Broj: 40114/19-033-1159/33
Podgorica, 19.09.2019. godine

KONAČNI IZVJEŠTAJ

O KONTROLNOJ REVIZIJI INFORMACIONOG SISTEMA
FONDA ZA ZDRAVSTVENO OSIGURANJE CRNE GORE

Podgorica, septembar 2019. godine

SADRŽAJ

I Opšti dio 3

1. Pravni osnov za vršenje revizije 3

2. Vrsta, predmet i cilj revizije 3

3. Djelatnost subjekta revizije, Integralni zdravstveni informacioni sistem i Integralni informacioni sistem zdravstva 4

3.1 Djelatnost subjekta revizije 4

3.2 Integralni zdravstveni informacioni sistem (IZIS) i Integralni informacioni sistem zdravstva (IISZ) 8

II Utvrđeno činjenično stanje 11

III Zaključak 28

I OPŠTI DIO

1. PRAVNI OSNOV ZA VRŠENJE REVIZIJE

Pravni osnov za vršenje kontrolne revizije informacionog sistema Fonda za zdravstveno osiguranje Crne Gore (u daljem tekstu: FZO) sadržan je u:

- Ustavu Crne Gore, član 144 („Sl. list CG“ br. 01/07 i 38/13);
- Zakonu o Državnoj revizorskoj instituciji, član 4 („Sl. list RCG“ br. 28/04, 27/06, 78/06 i „Sl. list CG“ br. 17/07, 73/10, 40/11, 31/14 i 70/17);
- Godišnjem planu revizije Državne revizorske institucije za 2019. godinu (Interno br. 06-369/18 od 12.12.2018. godine);
- Odluci o vršenju revizije od 14. juna 2019. godine (broj: 40114/19-033-1159/1) u sastavu: g. Radule Žurić (rukovodilac Kolegijuma) i dr Branislav Radulović (član Kolegijuma).

Revizija je izvršena u skladu sa:

- Poslovnikom Državne revizorske institucije („Sl. list CG“ br. 3/15);
- Uputstvom o metodologiji vršenja finansijske revizije i revizije pravilnosti („Sl. list CG“, br. 07/15);
- Međunarodnim standardima za vrhovne revizorske institucije (ISSAI-nivo III);
- INTOSAI priručnikom za sprovođenje revizije informacionih sistema za vrhovne revizorske institucije[1].

2. VRSTA, PREDMET I CILJ REVIZIJE

Državna revizorska institucija je izvršila **reviziju realizacije preporuka - kontrolnu reviziju.** Praćenje realizacije preporuka je dio procesa revizije koji ima za cilj jačanje uticaja revizije i poboljšava budući rad revizije. Praćenje realizacije preporuka je postupak kojim se određuje adekvatnost, efektivnost i pravovremenost radnji preduzetih od rukovodstva subjekta revizije u cilju otklanjanja utvrđenih nedostataka.

Predmet revizije je bila kontrola realizacije preporuka sadržanih u Konačnom izvještaju o reviziji informacionog sistema Fonda za zdravstveno osiguranje Crne Gore (broj: 40113/17-031-610/36 od 19.10.2017. godine), u daljem tekstu: Izvještaj o reviziji IS FZO.

Cilj revizije je bio sagledavanje i kontrola preduzetih aktivnosti subjekta revizije na otklanjanju revizijom konstatovanih nedostataka, kako u funkcionisanju informacionog sistema, obezbjeđenja bezbjednosti, tako i u donošenju, odnosno preciziranju podzakonskih akata, koji to u najvećem stepenu protokolišu i lociraju odgovornost za postupanja zaposlenih po ovim pitanjima iz izvještaja subjekta revizije o sprovedenim radnjama u cilju realizacije preporuka, i to:

– Akcioni plan za sprovođenje preporuka prema konačnom izvještaju DRI i reviziji IS Fonda za zdravstveno osiguranje br. 031-40113/17-610/39-1 od 18.12.2017.godine, u daljem tekstu: Izvještaj o realizaciji preporuka nakon 60 dana.

[1] Priručnik je usvojen na XXI INCOSAI kongresu održanom oktobra 2013. godine u Pekingu.

- Informacija o realizovanim aktivnostima u skladu sa dostavljenim akcionim planom br. 033-4043/18-575/1 od 26.03.2018. godine, u daljem tekstu: Izvještaj o realizaciji preporuka nakon 6 mjeseci i
- Dopis Fonda za zdravstveno osiguranje o preduzetim aktivnostima u cilju realizacije preporuka na obavještenje o vršenju kontrolne revizije (broj: 40114/19-033-1159/4 od 21.06.2019. godine), u daljem tekstu: Izvještaj nakon obavještenja o vršenju kontrolne revizije.

Bilo je potrebno utvrditi u kojoj mjeri su realizovane preporuke, date od strane DRI u Izvještaju o reviziji Fonda za zdravstveno osiguranje Crne Gore.

3. DJELATNOST SUBJEKTA REVIZIJE, INTEGRALNI ZDRAVSTVENI INFORMACIONI SISTEM (IZIS) I INTEGRALNI INFORMACIONI SISTEM ZDRAVSTVA (IISZ)

3.1 Djelatnost subjekta revizije

Fond za zdravstveno osiguranje Crne Gore (u daljem tekstu FZO ili Fond) obezbjeđuje ostvarivanje prava iz obaveznog zdravstvenog osiguranja osiguranim licima pod jednakim uslovima u skladu sa Zakonom o zdravstvenom osiguranju ("Službeni list Crne Gore", br. 06/16, 02/17, 22/17 i 13/18).

Odgovorno lice je Sead Čirgić direktor Fonda za zdravstveno osiguranje Crne Gore.

Fond obavlja sljedeće poslove[2]:

1) sprovodi zdravstveno osiguranje, u skladu sa Zakonom o zdravstvenom osiguranju;
2) učestvuje u sprovođenju zdravstvene politike u vezi sa obaveznim zdravstvenim osiguranjem;
3) obavlja poslove u vezi sa ostvarivanjem prava osiguranih lica, prati zakonitost ostvarivanja tih prava i pruža potrebnu stručnu pomoć u ostvarivanju prava i zaštiti njihovih interesa;
4) vodi evidenciju o ostvarenim pravima osiguranih lica iz obaveznog zdravstvenog osiguranja;
5) utvrđuje prioritete u finansiranju zdravstvene zaštite iz sredstava obaveznog zdravstvenog osiguranja, u skladu sa zdravstvenom politikom;
6) zaključuje ugovore sa davaocima zdravstvenih usluga;
7) utvrđuje kriterijume za utvrđivanje cijena zdravstvenih usluga koje su obuhvaćene obaveznim zdravstvenim osiguranjem i način plaćanja;
8) obezbjeđuje sprovođenje međunarodnih ugovora o obaveznom zdravstvenom osiguranju;
9) donosi godišnji program zdravstvene zaštite, godišnji plan javnih nabavki za zdravstvene ustanove čiji je osnivač država, usvaja nacrt godišnjeg finansijskog plana i završni račun sa izvještajem o poslovanju, u skladu sa zakonom;
10) vrši kontrolu izvršenja ugovora, cijena zdravstvenih usluga i kontrolu trošenja sredstava od strane davalaca zdravstvenih usluga sadržanih u ugovoru o pružanju zdravstvenih usluga;
11) razmatra stanje u oblasti zdravstvenog osiguranja i predlaže mjere za efikasno funkcionisanje zdravstvenog osiguranja u Crnoj Gori;

