ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ПОСЛЕРЕВИЗИОНИ ИЗВЕШТАЈ О МЕРАМА ИСПРАВЉАЊА РЕПУБЛИЧКОГ ФОНДА ЗА ЗДРАВСТВЕНО ОСИГУРАЊЕ, БЕОГРАД

по ревизији сврсисходности пословања на тему „Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање“

Број: 400-450/2023-07/27
Београд, 5. април 2024. године

Садржај:

1. УВОД

Државна ревизорска институција (у даљем тексту: „Институција) издала је Извештај о ревизији сврсисходности пословања на тему „Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање“ број: 400-450/2023-07/22 од 22. новембра 2023. године, у којем је навела закључке и налазе.

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

Субјект ревизије је доставио Одазивни извештај 01 Број: 180-902/2023-2 од 24. фебруара 2024. године и Допуну Одазивног извештаја 01 Број: 400-19/2024-1 од 20. марта 2024. године у којима су приказане мере исправљања утврђених несврсисходности, а које је потписало и печатом оверило одговорно лице субјекта ревизије.

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

У овом извештају:

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

2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА

ПРИОРИТЕТ 2 - означава несврсисходности које је могуће отклонити у року до годину дана.

2.1 РФЗО није донео ИТ стратегију за период 2022–2024. године.

2.1.1 Опис несврсисходности

Стратегија се по правилу усваја за период од пет до седам година, а остваривање њених циљева планира се и прати посредством акционог плана за спровођење стратегије.

Републички фонд за здравствено осигурање (у даљем тексту: „РФЗО“) није израдио ИТ стратегију за период 2022-2024. године и пратећи акциони план ради спровођења мера из ИТ стратегије. РФЗО је усвојио ИТ стратегију за период 2019-2021. године.

РФЗО наводи да због пандемије вируса COVID 19 и додатних послова и задатака није усвојио нову стратегију, за период 2022-2024. године.

Влада доноси Стратегију развоја здравствене заштите ради обезбеђивања и спровођења друштвене бриге за здравље на нивоу Републике Србије. Влада доноси програме здравствене заштите ради спровођења Стратегија развоја здравствене заштите (чл. 18 и 19 Закона о здравственој заштити). Друштвена брига за здравље на нивоу Републике Србије обухвата и обезбеђивање услова за развој ИЗИС. ИС МЕОП је саставни део ИЗИС-а. Влада није донела Стратегију развоја здравствене заштите.

Користи од усвајања ИТ стратегије и акционог плана јесу олакшано планирање развоја ИТ, сврсисходно коришћење расположивих финансијских средстава и унапређено ИТ управљање и тиме остваривање пословних циљева РФЗО.

2.1.2 Исказане мере исправљања и њихово вредновање (препорука 1)

РФЗО је дата препорука да донесе стратешки документ (ИТ стратегију) и акциони план, којим би се планирао развој и управљање информационим системима, рачунарским апликацијама, базама података и континуираном обуком запослених.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да ће формирати раду групу коју ће чинити представници филијала и дирекције која ће израдити нацрт Стратегије ИТ за период 2024-2027. године, преиспитати и ажурирати текст стратегије ИТ која је била усвојена за период 2019-2022. године. Радна група ће сачинити предлог Акционог плана за спровођење Стратегије и израдити модел анкете који ће бити достављен корисницима систсма како би свако од њих сагледао потребе за развојем и унапређењем постојећег система као и евентуалним ризицима.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 1. новембра 2024. године.

Доказ:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године.

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

2.2 ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета.

2.2.1 Опис несврсисходности

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.

Корисници јавних средстава успостављају финансијско управљање и контролу у складу са одредбама Закона о буџетском систему. Према одредбама Закона о информационој безбедности (члан 3 став 1 тачка 1), 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 ФУК у јавном сектору). Оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за управљање ризицима у области информационе безбедности (члан 2 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО није идентификовао све ИТ ризике, а последично ни планове и мере за умањење ризика. РФЗО је усвојио Стратегију управљања ризицима, а за период ревизије 2020-2022. године утврдио три ИТ ризика која се понављају сваке године.

