на годишњем нивоу. У одређеним случајевима, на захтев руководства, процена и третман ризика може се вршити и у краћем периоду".

ИТ управљање у Министарству

Министарство нема донет план развоја ИТ. Сектор за ИТ нема посебан буџетски програм, већ средства користи у оквиру буџета Сектора за развојне послове и послове планирања. Иако Министарство (Сектор за ИТ) има могућност да искаже потребе приликом планирања буџета и кроз План јавних набавки, за сваку од јавних набавки преко два милиона динара потребна је сагласност Министарства финансија пре покретања поступка јавне набавке[59]. Потенцијални ризици су недобијање сагласности, касно добијање сагласности за покретање поступака јавних набавки што доводи до кашњења у ИТ пројектима и давања предности мање значајним пројектима о у ИТ. На тај начин је успорен развој ИТ у Министарству, јер не постоје приоритети, што може довести и до неиспуњавања циљева из Акционог плана за спровођење Програма Владе 2023-2026. године.

Министарство није идентификовало ИТ ризике, као ни акционе планове за третман ИТ ризика. Министарство не врши годишњу процену и третман ризика за информациона средства организације, како је предвидело Методологијом управљања ризицима.

Такође, Министарство не спроводи активности у вези са управљањем ризицима, које су саставни део Акта о безбедности ИКТ система Министарства. У Министарству није систематизовано радно место Менаџер безбедности информација.

Министарство у свом раду користи 13 различитих ИС, два ИС су стављена ван употребе, (нпр „DMS" и Регистар повреда на раду. који су набављени 2020. године), а два најважнија ИС (Социјална карта и СОЗИС) нису у потпуности имплементирана. (Табела број 2).

[59] Закључак Владе РС 05 Број: 401-7214/2022 од 14 септембра 2022. године.

Табела број 2. Преглед информационих система који се користе у Министарству и оних који су стављени ван употребе[60]

Рб	Назив	Број корисника	Купљен или интерно креиран информациони систем	Година набавке/ креирања	Вредност почетног улагања (у хиљадама без ПДВ) само за ИС/апликације које су набављене у претходних 5 година (од 2019-2023. године)	Вредност додатног улагања (доградња/измена ИС/апликације) у хиљадама динара без ПДВ	Вредност годишњег одржавања ИС/апликације (у хиљадама динара без ПДВ)	Вредност улагања у лиценце на годишњем нивоу (у хиљадама динара без ПДВ)	% довршености ИС/апликације уколико није у пуној примени	Очекиван рок за пуну имплементацију (уколико су измене/доградња у току)
1	***2***	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
1	Апликативни софтвер за дечије и родитељске додатке и породиљско одсуство (подршка Закону о финансијској подршци породици са децом)	900	Купљено право коришћења	2003		20.000	8.000	1.800	100	
2	Социјална карта	МИНРЗС, сви центри за социјални рад, све службе дечије заштите, Завод за социјалну заштиту, РЗС, остали заинтересовани корисници (тренутно 1800 корисника, очекује се преко 5000 корисника)	Купљен	2019	124.891	107.989	65.000	37.109	80	2024 Према закљученом уговору, тада је рок завршетка пуне интеграције са ИС Борци србије, ИС ДД РД и СОЗИС

[60] Подаци добијени од субјекта ревизије.

Рб	Назив	Број корисника	Купљен или интерно креиран информациони систем	Година набавке/ креирања	Вредност почетног улагања (у хиљадама без ПДВ) само за ИС/апликације које су набављене у претходних 5 година (од 2019-2023. године)	Вредност додатног улагања (доградња/измена ИС/апликације) у хиљадама динара без ПДВ	Вредност годишњег одржавања ИС/апликације (у хиљадама динара без ПДВ)	Вредност улагања у лиценце на годишњем нивоу (у хиљадама динара без ПДВ)	% довршености ИС/апликације уколико није у пуној примени	Очекиван рок за пуну имплементацију (уколико су измене/доградња у току)
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
3	Софтвер за јединствену матичну евиденцију и исплату права корисника у области борачко-инвалидске заштите	300	Купљено право коришћења	2005	12.000	5.000	6.000		80	Зависно од расположивих финансијских средстава
4	NexTBIZ за економско-финансијско пословање	Око 40 корисника (Сектор за финансије)	Купљено право коришћења	2014		1.500	2.500		100	
5	Систем за заштиту и аутоматизацију инструмената социјалне заштите	Корисници из свих центара за социјални рад + МИНРЗС (процена око 5000)	Купљен	2021	670.000		130.000	Системски и апликативни софтвер, хардвер и лиценце	50	2026
6	Апликација за новчану социјалну помоћ (евиденција корисника, обрачун исплата)	25 корисника	властити развој	1996						
7	Апликација за помоћ и негу другог лица (евиденција корисника, обрачун исплата)	25 корисника	властити развој	1996						
8	Апликација за смештај лица у хранитељске породице и установе (евиденција	25 корисника	властити развој	1998						

Рб	Назив	Број корисника	Купљен или интерно креиран информациони систем	Година набавке/ креирања	Вредност почетног улагања (у хиљадама без ПДВ) само за ИС/апликације које су набављене у претходних 5 година (од 2019-2023. године)	Вредност додатног улагања (доградња/измена ИС/апликације) у хиљадама динара без ПДВ	Вредност годишњег одржавања ИС/апликације (у хиљадама динара без ПДВ)	Вредност улагања у лиценце на годишњем нивоу (у хиљадама динара без ПДВ)	% довршености ИС/апликације уколико није у пуној примени	Очекиван рок за пуну имплементацију (уколико су измене/доградња у току)
1	***2***	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
	корисника, обрачун исплата)									
9	Апликација за посебну новчану накнаду (евиденција корисника, обрачун исплата)	25 корисника	властити развој	2002						
10	Апликација за креирање извештаја о лицима у хранитељским породицама и установама за ЦСР и установе	25 корисника	властити развој	2019						
11	Апликација за финансије (извршење буџета)	преко 100 корисника	купљен	2021	100.000		30.000	24.000	80	Зависно од расположивих финансијских средстава
12	Апликација за евиденцију и генерисање ЈМБП-а	До 3корисника	властити развој	1998					100	
13	Регистар усвојења		Купљен	2018	5.000	3.000	1.000		80	Зависно од расположивих финансијских средстава

Рб	Назив	Број корисника	Купљен или интерно креиран информациони систем	Година набавке/ креирања	Вредност почетног улагања (у хиљадама без ПДВ) само за ИС/апликације које су набављене у претходних 5 година (од 2019-2023. године)	Вредност додатног улагања (доградња/измена ИС/апликације) у хиљадама динара без ПДВ	Вредност годишњег одржавања ИС/апликације (у хиљадама динара без ПДВ)	Вредност улагања у лиценце на годишњем нивоу (у хиљадама динара без ПДВ)	% довршености ИС/апликације уколико није у пуној примени	Очекиван рок за пуну имплементацију (уколико су измене/доградња у току)
1	***2***	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
Информациони системи који се више не користе										
1	DMS	МИНРЗС (до 350) + Инспекторат (око 300)	Купљен	2020	80.260	93.150	23.940			
2	Управа за безбедност и здравље на раду – Регистар повреда на раду	Сви послодавци	Купљен	2020	5.000					

Последица непрепознавања ИТ ризика може проузроковати немогућност брзог и адекватног реаговања на инцидент или хаварију, дужи период опоравка ИС након инцидента/хаварије и у крајњој мери непостизање пословних циљева и резултата. Последице могу бити и велики трошкови услед нежељених догађаја (инцидент/хаварија) или велики нефинансијски губици (података), због немогућности благовременог реаговања.

Министарство није препознало значај стратешког и оперативног управљања ИТ и ризицима повезаним са употребом ИТ. Разлог су мањак ИТ кадрова, велики број информационих система који се тренутно користе што уз значајну зависност од добављача онемогућава даљи развој ИТ. Број и географска разуђеност индиректних корисника Министарства су такође узроци неадекватног управљања ИТ у Министарству када је у питању ИС Социјална карта.

Последице великог броја ИС у употреби су непрепознавање свих ИТ ризика, стратегија за смањивање/отклањање ризика, неадекватно ИТ управљање и тиме могући проблеми у свакодневном функционисању информационих система.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да одреди приоритете развоја ИТ и успоставе управљање ИТ ризицима што подразумева евидентирање, класификацију, анализу свих ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

Налаз 1.3: Министарство није извршило пуну имплементацију ИС Социјална карта, јер поред недостатака у апликативним контролама, није омогућило да сви предвиђени корисници буду укључени у ИС Социјална карта.

Набавка ИС Социјална карта је започета 2018. године, а примена ИС је почела 4. априла 2022. године, на основу Одлуке министра о увођењу Регистра Социјална карта у оперативну употребу. Податке који се обрађују у Социјалној карти користе корисници података у органима надлежним за спровођење социјалне заштите, и то у ЦСР, ЈЛС које обављају поверене послове, Министарству, надлежном органу АП за спровођење социјалне заштите, надлежном републичком органу за спровођење активности унапређења социјалне заштите и другим органима државне управе и институцијама, у складу са законом.

У поступку ревизије смо утврдили да други корисници (ЈЛС које обављају поверене послове, надлежни орган АП за спровођење социјалне заштите) немају приступ ИС Социјална карта.

ИС Социјална карта је у примени од априла 2022. године. Тренутно се спроводи фаза „Доградња сервиса за интеграцију базе података ДД, РД, ПО са Регистром социјална карта“ и рок за завршетак ове фазе је 2024. година.

У поступку ревизије утврђени су и недостаци у апликативним контролама ИС Социјална карта које су детаљније описане на страни 38-39 страни Извештаја.

Представници Министарства наводе да други корисници[61] немају приступ ИС Социјална карта због непостојања L3VPN канала комуникације и да је то обавеза Канцеларије за

[61] Покрајински секретаријат за здравство, социјалну политику и демографију, Покрајински завод за социјалну заштиту, службе за дечију заштиту, службе за борачко - инвалидску заштиту.

ИТ и електронску управу[62]. Поједине установе наведене у конкурсној документацији за набавку ИС Социјална карта нису ни предвиђене Законом о социјалној карти као корисници[63].

Због чињенице да је ИС Социјална карта још увек у фази развоја и доградње са другим ИС који користи Министарство/регистрима изворних евиденција, као и чињеници да у претходним фазама није било могуће предвидети све апликативне контроле, јављају се недостаци у апликативним контролама.

Последице неукључивања свих корисника ИС Социјална карта (службе за социјалну и дечију и борачку-инвалидску заштиту при ЈЛС), огледају се у већем обиму послова у ЦСР, који решавају нотификације које се односе на службе за социјалну и дечију и борачку-инвалидску заштиту при ЈЛС.

Последице недостатака у апликативним контролама могу бити видљиве кроз велики број решења о правима са невалидним датумом, дупли захтеви/решења за остваривање права, нерешене нотификације и тиме грешке при исплатама права из области социјалне заштите.

Финансирање развоја и одржавања ИС Социјална карта

ИС Социјална карта је једна од кључних апликација за пословање Министарства. Ради се о ИС који је у изворном облику (коду) развила група понуђача „у јавној набавци 26/2018 „Набавка Информационог система Социјална карта – I фаза“.

Табела број 3. Преглед јавних набавки имплементације и одржавања ИС Социјална карта у периоду 2018-2024. године[64]

(у динарима)

Број јавне набавке	Назив	Добављач(и)	Година уговора	Вредност без ПДВ-а	Вредност са ПДВ-ом	Износ извршених расхода (плаћено добављачу)
1	*2*	*3*	*4*	*5*	*6*	*7*
26/2018	Набавка Информационог система Социјална карта – I фаза	Заједничка понуда: - „SAGA“ д.о.о. Београд „COMTRADE SYSTEM INTEGRATION“ д.о.о. Београд, „S&T Serbia“ д.о.о. Београд, *Подизвођач:* „ASSECO SEE“ д.о.о. Београд	2018.	174.866.000	209.839.200	209.839.200
4/2021	Услуге одржавања ИС Социјална карта I фаза, укључујући и лиценце	„SAGA“ д.о.о. Београд	2021.	38.499.900	46.199.880	46.199.880

[62] Према Споразуму о преузимању обавеза за услуге закупа оптичких влакана (L3VPN) закљученог између Министарства и Канцеларије за ИТ и електронску управу дана 17. јануара 2019. године.
[63] Установе за смештај, НСЗ, РФ ПИО и други органи.
[64] Извор: ДРИ и Министарство.

(у динарима)

Број јавне набавке	Назив	Добављач(и)	Година уговора	Вредност без ПДВ-а	Вредност са ПДВ-ом	Износ извршених расхода (плаћено добављачу)
1	*2*	*3*	*4*	*5*	*6*	*7*
12/2021	Набавка регистра Социјална карта - 2. фаза	Група понуђача: „SAGA“ д.о.о. Београд „S&T Serbia“ doo, Београд (Нови Београд)	2021.	107.988.800	129.586.560	129.586.560
31/2021	Услуге одржавања ИС Социјална карта I фаза, укључујући и лиценце	„SAGA“ д.о.о. Београд	2021.	38.499.900	46.199.880	46.199.880
39/2019	Услуге обнове лиценци за ИС Социјална карта (ORACLE, CISCO, DELL/EMC..)	„SAGA“ д.о.о. Београд	2020	19.986.258	23.983.510	23.983.510
28/2022	Услуге одржавања ИС Социјална карта, укључујући и лиценце	„SAGA“ д.о.о. Београд *Подизвођачи:* „Meteor JPL System“ doo, Београд	2022.	64.995.600	77.994.720	77.994.720
24/2023	Доградња и модификација система ИС Регистар социјална карта и интеграција са системима ИС СОЗИС, ИС ДД-РД, ИС Борачко инвалидске заштите	Група понуђача: „SAGA“ д.о.о. Београд „GiveSense“ д.о.о. Београд *Подизвођачи:* „Oracle Srbija & Crna Gora“ d.o.o Београд „CPU“ doo, Београд „Spark Analytics“ doo, Београд „Igmako“ smart solutions doo, Београд „Meteor JPL System“ doo, Београд	2023.	99.887.566	119.865.079	60.000.000
31/2023	Доградња сервиса за интеграцију базе података ДД, РД, ПО са Регистром социјална карта	„ОНОРА“ doo, Београд (Стари Град)	2023.	6.000.000	7.200.000	7.200.000

(у динарима)

Број јавне набавке	Назив	Добављач(и)	Година уговора	Вредност без ПДВ-а	Вредност са ПДВ-ом	Износ извршених расхода (плаћено добављачу)
1	*2*	*3*	*4*	*5*	*6*	*7*
30/2023	Доградња сервиса за интеграцију базе података Борци Србија са Регистром социјална карта	„Е-инфо“ д.о.о. Бања Лука	2023.	6.000.000	7.200.000	7.200.000
38/2023	Услуга одржавања ИС социјална карта укључујући лиценце	„SAGA“ д.о.о. Београд *Подизвођачи:* „GiveSense“ д.о.о. Београд „Meteor JPL System“ doo, Београд	2024.	50.833.000	60.999.600	48.475.800
		Укупно				656.679.550

Имплементација целокупног пројекта ИС Социјална карта је осмишљена тако да има неколико фаза. ИС Социјална карта представља додатни слој информатичке инфраструктуре на ком се синхронизују и обједињавају подаци из различитих евиденција Министарства и других евиденција од значаја за вођење социјалне политике и садржи имплицитну електронску базу социјално-економског статуса.