[2] Član 74 Zakona o zdravstvenom osiguranju

12) sprovodi postupak javnih nabavki za potrebe zdravstvenih ustanova čiji je osnivač država, u skladu sa zakonom;
13) vrši i druge poslove u vezi sa sprovođenjem i ostvarivanjem prava iz zdravstvenog osiguranja, u skladu sa Zakonom o zdravstvenom osiguranju, Statutom i drugim aktima Fonda.

Pored poslova utvrđenih zakonom, Statutom je predviđeno da Fond[3] vodi evidenciju svih podataka vezano za sprovođenje zdravstvenog osiguranja putem jedinstvenog informacionog sistema.

Finansiranje obaveznog zdravstvenog osiguranja obezbjeđuje se iz[4]:
1) doprinosa za obavezno zdravstveno osiguranje;
2) Budžeta Crne Gore;
3) sredstava utvrđenih na osnovu međunarodnih konvencija;
4) naknada štete, kamata, dividendi, renti, akciza i koncesija;
5) drugih izvora, u skladu sa zakonom.

Sredstva obaveznog zdravstvenog osiguranja koriste se za:
1) ostvarivanje prava osiguranih lica;
2) troškove sprovođenja obaveznog zdravstvenog osiguranja;
3) druge rashode, u skladu sa zakonom.

Unutrašnja organizacija

Poslovi Fonda za zdravstveno osiguranje Crne Gore su Pravilnikom o unutrašnjoj organizaciji i sistematizaciji[5], organizovani u okviru šest sektora, tri službe, dva odjeljenja, deset područnih jedinica i trinaest filijala.

1. Sektor za zdravstveno osiguranje
2. Sektor za zdravstvenu zaštitu
3. Sektor za kontrolu sprovođenja ugovora davaoca zdravstvenih usluga
4. Sektor za ekonomske poslove za zdravstvenu djelatnost
5. Sektor za javne nabavke za potrebe Fonda i javnih zdravstvenih ustanova
6. Sektor za informacione tehnologije i razmjenu podataka Integralnog informacionog sistema zdravstva
    6.1. Odsjek za upravljanje projektima
    6.2. Odsjek za razvoj informacionog sistema
    6.3. Odsjek za ICT podršku
7. Odjeljenje za internu reviziju
8. Odjeljenje za zastupanje i naknadu štete
9. Služba za odnose sa javnošću
10. Služba za opšte i kadrovske poslove
11. Služba za finansije.

[3] Član 10 Statuta Republičkog fonda za zdravstveno osiguranje ("Sl. list RCG", br. 070/05 od 23.11.2005).
[4] Član 57 Zakona o zdravstvenom osiguranju.
[5] Iz decembra 2018. godine

Organizacija Sektora za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva (IISZ)

Odgovorno lice je mr Vladimir Raičković, pomoćnik direktora za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva.

U Sektoru za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva obavljaju se poslovi Fonda koji se odnose na: planiranje i organizovanje rada sektora i saradnju sa ostalim organizacionim jedinicama; pripremanje godišnjeg plana aktivnosti iz djelokruga rada sektora; pripremanje godišnjeg izvještaja o radu iz svog djelokruga rada; obezbjeđivanje evidencije i čuvanja podataka putem jedinstvenog informacionog sistema za potrebe ostvarivanja prava iz obaveznog zdravstvenog osiguranja; učestvovanje u pružanju podrške definisanju razvoja i implementaciji jedinstvenog zdravstvenog informacionog sistema; obezbjeđivanje elektronske razmjene podataka između davaoca zdravstvene zaštite i upravljača zbirki podataka odnosno sa ostalim institucijama u državi u skladu sa Zakonom; učestvovanje u izradi programa razvoja informacionog sistema zdravstva u državi; saradnju sa drugim organima i institucijama iz zemlje i inostranstva u oblasti informacionih tehnologija; poslove zaštite i bezbjednosti podataka i sistema; predlaganje programa stalnog stručnog usavršavanja kadrova iz oblasti ICT; usklađivanje razvoja informacionog sistema Fonda u cilju povezivanja sa eksternim informacionim sistemima; učešće u razvojnim projektima iz sistema zdravstvenog osiguranja i zdravstvene zaštite; izvršavanje ostalih zadataka iz djelokruga rada sektora i ostalih zadataka po planu rada odnosno po nalogu direktora.

U Odsjeku za upravljanje projektima obavljaju se poslovi koji se odnose na: analiziranje i usvajanje zahtjeva iz zdravstvenog sistema za uvođenje ili unapređenje informatičke (softverske) podrške u dijelu poslovnih aplikacija; upravljanje projektima iz domena informatičke (softverske) podrške u dijelu poslovnih aplikacija (kadrovska evidencija, finansijsko poslovanje, obračun zarada, apotekarsko poslovanje, itd) u saradnji sa Odsjekom za razvoj IS i ostalim sektorima; predlaganje promjena i mogućih poboljšanja (optimizacije) informatičkih usluga i podrške iz svog domena; praćenje postavki sistema i davanje smjernica za upravljanje parametrima poslovnih aplikacija u saradnji sa ostalim sektorima Fonda; učestvovanje u definisanju indikatora za praćenje realizacije ugovora sa zdravstvenim ustanovama, učestvovanje u pripremanju parametara za ugovaranje zdravstvenih usluga sa davaocima; sarađivanje u spoljnim razvojnim projektima; učestvovanje u definisanju analiza i izvještaja iz poslovnih aplikacija; ostale poslove po nalogu direktora i neposrednog rukovodioca koji po sadržaju spadaju u rad odsjeka.

U Odsjeku za razvoj informacionog sistema obavljaju se poslovi Fonda koji se odnose na: sprovođenje i realizaciju usvojenih koncepcija i projektnih rješenja za razvoj informacionog sistema; usklađivanje procesa, poslova i dokumentacije sa standardima u sektoru; praćenje razvoja novih dostignuća iz oblasti informacionih tehnologija i predlaganje primjene odgovarajućih rješenja; razvijanje informacionog sistema Fonda; administraciju i projektovanje nadogradnje aplikacija u informacionom sistemu Fonda; staranje o postojećim i razvoj novih aplikativnih rješenja i prezentiranje njihove faze razvoja i rezultata; pružanje operativnih parametara pojedincima i poslovnim jedinicama u korišćenju IS; pružanje neposredne pomoći u upotrebi softvera i upravljanju podacima za sve funkcionalne oblasti u organizaciji; ostale poslove po nalogu direktora i neposrednog rukovodioca koji po sadržaju spadaju u rad odsjeka.