У Сектору за развој и ИТ у Дирекцији РФЗО у Београду на 34 систематизована радна места, запослено је 15 лица. У 29 филијала РФЗО, попуњеност радних места на ИТ пословима је 63%.

РФЗО није препознао све ИТ ризике због мањка ИТ кадрова и неучествовања запослених на ИТ пословима у филијалама РФЗО у идентификовању ИТ ризика при изради Стратегије управљања ризицима.

Значајно ограничење у развоју ИКТ система је и недовољан број запослених у Сектору за развој и ИТ и смањена могућност запошљавања нових кадрова, што последично утиче и на спровођење мера за умањење ИТ ризика.

Последице непрепознавања ИТ ризика могу бити непотребно велики трошкови у случају настанка нежељеног догађаја (који се могао спречити) или велики нефинансијски губици (у првом реду података) због немогућности благовременог предузимања мера.

2.2.2 Исказане мере исправљања и њихово вредновање (препорука 3)

РФЗО је дата препорука да успостави управљање ИТ ризицима, што подразумева евидентирање, класификацију, анализу свих ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да је Сектор за развој и информационе технологије доставио предлог нових ризика и да су исти усвојени на радној групи финансијског управљања и контроле, у Регистру ризика за 2023. годину. Такође, приликом израде Регистра ризика били су укључени представници филијала.

Такође, у одазивном извештају се наводи и да ће, с обзиром да постојећа Стратегија за управљање ризицима важи за период 2021-2024. године, у току 2024. године бити донета нова стратегија управљања ризицима у којој ће посебна тачка бити управљање ИТ ризицима.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 31. јула 2024. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године;

- Записник са састанка Радне групе за одржавање и редовно ажурирање система финансијског управљања и контроле у Републичком фонду за здравствено осигурање, одржаног дана 27. децембра 2023. године, 30-12 број: 110-41/2022-3 од 27. децембра 2023. године;
- Регистар ризика за 2023. годину.

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

2.3 РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података.

2.3.1 Опис несврсисходности

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).

РФЗО је успоставио организациону структуру са утврђеним пословима и одговорностима запослених за ИТ безбедност. Међутим, РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података, иако је Правилником о организацији и систематизацији послова је систематизовано 12 радних места. Запослени на ИТ пословима су учествовали на две обуке за ИТ безбедност у периоду ревизије (2020-2022. година).

Узроци су мањи број запослених од предвиђеног броја (систематизованог), већина запослених у опису послова имају задужење везано за информациону безбедност, а да им то није превасходни радни задатак и неучествовање на обукама из информационе безбедности.

Организација ИТ безбедности у РФЗО није успостављена тако да обухвата примену адекватних прописа која уређују ову област – Закона о информационој безбедности, Закона о здравственој документацији и евиденцијама у области здравства, Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, Акта о информационој безбедности и других интерних аката, као и примену других мера заштите ИКТ система, што за последицу има већи степен рањивости информационог система.

2.3.2 Исказане мере исправљања и њихово вредновање (препорука 5)

РФЗО је дата препорука да предузме мере на кадровском јачању Сектора за информациону безбедност и заштиту података.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да је упутио лице овлашћено за заштиту података у РФЗО на обуку лица за заштиту података, у организацији Канцеларије за ИТ и Е управу.

Такође, РФЗО у одазивном извештају наводи и да је у претходном периоду ступио у контакт са свим факултетима који имају информатички смер у циљу регрутације кадра на пословима ИТ безбедности. Исто тако, РФЗО је извршио анализу постојећег кадра у организационим јединицама и у наредном периоду ће на послове везане за информациону безбедност и заштиту података бити распоређен постојећи кадар.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 1. новембра 2024. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-43/2024-1 од 29. јануара 2024. године.

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

2.4 РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података.

2.4.1 Опис несврсисходности

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).

РФЗО је успоставио организациону структуру са утврђеним пословима и одговорностима запослених за ИТ безбедност. Међутим, РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података, иако је Правилником о организацији и систематизацији послова је систематизовано 12 радних места. Запослени на ИТ пословима су учествовали на две обуке за ИТ безбедност у периоду ревизије (2020-2022. година).