Подаци који треба да буду обухваћени у ИС Социјална карта треба да се користе током одлучивања у управним поступцима при решавању поднетих захтева за остваривање права из социјалне заштите или у поступцима покренутим по службеној дужности у службама надлежним за њихово решавање.

Подаци из ИС Социјална карта треба да се користе и као подршка у процесу креирања социјалне политике, доношења законских решења и анализа утицаја донетих мера социјалне заштите.

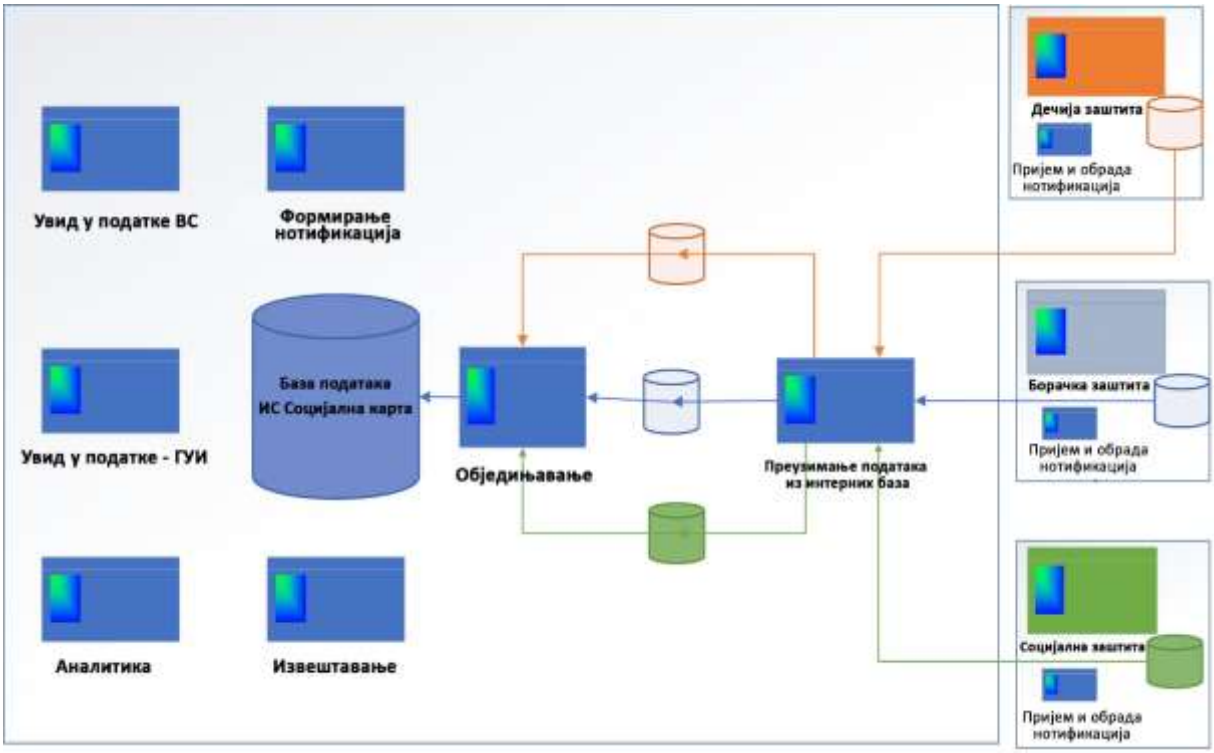
I фаза имплементације ИС Социјална карта

ИС Социјална карта - I фаза генерално је подразумевала:

- Успостављање окружења за ИС Социјална карта (технички предуслови, нефункционални захтеви).
- Успостављање функционалности за иницијално формирање базе социјално-економског статуса грађана преузимањем и обједињавањем података из постојећих евиденција унутар МИНРЗС приказаних у Табели 1 (т. 1.3.1), као и успостављање функционалности за ажурирање формиране базе на основу појединачних промена које се дешавају у тим евиденцијама.
- Успостављање функционалности за увид у податке путем веб апликације.
- Успостављање функционалности за увид у податке путем електронских сервиса.
- Успостављање функционалности за формирање нотификација према свим корисницима ИС Социјална карта и управљање нотификацијама.

– Успостављање функционалности за основне аналитичке обраде и извештавање.[65]

Слика број 6: ИС Социјална карта након иницијалног формирања[66]



II фаза имплементације ИС Социјална карта

Захтеване функционалности у 2. фази које изабрани понуђач треба да обезбеди, али се тиме не ограничавају, су:

1) Доградња Социјалне карте из 1. фазе и проширење базе података условљено преузимањем података из изворних службених евиденција органа јавне управе, података из интерних евиденција Министарства и било којих других објективних разлога.
2) Обезбеђење повезивања Социјалне карте са регистрима и евиденцијама у надлежности других органа јавне управе, начина преноса података и иницијално преузимање података (иницијално преузимање података се односи на податке лица чији су подаци преузети из интерних евиденција Министарства).
3) Обезбеђење повезивања Социјалне карте са новим системима Министарства (који су у развоју - Систем за заштиту и аутоматизацију инструмената социјалне заштите, Софтверско решење за потребе борачко-инвалидске заштите, …), а којима се замењују евиденције са којима је обезбеђена комуникација и размена у 1. фази развоја, начина преузимања података и преузимање података.
4) Функционалност преузимања података из регистара и евиденција органа јавне управе и из евиденција Министарства за лица (појединац(и) и са њим повезана лица) која улазе у регистар Социјална карта и њихово обједињавање.
5) Ажурирање података у регистру Социјална карта (периодично преузимање и обједињавање података из регистара и евиденција органа јавне управе и из

[65] КД ЈН26/2018 „Набавка Информационог система Социјална карта – I фаза“, стр. 13/125.
[66] КД ЈН26/2018 „Набавка Информационог система Социјална карта – I фаза“, стр. 14/125.

евиденција Министарства (и нових евиденција и система у развоју), за кориснике права уписане у регистар Социјална карта, у складу са динамиком која ће се утврдити у фази анализе и дизајна.

6) Прибављање и упис података за *лица из социјално угрожених и рањивих група којима право утврђује Влад*а (члан 6. Закона о социјалној карти) из регистара и евиденција органа јавне управе и евиденција Министарства у Социјалну карту. Циљ је извршење избора конкретних лица из наведених група којима ће се доделити одговарајућа помоћ према дефинисаном критеријуму.
7) Приступ и коришћење података из Социјалне карте за кориснике података.

   Корисници података су дефинисани у члану 11. Закона и зависно од дефинисаног циља успостављања и вођења Социјалне карте (чл. 3.) и сврхе обраде података (чл. 4.) користе податке.
8) Успостављање функционалности које се односе на увид у податке, формирање додатних обавештења (нотификација) према корисницима интерних евиденција Министарства, пријем и њихова обрада, односно формирање и слање нотификација према интерним евиденцијама и системима код којих је то изводљиво.
9) Повезивање Социјалне карте са Порталом еУправа ради обезбеђења увида у личне податке од стране корисника права (физичких лица чији се подаци воде у Социјалној карти) и обезбеђење функционалности за подношење захтева за измену личних података од стране корисника права.

   Корисницима права чији се подаци чувају у Социјалној карти се *обезбеђује приступ својим подацима путем Портала еУправа* уз поштовање прописаног поступка идентификације двофакторским начином аутентикације - шемом електронске идентификације средњег нивоа поузданости, те у складу са законом којим се регулише заштита података о личности имају право да поднесу захтев за измену одређених личних података ако сматрају да подаци нису тачни. Након тога треба да се обезбеди прослеђивање захтева за изменом изворном органу јавне управе и да се да Обавештење кориснику права о извршеним изменама у изворној евиденцији и подацима који су пренети у Социјалну карту.
10) Успостављање функционалности које се односе на извештавање и проширене аналитичке обраде.
11) Доградња и усклађивање техничких и организационих мера заштите података и мера заштите приступа Социјалној карти у складу са законским решењима.[67]

Доградња и модификација ИС Регистар социјална карта и интеграција са системима ИС СОЗИС, ИС ДД-РД и ИС Борачко-инвалидске заштите[68]

Конкурсном документацијом јавне набавке[69] циљ унапређења регистра Социјална карта је да се изврши његова потпуна интеграција са информационим системом из области социјалне заштите СОЗИС, са системом из области финансијске подршке породици са децом ДД-РД, са системом из области борачко-инвалидске заштите, доградња и унапређење неких функционалности самог регистра, као и да се унапреде одговарајући

[67] преузето из КД ЈН 12/2021 – „Набавка регистра Социјална карта – 2.фаза“, стр. 35-37/74.
[68] ЈН 24/2023.
[69] Доградња и модификација ИС Регистар социјална карта и интеграција са системима ИС СОЗИС, ИС ДД-РД и ИС Борачко-инвалидске заштите- јун 2023. године.

аспекти интеграције са евиденцијама других органа и са елементима еУправе за које је надлежна Канцеларија за ИТ и еУправу. Рок за завршетак пројекта је 2024. година.

С обзиром да ће потпуна имплементација ИС СОЗИС бити завршена 2026. године, постоји могућност да планирани циљ ове набавке не буде реализован.

Корисници ИС Социјална карта

Према одредбама Закона о Социјалној карти (члан 11) корисници података су органи надлежни за спровођење социјалне заштите, и то у ЦСР, ЈЛС које обављају поверене послове, Министарству, надлежном органу АП за спровођење социјалне заштите, надлежном републичком органу за спровођење активности унапређења социјалне заштите и другим органима државне управе и институцијама, у складу са законом.

У конкурсној документацији за набавку регистра Социјална карта корисници ИС Социјална карта су запослени у институцијама надлежним за спровођење социјалне заштите у складу са својим овлашћењима.

Препознате су следеће институције:

1) *Центри за социјални рад*

У центрима, који се налазе у свакој општини, обавља се свакодневни оперативни посао са корисницима социјалне заштите. Спектар услуга које обавља центар је широк и тиче се материјалне помоћи, породично правне заштите и услуга социјалне заштите према Закону о социјалној заштити и Породичном закону.

2) *Установе за смештај*

Установе социјалне заштите пружају услуге домског смештаја у складу са Законом о социјалној заштити. У свом раду тесно сарађују са центрима за социјални рад.

3) *Службе за социјалну и дечију заштиту*

У свакој општини постоје службе које обављају поверене послове из области дечије и социјалне заштите и организоване су унутар јединице локалне самоуправе.

4) *Службе за борачко - инвалидску заштиту*

У свакој општини постоји служба која обавља поверене послове из области борачко инвалидске заштите.

5) *Министарство за рад, запошљавање, борачка и социјална питања*

У оквиру Министарства постоји више служби које обављају послове у вези са социјалном, породичном и борачко инвалидском заштитом. Осим другостепеног управног поступка у министарству се обављају послови анализе, планирања, креирања социјалне политике, послови инспекције социјалне заштите и други.

6) *Покрајински секретаријат за здравство, социјалну политику и демографију*

У оквиру Покрајинског секретаријата се обављају послови у вези са социјалном, породичном и борачко инвалидском заштитом. Осим другостепеног управног поступка у секретаријату се обављају послови од покрајинског значаја у вези са социјалном, породичном и борачко инвалидском заштитом.

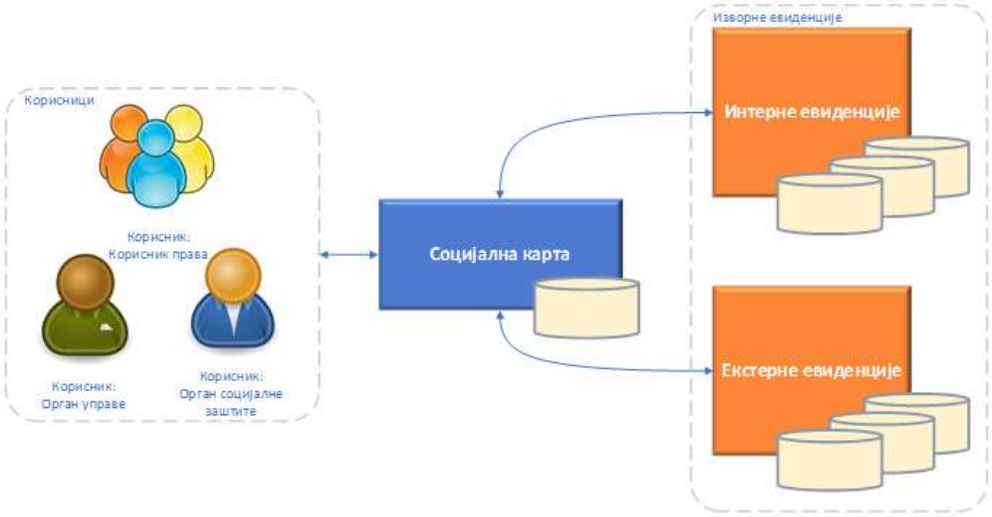
7) *Заводи за социјалну заштиту*

Делатност завода за социјалну заштиту подразумева праћење и унапређивање социјалне заштите, подстицање развоја, обављање истраживачких и других послова у области социјалне заштите.