U Odsjeku za ICT podršku obavljaju se poslovi Fonda koji se odnose na: sprovođenje i realizaciju usvojenih koncepcija i projektnih rješenja za razvoj informacionog sistema; praćenje razvoja novih dostignuća iz oblasti informacionih tehnologija i predlaganje primjene odgovarajućih rješenja; nadzor nad radom računarskog sistema; planiranje i izradu dopunske sistemske programske opreme; upravljanje i administraciju serverskom infrastrukturom; upravljanje i administraciju komunikacionom infrastrukturom; upravljanje storage sistemom; obezbjeđivanje operativnosti baze podataka; usklađivanje razvoja komunikacione infrastrukture u drugim djelovima zdravstvenog informacionog sistema sa već odabranim standardima korišćenim u Fondu; testiranje razvoj i implementaciju nekih aplikativnih rješenja za podršku sistemskim zahjevima procesima i procedurama; razvoj i rješenja u okviru virtualizacione platforme; nadzor modifikacije i proširenja resursa informacionog sistema; rukovođenje prijemom i brigu o smještaju hardvera i njegovom puštanju u funkciju; obezbjeđivanje i brigu o radu na backup-u podataka u cijelom sistemu za koji je odgovoran sektor; administraciju računarskog operativnog sistema; planiranje i održavanje računarske opreme; obezbjeđenje i zaštitu računarske opreme i podataka od uništenja i neovlašćenog pristupa; uvođenje aplikacionih rješenja; organizaciju i pružanje pomoći prilikom ispada računarskog sistema; savjetovanje i pomoć pri korišćenju računarske opreme i računarskih aplikacija; staranje o pravilnoj upotrebi i ispravnosti hardvera; brigu o nabavci neophodnih rezervnih djelova, alata i softverskih dijagnostičkih alatki; primjenu i projektovanje naprednih informatičkih tehnologija; koncipiranje i realizaciju sistemskih zahtjeva i rješenja; ostale poslove po nalogu direktora i neposrednog rukovodioca koji po sadržaju spadaju u rad odsjeka.

Sistematizacija radnih mjesta i stanje IT ljudskih resursa

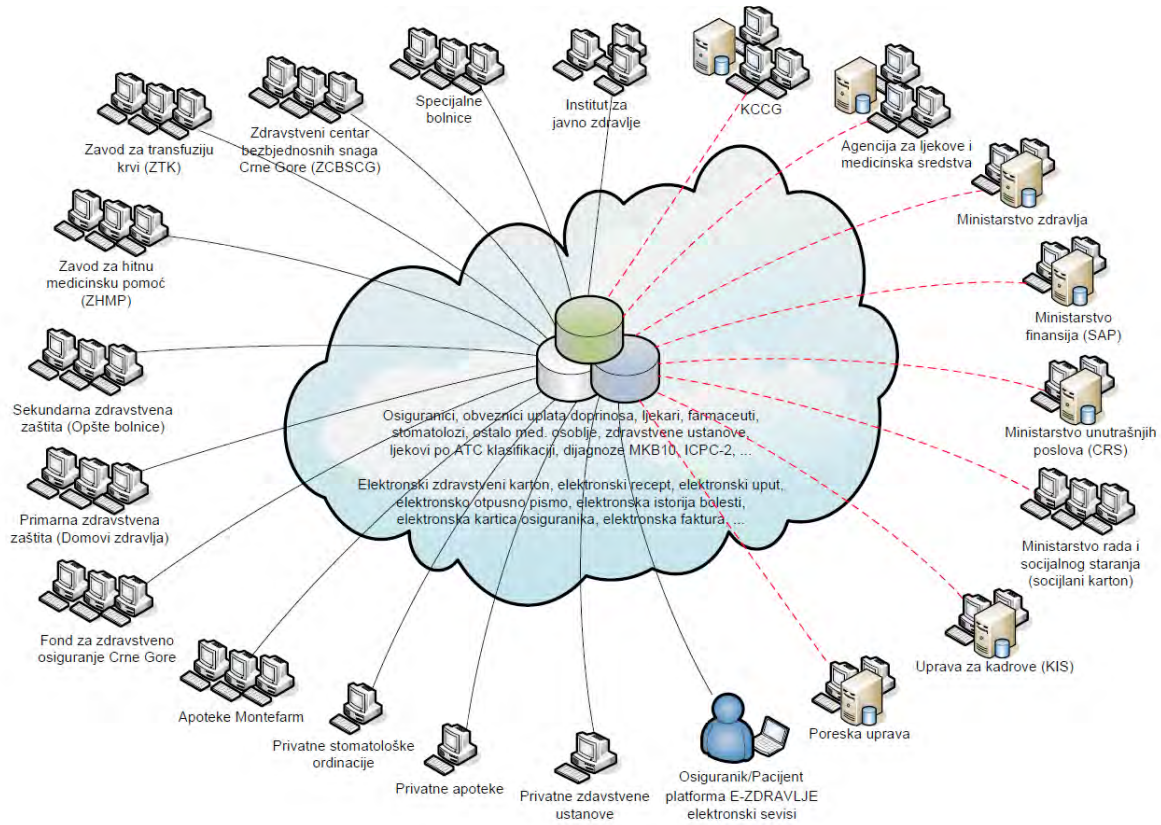
Po Pravilniku o unutrašnjoj organizaciji i sistematizaciji u Fondu za zdravstveno osiguranje Crne Gore, predviđeno je 259 radnih mjesta (izvršilaca), što je za 26 manje u odnosu na period vršenja prethodne revizije.

U Sektoru za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva predviđeno je 20 radnih mjesta, što je za dva manje u odnosu na period vršenja prethodne revizije. Od 20 predviđenih radnih mjesta, 16 je popunjeno, što je za jedan manje u odnosu na period vršenja prethodne revizije.

Sektor za informacione tehnologije i razmjenu podataka Integralnog informacionog sistema zdravstva	Predviđeno	Popunjeno
Pomoćnik direktora	1	1
Odsjek za upravljanje projektima	4	3
Odsjek za razvoj informacionog sistema	6	4
Odsjek za ICT podršku	9	8
U K U P N O	**20**	**16**

3.2. Integralni zdravstveni informacioni sistem (IZIS) i Integralni informacioni sistem zdravstva (IISZ) [6]

Proces planske informatizacije u sistemu zdravstva počeo je 2000. godine u oblasti zdravstvenog osiguranja, razvojem informatičke podrške poslovnim procesima Fonda za zdravstveno osiguranje. Razvoj je počeo uspostavljanjem baze osiguranika kao temelja za dalju nadogradnju sistema, a u skladu sa projektom informatizacije u oblasti zdravstvenog osiguranja. Do 2004. završen je i implementiran Projekat evidencije osiguranika i obaveznika uplate doprinosa i Projekat kontrole, distribucije i potrošnje ljekova u Crnoj Gori.