Узроци су мањи број запослених од предвиђеног броја (систематизованог), већина запослених у опису послова имају задужење везано за информациону безбедност, а да им то није превасходни радни задатак и неучествовање на обукама из информационе безбедности.

Организација ИТ безбедности у РФЗО није успостављена тако да обухвата примену адекватних прописа која уређују ову област – Закона о информационој безбедности, Закона о здравственој документацији и евиденцијама у области здравства, Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, Акта о информационој безбедности и других интерних аката, као и примену других мера заштите ИКТ система, што за последицу има већи степен рањивости информационог система.

2.4.2 Исказане мере исправљања и њихово вредновање (препорука 6)

РФЗО је дата препорука да предузме активности у циљу континуиране едукације запослених који обављају ИТ послове.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да је усвојен План стручног усавршавања запослених у Републичком фонду за здравствено осигурање број: 30-12/2-151-46/2024 од 30.01.2024. године и да су одобрена усавршавања за укупно 12 запослених из ИТ која су у току или ће бити окончана у току године. Такође, РФЗО наводи и да су Планом стручног усавршавања запослених у Републичком фонду за здравствено осигурање су обухваћене и интерне обуке за запослене из филијала из области МЕОП и заштите података које ће бити спроведене у току године. Правилником о стручном усавршавању запослених биће уведена обавезна континуирана едукација запослених на ИТ пословима.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 1. новембра 2024. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године;
- План стручног усавршавања запослених у Републичком фонду за здравствено осигурање, број: 30-12/2-151-46/2024 од 30. јануара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-43/2024-1 од 29. јануара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-45/2024-1 од 29. јануара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-44/2024-1 од 29. јануара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-50/2024-1 од 14. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-53/2024-1 од 26. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-54/2024-1 од 26. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-52/2024-1 од 26. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање, број: 30-12/2-151-51/2024-1 од 26. фебруара 2024. године.

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

2.5 РФЗО није у потпуности успоставио процес праћења и контроле приступа ИС МЕОП од стране ЗУ и запослених у РФЗО.

2.5.1 Опис несврсисходности

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 и члан 22 Акта о безбедности информационо-комуникационог система РФЗО).

РФЗО бележи приступ ИС МЕОП (од стране запослених у РФЗО-у и ЗУ) путем записа о догађајима (логови фајлова).

РФЗО нема успостављена правила и процедуре редовног праћења и контроле записа о догађајима (лог фајлова) у одређеном периоду, већ се зависно од случаја до случаја ради проверу записа о догађајима (лог фајлова).

Записи о догађајима (лог фајлови) су веома обимни и захтевају редовно праћење и контролу. Користи од праћења и редовне контроле записа о догађајима (лог фајлова) су брже откривање/реаговање на инциденте/нежељене догађаје а тиме и мања могућност злоупотреба података из ИС МЕОП.

2.5.2 Исказане мере исправљања и њихово вредновање (препорука 7)

РФЗО је дата препорука да успостави правила и процедуре за редовну контролу и праћење приступа ИС МЕОП.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да је РФЗО у току поступка ревизије доставио Извештај о контролама управљања корисничким

налозима за филијале Београд, Зрењанин и Панчево, као и матрицу привилегија администраторских и корисничких налога за ИС МЕОП након извршене анализе администраторских и корисничких налога.

У Плану јавних набавки РФЗО за 2024. годину 30-01/2 број: 110-20/2024-3 од 23.2.2024. године, планирана је набавка софтверског решења за заштиту база података. Након спроведене јавне набавке „Система за заштиту база података“, било би имплементирано софтверско решење које би повећало сигурност самих база.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 1. новембра 2024. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године;
- План јавних набавки Републичког фонда за здравствено осигурање за 2024. годину, 30-01/2 број: 110-20/2024-3 од 23. фебруара 2024. године.

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

2.6 РФЗО није успоставио (уредио) однос са пружаоцем услуга одржавања ИС МЕОП у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

2.6.1 Опис несврсисходности

РФЗО је дужан да споразумом регулише обавезе пружаоца услуге у вези са информацијама и средствима која су доступна пружаоцима услуге (према одредби члана 26 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО 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).
- одговорно за информациону безбедност и контролу приступа и надзора над извршењем уговорних обавеза, као и поштовање одредби правилника којима су такве активности дефинисане (према одредби члана 30 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање).
- одговорно за информациону безбедност које редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама (према одредби члана 31 Акта о безбедности информационо-комуникационог система Републичког фонда за здравствено осигурање).