8) Други органи државне управе

Овде се пре свега мисли на оне органе државне управе који према законској регулативи имају право на информације о појединостима социјално-економског статуса појединца, као што су Национална служба за запошљавање, Фонд ПИО или институције задужене за вођење података о особама које посебно погађа елементарна и друга непогода и други органи.[70]

Слика број 7: Преглед корисника ИС Социјална карта[71]



У поступку ревизије, анализом матрице администраторских (привилегованих) и корисничких налога у ИС Социјална карта[72], на бази податка о називу институције из које долазе администратори/корисници, утврђено је да нису сви предвиђени корисници укључени у ИС Социјална карта тј. немају отворене налоге у ИС Социјална карта како је то предвиђено конкурсном документацијом имплементације ИС Социјална карта I фаза, и то:

1. Службе за социјалну и дечију заштиту,
2. Службе за борачко - инвалидску заштиту,
3. Покрајински секретаријат за здравство, социјалну политику и демографију,
4. Заводи за социјалну заштиту (делатност завода за социјалну заштиту подразумева праћење и унапређивање социјалне заштите, подстицање развоја, обављање истраживачких и других послова у области социјалне заштите). Ту спадају: Завод за васпитање деце и омладине Београд, Завод за васпитање омладине Ниш, Завод за васпитање деце и омладине-Књажевац, Завод за смештај одраслих „Мале пчелице“ Крагујевац.

Представници Министарства су навели да други корисници немају приступ ИС Социјална карта због непостојања L3VPN канала комуникације, а да је обавеза Канцеларије за ИТ и електронску управу да изврши услуге телехаусинга, закупа виртуелних сервера и оптичких влакана (L3VPN) за поменуте кориснике. Министарство и Канцеларија за ИТ и електронску управу су потписале Споразум о преузимању обавеза за услуге телехаусинга, закупа виртуелних сервера и оптичких влакана (L3VPN) у коме је наведено да

[70] преузето из КД ЈН 26/2018 – „Набавка Информационог система Социјална карта – I фаза“, стр. 8/125.
[71] преузето из КД ЈН 12/2021 „Набавка регистра Социјална карта – 2. фаза“, стр. 38/74.
[72] достављене од стране Министарства по Захтеву за доставу података.

- Канцеларија за ИТ и електронску управу врши плаћање услуге закупа оптичких влакана (L3VPN) на територији Р. Србије-за 280 постојећих локација које се налазе у L3VPN мрежи Министарства и за будућих 350 локација којим ће се повезати општинске и градске службе за породичну и дечју заштиту и службе за борачко-инвалидску заштиту у L3VPN Министарства.
- Канцеларија је у циљу преузимања обавеза за наведене услуге Министарства обавезна да планира неопходна финансијска средства за услугу закупа оптичких влакана (L3VPN).
- је споразум потписан на неодређено време и примењује се од 16. јануара 2019. године.

Поједине установе[73] наведене у конкурсној документацији за набавку ИС Социјална карта нису ни предвиђене Законом о социјалној карти као корисници.

Систем за заштиту и аутоматизацију инструмената социјалне заштите СОЗИС

Систем за заштиту и аутоматизацију инструмената социјалне заштите (СОЗИС) је софтверско решења за вођење евиденције, прикупљање података о корисницима система социјалне заштите у центрима за социјални рад, умрежавање са другим секторима и генерисање података за друге апликације које су активне у систему социјалне заштите[74].

СОЗИС је модуларни систем који прати шему послова као и организациону шему центара за социјални рад и треба да омогући бржи и ефикаснији рад центара за социјалну заштиту, као и лакше повезивање и проток инфомација и докумената између ЦСР и Министарства. СОЗИС треба да садржи модуле: Пријем, Регистар корисника социјалне помоћи, Стручни рад, Финансијско административни послови и Аналитика.

Представници Министарства су навели да је завршена прва фаза пројекта, а да се потпуна имплементација ИС СОЗИС очекује до краја 2026. године. До сада је у ИС СОЗИС уложено 800 милиона динара.

Апликативне контроле у ИС Социјална карта

Након извршене анализе коришћења ИС Социјална карта у четири ЦСР утврђени су следећи недостаци у апликативним контролама:

- Обавештење (нотификације) по којој је овлашћено службено лице (ОСЛ) дужно да поступи и да га реши, могуће је „заобићи“ у ИС Социјална карта, уносом било каквог образложења, а потом и променом статуса нотификације у „Решено“ (а да у ствари није решена, односно овлашћено службено лице није проверило измене за корисника социјалне помоћи које су се десиле у некој од изворних евиденција). На тај начин, могуће је да ће кориснику одређеног права или услуге из области социјалне заштите право/услуга бити и даље исплаћивано, а да му то право не припада;
- У ИС Социјална карта је могућ унос новог захтева (са истим бројем захтева који већ постоји у ИС) за исто право/услугу из социјалне заштите;
- У ИС Социјална карта је могућ унос невалидног датума, тачније могућ је унос невалидног броја године (нпр. „0202“), као што је могућ и избор датума у прошлости (без лимита за унос године из прошлости);

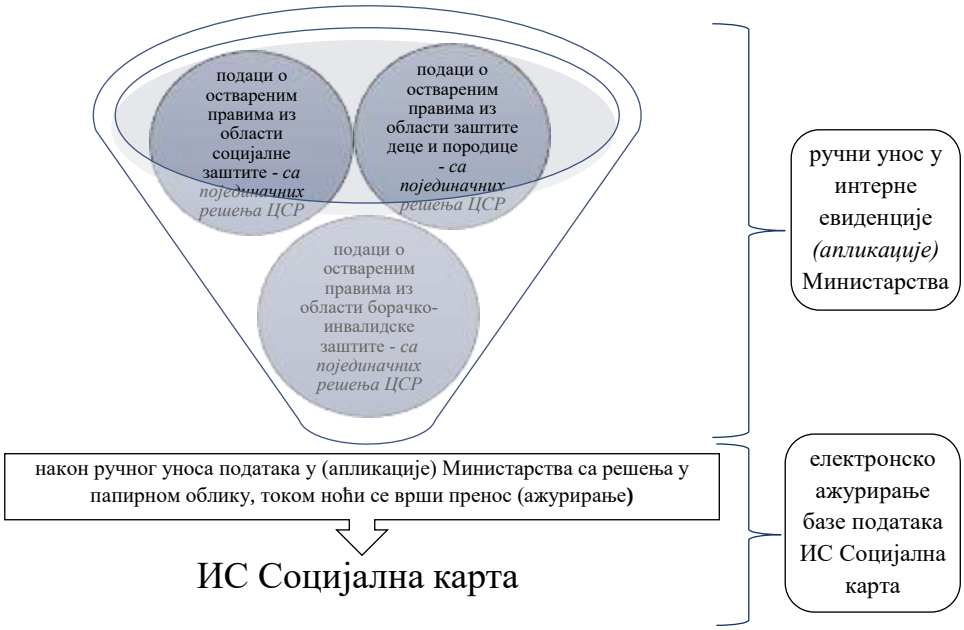
[73] Покрајински секретаријат за здравство, социјалну политику и демографију, Покрајински завод за социјалну заштиту, службе за дечију заштиту, службе за борачко - инвалидску заштиту.
[74] Јавна набавка ЈН 7/2020 - Набавка система за заштиту и аутоматизацију инструмената социјалне заштите.

- У тренутку када се већина ОСЛ улогује на ИС СОЗИС и ИС Социјална карта у истом тренутку, долази до загушења протока, а услед мале брзине интернет везе коју обезбеђује провајдер „Телеком Србија ад“. У пракси то значи да често ИС Социјална карта није доступна у краћем или дужем временском периоду;
- Проблем пристизања нотификација везаних за службе за социјалну и дечију заштиту и за службе за борачко - инвалидску заштиту, које још увек нису укључене у ИС Социјална карта (иако су предвиђени као корисници конкурсном документацијом ИС Социјална карта). У таквим случајевима, ОСЛ из ЦСР решавају нотификације за које нису надлежни (нпр. за решавање по питању права на дечији додатак);
- Проблем пристизања нотификација које проистичу из (правописних) грешака у уносу оперативних радника у Министарству – приликом уноса података са решења у интерне евиденције поменутог Министарства. У пракси процедура је следећа: решење ЦСР се шаље у Министарство, где се ручно уноси у интерне евиденције, те се деси да оперативни радник погреши приликом уноса[75] (нпр. имена или презимена корисника права). У таквим случајевима долази до ситуације –да ЦСР (по нотификацији) треба да обавештава Министарство о исправци грешке. Такође ЦСР може да погреши при доношењу решења, али се та грешка исправља тако што се доноси решење о исправци грешке, уз достављање личне карте корисника. Подаци у наведене интерне евиденције уносе се ручно са решења која достављају ЦСР. Наведене интерне евиденције Министарства су технолошки застареле, а сам начин уноса података са решења је подложан прављењу људских грешака и захтева велико ангажовање људских ресурса за ту намену. Грешке овакве врсте би се могле превазићи када би из ИС СОЗИС Министарство могло да „повуче“ податке у своје интерне евиденције;
- И поред обавезне примене ИС Социјална карта (сходно Закону о социјалној карти), у појединим ЦСР, уместо коришћења ИС Социјална карта, утврђена је употреба Система за размену података (еЗУП) за одлучивање о правима из социјалне заштите.

Такође, утврђено је да не постоји координација два сектора (Сектора за ИТ и Сектора за социјалну заштиту) у надзору над применом ИС Социјална карта (посебно у делу контроле нотификација) и то на основу увида у полугодишње извештаје о разрешавању обавештења из регистра Социјална карта (добијене у току поступка ревизије од Сектора за социјалну заштиту Министарства) и у извештаје које је сачињавало лице из Сектора за ИТ Министарства.

[75] Погледати Слика број 8: овог извештаја.

Слика број 8: Приказ тренутног начина ажурирања података у ИС Социјална карта подацима из интерних евиденција Министарства[76]



Због чињенице да је ИС Социјална карта још увек у фази развоја и доградње са другим ИС који користи Министарство/регистрима изворних евиденција, као и чињеници да у претходним фазама није било могуће предвидети све апликативне контроле, јављају се недостаци у апликативним контролама.

Последице неукључивања свих корисника ИС Социјална карта (службе за социјалну и дечију и борачку-инвалидску заштиту при ЈЛС), огледају се у већем обиму послова у ЦСР, који решавају нотификације које се односе на службе за социјалну и дечију и борачку-инвалидску заштиту при ЈЛС.

Последице недостатака у апликативним контролама могу бити видљиве кроз велики број решења о правима са невалидним датумом, захтеви под истим бројем, нерешене нотификације и тиме грешке при исплатама права из области социјалне заштите.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да омогући приступ ИС Социјална карта и другим (предвиђеним) корисницима у складу са одредбама Закона о социјалној карти, потписаним Споразумом са Канцеларијом за ИТ и електронску управу, или на други адекватан начин.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да отклоне уочене недостатке у апликативним контролама информационог система Социјална карта и да прецизно дефинишу активности надзора и контроле решавања нотификација у коришћењу ИС Социјална карта.

[76] Извор: ДРИ.

ЗАКЉУЧАК 2: Министарство није успоставило свеобухватне мере којима се обезбеђује континуитет пословања, у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта, укључујући и управљање резервним копијама.

Циљ овог дела извештаја је да одговоримо на друго ревизијско питање, односно у којој мери је успостављено управљање континуитетом пословања ИС Социјална карта у случају ванредних околности, хаварија и евентуалног раскида уговора са пружаоцем услуге развоја и одржавања ИС.

На основу анализе законских и подзаконских аката, документације субјекта ревизије и одржаних интервјуа, донели смо закључак који темељимо на следећим налазима.

Налаз 2.1: Министарство није успоставило план континуитета пословања у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта.

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.
Мере заштите ИКТ система односе се и на континуитет пословања у ванредним околностима (члан 7 Закон о информационој безбедности).

Такође, одредбама члана 29 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, прописане су мере које обезбеђују континуитет обављања посла у ванредним околностима.

Министарство није успоставило и имплементирало план континуитета пословања, као ни план опоравка ИТ од хаварије. Такође, Министарство није обезбедило могућност функционисања ИС Социјална карта у случају прекида сарадње са пружаоцем услуге одржавања ИС.

Недостататак стручног кадра, зависност од добављача, уз фокус на формално испуњење обавезе доношења Акта о информационој безбедности, без могућности да се он имплементира и спроводе, главни су разлози за непостојање правила и процедуре за континуитет пословања у случају ванредних околности, хаварија и прекида сарадња са пружаоцем услуга.

Поред тога што је то законска обавеза, план континуитета пословања пружа значајан одговор на ризике који постоје у вези са губитком података и треба да буде успостављен и периодично тестиран. Ризик је већи када је у питању раскид сарадње са пружаоцима услуга одржавања ИС, јер у том случају недостаје неопходно знање потребно за наставак одржавања и развоја, а нарочито у случају потенцијалне миграције података.

Према одредбама члана 7 Закона о информационој безбедности, прописано је, између осталог да оператор ИКТ система одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Мере заштите ИКТ система односе се и на континуитет пословања у ванредним околностима (члан 7 став 3 тачка 28) Закона о информационој безбедности).

Одредбама члана 29 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, прописане су мере које обезбеђују континуитет обављања посла у ванредним околностима и то:

- 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.

План континуитета пословања (BCP) треба да обухвати: донета правила и процедуре које уређују континуитет пословања, успостављање плана опоравка од катастрофе, управљање резервним копијама и тестирање ових планова и резервних копија. Сврха плана опоравка од катастрофе је да се, за случај појаве хаварије или другог прекида у пословању, детаљно одреди на који начин ће Министарство опоравити ИТ инфраструктуру и ИТ услуге у што краћем року.

План опоравка од хаварије чине процеси, мере и процедуре које обезбеђују припремање опоравка (враћања у стање пре катастрофе) или евентуални наставак функционисања кључних процеса у другачијим условима, што обавезује Министарство да обезбеди резервну технолошку инфраструктуру.

План опоравка од хаварије треба да садржи:

- процедуре за опоравак информационог система кад наступе катастрофални догађаји;
- приоритете опоравка ресурса информационог система;
- податке о тимовима и члановима тимова који ће бити одговорни за опоравак информационог система, њихове дужности и одговорности;
- резервну локацију за опоравак информационог система, односно локацију резервног рачунарског центра[77].

Као саставни део Акта о безбедности ИКТ система Министарства[78], донете су следеће процедуре:

- Оперативне процедуре информационе безбедности;
- „Back up“ и „Restore“ процедура[79];
- Процедура организације система безбедности.

[77] Одлука о минималним стандардима управљања информационим системом финансијске институције, „Службени гласник РС“ 23/2013-7, 113/13-99, 2/17-31, 88/19-80, 37/21-216, 100/23-59 (др. одлука).
[78] бр. 030-03-25/2020-01 од 9. октобра 2020. године.
[79] Ближе описано у оквиру Налаза 2.3. овог Извештаја.