Slika 1: Na slici su prikazani svi sistemi koji postoje i međusobno komuniciraju u okviru IZIS-a. Crnom punom linijom označeni su sitemi koji su u nadležnosti Sektora za IT i razmjenu podataka u IISZ - razvoj, administracija, održavanje, a crvenom isprekidanom linijom ostali sistemi koji su u nadležnosti drugih institucija, ustanova, sa kojima IISZ komunicira i razmjenjuje podatke.

Od 2004.godine, u skladu sa „Projektom unapređenja sistema zdravstva Crne Gore“, koji je vodilo Ministarstvo zdravlja, počinje informatizacija zdravstvenog sistema po nivoima zdravstvene zaštite, kroz informatičku podršku reformi primarne zdravstvene zaštite, a nastavljena informatičkom podrškom sekundarne zdravstvene zaštite i zdravstveno-statističkom izvještavanju. U kasnijem periodu implementirani su i drugi projekti u oblasti informatizacije sistema zdravstva što je rezultiralo izgradnjom integralnog informacionog sistema zdravstva (IISZ) koji je razvijan, unapređivan i održavan od strane Fonda za zdravstveno osiguranje u saradnji sa drugim institucijama u sistemu zdravstva.

Uporedo sa ovim, druge institucije u okviru javnog zdravstvenog sistema Crne Gore, razvijale su i pojedinačna informatička rješenja za podršku procesima rada u tim institucijama.

[6] Iz Strategije razvoja Integralnog zdravstvenog informacionog sistema i e-zdravlja (2018-2023).

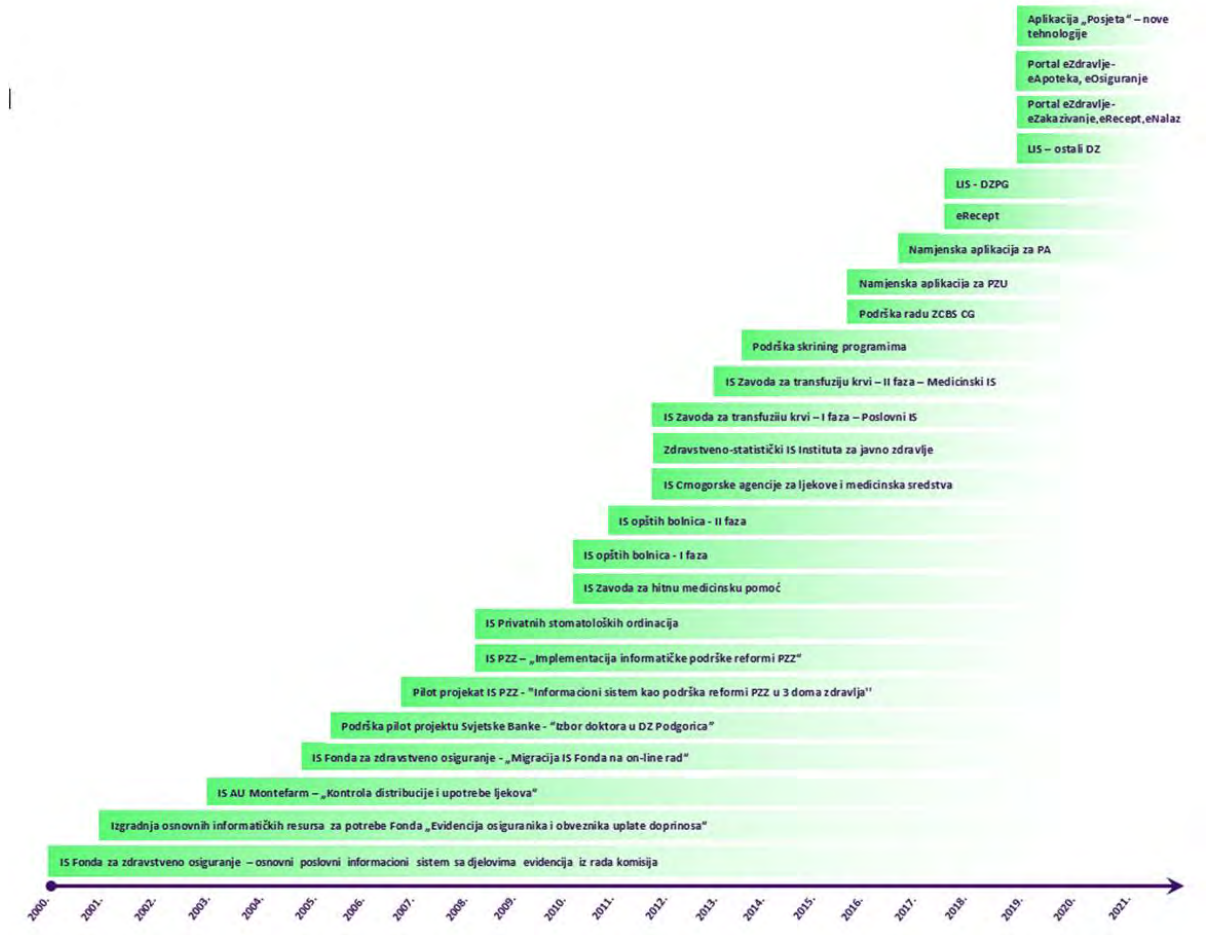
Do maja 2018. godine u IISZ su integrisani informacioni sistemi sljedećih institucija: Fond za zdravstveno osiguranje, ZU Apoteke Crne Gore "Montefarm", primarna zdravstvena zaštita (PZZ) - domovi zdravlja, opšte bolnice, specijalne bolnice, Zavod za hitnu medicinsku pomoć Crne Gore, Zavod za transfuziju krvi Crne Gore, Institut za javno zdravlje Crne Gore, Agencija za ljekove i medicinska sredstva (CALIMS), Zdravstveni centar bezbjednosnih snaga Crne Gore, privatne stomatološke ambulante koje su dio zdravstvene mreže, privatne apoteke koje su dio zdravstvene mreže i privatne zdravstvene ustanove koje su dio zdravstvene mreže.

Informacioni sistemi sljedećih institucija zdravstvenog sistema su samo djelimično povezani sa IISZ-om:

- Klinički centar Crne Gore,
- Ministarstvo zdravlja,
- Ostali pružaoci zdravstvenih usluga.

IISZ predstavlja temelj i polaznu osnovu budućeg IZIS-a, koji će obuhvatiti razvijena informatička rješenja i informacione sisteme drugih institucija u sistemu zdravstva Crne Gore. IISZ je povezan sa informacionim sistemima od ključne važnosti u Crnoj Gori: Centralnim registrom osiguranika i obveznika (CROO) koji se nalazi u Poreskoj upravi, Centralnim registrom stanovništva u MUP-u, Ministarstvom finansija, Ministarstvom rada i socijalnog staranja i Upravom za kadrove.