РФЗО није дефинисао правила и процедуре којима се уређује сарадња са пружаоцем услуге одржавања ИС МЕОП, 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 МЕОП у овом делу подразумева управљање информационом безбедношћу за шта је потребно јачати кадровске капацитете и стручна знања.

Као што смо навели, информациона безбедност није кадровски успостављена у РФЗО, што може имати утицаја на реализацију уговора о одржавању ИС МЕОП, квалитет извршених услуга, контролу приступа ИС, надзор над извршењем уговорних обавеза и заштиту података.

2.6.2 Исказане мере исправљања и њихово вредновање (препорука 8)

РФЗО је дата препорука да успостави правила и процедуре сарадње са пружаоцем услуга развоја и одржавања ИС МЕОП, што подразумева дефинисање нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да је спроведен поступак јавне набавке услуге одржавања дела софтверских система РФЗО. РФЗО наводи и да ће на основу закљученог уговора пружалац услуге бити у обавези да закључи уговор о обради података о личности који ће дефинисати нивое доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

У Плану набавки РФЗО за 2024. годину, планирана је набавка унапређења система цМЕОП у области међународне сарадње, интеграција са системом еБоловања и системом за издавање КЗО[1]. Такође, након спроведене набавке унапређења система цМЕОП у области међународне сарадње, интеграције са системом еБоловања и системом за издавање КЗО, са пружаоцем услуге ће бити закључен уговор о обради података о личности. У допуни Одазивног извештаја, РФЗО је навео да ће у складу са одредбама Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, Закона о информационој безбедности и Акта о информационој безбедности, РФЗО ажурирати правила и процедуре урђења односа са пружаоцем услуга, тако да део везан за заштиту података о личности буде део тих правила, процедура и споразума који су предвиђени прописима.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 1. новембра 2024. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године;
- План јавних набавки Републичког фонда за здравствено осигурање за 2024. годину, 30-01/2 број: 110-20/2024-3 од 23. фебруара 2024. године.

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

2.7 РФЗО није предвидео мере које обезбеђују континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

2.7.1 Опис несврсисходности

Према одредбама члана 7 Законом о информационој безбедности, прописано је, између осталог да оператор ИКТ система одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мере заштите ИКТ система односе се и на континуитет пословања у ванредним околностима (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.

Мерама заштите ИКТ система се обезбеђује превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру

[1] картица здравственог осигурања.

пружања услуга другим лицима. За РФЗО је од великог значаја анализа процеса континуитета пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

РФЗО је знатно зависан од добављача, тј пружаоца услуге развоја и одржавања ИС МЕОП и у случају раскида/отказа уговора, РФЗО у дужем временском периоду неће бити у стању да врши неопходне измене ИС МЕОП. Такође, у уговору о одржавању ИС МЕОП није дефинисан миграција података у случају да РФЗО промени пружаоца услуга развоја ИС.

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 информационог система, јер у том случају недостаје неопходно знање потребно за наставак одржавања и развоја, а нарочито у случају потенцијалног преласка на нови систем и неопходну миграцију података.

2.7.2 Исказане мере исправљања и њихово вредновање (препорука 9)

РФЗО је дата препорука да предузме активности у циљу успостављања континуитета пословања у делу измена/доградње информационог система МЕОП и евентуалне миграције података, у случају прекида сарадње са пружаоцем услуге.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да је од пружаоца услуге затражено да достави комплетну шему пословних процеса и структуру програмског кода, у циљу анализе достављене шеме пословних процеса и структуре програмског кода од стране запослених у сектору за ИТ.

Такође, РФЗО у Одазивном извештају наводи и ће у наредном периоду изменити Политику континуитета пословања и предвидети могућност непродужење/раскида уговора са пружаоцем услуга одржавања ИС, односно начин наставка пословања у измењеним/отежаним условима. Такође, анексом постојећег уговора са пружаоцем услуга, биће прописана обавеза пружаоца услуге одржавања ИС МЕОП да обезбеди континуитет пословања за ИКТ системе.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 1. новембра 2024. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године.