Оперативне процедуре информационе безбедности у Министарству

Циљ процедуре је одређивање одговорности и процедуре за обезбеђивање исправног и безбедног рада средстава за обраду информација у Министарству, контрола свих промена у капацитетима средстава за обраду информација, контрола софтвера, успостављање дужности са циљем смањења ризика од намерне и ненамерне злоупотребе система, као и менаџмент техничких рањивости.

Процедура организације система безбедности

Процедура дефинише методе физичке заштите у ИС организације и разматра се у две основне области:

- Безбедне области (циљ ове области је да се спречи неовлашћени физички приступ, уништење или ометање информација и просторија;
- Заштита опреме (циљ ове области је да се спречи губитак, оштећење, крађа или компромитација имовине и прекид пословања организације).

Опрема треба да буде заштићена од проблема насталих услед неисправног електричног напајања и других нерегуларности који су последица отказа помоћних функција за подршку процесуирању података. За подршку опреми која подржава критичне пословне операције, препоручује се уређај за непрекидно напајање (UPS – Uninterruptable Power Supply) којим се обезбеђује реализација стандардне процедуре прекида рада или непрекидан рад у одговарајућем временском периоду. Планови за непрекидно напајање треба да обухвате и процедуре које је потребно предузети када откаже UPS уређај.

Уколико процес обраде података треба наставити и у случају дужег прекида напајања, треба размотрити примену генератора електричног напајања – агрегата.

Уређај за непрекидно напајање и генераторе треба редовно проверавати како би се осигурало да они имају адекватни капацитет, као и вршити њихово тестирање у складу са препорукама произвођача.

Када је у питања ИС Социјална карта све обавезе физичко-техничке заштите спроводи Канцеларија за ИТ и електронску управу. Канцеларија је обезбедила простор, инфраструктурне, мрежне и остале техничке услове, одговарајућу противпожарну заштиту и мере безбедности непрекидног електричног напајања и одговарајуће микроклиматске услове за несметан рад опреме у Државном дата центру.[80]

Уговор о услузи одржавања информационог система Социјална карта за 2022. и 2023. годину

Министарство има право да једнострано откаже уговор са пружаоцем услуге (добављачем), са отказним роком од 15 дана од дана достављања писменог обавештења о отказу, ако Добављач не извршава обавезе на начин и у роковима предвиђеним уговором, или ако у уговореним роковима не отклони недостатке у извршењу уговорених обавеза, о чему писмено обавештава Добављача[81].

[80] Одговор Канцеларија за ИТ и електронску управу на питања у вези обавеза из Закона о социјалној карти.
[81] Члан 11 Уговора о услузи одржавања информационог система Социјална карта, укључујући и лиценце (за 2022. и 2023. годину).

План опоравка ИТ услед катастрофе (хаварије)

Тим за ревизију извршио је увид у План опоравка ИТ услед катастрофе, који чини саставни део Акта о безбедности ИКТ система Министарства и утврдио да план није попуњен, тј. захтеви поменутог плана опоравка ИТ услед катастрофе нису прилагођени Министарству као организацији која, у случају катастрофе треба да предузме мере опоравка ИТ.

Министарство није имплементирало план континуитета пословања, као ни план опоравка ИТ од хаварије. Такође, Министарство није обезбедило могућност функционисања ИС Социјална карта у случају прекида сарадње са пружаоцем услуге одржавања ИС. Поред тога што је то законска обавеза, план континуитета пословања пружа одговор на ризике који постоје у вези са губитком података и треба да буде успостављен и периодично тестиран. Ризик је већи када је у питању раскид сарадње са пружаоцима услуга одржавања ИС, јер у том случају недостаје неопходно знање потребно за наставак одржавања и развоја, а нарочито у случају потенцијалног преласка на нови ИС и неопходну миграцију података.

Поред недостатка стручног и обученог кадра, Министарство је зависно од пружаоца услуга, и у случају раскида/отказа уговора, Министарство у дужем временском периоду неће бити у стању да одржава/врши неопходне измене ИС Социјална карта. Такође, у уговорима о одржавању ИС Социјална карта није прописана обавеза пружаоца услуге развоја ИС да обезбеди континуитет пословања за ИКТ системе, односно није дефинисана миграција података у случају да Министарство промени пружаоца услуга. Потребно је обезбедити да план континуитета пословања као и уговор о услузи одржавања ИС обухвате и евентуални случај прекида сарадње са пружаоцем услуге одржавања ИС.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да успостави план континуитета пословања што подразумева усвајање и имплементацију правила и процедура континуитета пословања у случају ванредних околности, хаварија и прекида сарадње са пружаоцем услуге одржавања ИС Социјална карта.

Налаз 2.2: Министарство не врши свеобухватно управљање резервним копијама зато што није обезбедило обуку запослених и тестирање резервних копија података.

Управљање резервним копијама података и тестирање резервних копија података су саставни део Плана континуитета пословања.

Заштита од губитка података постиже се редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за израду резервних копија. Оператор ИКТ система дефинише време чувања и заштите резервних копија, обим и учесталост резервних копија, безбедно место чувања резервних копија, обезбеђује физичку заштиту резервних копија и заштиту од спољашњих утицаја, проверава носаче података како би се осигурало њихово исправно функционисање и поузданост у складу са планом израде резервних копија. Резервне копије података треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима (члан 17 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

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 (члан 29 ст. 2-3 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

Министарство је у оквиру набавке ИС Социјална карта-I фаза од пружаоца услуге развоја и одржавања обезбедило „tape unit“ за складиштење „back up“ копије ИС Социјална карта.

Министарство је поред „back up“ копије ИС Социјална карта, у две одвојене јавне набавке, набавило и два централизована система за заштиту података у реалном времену („backup/restore oracle database“), један за примарну, а други за резервну локацију. У ова два система уложено је 162.096.000 динара са ПДВ-ом. Централизован систем за заштиту података у реалном времену за резервну локацију још увек није стављен у употребу.

Пре спровођења набавке додатних копија података ИС (у овом случају Социјална карта) било је потребно спровести „cost-benefit“ анализу, а након набавке спровести и тестирање функционалности набављених система за израду резервних копија података.

Министарство за све три резервне копије не врши провере исправности резервних копија података.

Министарство не спроводи активности из Процедуре за „Back up/restore“ података, која је саставни део Акта о безбедности ИКТ система Министарства.

Министарство нема обучене кадрове који могу спровести активности из Процедуре за „Back up/restore“ података, односно експертизу да креирају и прате ток креирања резервних копија и ураде поврат података са резервних копија.

Необученост кадрова, експертизе запослених, недостатак инфраструктуре (опреме) за „restore“ података и непреношење знања од пружаоца услуге ка Министарству су узроци неспровођења тестирања резервних копија података.

Због неспровођења редовне израде и провере (тестирања) резервних копија података ИС Социјална карта, постоји ризик да у случају наступања ванредних околности, ИС Социјална карта неће функционисати у дужем или краћем временском периоду.

Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја

Управљање резервним копијама података и тестирање резервних копија података су саставни део Плана континуитета пословања.

Заштита од губитка података постиже се редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за израду резервних копија. Оператор ИКТ система дефинише време чувања и заштите резервних копија, обим и учесталост резервних копија, безбедно место чувања резервних копија, обезбеђује физичку заштиту резервних копија и заштиту од спољашњих утицаја, проверава носаче података како би се осигурало њихово исправно функционисање и поузданост у складу са планом израде резервних копија. Оператор ИКТ система врши израду резервних копија података које треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима (члан 17 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

Према одредбама члана 29 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, оператер ИКТ система треба да успостави, документује, имплементира

и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације и да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.

Оперативне процедуре информационе безбедности у Министарству

Министарство је процедуром дефинисало да се регуларни „backup“ ИС ради због поврата свих података у случају инцидента, катастрофе, проблема са медијима и осталих проблема. Такође, дефинисано је и да се „back up“ проверава једном квартално путем „restore” процедуре како би се утврдила његова фунционалност. Такође је дефинисано да део података који има велику важност за организацију се аутоматски копира (реплицира) на посебан сервер. Копирање (репликација) се изводи једном недељно.

„Back up“ и „Restore“ процедура

„Back up“ и „Restore“ процедуром, као саставним делом Акта о безбедности ИКТ система Министарства, уређено је на који начин се врши процедура израде резервних копија података тј. Back up у Министарству, укључујући:

- учесталост backup-a,
- врсте backup-a,
- време вршења backup-a,
- за шта се врши backup,
- на који начин се користе и како се управља медијумима,
- договор око чувања медијума на другој локацији,
- политика задржавања медијума,
- који редовни извештаји се састављају и
- како се чувају информације о опоравку након катастрофе.

Процедура израде резервних копија података, тј. „backup“ у оквиру организације врши се за ИС (база података, база докумената, апликације, source code и др.) као и за сервисе, као и свих корисничких радних станица.

Процедуром је дефинисано да се спроводи редовни „back up“ главних пословних информација, како би се осигурало да се организација може опоравити након катастрофе, грешке или квара на медијумима. „Backup“ се врши помоћу „Veritas NetBackup“ система/софтвера, који омогућава чување података са свих сервера на дисковима (HDD) backup storage-a. Копија овог „backup“-а преноси се једном седмично на удаљену локацију („remote“) у Дата центру Телекома/Београд.

Као део процедуре за израду безбедносних копија података, спада и „Restore“ процедура враћања заштићених података и провера њихове валидности. Потребно је да служба за ИТ подршку податке или апликације које се backup-ују у оквиру организације на сваких шест месеци уради restore података са безбедносних копија за све типове „backup“-а. Ако је реч о бази података, власник/корисник делова система прави проверу валидности података и потврђују тачност података. Потврда се прави преко Записа Restore података са безбедносне копије.

Извештаји се састављају једном месечно од стране службе за ИТ подршку и прослеђују Менаџеру безбедности информација, како би се пратио обим сачуваних података и време утрошено на њихово чување. Форма овог извештаја треба да прати форму Записа „Backup“ план. Наведеном процедуром је уређено и да комплетна backup документација, укључујући и комплетне записе о томе шта је backup-овано заједно са restore записима о

опоравку су архивирани на удаљеној локацији, осим копија које се налазе на главној локацији. Исто тако, потребно је и да се редовно спроводи „restore“ тј. повраћај информација са „backup“ медија, како би се проверила поузданост backup медија и процеса опоравка.

Систем Библиотеке за “back up“ (саставни део набавке ИС Социјална карта)

За потребе “back up“ користи се Oracle StorageTek SL150 Tape Library, који поседује четири LTO 7 tape drive-а, са редудантним FC портовима брзине до 8Gbit/s. Tape drive-ови су повезани директно на Management сервер, где се налази бекап софтвер. Библиотека поседује 60 слотова за траке у 2 модула (базни и један додатни), односно у 4 магазина по 15 слотова.

Представници Министарства и пружаоца услуге су навели да је у оквиру I фазе имплементације ИС Социјална карта, постављен „tape unit” систем за складиштење „backup“ копије и извршена тестна провера, а да након тога нису вршене провере функционалности резервних копија података ИС Социјална карта.

Уговор о набавци система за backup/restore Oracle database (централизованог система заштите података у реалном времену)[82] из 2022. године и истог система за резервну локацију из 2023. године[83]

Министарство је набавило два централизована система за заштиту података у реалном времену („backup/restore oracle data base“), један за примарну, а други за секундарну локацију. У ова два система је уложено 162.095 хиљада динара.

Предмет јавних набавки (ЈН 12/2022 и ЈН 5/2023) био је испорука, имплементација и касније одржавање система backup-а и заштите података у реалном времену за Oracle базе података и интеграцију у постојеће продукционо окружење, независно од платформе, верзије или количине података које се налазе у бази. Сагласно члану 5 став 4 Уговора, добављач у потпуности одговара наручиоцу (Министарству) за извршење свих обавеза из тог уговора, укључујући и обавезе које је поверио подизвођачу.

Саставни део уговора за набавку система за примарну локацију је: техничка спецификација, којом су прописани минимални технички захтеви опреме „Интегрисани систем заштите података у реалном времену“ и то да, између осталог мора да буде заснован на „delta only“ архитектури backup-а, где се након комплетног backup-а, инкрементално заувек наставља процес, са могућношћу опоравка или враћања у било ком моменту времена, као и да мора да има потпуну интеграцију са Oracle RMAN алатом и процедурама за backup база података, без употребе додатног софтвера који ће контролисати процес и водити рачуна о току и механизму израде копија. Такође, техничком спецификацијом предвиђено је и да понуђач мора да уз понуђено решење понуди професионалне сервисе инсталације и интеграције који укључују, између осталог и да се на једном примеру уради backup/restore тест план као и генерисање документације изведеног стања.

Саставни део уговора за набавку система за резервну локацију је техничка спецификација, којом је дефинисано да је потребно извршити инсталацију предметне опреме у дата центар наручиоца и имплементирати у постојеће окружење. Инсталација је потребно да обухвата, између осталог успостављање бекапа са одговарајућим базама на резервној (ДР) локацији, успостављање бидирекционе репликације са примарним

[82] бр. 404-02-63/9/2022-22 од 20. јуна 2022. године.
[83] бр. 404-02-31/9/2023-22 од 26. априла 2023. године

системом, финалну верификацију и тестирање система и израду документације изведеног стања. Такође, техничком спецификацијом предвиђено је и да понуђач мора да уз понуђено решење понуди професионалне сервисе инсталације и интеграције који укључују, између осталог и да се на једном примеру уради backup/restore тест план као и генерисање документације изведеног стања.

Тестирање функционалности резервних копија података ИС Социјална карта

Министарство је у оквиру набавке ИС Социјална карта од пружаоца услуге развоја и одржавања обезбедило и „tape unit“ за складиштење „back up“ копије ИС Социјална карта.
Министарство је поред „back up“ копије ИС Социјална карта која је саставни део набавке ИС Социјална карта набавило и два централизована система за заштиту података у реалном времену („backup/restore oracle data base“), један за примарну, а други за резервну локацију. У ова два система је уложено 162.096.000 динара. Централизован систем за заштиту података у реалном времену за резервну локацију није стављен у употребу.

Пре спровођења набавке додатних копија података ИС (у овом случају Социјална карта) било је потребно спровести „cost-benefit“ анализу, а након набавке спровести и тестирање функционалности набављених система за израду резервних копија података.
Министарство за све три резервне копије не врши провере исправности резеревних копија података.

Министарство не спроводи активности из Процедуре за „Back up/restore“ података које су саставни део Акта о безбедности ИКТ системаМинистарства.

Министарство нема обучене кадрове који могу спровести активности из Процедуре за „Back up/restore“ података, односно експертизу да креирају и прате ток креирања резервних копија и ураде поврат података са резервних копија.