Na sledećoj slici je predstavljena hronologija razvoja sistema



Slika 2: Hronologija razvoja IISZ-a

Sektor za informacione tehnologije i razmjenu podataka IIZS-a Fonda za zdravstveno osiguranje pruža tehničku podršku za aplikacije i baze podataka dijela Integralnog informacionog sistema zdravstva Crne Gore koji obuhvata: IS Fonda za zdravstveno osiguranje, IS ZU Apoteke Crne Gore "Montefarm", IS primarne zdravstvene zaštite – domovi zdravlja, IS Zavoda za hitnu medicinsku pomoć Crne Gore, IS opštih bolnica, IS Zavoda za transfuziju krvi Crne Gore, IS privatnih zdravstvenih ustanova – stomatološke ambulante, IS privatnih apoteka, IS Instituta za javno zdravlje, IS privatnih zdravstvenih ustanova i isporučioca pomagala, IS Zdravstvenog centra bezbjednosnih snaga Crne Gore, IS specijalnih bolnica i sistema za razmjenu podataka, testiranje i razmjenu poruka.

Numerički prikaz Integralnog informacionog sistema zdravstva [7]

Sledeća tabela predstavlja numerički prikaz IISZ-a sa navedenim brojem lokacija, brojem servera, brojem računara i brojem aplikativnih korisnika za svaki njegov segment pojedinačno.

	Informacioni sistem	Broj lokacija	Broj računara	Broj aplikativnih korisnika	Serveri		
					Bazni	Aplikativni	Izvještajni
1	IS Fonda za zdravstveno osiguranje	23	210	200	2	2	1
2	IS ZU Apoteke Crne Gore "Montefarm"	54	175	314	2	2	1
3	IS primarne zdravstvene zaštite - domovi zdravlja	75	1.201	2.322	2	3	1
4	IS Zavoda za hitnu medicinsku pomoć	21	67	336	0	0	0
5	IS opštih bolnica (ISOB)	13	695	1.477	2	3	1
6	IS Zavoda za transfuziju krvi	9	51	69	0	0	0
7	IS privatnih zdravstvenih ustanova – stomatološke ambulante	212	212	379	2	1	0
8	IS privatnih apoteka	164	164	214	1	1	0
9	IS Instituta za javno zdravlje	1	95	142	2	1	0
10	IS privatnih zdravstvenih ustanova i isporučioca	60	60	103	0	1	0
11	IS zdravstvenog centra bezbjednosnih snaga CG	5	37	31	0	0	0
12	IS specijalnih bolnica	3	144	239	2	1	0
13	- Sistem za razmjenu podataka - Sistem za testiranje - Sistem za razmjenu poruka	0	0	0	8	8	0
U K U P N O		**640**	**3.111**	**5.826**	**23**	**24[8]**	**4**

Broj aplikativnih korisnika IISZ-a je 5.826 koji na neposredan način pristupaju bazi osiguranika koja je centar Integralnog zdravstvenog informacionog sistema i Integralnog informacionog sistema zdravstva. Broj računara sa kojih se pristupa IISZ je 3.111 sa neke od 640 lokacija. Broj servera u okviru IISZ-a je: 23 bazna, 24 aplikativna i 4 izvještajna.

[7] Iz odgovora na Upitnik za Fond za zdravstveno osiguranje Crne Gore – Centrala br. 04-5065 od 01.08.2019. g.
[8] Uključujući jedan server za portal eZdravlje

II UTVRĐENO ČINJENIČNO STANJE

Revizija koju je sprovela Državna revizorska institucija 2017. godine, ukazala je na postojanje propusta u radu Fonda za zdravstveno osiguranje Crne Gore. Nadležni Kolegijum DRI, sačinio je pregled osnovnih konstatovanih nepravilnosti i nedostataka i izradio preporuke u cilju njihovog otklanjanja.

Predmetnom revizijom izvršena je kontrola realizacije preporuka datih u **Konačnom izvještaju o reviziji informacionog sistema Fonda za zdravstveno osiguranje Crne Gore.**

U cilju realizacije datih preporuka Fond za zdravstveno osiguranje je u prethodnom periodu, uz angažovanje inostranog konsultanta sačinio detaljnu GAP analizu[9], kao osnov za implementaciju standarda ISO:9001 i ISO:27001. Sklopljen je ugovor za implementaciju procesa sistema upravljanja kvalitetom i sigurnosti informacija i revizije primjene tehničkih kontrola u informacionom sistemu. U 2018. godini implementirani su sistemi upravljanja kvalitetom i sigurnosti informacija prema zahtjevima ISO 9001:2015 i ISO 27001:2013 i revizija primjene tehničkih kontrola u informacionom sistemu prema zahtjevima Anex-a A standarda ISO 27001:2013.

Fond za zdravstveno osiguranje Crne Gore – Sektor za IT je provjeren i sertifikovan prema zahtjevima standarda ISO 27001:2013 za sledeći djelokrug rada i Izjavu o primenljivosti: Razvoj i održavanje informacionog sistema Fonda za zdravstveno osiguranje Crne Gore u skladu sa Izjavom o primenljivosti od 28. juna 2019. godine. Sertifikat je važeći tri godine i ostaje validan ukoliko su nadzorne provjere zadovoljavajuće od strane kompanije koja je izdala sertifikat.

Takođe, Fond za zdravstveno osiguranje Crne Gore – Sektor za IT je provjeren i sertifikovan prema zahtjevima standarda ISO 9001:2015 za sledeći djelokrug rada: Razvoj i održavanje informacionog sistema Fonda za zdravstveno osiguranje Crne Gore. Sertifikat je važeći tri godine i ostaje validan ukoliko su nadzorne provjere zadovoljavajuće od strane kompanije koja je izdala sertifikat.

Fond za zdravstveno osiguranje Crne Gore ima u planu da pomenute standarde uvede na nivou cijelog Fonda.

U sklopu uvođenja standarda usvojena su sledeća dokumenta:

- POL 01 Politika upravljanja kvalitetom i sigurnosti informacija
- POL 02 Politike sigurnosti
- PR 01 Procedura upravljanje dokumentovanim informacijama
- PR 02 Procedura upravljanje obukama
- PR 03 Procedura interne provjera
- PR 04 Procedura za korektivne / mjere poboljšanja
- PR 05 Procedura za preispitivanje IMS-a
- PR 06 Procedura za upravljanje rizicima i sigurnosti informacija
- PR 07 Procedura za upravljanje servisnim zahtjevima - service desk
- PR 08 Procedura za upravljanje incidentima

[9] GAP analiza – najvažniji korak u usaglašavanju poslovnog sistema sa sistemom kvaliteta koje ima za cilj analizu postojećeg načina poslovanja organizacije i njeno poređenje sa zahtjevima standarda.