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

ПРИОРИТЕТ 3 - означава несврсисходности које је могуће отклонити у року до три године.

2.8 ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета.

2.8.1 Опис несврсисходности

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.

Корисници јавних средстава успостављају финансијско управљање и контролу у складу са одредбама Закона о буџетском систему. Према одредбама Закона о информационој безбедности (члан 3 став 1 тачка 1), 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 ФУК у јавном сектору). Оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за управљање ризицима у области информационе безбедности (члан 2 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО није идентификовао све ИТ ризике, а последично ни планове и мере за умањење ризика. РФЗО је усвојио Стратегију управљања ризицима, а за период ревизије 2020-2022. године утврдио три ИТ ризика која се понављају сваке године.

У Сектору за развој и ИТ у Дирекцији РФЗО у Београду на 34 систематизована радна места, запослено је 15 лица. У 29 филијала РФЗО, попуњеност радних места на ИТ пословима је 63%.

РФЗО није препознао све ИТ ризике због мањка ИТ кадрова и неучествовања запослених на ИТ пословима у филијалама РФЗО у идентификовању ИТ ризика при изради Стратегије управљања ризицима.

Значајно ограничење у развоју ИКТ система је и недовољан број запослених у Сектору за развој и ИТ и смањена могућност запошљавања нових кадрова, што последично утиче и на спровођење мера за умањење ИТ ризика.

Последице непрепознавања ИТ ризика могу бити непотребно велики трошкови у случају настанка нежељеног догађаја (који се могао спречити) или велики нефинансијски губици (у првом реду података) због немогућности благовременог предузимања мера.

2.8.2 Исказане мере исправљања и њихово вредновање (препорука 2)

РФЗО је дата препорука да у циљу успостављања организационе структуре за ИТ управљање, предузме мере за јачање кадровских капацитета кроз повећање броја и/или стручних знања запослених.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да је, у периоду након спровођења ревизије, запослио на ИТ пословима четири извршиоца. Усвојен је План стручног усавршавања запослених у Републичком фонду за здравствено осигурање број: 30-12/2-151-46/2024 од 30. јануара 2024. године којим су одобрена стручна усавршавања за укупно 12 запослених из ИТ која су у току или ће бити окончана у току године. Такође, Планом стручног усавршавања запослених у РФЗО су обухваћене и интерне обуке за

запослене из филијала из области МЕОП и заштите података које ће бити спроведене у току године.

Такође, РФЗО у одазивном извештају наводи и да ће упутити Националној служби за запошљавање потребе за запошљавањем лица одговарајућег ИТ профила. Путем непосредног контакта са професорима факултета информатичке струке тражиће се могућност одабира одговарајућег кадра у току студија за касније запошљавање у РФЗО. Такође, покренуће се акција обављања стручне праксе и закључивању споразума са високошколским установама за слање студената на праксу у циљу подстицања стварања могућности за запослење. РФЗО ће наставити са регрутацијом и обучавањем постојећег кадра за информатичке послове.

Кроз Програм запошљавања младих Националне службе за запошљавање „Моја прва плата“, РФЗО је током 2023. године примио у радни однос 72 лица, а ове године на стручну праксу 36 лица. Нажалост, ниједно лице није информатичке струке, али РФЗО ће у складу са афинитетима запослених подстицати наставак школовања па ИТ студијама и признање стручне спреме запосленима који су накнадно стекли виши степен.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 1. новембра 2026. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године;
- Анекс уговора о раду 30-12 број: 112.01-44/2024 од 15. јануара 2024. године;
- Анекс V уговора о раду 01 број: 112.01-58/2024 од 15. јануара 2024. године;
- Уговор о раду број 30-12-112.01-971/2023 од 16. октобра 2023. године;
- Уговор о раду број 30-12-112.01-970/2023 од 16. октобра 2023. године;
- План стручног усавршавања запослених у Републичком фонду за здравствено осигурање број: 30-12/2-151-46/2024 од 30. јануара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-43/2024-1 од 29. јануара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-45/2024-1 од 29. јануара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-44/2024-1 од 29. јануара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-50/2024-1 од 14. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-53/2024-1 од 26. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-54/2024-1 од 26. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-52/2024-1 од 26. фебруара 2024. године;
- Решење о упућивању на стручно усавршавање број: 30-12/2-151-51/2024-1 од 26. фебруара 2024. године.