Необученост кадрова, експертизе запослених, недостатак инфраструктуре (опреме) за „restore“ података и непреношење знања од пружаоца услуге ка Министарству су узроци неспровођења тестирања резервних копија податка.

Због неспровођења редовне израде и провере (тестирања) резервних копија података ИС Социјална карта, постоји ризик да у случају наступања ванредних околности, ИС Социјална карта неће функционисати у дужем или краћем временском периоду.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да успостави свеобухватно управљање резервним копијама података што подразумева активности на обуци кадрова и проверу исправности резервних копија података у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.

ЗАКЉУЧАК 3: Министарство није успоставило управљање информационом безбедношћу на свеобухватан начин, јер није ускладило Акт о безбедности са прописима, као ни организационо и кадровски успоставило управљање информационом безбедношћу, док на нивоу ИС Социјална карта не постоје правила и процедуре праћења и контроле записа о догађајима (логова) нити сарадње са пружаоцем услуге одржавања, што може довести до нарушавања безбедности ИС.

Циљ овог дела извештаја је да одговоримо на треће ревизијско питање, односно да ли успостављене мере информационе безбедности обезбеђују поузданост ИС Социјална карта.

На основу анализе законских и подзаконских аката, документације субјекта ревизије и одржаних интервјуа, донели смо закључак који темељимо на следећим налазима.

Налаз 3.1: Акт о безбедности ИКТ система Министарства није усклађен са Законом о информационој безбедности, променама у окружењу и са ИКТ системом Социјална карта.

Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система. Актом о безбедности ИКТ система одређују се 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. Такође, Акт мора да буде усклађен с променама у окружењу и у самом ИКТ систему (члан 8 Закона о информационој безбедности).

Оператор ИКТ система од посебног значаја дужан је да ИКТ систем од посебног значаја којим управља упише у евиденцију ИКТ система од посебног значаја (члан 6б став 2 Закона о информационој безбедности).

Сагласно одредби члана 6а став 1 тачка 4) Закона о информационој безбедности, оператор ИКТ система од посебног значаја врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње.

Министарство је донело Акт о безбедности ИКТ система у 2019. години, који није усклађен са одредбама Закона о информационој безбедности и Уредбе о ближем садржају акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја.

У поступку ревизије смо утврдили да Министарство није:

- извршило упис ИКТ система Министарства у евиденцију ИКТ система од посебног значаја;

- прилагодило одредбе Акта о безбедности ИКТ система Министарства важећим законским и подзаконским прописима из области информационе безбедности;

- у већини делова прилагодило садржину акта организационим, кадровским и функционалним захтевима Министарства;

- усвојило и имплементирало нови Акт о безбедности ИКТ система, набављен 2023. године;

- вршило проверу усклађености примењених мера заштите ИКТ система са Актом о безбедности ИКТ система Министарства најмање једном годишње.

Министарство је процес израде Акта о безбедности ИКТ система Министарства поверило добављачу, а након израде (усвајања) није извршило тестирање (проверу) примењивости и усклађености Акта са законом и подзаконским прописима, као ни у наредним годинама нису вршене провере усклађености са законским прописима.

Информациона безбедност је најзначајније питање у свим организацијама које користе ИКТ системе од посебног значаја, док непримењивање Акта о безбедности ИКТ система Министарства доводи до ризика рањивости ИС и немогућности благовременог реаговања у ванредним околностима.

Према одредбама члана 8 став 1 Закона о информационој безбедности, оператор ИКТ система дужан је да донесе акт о безбедности ИКТ система, док је ставом 2 истог члана прописано да се тим актом 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.

Оператор ИКТ система од посебног значаја дужан је да ИКТ систем од посебног значаја којим управља упише у евиденцију ИКТ система од посебног значаја (члан 6б став 2 Закона о информационој безбедности).

Министарство је у току поступка ревизије извршило проверу уписа у евиденцију оператера ИКТ система од посебног значаја (телефонским путем) и том приликом извршило поновно попуњавање и слање захтев за упис података у поменуту евиденцију.

Сагласно одредби члана 6а став 1 тачка 4) Закона о информационој безбедности, оператор ИКТ система од посебног значаја врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње.

Закон о информационој безбедности ступио је 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 био 17. фебруар 2017. године.

Министарство је усвојило акт о безбедности информационог система под називом „Акт о безбедности информационо-комуникационог система Министарства за рад, запошљавање, борачка и социјална питања“[84].

Министарство је израду акта о информационој безбедности (и имплементације стандарда ИСО 27001) поверило добављачу и за ту услугу извршило плаћање у износу од 5.940 хиљада динара[85]. Саставни део Акта је пратећа документација (процедуре, планови, описи радних места, каталог запослених, упитници, итд).

Актом о безбедности ИКТ система Министарства нису прописане и одређене мере заштите, принципе, начине, процедуре за постизање и одржавања адекватног нивоа безбедности система, као ни овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја. Добављач при изради Акта није уважио организационе, техничко-технолошке, кадровске специфичности Министарства и прилагодио одредбе Акта тако да буду примењиве на конкретно Министарство.

[84] који је заведен под бројем 030-03-25/2020-01 од 9. октобра 2020. године.
[85] Јавна набавка 10/2019-услуга израде и имплементације стандарда ИСО 27001 и Акта о информационој безбедности ИКТ система Министарства.

Министарство је током 2023. године извршило набавку „Ажурирање акта о ИКТ безбедности и подршка примени стандарда и имплементацији стандарда ИСО 27001 и примену Акта о безбедности ИКТ система Министарства“[86]. Вредност набавке је била 7.166 хиљада динара. Новонабављени Акт о безбедности ИКТ система Министарства није усвојен и имплементиран до датума израде Извештаја о ревизији.

У поступку ревизије смо утврдили да Министарство није:

- извршило упис ИКТ система Министарства у евиденцију ИКТ система од посебног значаја;
- прилагодило одредбе Акта о безбедности ИКТ система Министарства важећим законским и подзаконским прописима из области информационе безбедности;
- у већини делова прилагодило садржину акта организационим, кадровским и функционалним захтевима Министарства;.
- усвојило и имплементирало нови Акт о безбедности ИКТ система, набављен 2023. године;
- вршило проверу усклађености примењених мера заштите ИКТ система са Актом о безбедности ИКТ система Министарства најмање једном годишње.

Министарство је процес израде Акта о безбедности ИКТ система Министарства поверило добављачу, а након израде (усвајања) није извршило тестирање (проверу) примењивости и усклађености Акта са законом и подзаконским прописима, као ни у наредним годинама нису вршене провере усклађености са законским прописима.

Информациона безбедност је најзначајније питање у свим организацијама које користе ИКТ системе од посебног значаја, док непримењивање Акта о безбедности ИКТ система Министарства доводи до ризика рањивости ИС и немогућности благовременог реаговања у ванредним околностима.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да Акт о безбедности ИКТ система усклади са одредбама Закона о информационој безбедности и да усвоји и имплементира процедуре постизања и одржавања адекватног нивоа безбедности ИС Социјална карта.

Налаз 3.2: Министарство није у потпуности успоставило организацију ИТ безбедности у смислу обезбеђивања одговарајућих организационих и кадровских капацитета.

Према одредби члана 7 став 3 тачка 1) Закона о информационој безбедности, мере заштите ИКТ система односе се на успостављање организационе структуре са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система. Такође, оператор ИКТ система дужан је да у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања, утврди послове и одговорности запослених, у циљу управљања информационом безбедношћу (члан 2 став 1 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

Министарство није успоставило организациону структуру са утврђеним пословима и одговорностима запослених за ИТ безбедност. Министарство нема запослене на пословима информационе безбедности.

[86] Јавна набавка 16/2023.

Министарство није именовало менаџера безбедности информација како је то дефинисано одредбама Акта о безбедности ИКТ система Министарства.

Недовољни кадровски капацитети, уз значајну ослоњеност да ће пружалац услуге одржавања информационих система заштити рачунарске системе од потенцијалних напада су главни разлози зашто Министарство није успоставило управљање информационом безбедношћу.

Управљање информационом безбедношћу је изузетно важна област и захтева одговарајућу организацију и запослене који могу заштитити ресурсе Министарства, опрему и информационе системе од неовлашћеног упада и приступа подацима.

Закон о информационој безбедности

Према одредби члана 7 став 3 тачка 1) Закона о информационој безбедности, мере заштите ИКТ система односе се на успостављање организационе структуре са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система.

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја

Оператор ИКТ система дужан је да у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања, утврди послове и одговорности запослених, у циљу управљања информационом безбедношћу (члан 2 став 1 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Оператор ИКТ система утврђује у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности (члан 2 став 2 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја) .

Подела одговорности запослених треба да се изврши тако да се онемогући неовлашћена или ненамерна измена, оштећење или злоупотреба средстава, односно информационих добара оператора ИКТ система, као и да се онемогући приступ, измена или коришћење средстава без овлашћења и без евиденције о томе (члан 2 став 3 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Правилник о организацији и систематизацији послова у Министарству у делу који се односи на информационе технологије

Министарство је у поступку ревизије доставило извод из Правилника о организацији и систематизацији послова у Министарству у делу који се односи на информационе технологије[87].

Правилником о организацији и систематизацији послова у Министарству у оквиру два одељења при Сектору за ИТ имају следећа задужења:

1. Одељење за анализу, развој и унапређење информационог система и техничку подршку обавља послове који се поред осталих односе на „вршење анализе ризика и

[87] Број: 011-00-281/1/2023-05 од 11. јула 2023. године, са изменама и допунама број: 011-00-281/2/2023-05 од 20. новембра 2023. године.

унапређење система информационе безбедности“ и „других мера које се односе на укупну безбедност информационог система“.
2. Одељење за апликативни развој, обраду података, аналитику и извештавање поред осталог обавља послове који се односе на: „праћење рада и имплементацију механизама и стандарда у домену безбедности ИС у оквиру својих надлежности“.

Правилником о организацији и систематизацији послова у Министарству није дефинисано шта је од ових послова у описима радних места запослених у том одељењу, осим за два непопуњена радна места начелника одељења[88] (погледати Табела број 1 овог извештаја) и радног места администратора мреже и мрежних сервиса[89]. У одговору на упитник о стању ИТ у Министарству[90], као одговор на питање да ли Министарство има запослено лице одговорно за безбедност ИС, одговорна лица Министарства су истакла да није именовано лице за безбедност ИТ система. У Акту о безбедности ИКТ система Министарства предвиђено је радно место Менаџер информационе безбедности. Правилником о организацији и систематизацији послова у Министарству није предвиђено радно место са таквим називом и задужењима.

Министарство није успоставило организациону структуру са утврђеним пословима и одговорностима запослених за ИТ безбедност. Министарство није именовало менаџера безбедности информација како је то дефинисано одредбама Акта о безбедности ИКТ система Министарства.

Недовољни кадровски капацитети, уз значајну ослоњеност да ће пружалац услуге одржавања информационих система заштити рачунарске системе од потенцијалних напада су главни разлози зашто Министарство није успоставило управљање информационом безбедношћу.

Управљање информационом безбедношћу је изузетно важна област и захтева одговарајућу организацију и запослене који могу заштитити ресурсе Министарства, опрему и информационе системе од неовлашћеног упада и приступа подацима.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да предузме мере на организационом и кадровском успостављању информационе безбедности, кроз јачање кадровских капацитета и обуку запослених у циљу обављања послова заштите безбедности информационих система.

Налаз 3.3: Министарство није успоставило механизам за редовно праћење и контролу записа о догађајима (логова) на нивоу целокупног ИС Социјална карта.

Оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати (члан 18 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Оперативном процедуром информационе безбедности Акта о безбедности ИКТ система Министарства, прописано је које информације треба да садрже дневници логова система/сервера, да дневнике у којима су се водили записи о изузецима и осталим

[88] „планира и организује активности развоја безбедности информационог система и предлаже, планира и организује и реализује имплементацију нових технологија у оквиру надлежности Одељења“.
„планира и организује активности на успостављању безбедности информационог система и обезбеђењу континуитета пословања за апликације у надлежности одељења;“.
[89] „иницира, планира и организује активности развоја безбедности мрежне инфраструктуре“.
[90] послатог Министарству електронском поштом, дана 13. новембра 2023. године.

догађајима везаним за безбедност треба чувати барем шест месеци, као и да треба спречити самоиницијативно брисање или деактивирање дневника од стране систем администратора. Дневнике треба редовно проверавати, како би били сигурни да се прате одговарајуће процедуре. У случају проблема (нарушени рад оперативног система, system health check) систем шаље e-mail поруку администратору. Мониторинг се ради за све важне сервере, апликације, мрежну опрему и штампаче. Једном дневно администратор прегледа логове са циљем анализирања и откривања нетипичних или недозвољених активности. Сви логови се чувају и одлажу у складу са „Backup“ и „Restore“ процедуром Акта о безбедности ИКТ система Министарства.

Министарство није успоставило механизам за редовно праћење и контролу записа о догађајима (логова) на нивоу целокупног ИС Социјална карта.

Министарство не врши редовни преглед записа о догађајима, нити се записи о догађајима одлажу и чувају како је то дефинисано у Оперативној процедури информационе безбедности.

Услед недостатка кадровских капацитета и неспровођења одредби Закона о информационој безбедности и Акта о безбедности ИКТ система Министарства, Министарство је омогућило да пружалац услуге одржавања ИС Социјална карта има приступ свим записима о догађајима (логовима).

Користи од праћења и редовне контроле записа о догађајима (логова) су обезбеђивање безбедности информација, анализа неуобичајених уноса у информациони систем, брже откривање/реаговање на инциденте/нежељене догађаје, а тиме и мања могућност злоупотреба података из ИС Социјална карта.

Креирање лог фајлова

Оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати. Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене. У оквиру ИКТ система записују се активности администратора и корисника и редовно преиспитују у циљу заштите. У циљу обезбеђивања поузданости записа, времена у свим подсистемима ИКТ система морају бити синхронизована међусобно, као и са референтним тачним временом[91].

Оперативна процедура информационе безбедности

Као саставни део Акта о безбедности ИКТ система Министарства, усвојена је и Оперативна процедура информационе безбедности. Процедуром информационе безбедности, прописано је да дневници логова система/сервера морају садржати следеће информације:

- идентитет система;
- идентификација корисника;
- успешно/неуспешно пријављивање;
- успешно/неуспешно одјављивање;
- неовлашћени приступи апликацији;
- промене у конфигурацији система;

[91] члан 18 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

– коришћење привилегованих налога (нпр. за управљање налогом, политику промена, конфигурацију уређаја).