PR 09 Procedura upravljanje problemima
PR 10 Procedura upravljanje promjenama
PR 11 Procedura upravljanja verzijama i konfiguracijama
PR 12 Procedura upravljanje projektima
PR 13 Procedura funkcionalno testiranje
PR 14 Procedura upravljanja rizicima i prilikama
PR 15 Procedura upravljanja nabavkama i ocjenom dobavljača
UP 6.1 Uputstvo za tretman rizika
UP 6.2 Uputstvo za upravljanje fizičkom sigurnošću
UP 6.3 Uputstvo za upravljanje korisničkim nalozima i lozinkama
UP 6.4 Uputstvo za backup
UP 6.5 Uputstvo za upravljanje kontinuitetom poslovanja
UP 15.1 Uputstvo za ocjenu i rangiranje dobavljača.

Procedurom za preispitivanje IMS-a (Integrisani sistem upravljanja kvalitetom i sigurnosti informacija) propisano je da se preispitivanje sprovodi najmanje jednom godišnje i da se vrši praćenje realizacije propisanih mjera.

Preporuka broj 1

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da nije donijeta Strategija razvoja Integralnog zdravstvenog informacionog sistema, tako da ni Fond za zdravstveno osiguranje nema IT strategiju odnosno akcioni plan kojim bi bili definisani koraci razvoja informacionog sistema Fonda kao dijela IZIS-a.

Nedonošenjem IT strategije Integralnog zdravstvenog informacionog sistema postoji **rizik** od neispunjavanja ciljeva iz Master plana razvoja zdravstva Crne Gore 2015-2020 i ostvarivanja poslovnih ciljeva Fonda u sistemskom, razvojnom i kadrovskom smislu.

Ministarstvu zdravlja **preporučeno je** da preduzme dalje aktivnosti na izradi i usvajanju strateškog dokumenta, u okviru kog bi se planirao dalji razvoj Integralnog zdravstvenog informacionog sistema i u sklopu njega informacioni sistem Fonda za zdravstveno osiguranje Crne Gore.

Utvrđeno činjenično stanje za preporuku br. 1:

Kontrolnom revizijom utvrđeno je da je strateški dokument razvoja Integralnog zdravstvenog informacionog sistema - Strategija razvoja integralnog zdravstvenog informacionog sistema i eZdravlja (2018 - 2023) sa akcionim planom za period 2018 - 2021. godina, **usvojen** na sjednici Vlade 28. juna 2018. godine.

Članovi radne grupe za izradu strategije, pored predstavnika iz Ministarstva zdravlja su bili i predstavnici Instituta za javno zdravlje Crne Gore, Fonda za zdravstveno osiguranje Crne Gore, Kliničkog centra Crne Gore, Ministarstva javne uprave, Ministarstva finansija i ogranizacija UNDP kao spoljni saradnik na projektu. Strategija razvoja integralnog zdravstvenog informacionog sistema i eZdravlja (2018 - 2023) odnosi se i na Integralni informacioni sistem zdravstva koji je u nadležnosti Fonda za zdravstveno osiguranje Crne Gore.

U Strategiji se navodi da će zdravstveni sektor zacrtanu viziju ostvariti kroz Integralni zdravstveni informacioni sistem (IZIS) Crne Gore, dijelom na osnovama postojećih segmenata do sada razvijenog informacionog sistema, kroz njihovo unapređenje, nadogradnju i dalju funkcionalnu integraciju, kao i povezivanje sa informacionim sistemima drugih sektora, uz inoviranje i jačanje neophodnih resursa shodno napretku informacionih tehnologija i medicine.

U skladu sa Strategijom, u Ministarstvu zdravlja su prepoznali potrebu za formiranjem tijela za kordinaciju svih poslova na nivou informacionih sistema i podsistema u zdravstvenom sistemu Crne Gore. U maju 2019. godine formirano je Odjeljenje za IZIS i eZdravlje, u kojem se obavljaju poslovi koji se odnose na: upravljanje, implementaciju, unapređenje, funkcionisanje, projektovanje i plansko razvijanje IZIS-a u skladu sa definisanim standardima i korišćenjem zajedničkih resursa, dok Fond za zdravstveno osiguranje ima iste nadležnosti koje je imalo i ranije.

Planirano je revidiranje Akcionog plana koje se odnosi na promjene u datumima i rokovima.

Preporuka je realizovana.

Preporuka broj 2

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje nema uspostavljen plan kontinuiteta poslovanja koji treba da ima za cilj uspostavljanje mjera oporavka za prekide u poslovnim aktivnostima, kako bi se kritični poslovni procesi zaštitili od uticaja većih otkaza i da bi se osiguralo njihovo blagovremeno nastavljanje.

Zbog nepostojanja plana kontinuiteta poslovanja postoji **rizik** od neblagovremenog pokretanja procesa oporavka, što može dovesti do prekida u procesu rada.

Fondu za zdravstveno osiguranje Crne Gore **preporučeno je** da izradi plan kontinuiteta poslovanja koji će obezbijediti blagovremeno nastavljanje svih kritičnih poslovnih aktivnosti.

Utvrđeno činjenično stanje za preporuku br. 2:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, Fond za zdravstveno osiguranje Crne Gore je **donio** Politiku sigurnosti (POL 02) od 01.09.2018. godine i Uputstvo za upravljanje kontinuitetom poslovanja (UP 6.5) od 14.11.2018. godine, čime je **uspostavljen** plan kontinuiteta poslovanja.

Utvrđeno je da Uputstvo za upravljanje kontinuitetom poslovanja propisuje način postupanja u kriznim situacijama, koje mogu ugroziti bezbjednost informacija i integrisani sistem upravljanja, kako bi se obezbijedio kontinuitet poslovanja. Uputstvo sadrži opis aktivnosti i odgovornosti vezane za: scenario kriznih situacija, odgovornosti za navedene krizne situacije, kriznu komunikaciju, normalizaciju krizne situacije, rad kriznog štaba u upravljanju kriznom situacijom, vraćanje u normalan režim rada, prestanak rada kriznog štaba i objavu kraja krizne situacije, simulaciju i preispitivanje efektivnosti primjene uputstva i njegovu dopunu. Kao moguće krizne situacije prepoznate su situacije izazvane: požarom, nedostatkom dovoljnog broja radno sposobnih zaposlenih, nestankom struje, gubitkom IT sistema i nedostatkom radno sposobnih, gubitkom IT sistema i infrastrukture radnih mjesta.

Kako je navedeno u Uputstvu za upravljanje kontinuitetom poslovanja, najmanje jednom dvogodišnje vršiće se preispitivanje efektivnosti Uputstva i njegova dopuna adekvatnim elementima u skladu sa stečenim iskustvom.