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

2.9 РФЗО није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства.

2.9.1 Опис несврсисходности

Исправа о осигурању је КЗО и потврда о здравственом осигурању (члан 25 и 26 Закона о здравственом осигурању. Према одредбама Правилника о исправи о осигурању (члан 10 став 2 и 3) ако се промене подаци садржани у ЧИП-у картице, осигураном лицу се не издаје нова картица, већ се електронским путем врши промена података у матичној евиденцији и на усмени захтев осигураног лица, у случају промене података (осигураног лица), матична филијала врши физичку синхронизацију података садржаних у ЧИП-у картице са подацима који су измењени у матичној евиденцији.

РФЗО синхронизацију података на контактном микроконтролору (у даљем тексту: ЧИП) КЗО не врши електронским путем, већ је потребна физичка синхронизација података на ЧИП-у.

КЗО се не користи у свим ЗУ на идентичан начин, јер се подацима матичне евиденције може приступити без идентификације корисника (учитавањем КЗО или коришћењем минимум два податка - ЈМБГ и ЛБО/број здравствене исправе).

РФЗО није обезбедио да ЗУ приступају подацима матичне евиденције осигураника на јединствен начин, који би обезбедио већу поузданост и заштиту личних података осигураника.

КЗО су почеле да се користе 2013. године и за претходних 10 година је технолија израде картица значајно напредовала. У пракси ЗУ КЗО користи као „обичну“ књижицу и само један податак (ЛБО или број ЗИ), а не минимум два ради идентификације осигураника.

Последице приступа матичној евиденцији осигураника без уноса минимум два податка (или учитавањем КЗО) оставља могућност да се од стране корисника система оствари увид у личне податке осигураника и у случајевима када он није присутан, идентификован на други начин или када то уопште није потребно.

2.9.2 Исказане мере исправљања и њихово вредновање (препорука 4)

РФЗО је дата препорука да успостави правила управљања подацима матичне евиденције осигураника којима би се, уз обавезно физичко присуство осигураника, омогућио приступ личним подацима осигураника.

РФЗО је доставио оверен одазивни извештај у форми акционог плана у коме је навео да ће у наредном периоду изменити начин коришћења и приступа веб сервиса којим здравствене установе приступају подацима из базе МЕОП. Измена ће се односити на начин приступа тако што ће се у сврху увида у податке користити два податка. Измена ће бити у сервису и у документу Техничко упутство за коришћење REST сервиса за online проверу осигурања и проверу изабраног лекара.

Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији предвиђено је да РФЗО ове активности спроведе до 30. јун 2025. године.

Докази:

- Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији 01 Број: 180-902/2023-2 од 24. фебруара 2024. године.

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

3. МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА

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

Вредновање мера исправљања смо оценили на основу њиховог описа и достављене документације. Сматрамо да смо добили довољне и одговарајуће доказе да можемо изрећи мишљење да ли су мере исправљања задовољавајуће.

Оцењујемо, да су планиране мере исправљања, наведене у акционом плану и описане у одазивном извештају који је поднео Републички фонд за здравствено осигурање, задовољавајуће.

Напомена: У складу са одредбама члана 37 Закона о Државној ревизорској институцији, а након истека рокова исказаних у одазивном извештају, потребно је да обавештавате Државну ревизорску институцију о предузетим мерама и активностима на отклањању откривених несврсисходности према роковима из одазивног извештаја и доставите одговарајуће доказе. По истеку три године Државна ревизорска институција ће утврђивати ефекте остварене након спровођења препорука и отклањања откривених несврсисходности. У ове ефекте укључиће се и ефекти које будете исказали предузетим мерама и активностима из одазивног извештаја.

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
5. април 2024. године