Такође, истом процедуром прописано је да дневнике у којима су се водили записи о изузецима и осталим догађајима везаним за безбедност, треба чувати барем шест месеци, као и да је потребно заштитити приступ дневницима од неовлашћеног приступа који могу да доведу до крађе или брисања забележених информација.

Потребно је спречити самоиницијативно брисање или деактивирање дневника од стране систем администратора. Оперативно особље и систем администратори морају водити дневник својих активности. Сви администраторски логови се чувају у различитим фајловима, и приступ њима има само Менаџер безбедности информација.

Дневници треба да укључују:

– време спровођења backup и детаље о размени backupa;
– време почетка и завршетка системског догађаја и ко је био укључен у њега;
– системске грешке (које, датум и време) и предузете корективне мере.

Дневнике треба редовно проверавати, како би били сигурни да се прате одговарајуће процедуре.

У случају проблема (нарушени рад оперативног система, system health check) систем шаље e-mail поруку администратору. Мониторинг се ради за све важне сервере, апликације, мрежну опрему и штампаче. Једном дневно администратор прегледа логове са циљем анализирања и откривања нетипичних или недозвољених активности. Сви логови се чувају и одлажу у складу са „Backup“ и „Restore“ процедуром Акта о безбедности ИКТ система Министарства.

Министарство не врши редовни преглед записа о догађајима, нити се записи о догађајима одлажу и чувају како је то дефинисано у Оперативној процедури информационе безбедности.

Закон о социјалној карти, члан 19 став 3

Сваки приступ Социјалној карти мора бити аутоматски забележен јединственим идентификатором лица које је приступило подацима, са тачним временом приступа, а систем такође бележи изворе из којих је преузет податак, поступак којим је неки податак промењен, као и датум и време измене податка (члан 19 став 3 Закона о Социјлној карти). Представници Министарства су навели да лице са улогом „администратор система“ у ИС Социјална карта, има могућност претраге лог фајлова:

– „Преглед логова упита“, којим је омогућено проналажење корисника који су претраживали базу социјално-економског статуса лица, сортираних према датуму и времену упита;
– „Преглед пријава на систем“, којим је омогућен увид у податке о приступању корисника систему, сортираних према датуму и времену приступа;
– „Преглед промена матичних података лица“, којим је омогућен увид у матичне податке о лицу и како су се ти подаци појављивали везано уз решења која су доношена;
– „Логови извршења изворних сервиса“ – ИС Социјална карта прати и када је који сервис позван, као и да ли је успешно извршен.

На захтев да се записи о догађајима (логови) ИС Социјална карта за 2022. и 2023. годину извезу и доставе у електронској форми, Министарство је навело да на корисничком

интерфејсу апликације регистра не постоји могућност да се ови подаци извезу, управо ради спречавања могућности да неко од корисничких рола преузме податке из регистра Социјална карта. Такође, Министарство у свом одговору наводи да се увид у записе о догађајима (логове) једино може извршити посебним захтевом Министарства према пружаоцу услуге одржавања ИС Социјална карта, који нема уговорну обавезу за тај посао, али с обзиром да би то представљало обраду података о личности, Министарство би морало да постигне аранжман у којем би један од обавезних докумената био закључивање акта са добављачем као „обрађивачем података“ о личности за ту намену.

Према изјави представника Министарства пружалац услуге одржавања ИС Социјална карта има могућност приступа свим записима о догађајама (логовима), са мрежне стране у сврху развоја и одржавања ИС и то му је уговорна обавеза уколико решава проблем у функционисању ИС Социјална карта.

Као што је наведено у Налазу 3.5. пружалац услуге одржавања ИС Социјална карта има приступ „продукционом“ окружењу преко VPN линије. Пружалац услуге одржавања ИС Социјална карта има техничку и стручну компетенцију да изврши увид, извоз и анализу записа о догађајима (логова).

Министарство не врши редовно праћење и контролу записа о догађајима (логова) у одређеном периоду како је то прописано чланом 18 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја. Праћење и контролу записа о догађајима (логова) једино може извршити пружалац услуге одржавања ИС на захтев Министарства.

Услед недостатка кадровских капацитета и неспровођења одредби Закона о информационој безбедности и Акта о безбедности ИКТ система Министарства, Министарство је омогућило да пружалац услуге одржавања ИС Социјална карта има приступ свим записима о догађајима (логовима).

Користи од праћења и редовне контроле записа о догађајима (логова) су обезбеђивање безбедности информација, анализа неуобичајених уноса у информациони систем, брже откривање/реаговање на инциденте/нежељене догађаје, а тиме и мања могућност злоупотреба података из ИС Социјална карта.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да успостави механизам редовног праћења и контроле записа о догађајима (логова) на нивоу целокупног ИС Социјална карта.

Налаз 3.4: Министарство није уредило управљање ИТ пословима (администрирање система) на начин да те послове обављају искључиво државни службеници.

Оператер 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 (члан 10 став 1 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја). Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (члан 10 став 4 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Министарство именује администратора органа који управља налозима администратора органа корисника података, док корисник података именује администратора органа који

управља налозима овлашћених службених лица која у оквиру својих надлежности обрађују податке, у складу са прописима којима се уређује електронска управа (члан 13 Закона о социјалној карти).

Према одредбама члана 84 Закона о државној управи послове из делокруга државне управе врше државни службеници.

Правилником о унутрашњем уређењу и систематизацији радних места у Министарству прецизније су уређени послови који се обављају у оквиру Министарства, тачније у Сектору за ИТ, међу којима и радна места предвиђена за администраторе система.

Према одредби члана 197 Закона о раду, послодавац може за обављање послова који су по својој природи такви да не трају дуже од 120 радних дана у календарској години да ангажује лица по уговора о привременим и повременим пословима.

Улогу администратор система Социјална карта имају и лица која су ангажована ван радног односа (по основу уговора о привременим и повременим пословима), што није у складу са одредбама члана 84 Закона о државној управи да послове из делокруга органа државне управе врше државни службеници.

Министарство је улогу администратора система ИС Социјална карта доделило и лицима ангажованим по основу уговора о привременим и повременим пословима иако су то стални, континуирани послови, који захтевају ангажовање 365 дана у години.

Такође, у описима послова лица ангажована по уговора о привременим и повременим пословима није наведено да обављају послове „администратор система“ ИС Социјална карта. Недостатак кадровских капацитета, неадекватна кадровска политика и подела послова и дужности унутар Министарства су разлози за ангажовање спољних сарадника за послове из делокруга рада Министарства.

Ангажовање спољних сарадника за послове из делокруга органа државне управе доводи до ризика да у наредном периоду све послове обављају спољни сарадници и непреношења знања на запослене у Министарству што у дужем року онемогућава Министарства да управља ИС Социјална карта.

Оператер 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 (члан 10 став 1 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (члан 10 став 4 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Одредбом члана 13 Закона о социјалној карти, Министарство именује администратора органа који управља налозима администратора органа корисника података, док корисник података именује администратора органа који управља налозима овлашћених службених лица која у оквиру својих надлежности обрађују податке, у складу са прописима којима се уређује електронска управа.

Према одредбама члана 84 Закона о државној управи послове из делокруга државне управе врше државни службеници. Законом о државним службеницима регулисан је радно правни положај државних службеника и њихова права и дужности, као и поступак и процедура ангажовања која подразумева по правилу заснивање радног односа на

неодређено време, али даје могућност заснивања и радног односа на одређено време. Законом о министарствима (члан 19) прописано је да Министарство обавља послове државне управе који се, између осталог односе и на систем социјалне заштите, борачку и инвалидску заштиту, остваривање права и интеграцију избеглих и расељених лица, итд.

Правилником о унутрашњем уређењу и систематизацији радних места у Министарству прецизније су уређени послови који се обављају у оквиру Министарства, тачније у Сектору за ИТ, међу којима и радна места предвиђена за администраторе система.

Администратор система Социјална карта

У ИС Социјална карта поред улоге администратор система коју има 10 лица, постоје и улоге администратор ОЈ, Руководилац ОЈ, овлашћено службено лице (ОСЛ), администратор пријемног органа, службено лице за одлуке Владе, „ВІ“ улоге. Администратори система као и корисници се на ИС Социјална карта пријављују квалификованим електронским сертификатом или путем мобилне апликације. Оба начина пријаве су пријаве високог нивоа поузданости.

Улоге (роле) у ИС Социјална карта су отворене на основу Решења помоћника министра[92] и Решења помоћника министра[93]. Укратко, наведеним решењима је уређено да ће лице са улогом „Администратор система“ обављати послове управљања корисничким налозима, врши контролу унетих корисничких налога, управља администрацијом нотификација.

Табела број 4. Приказ налога „администратора система“ ИС Социјална карта из Сектора за ИТ Министарства[94]

Назив радног места/врста ангажовања	Улога (рола) у ИС Социјална карта	Активан/Пасиван налог
1	*2*	*3*
администратор обраде података и техничке подршке	Администратор система	Активан
администратор мреже и мрежних сервиса	Администратор система	Активан
оператер и контролор података	Администратор система	Активан
уговор о привременим и повременим пословима	Администратор система	Активан
уговор о привременим и повременим пословима	Администратор система	Активан
оператер и контролор података	Администратор система	Активан
оператер и контролор података	Администратор система	Активан
оператер и контролор података	Администратор система	Активан
оператер и контролор података	Администратор система	Активан
оператер и контролор података	Администратор система	Активан

Као што је приказано у Табела број 4, од укупно 10 активних налога администратора система ИС Социјална карта, два лица нису запослена у Министарству, већ су ангажована по уговору о привременим и повременим пословима.

Уговори о привременим и повременим пословима:

1. представљају рад ван радног односа;

[92] број: 021-01-00021/154/2022-14 од 11. априла 2022. године.
[93] број: 021-01-00021/154-1/2022-14 од 11. априла 2022. године.
[94] Извор: ДРИ.

2. по својој природи такви да не трају дуже од 120 радних дана у календарској години и
3. могу се закључити са незапосленим лицем; запосленим који ради непуно радно време - до пуног радног времена; корисником старосне пензије (члан 197 Закона о раду).

Улогу администратор система Социјална карта имају и лица која су ангажована ван радног односа (по основу уговора привременим и повременим пословима) што није у складу са одредбама члана 84 Закона о државној управи да послове из делокруга органа државне управе врше државни службеници.

Министарство је улогу администратора система ИС Социјална карта доделило и лицима ангажованим по основу уговора о привременим и повременим пословима иако су то стални, континуирани послови, који захтевају ангажовање 365 дана у години.

Ангажована лица по уговорима о привременим и повременим пословима током 2022. и 2023. године континуирано су обављали исте/сличне послове, с тим да су им уговори незнатно мењани. На овај начин наведени послови нису привременог и повременог карактера већ је потреба за тим пословима стална (континуирана).

У описима послова лица ангажована по уговора о привременим и повременим пословима није наведено да обављају послове администрације систем Социјална карта.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да за послове из делокруга органа државне управе, односно администраторе система ИС Социјална карта именује искључиво лица запослена у Министарству за рад, запошљавање, борачка и социјална питања.

Налаз 3.5: Министарство није успоставило (уредило) однос са пружаоцем услуге одржавања ИС Социјална карта у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

Министарство је дужно да заштити средства која су доступна пружаоцима услуга што подразумева[95]:

-ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине приступа информацијама и средствима и надзор над приступом;

-идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације;

-споразумом регулише обавезе пружаоца услуге у вези са информацијама и средствима која су доступна пружаоцима услуге.

Министарство је такође у обавези да именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности (према одредби члана 27 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

Министарство није дефинисало правила и процедуре којима се уређује сарадња са пружаоцем услуге одржавања ИС Социјална карта, у делу нивоа доступности и врсте информација којима може да приступи пружалац услуге, начине приступа информацијама и средствима и надзора над приступом. Регулисање односа са пружаоцем услуга одржавања ИС Социјална карта у овом делу подразумева и управљање

[95] према одредби члана 26 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја.

информационом безбедношћу за шта је потребно јачати кадровске капацитете и стручна знања.

Министарство има потписан споразум са пружаоцем услуге одржавања ИС Социјална карта о поступању са поверљивим информацијама, који се не може сматрати споразумом прописаном чланом 26 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја.

Пружалац услуге има приступ „продукционом окружењу“, односно бази података са свим подацима корисника права преко VPN линије. Министарство није именовало лице за контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора како је предвиђено чланом 27 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

Узрок је зависност од пружаоца услуге, која се повећава из године у годину, набавкама нових ИС (уз модернизацију постојећих) без утврђеног приоритета у набавкама и мањку обучених кадрова.

Последица је могућност да пружалац услуге приступа ИС Социјална карта и свим базама података, као и да врши увид у личне (осетљиве) податке о личности и остварена права корисника система социјалне заштите.

Закон о информационој безбедности

Мере заштите ИКТ система су уређене одредбама члана 7 Закона о информационој безбедности. Оператор ИКТ система одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се, између осталог, односе на:

- заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга (став 3 тачка 25) и
- одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга (став 3 тачка 26).

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја

Према одредбама члана 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, оператор ИКТ система у својим процедурама предвиђа:

- ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга,
- начине приступа информацијама и средствима и
- надзор над приступом.

Оператор ИКТ система треба да идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације (члан 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга оператора ИКТ система, регулишу се споразумом између оператора

ИКТ система и пружаоца услуга, чијим одредбама се обезбеђује адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима (члан 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Оператор ИКТ система дужан је да обезбеди да пружалац услуга обавља поверене активности у складу са актом о безбедности ИКТ система, односно другим актима којима се уређује безбедност његовог информационог система (члан 26 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

Према одредбама члана 27 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, у циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, оператор ИКТ система успоставља механизме надзора над пружањем услуга, именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора.

Оперативне процедуре информационе безбедности[96]

Процедуром је дефинисано да су развојно софтверско окружење и тестно окружење, одвојени од оперативног, продукционог окружења, како би се смањио ризик случајних промена или неовлашћеног приступа. Такође, дефинисано је и да је потребно одвојити развојно и окружење за тестирање путем најприкладнијих контрола које укључују, али нису коначне, следеће контроле:

1. Рад на одвојеним рачунарима, доменима, инстанцама и мрежама,
2. Различита корисничка имена и лозинке,
3. Одвојити дужности оних који имају приступ развоју и оних који тестирају софтвер.