Internom provjerom o kojoj je sačinjen Izvještaj sa interne provjere od 03.07.2019. godine (OB 3.3), izvršena je između ostalog i provjera procesa Upravljanje kontinuitetom poslovanja. U Izvještaju je konstatovano da svi zaposleni nisu upoznati u potpunosti sa uputstvom, da ne postoji disaster recovery lokacija i da nije vršena simulacija kontinuiteta poslovanja. Za navedene neusaglašenosti date su sledeće korektivne mjere:

- da treba poslati obavještenje svim zaposlenima u Sektoru za IT i ključnim zaposlenima Fonda
- da treba obezbijediti disaster recovery sajt na odgovarajućoj lokaciji
- i da nakon uspostavljanja disaster recovery lokacije i nakon uvođenja ISO standarda na nivou Fonda, treba izvršiti simulaciju krizne situacije.

Za svaku korektivnu mjeru navedeno je odgovorno lice i rok za njegovu realizaciju. Za prvu mjeru rok za realizaciju je jul 2019. godine, dok je rok za realizaciju druge dvije mjere predviđen za decembar 2020. godine.

U planu je uvođenje standarda na nivou Fonda čime će kontinuitet poslovanja biti dodatno unaprijeđen.

Što se tiče problema sa prekidom u napajanju električnom energijom, u Fondu je prošle godine instaliran novi agregat koji napaja Data centar, tako da u slučaju ispada glavnog agregata obezbijeđeno je funkcionisanje Data centra.

Preporuka je realizovana.

Preporuka broj 3

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da u Fondu za zdravstveno osiguranje ne postoji plan oporavka od katastrofe, pa iako se rezervne kopije podataka čuvaju, u slučaju otkaza postoji mogućnost prekida u procesu rada u dužem vremenskom periodu.

Neobezbjeđivanjem sekundarne lokacije postoji **rizik** od prekida u procesu rada u slučaju većih kvarova na hardveru, na instalaciji ili nekog drugog nepredviđenog događaja zbog kojeg bi došlo do otkaza u radu servera na primarnoj lokaciji, čime bi bili ugroženi poslovni procesi cijelog zdravstvenog sistema Crne Gore.

Fondu za zdravstveno osiguranje Crne Gore **preporučeno je** da izradi plan oporavka od katastrofe i implementira ga kroz projekat Disaster Recovery, s obzirom da je Disaster Recovery Data centar u Bijelom Polju u funkciji.

Utvrđeno činjenično stanje za preporuku br. 3:

Fond za zdravstveno osiguranje Crne Gore **nije završio** projekat Disaster Recovery u Bijelom Polju za kritične servise. Urađen je projektni zadatak i pripremljena je specifikacija opreme čija je procijenjena nabavna vrijednost oko 70.000€. S obzirom da projektni zadatak i koncept

implementacije nije bio spreman kada se kreirao budžet za 2019. godinu, to ova sredstva nisu ni tražena, već su uvrštena u budžet za 2020. godinu.

Takođe, kako je prethodno navedeno u Izvještaju sa interne provjere u okviru provjere procesa Upravljanje kontinuitetom poslovanja je konstatovano da ne postoji disaster recovery lokacija. Data je korektivna mjera da treba obezbijediti disaster recovery sajt na odgovarajućoj lokaciji sa rokom realizacije decembar 2020. godine.

Preporuka nije realizovana.

Preporuka broj 4

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje nije vršio procjenu efikasnosti mjera fizičke zaštite shodno članu 9 Uredbe o mjerama informacione bezbjednosti.

Nevršenjem procjene efikasnosti mjera fizičke zaštite prostora u kojem se nalaze serveri, mrežna i komunikaciona oprema postoji **rizik** po bezbjednost Integralnog zdravstvenog informacionog sistema.

Fondu za zdravstveno osiguranje **preporučeno je** da najmanje jednom godišnje, vrši procjenu efikasnosti mjera informacione bezbjednosti fizičke zaštite objekata i prostorija u kojima se nalaze podaci, kao i kad dođe do promjene namjene lokacije ili elemenata u informacionom sistemu, shodno članu 9 Uredbe o mjerama informacione bezbjednosti.

Utvrđeno činjenično stanje za preporuku br. 4:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, Fond za zdravstveno osiguranje je **donio:** Uputstvo za upravljanje fizičkom sigurnosti (UP 6.2), Proceduru upravljanja rizicima i sigurnosti informacija (PR 06), Uputstvo za tretman rizika (UP 6. 1), Registar rizika (OB 6.1) i Proceduru upravljanja rizicima i prilikama (PR 14).

Uputstvo za upravljanje fizičkom sigurnosti (UP 6.2) propisuje način upravljanja fizičkom sigurnošću u IT Fonda. Odnosi se na sve zaposlene i na poslovne prostore u kojima se nalazi IT Fonda. Uputstvom je, u skladu sa procesima koji se odvijaju u poslovnim prostorijama, Fond podijeljen u odgovarajuće zone: crvena zona – zona visoke fizičke zaštite, narandžasta zona – zona srednje fizičke zaštite i zelena zona – zona niske fizičke zaštite. Definisana su pravila koja moraju da poštuju sva lica koja koriste obezbijeđenu prostoriju (crvena zona). Uputstvom je takođe obuhvaćena zaštita od spoljnih prijetnji, fizičko-tehničko obezbjeđenje, zaštita od nestanka ili poremećaja u napajanju električnom energijom i obezbjeđenje kablova.

Utvrđeno je da je Fond za zdravstveno osiguranje Crne Gore **vršio** procjenu efikasnosti mjera informacione bezbjednosti fizičke zaštite objekata i prostorija u kojima se nalaze podaci, u sklopu šire oblasti vezano za rizike o čemu je sačinjen Izvještaj sa interne provjere od 03.07.2019. godine (OB 3.3), **u skladu** sa članom 9 Uredbe o mjerama informacione bezbjednosti.

U Izvještaju sa interne provjere, izvršena je između ostalog i provjera procesa Upravljanje fizičkom sigurnošću. U Izvještaju su konstatovane neusaglašenosti:

- ulazak u server salu nije zaštićen karticom i lozinkom za otvaranje vrata,
- ulazak u server salu nije pod video nadzorom
- ne postoji sef u kancelariji direktora za IT
- ormari sa instalacijama u prostorijama filijale i na prvom spratu Fonda se ne zaključavaju
- opasan i zapaljiv materijal se čuva u ormarima sa instalacijama koji pripadaju crvenoj zoni
- ne postoji kapsula za gašenje požara u server sali.

Za navedene neusaglašenosti predložene su adekvatne korektivne mjere od kojih je jedan dio realizovan u toku vršenja revizije. Takođe su navedena odgovorna lica i rok za realizaciju mjera.

Preporuka je realizovana.

Preporuka broj 5

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje ne vrši procjenu rizika vezanu za procese pokrivene informacionim tehnologijama. Rizici nisu identifikovani i nisu uspostavljene odgovarajuće strategije ili procedure.