Затим, приликом постављања нових верзија, тестно окружење се креира репликацијом (виртуелизација или друга метода) продукционог окружења, која омогућава идентично окружење и тестирање у реалним условима. При том се посебна пажња посвећује репликацији: увек када је могуће избегава се коришћење продукционих тј. реалних података при тестирању. У случају када то није могуће, ради се обавезно „маскирање“ података. Тестирање на реалним подацима у тестном окружењу је дозвољено само уз сагласност Менаџера безбедности информација и само од стране запослених који имају право приступа тим информацијама.

Уколико се приликом развоја и тестирања апликативног софтвера користе подаци о личности, они морају бити заштићени и контролисани у складу са Законом о заштити података о личности и када постоји могућности, треба их деперсонализовати.

Уговор о услузи одржавања информационог система Социјална карта – I и II фаза укључујући и лиценце (за 2022. [97] и 2023.[98] годину)

Према одредбама члана 4 наведених уговора, уговорне стране се обавезују да ће поступати у складу са прописима који регулишу заштиту тајности података приликом и у вези са извршењем предмета тог Уговора, о чему ће уговорне стране приликом закључења тог Уговора, о чему ће уговорне стране приликом закључења тог Уговора, закључити и Споразум о поступању са поверљивим информацијама, који је саставни део

[96] Акт о безбедности ИКТ система Министарства.
[97] број: 404-02-152/9/2021-22 од 9. децембра 2021. године.
[98] број: 404-02-128/10/2022-22 од 25. јануара 2023. године.

тог Уговора. Добављач се обавезује да чува поверљивост података који се налазе у ИС Социјална карта, да не врши размену, објављивање, односно достављање поверљивих података трећим лицима на било који начин, без сагласности Наручиоца. Уколико Добављач прекрши неку од одредби овог члана, па Наручилац претрпи услед тога штету, установљава се обавеза накнаде штете у пуном износу.

Министарство је доставило споразуме о поступању са поверљивим информацијама (за 2022. [99] и 2023. [100] годину), закључених између Министарства и пружаоца услуге одржавања (добављач), чији је предмет регулисање међусобних односа у погледу поступања са поверљивим информацијама, подацима и документима (члан 1). Одредбом члана 6 наведених Споразума, добављач је дужан да обезбеди да сва лица која су ангажована на реализацији овог споразума чувају као поверљиве информације, документа и податке до којих дођу или које им постану доступне у поступку реализације уговора.

Министарство:

- није усвојило процедуре којим се ближе уређују услови пружање услуга од стране пружаоца услуге (добављача),
- није регулисало споразумом обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга,
- није именовало лице за контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора, како је предвиђено чланом 26 и 27 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

Споразум о поступању са поверљивим подацима се не може сматрати споразумом прописаним чланом 26 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја.

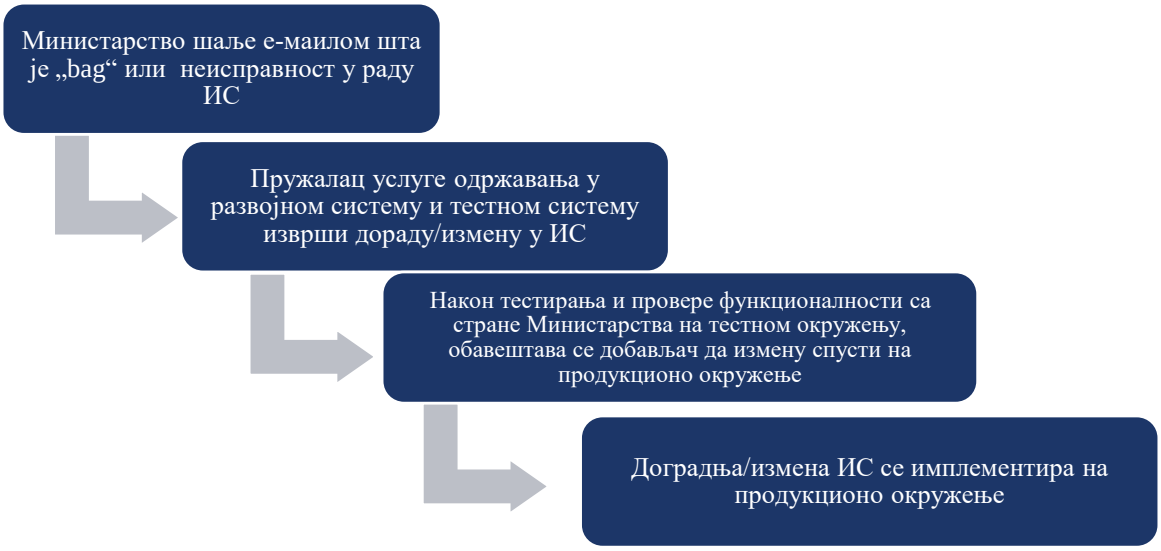
Приступ продукционом окружењу ИС Социјална карта

Одговорна лица Министарства нису доставила уговоре о обради података о личности закључене у 2022. и 2023. години са пружаоцем услуге одржавања ИС Социјална карта, јер, према изјави представника Министарства[101], пружалац услуге одржавања ИС Социјална карта не врши обраду података о личности у смислу Закона о заштити података о личности, нити има својство „обрађивача", нити обрађује податке о личности у име руковаоца, односно Министарства.

Представници Министарства наводе да се све измене и решавање проблема у ИС Социјална карта спроводе према шеми наведеној на следећем графику.

[99] број 404-02-152/10/2021-22 од 9. децембра 2021. године.
[100] број: 404-02-128/11/2022-22 од 25. јануара 2023. године.
[101] Одговор Министарства на питање да ли потписују уговор о обради података о личности са пружаоцем услуге одржавања ИС Социјална карта.

Слика број 9: Шема комуникације са пружаоцем услуге приликом измена/дорада ИС Социјална карта[102]



Представници пружаоца услуге одржавања (добављач) ИС Социјална карта су изјавили да целокупан поступак тестирања развојног система врши на „тест“ окружењу, односно да ниједног тренутка нису имали приступ „продукционом“ окружењу и да је њихов принцип пословања да не приступају „продукционом“ окружењу. Такође, навели су да „окружења“ припадају Министарству и да њима могу приступити преко VPN конекције која омогућава само надзор опреме, односно да немају приступ базама података, подацима корисника и сл.

У поступку ревизије утврђено је пружалац услуге одржавања ИС Социјална карта има приступ „продукционом“ окружењу преко VPN линије.

Када се врши измена/доградња ИС Социјална карта или се врши увид у појединачно решење за одређеног корисника права или услуге из социјалне заштите, овлашћено лице пружаоца услуге (добављача) у циљу реализације тражених измена у ИС Социјална карта или измене у web сервису, приступа осетљивим личним подацима личности корисника права или услуге из области социјалне заштите.

Узроци су зависност од пружаоца услуге, која се повећава из године у годину, набавке нових ИС (уз модернизацију постојећих) без утврђеног приоритета у набавкама и мањку обучених кадрова.

Последица је могућност да пружалац услуге приступа ИС Социјална карта и свим базама података, као и да врши увид у личне (осетљиве) податке о личности и остварена права корисника система социјалне заштите.

Препоручујемо Министарству за рад, запошљавање, борачка и социјална питања да уреди однос са пружаоцем услуге одржавања ИС Социјална карта у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

[102] Извор: ДРИ.

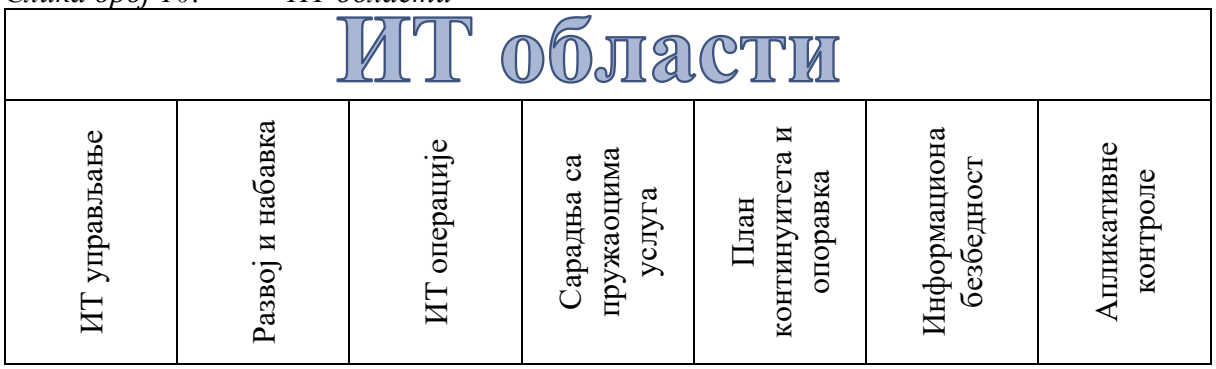
V Прилози

1. Прилог 1 – Методологија у поступку рада

Ревизија је спроведена у складу са Методолошким правилима и смерницама за ревизију сврсисходности пословања.

Да бисмо одговорили на ревизијска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions), Методолошка правила и смернице за ИТ ревизију као и све податке добијене од субјекта ревизије и извора информација – здравствених установа. Анализирали смо податке и информације за период од 2020. до 2023. године. На основу прикупљених података у току предстудије и у складу са Приручником за спровођење ревизије, одабране су три ИТ области у оквиру којих су обављени поступци ревизије: ИТ управљање, Сарадња са пружаоцем услуга и Информациона безбедност.

Слика број 10: ИТ области



У фази планирања ревизије, са представницима Министарства смо обавили разговор (интервју) на којем су постављена следећа питања:

1. Навести информационе системе које користите (уз кратко објашњење за шта се користе, од када, у којој су фази имплементације, где су смештени сервери, резервне копије, ко су корисници ИС, и да ли је неки ИС интерно креиран, да ли је обезбеђена раздвојеност развојног, тестног и продукционог окружења)
2. Кадровски ИТ капацитети *(одговорна лица, запослени, места рада, обуке)*
    a. које послове обављају запослени на ИТ пословима
3. Да ли је рађена интерна или екстерна ревизија ИС?
4. Да ли постоји и користи се стратешки план *(или план највишег нивоа управљања)* којим се планира употреба и развој ИТ капацитета?
5. Да ли постоји и користи се оперативни *(акциони)* план употребе и развоја ИТ капацитета?
6. Да ли постоји процедура/акт којим се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга *(развоја и одржавања информационих система)*?
7. На који начин се прати и анализира квалитет пружених услуга од стране добављача?
8. Да ли су донети и у употреби План континуитета пословања, План опоравка у случају хаварије?
9. Да ли се спроводи тестирање планова?
10. Да ли постоје тимови за управљање континуитетом пословања и управљања активностима у случају хаварија?

11. Да ли је било тежих инцидената у претходне 2 године ?
12. Да ли постоје и где се чувају резервне копије података?
13. Да ли је усвојен и користи се Акт о информационој безбедности
14. Да ли је омогућен удаљен приступ?
15. Број администратора и корисника по сваком ИС
16. Да ли постоје матрица привилегија за сваки ИС
17. Да ли је обезбеђено генерисање лог фајлова у ИС/7
18. Употреба лозинки, мењања истих.
19. Да ли је могућа употреба екстерних уређаја за складиштење података?
20. Да ли право приступа ИС Социјална карта имају само овлашћена лица? *(сви запослени, и/или постоје одређена ограничења)*
21. Да ли је могућ извоз података о корисницима права у неким од стандардних формата (excel, word, pdf, hml), извештаји, штампа извештаја итд.

Ревизијско питање 1:

- Анализа белешки са састанака руководства да би се проценило да ли се адекватно планирају, реализују и прате ИТ пројекти дефинисани законима/подзаконским актима/програмима развоја, у којима је субјект ревизије одређен за носиоца активности имплементације и развоја.
- Анализа белешки са састанака руководства да би се осигурало да су стратешке ИТ одлуке субјекта ревизије донете на највишем нивоу управљања.
- Интервјуисање руководства субјекта ревизије да би се утврдили неопходни ресурси ИС и начин на који су исти утврђени и одобрени.
- Интервјуисање руководства или других одговорних лица за одобравање пројеката да би се утврдило да су узете у обзир ИТ организационе способности субјекта ревизије, вештине, ресурси и потреба за обуком, као и могућност да се користе (и/или развију) нови ИТ софтвер (алати), методе или процедуре.Анализа одобрених и/или одбијених захтева за покретање поступака набавки да би се проценило да ли су исти у складу са стратегијом и акционим планом и/или другим стратешким документом субјекта ревизије, или дефинисани законима/подзаконским актима/програмима развоја.
- Разговори са запосленима да би се утврдила учесталост извештавања вишег руководства о резултатима поступака набавки и/или покренутих ИТ пројеката.
- Интервјуисање руководства или других одговорних лица да би се утврдило како организација анализира, успоставља приоритете и управља захтевима корисника ИС.
- Анализа организационе шеме како би се утврдило да ли је ИТ организација успостављена на стратешком нивоу.
- Анализа ИТ организационе шеме како би се утврдило да ли у складу са законским обавезама и организована тако да пружа потребну подршку .
- Анализа извештаја о планираним и спроведеним обукама у вези са ИТ темама (укључујући и пратећу документацију која се тиче захтева за одржавање обуке, распореда одржавања обука и сл.).
- Анализа документације да би се утврдило да ли су ИТ ризици део општег оквира за управљање ризицима и усклађености.
- Анализа плана за управљање ризицима и/или осталих докумената у циљу потврђивања да ли су одговорности за управљање ИТ ризицима јасно и недвосмислено додељене.

- Преглед белешки са састанка да би се осигурало да су нови/потенцијални ИТ ризици анализирани.
- Интервјуисање руководства и/или преглед белешки са састанака да би се утврдило да је руководство свесно и осталих ризика и да периодично прати њихов статус.

Ревизијско питање 2:

- Процена да ли организација има адекватна правила и процедуре за ангажовање спољних сарадника (пружалаца услуга одржавања ИС).
- Анализа да ли уговорни услови дефинишу безбедносна ограничења и обавезе којима се контролишу како ће извођачи користити имовину организације и приступати ИС.Анализа захтева за изменама/ажурирањем ИС у циљу сагледавања да ли се приликом измене/ажурирања ИС примењују правила и процедуре заштите осетљивих података о личности (*псеудонимизација, енкрипција и сл.*).
- Анализа да ли се организација постарала да је континуитет пословања (*у смислу задржавања пословног знања и власништва над пословним процесом*) садржан у уговору/споразуму о пружању услуге са добављачем.
- Анализа да ли је субјект ревизије упознат са ризицима непродужења/отказивања пружања услуге одржавања и развоја ИС Социјална карта, као и да ли су предузете одговарајуће мере у циљу ублажавања наведених ризика.
- Процена да ли организација има адекватна правила и процедуре за одржавање континуитета пословања, односно адекватна правила и процедуре којима се обезбеђује обављање послова у ванредним околностима.
- Преглед документације у циљу процене да ли правила и процедуре узимају у обзир захтеве за континуитет пословања кроз дефинисање организационих циљева за непредвиђене ситуације.
- Преглед документације или интервјуисање запослених у циљу утврђивања да ли се врши ажурирање правила и процедуре за континуитет пословања у случају промењених услова пословања.
- Преглед документације или интервјуисање запослених у циљу утврђивања примарних контрола физичке безбедности субјекта ревизије, као и провера да ли одговарају најновијој анализи/процени ризика.
- Преглед документације или интервјуисање запослених у циљу утврђивања локацијских и физичких мера предострожности у смислу кључних елемената ИТ инфраструктуре, као и провера успостављених контрола за заштиту животне средине (*апарат за гашење пожара, алармни систем, системи за напајање и сл.*)
- Преглед докуменатације да би се проценило да су израђене детаљне процедуре за прављење резервних копија базе података.
- Преглед докуменатације да би се проценило да план за прављење резервних копија садржи све кључне хардвере, податке и апликативне софтвере.
- Преглед докуменатације и интервијисање запослених у ИТ сектору да би се проценило да ли се план за прављење резервних копија базе података адекватно спроводи.
- Преглед докуменатације да би се проценила адекватност локације резервне копије базе података и поузданости начина транспорта датотека (података, фајлова и сл.) на локацију резервне копије базе података.

- Провера да ли је адекватна логичка и физичка безбедност локације резервне копије базе података.
- Преглед документатације да би се проценило да ли се у прописаним временским интервалима реализују тестирања резервних копија базе података.
- Провера да ли субјект ревизије контролише да ли се врши редовно тестирање резервне копије базе података и плана за опоравак након катастрофе, у случају да се резервна копија базе података води код спољно ангажоване агенције.
- Преглед докумената да би се проценило да су препоруке након тестирања адекватно праћене и да ли се план за континуитет пословања и план за опоравак након катастрофе адекватно ажурирају.

Ревизијско питање 3:

- Анализа да ли ИТ Стратегија идентификује: улоге и одговорности руководства и свих корисника, свест и обуку о безбедности.
- У одсуству ИТ стратегије, интервјуи са највишим руководством, руководством средњег нивоа и запосленима како би се утврдило разумевање стратешке улоге безбедности информација.
- Анализа да ли акт о безбедности ИКТ система и политике и процедуре за ИТ идентификују: улоге и одговорности руководства и свих корисника, свест и обуку о безбедности.
- Анализа документације како би се проценило да ли су израђене детаљне процедуре за одговарајући ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине приступа информацијама и средствима и надзор над приступом.
- Анализа документације да би се проценило да правила и процедуре узимају у обзир захтеве за заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга, ради обезбеђивања информационе безбедности.
- Анализа механизама (електронске, физичке поште, обука, итд.) да би се осигурало да су правила о безбедности ИТ система дистрибуирана запосленима онда када се ажурирају или када за то постоји потреба.
- Анализа правилника о унутрашњем уређењу и систематизацији радних места у делу који се односи на информациону безбедност (*утврдити да ли је одговорност за ИТ безбедност формално и јасно наведена*).
- Анализа извештаја о спроведеним обукама запослених на тему информационе безбедности *(распоред обука, резултати завршних тестова, оцена ефективности обуке).*
- Анализа да ли постоји документована процедура за реаговање на безбедносне инциденте и да ли су корисници упознати са процедуром и опасностима од угрожавања безбедности информација.
- Анализа извештаја о безбедносним инцидентима и докумената за праћење како би се утврдило које активности субјект ревизије предузима када појединци крше безбедносна правила и процедуре.
- Анализа извештаја о безбедносним инцидентима да би се идентификовао број кршења безбедности информација од стране запослених или трећих лица у датом периоду, у циљу процене ефективности правила и процедура.
- Анализа документације у циљу утврђивања да ли су добављачи услуге одржавања и развоја ИС Социјална карта извршили повреде безбедности информација. Провера активности руководства у погледу таквих кршења.

- Анализа да ли постоји адекватно обучен тим за реаговање у случају инцидента који има адекватан алат, ресурсе и подршку вишег руководства за решавање инцидената.
- Анализа процедуралних мера које је субјект ревизије предузео како да би се ускладио са захтевима поверљивости података.
- Преглед документације или интервјуисање запослених у циљу провере поштовања одредби акта о информационој безбедности у делу односа са пружаоцем услуге развоја и одржавања ИС Социјална карта.
- Анализа докумената како би се утврдило које матрице основних услуга су обухваћене уговором између Министарства и добављача услуге одржавања ИС Социјална карта.
- Анализа матрица улога за утврђивање одговорности за администрирање конфигурације и опсега контроле конфигурације у оквиру ИС Социјална карта.
- Утврђивање да ли су се у прошлости јављали проблеми због конфигурацијских недоследности. Ако је тако, интервјуи са руководиоцима организационих јединица да би се утврдило који су поступци примењени у отклањању конфигурацијских недоследности.
- Анализа процедура и/или праксе субјекта ревизије у циљу утврђивања учесталости прегледања различитих приступа и привилегија које запослени или корисници имају у ИС Социјална карта.
- Одабир (по систему ревизијског узорка) корисничких и системских налога како би се утврдило постојање јасно дефинисане улоге и/или привилегије мапиране према функцијама посла, као и овлашћење власника података и руководства (тј. потписане/ писане сагласности).
- Интервјуи са корисницима (из ревизијског узорка) и провера упутстава, како би се утврдио начин на који су корисници упознати са својим одговорностима за заштиту осетљивих информација или имовине, у тренутку одобравања приступа ИС.
- Провера да ли су квалитативни захтеви за подешавање лозинки за приступ ИС дефинисани и примењени системом за управљање мрежом и/или оперативним системом заснованим на локалним захтевима/ организационим правилима и/или процедурама и/или најбољој пракси.
- Анализа документације везане за пријаву и решавање проблема корисника у коришћењу ИС Социјална карта.

Као део поступка прикупљања података у ревизији, на адресе електронске поште 21 ЦСР[103] послат је упитник са следећим питањима:

1. Колико је запослених запослено на ИТ пословима у Вашој установи ?
   ** укључујући и запослене на ИТ пословима на одређено време, по ПП пословима, уговорима о делу и сл.*
   ** укључујући и радна места као што су администратор система, администратор мреже, аналитичари информационих система, администратори база података и сл."*
2. Да ли је Ваша установа повезана на информациони систем (ИС) Социјална карта и да ли има регистроване кориснике?

[103] ЦСР Ниш, ЦСР Панчево, ЦСР Нови Пазар, ЦСР Зајечар, ЦСР Сурдулица, ЦСР Љубовија, ЦСР Пирот, ЦСР Горњи Милановац, ЦСР Нови Сад, ЦСР Београд, ЦСР Зрењанин, ЦСР Шабац, ЦСР Крагујевац, ЦСР Ужице, ЦСР Јагодина, ЦСР Лесковац, ЦСР Крушевац, ЦСР Суботица, ЦСР Ваљево, ЦСР Бачка Топола, ЦСР Александровац.

** уколико је одговор ""не"", молимо Вас да наведе разлоге због којих установа још увек није повезана на ИС Социјална карта и не користи га"*

3. Колико запослених Ваше установе користе ИС Социјална карта у свом раду ? *(доставити преглед корисника са називом додељене улоге-име, презиме, радно место, улога у ИС Социјална карта)*
4. Да ли су сви запослени Ваше установе (који имају отворен администраторски/кориснички налог у ИС Социјална карта) прошли обуку за употребу ИС Социјална карта ?
   ** потребно је унети податак о томе који број запослених је прошао обуку, а који број још увек није прошао обуку (од укупног броја запослених који користе ИС Социјална карта)"*
5. Да ли је званично усвојена процедура отварања/укидања/промене корисничких рола (улога) у ИС Социјална карта ?
   ** уколико јесте, доставити акти, навести број и датум од када се процедура/одлука/упутство/инструкција примењује*
6. Ко је задужен за отварање, укидање и промену корисничких улога (рола) у ИС Социјална карта у Вашој установи ?
   ** укључујући улоге: "Администратор система", "Администратор у ОЈ", "Руководилац ОЈ"" и "Овлашћено службено лице", "Администратор пријемног органа" - уколико постоји*
   ** потребно је навести задужено лице за отварање, укидање и промене сваке улоге (роле) у ИС Социјална карта појединачно*
7. Да ли се отварање корисничких улога (рола) у ИС Социјална карта врши на основу претходне одлуке директора установе ?
8. Да ли се врши, ко врши и на који начин се врши контрола доделе, укидања и промене корисничких улога (рола) у ИС Социјална карта у Вашој установи ?
9. Да ли корисници ИС Социјална карта из Ваше установе потписују изјаве о поверљивости података и неодавању информација ?
   ** Да ли су такви захтеви део уговора о раду закљученим са тим лицима ? Да ли су ти захтеви предвиђени неким другим актом (навести којим) ?*
10. Да ли постоји званично усвојена процедура контроле активности корисника (лог фајлова) у ИС Социјална карта ?
11. Да ли се врши анализа/контрола активности корисника (лог фајлова) у ИС Социјална карта у Вашој установи, или то ради неко из Министарства за рад, запошљавање, борачка и социјална питања?

** примери таквих активности могу бити:*
1. да ли се запослени (корисници) свакодневно логују на ИС Социјална карта
2. идентификовање нелогичности - логовање у ИС Социјална карта под именом запосленог који је на годишњем одмору, боловању и сл.
3. претрага логова приступа тј. подацима којих корисника се приступа → у циљу потврђивања да ли је то овлашћено службено лице задужено за конкретног корисника и сл.
4. претрага логова приступа тј. подацима којих корисника се приступа → у циљу утврђивања да ли су подаци којима се приступа одлучујући за дато право или не
5. провера доделе статуса лицима од стране ОВЛ: „У провери“ и/или „Непознато – (или) лице са генерисаним привременим бројем“ и исправка грешака и сл.

12. Да ли је званично усвојена процедура контроле решавања нотификација у ИС Социјална карта и/или периодичне анализе/контроле нотификација у статусу „Разрешена“ ?
    ** уколико јесте, доставити акт и навести број и датум процедуре/одлуке/упутства/инструкције"*
13. Уколико није усвојена званична процедура контроле решавања нотификација у ИС Социјална карта, да ли се врши контрола, ко је врши и на који начин се врши анализа/контрола решавања нотификација у ИС Социјална карта, а посебно нотификација у статусу „Разрешена“ ?
14. Након успешно решене нотификације у ИС Социјална карта, на који начин се измена података о појединцу/повезаном лицу преносе у интерне електронске евиденције Министарства (из којих део података долазе у Регистар социјална карта) ?
    ** електронским сервисима или ручно (у папирном облику)*
15. Колико често се врши ажурирање/освежавање података о кориснику права и/или са њим повезаним лицима у ИС Социјална карта ?
16. Да ли је званично донета/усвојена одлука директора Ваше установе о учесталости ажурирања/освежавања података о кориснику права или са њим повезаним лицима у ИС Социјална карта ?
17. Да ли вршите ажурирање/освежавање података о кориснику права у ИС Социјална карта непосредно пре одлучивања о додели права из социјалне заштите?

    Да ли вршите ажурирање/освежавање података о кориснику права у ИС Социјална карта непосредно пре исплате права из социјалне заштите?"

18. Да ли сте пријављивали проблеме/предлоге за унапређењем у функционисању ИС Социјална карта од почетка његове примене ?
19. Наведите до три предлога/проблема у рада са ИС Социјална карта (по могућству да се односе на рад информационог система, застоја у раду, прекида интернет конекције, приступа систему, ажурности података)
20. На који начин су проблеми/предлози за унапређењем пријављивани у пракси?
    ** мејл адресом, званичним дописом добављачу/Министарству и/или на други начин*
21. Да ли су пријављени проблеми/предлози за унапређењем решени/спроведени ?
22. Назив установе, име, презиме, број телефона, фунција (радно место) лица које је попунило упитник.

Сви ЦСР којима је послат упитник су на исти и одговорили.

Канцеларији за ИТ послали смо допис и поставили следећа питања:

1. На који начин сте уредили сарадњу са Министарством за рад, запошљавање, борачка и социјална питања сходно одредбама Закона о социјалној карти (Сл. гласник број 14/2021) - *члан 5 и 18 Закона*?
2. На који начин сте уредили и како спроводите послове техничке подршке Министарству за рад, запошљавање, борачка и социјална питања у успостављању и одржавању информационог система Социјална карта, односно послове који се односе на чување, спровођење мера заштите и

обезбеђивање сигурности и безбедности података у оквиру Социјалне карте? *(члан 5 Закона о социјалној карти)*

3. Да ли и на који начин предузимате одговарајуће безбедносне мере у циљу заштите података од незаконитог уништења или губитка, мењања, неовлашћеног обелодањивања или приступа када се обрада података врши употребом информационо-комуникационих технологија? *(члан 18 Закона о социјалној карти)*
4. Да ли је у периоду од 2022. године до данас било покушаја неовлашћеног приступа Социјалној карти и да ли сте о томе обавештавали Министарство за рад, запошљавање, борачка и социјална питања ?
5. Где се налазе примарна и секундарна база података Социјалне карте и на који начин се обезбеђује физичка заштита истих?
6. Да ли Канцеларија за ИТ и електронску управу креира резервну копију података сервера на ком се налази информациони систем Социјална карта?
7. Да ли вршите (повремени) „restore“ података са „backup“ копије за информациони систем Социјална карта?

У току спровођења ревизије обишли смо четири ЦСР (ЦСР „Дунав“ Инђија, ЦСР „Сава“ Сремска Митровица, Градски ЦСР Београд и ЦСР Града Новог Сада), одржали састанке са представницима ЦСР и поставили питања у вези са ИС Социјална карта а у циљу стицања ближег разумевања о:

- функционисању интернет везе за конекцију на ИС Социјална карта у ЦСР;
- увид у ИС Социјална карта у улогама „Администратор у ОЈ“, „Руководилац ОЈ“ и „ОСЛ“);
- провера могућности уноса невалидног датума захтева у ИС Социјална карта;
- увид у начин решавања обавештења (нотификација) од стране ОСЛ по ЦСР.