Postoji **rizik** od nastanka negativnih efekata koji bi se reflektovali na funkcionisanje cjelokupnog sistema zdravstva Crne Gore, jer se ne vrši procjena rizika za procese pokrivene informacionim tehnologijama.

Fondu za zdravstveno osiguranje **preporučeno je** da identifikuje rizike koji su povezani sa informacionim tehnologijama i da vrši redovnu godišnju procjenu rizika i re-procjenu rizika kad god planira da uvede nov informacioni sistem, nadogradnju ili prelazak na noviju verziju.

Utvrđeno činjenično stanje za preporuku br. 5:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, Fond za zdravstveno osiguranje Crne Gore je **identifikovao** rizike koji su povezani sa informacionim tehnologijama i **donio** sledeće propise: Politike sigurnosti (POL 02), Proceduru upravljanja rizicima i sigurnosti informacija (PR 06), Uputstvo za tretman rizika (UP 6. 1), Registar rizika sa planom tretmana (OB 6.1), Proceduru upravljanja rizicima i prilikama (PR 14) i Registar rizika i prilika sa planom tretmana (OB 14.1).

Politika sigurnosti (POL 02) propisuje procjenjivanje sigurnosnog rizika koje se sprovodi u cilju identifikacije specifičnih prijetnji informacionom sistemu i njegovih ranjivosti. Rezultati procjene sigurnosnog rizika određuju prioritete mjera i akcija koje moraju biti sprovedene u cilju zaštite. Troškovi primjene mjera sigurnosti moraju biti proporcionalni sa osjetljivošću i vrijednošću informacija koje se štite.

Procedura upravljanja rizicima i sigurnosti informacija (PR 06) opisuje upravljanje rizicima sigurnosti informacija u Fondu za zdravstveno osiguranje Crne Gore i primjenjuje se na sistem

upravljanja sigurnošću informacija IT FZO. Izvršena je identifikacija informatičke imovine Fonda, grupisana i popisana u Registru rizika sa planom tretmana, prema sledećim grupama: informaciona imovina (hardware), softverska imovina (aplikacije, podaci, informacije, dokumenta, itd), fizička imovina (zgrada), papirna dokumentacija i zapisi, ljudski resursi, udaljene lokacije, imidž i reputacija. Izvršeno je vrednovanje identifikovane imovine u odnosu na povjerljivost, integritet i raspoloživost, čime se utvrđuju ranjivosti i prijetnje kojima je ova imovina izložena i popisuju se u Registru rizika sa planom tretmana (OB 6.1) za svaku imovinu posebno. Nakon toga se utvrđuje vjerovatnoća njihovog pojavljivanja i posledica koje njihovo pojavljivanje može imati na određenu imovinu određivanjem vjerovatnoće pojavljivanja prijetnje, stepena ranjivosti i nivoa uticaja i posledice na posao. Ocjena rizika dobija se sabiranjem vrijednosti imovine sa proizvodom stepena ranjivosti, vjerovatnoće prijetnje i nivoa uticaja. Ova ocjena se upisuje u Registar rizika sa planom tretmana i vrši se klasifikacija rizika na: nizak (2-22), srednji (23-48), visok (49-79) i veoma visok (80-91). Za svaki rizik koji ima visok ili veoma visok nivo izrađuje se plan tretmana rizika radi njegovog smanjivanja na prihvatljiv nivo (nizak ili srednji). Procedurom je propisano da se preispitivanje Plana tretmana rizika vrši najmanje jednom godišnje.

Uputstvo za tretman rizika (UP 6.1) propisuje način tretmana rizika, izradu plana tretmana, praćenje realizacije i ocjenu efektivnosti sprovedenih mjera/kontrola i primjenjuje se na sve rizike koji imaju visok ili veoma visok nivo rizika. Tretman rizika podrazumijeva odabir jedne ili više opcija, a kako one po pravilu nisu uzajamno isključive i odgovarajuće u svim okolnostima, i kako tretman jednog rizika može da ima uticaj na drugi rizik u drugom procesu, bira se opcija koja najviše balansira troškove i trud koji se ulažu u njeno sprovođenje, u odnosu na koristi koje će se dobiti. Moguće opcije za tretman rizika su prihvatanje, smanjenje, prenos ili izbjegavanje. Opcija prihvatanja podrazumijeva da su troškovi oštećenja ili gubitka imovine manji od primjene određenih zaštita i kontrola, pa u tom slučaju nije potrebno raditi plan tretmana ili preduzimati mjere za zaštitu imovine. Ako je za rizike izabrana opcija smanjenje, prenos ili izbjegavanje onda je neophodno izraditi plan tretmana kako bi se nivo rizika smanjio na srednji ili nizak nivo.

Procedura upravljanja rizicima i prilikama (PR 14) opisuje upravljanje rizicima/prilikama u IT Fonda uključujući identifikaciju procesa, rizika/prilika sa vjerovatnoćom njihovog pojavljivanja i stepenom uticaja na procese u IT-u i životni ciklus informacionog sistema, kao i izradu plana tretmana rizika/prilika. Primjenjuje se na sistem upravljanja kvalitetom u Sektoru za IT Fonda. Procedura propisuje identifikaciju svih procesa u IT Fonda i definisanje koraka/aktivnosti za pojedine procese, utvrđivanje mogućih rizika/prilika i njihov uticaj na procese u IT-u i životni ciklus informacionog sistema, vrednovanje tj. utvrđivanje vjerovatnoće njihovog pojavljivanja i posledica koje njihovo pojavljivanje može imati na određeni procesni korak, određivanje stepena uticaja tj. težina posledica na posao. Ocjena rizika/prilika je ocjena potencijalne štete/koristi za IT Sektor Fonda. Nakon toga se vrši klasifikacija rizika/prilika koja se upisuje u Registar rizika/prilika sa planom tretmana (OB 14.1). Za svaki rizik koji ima visok (9-15) ili veoma visok nivo (16), izrađuje se Plan tretmana rizika/prilika, koji se odobrava, prati realizacija njegovog tretmana i vrši se njegovo preispitivanje, slično kao u Proceduri upravljanja rizicima i sigurnosti informacija (PR 06).

Osim ovih dokumenata, u vezi rizika koji su povezani sa informacionim tehnologijama, usvojena su i sledeća dokumenta: Uputstvo za upravljanje fizičkom sigurnošću (UP 6.2), Uputstvo za upravljanje korisničkim nalozima i lozinkama (UP 6.3), Uputstvo za backup (UP 6.4) i Uputstvo za upravljanje kontinuitetom poslovanja (UP 6.5). Ova dokumenta su vezana

za neke od drugih preporuka iz Izvještaja o reviziji IS FZO u okviru kojih je vršena detaljna provjera.[10]

Revizijom je **utvrđeno** da su rizici povezani sa informacionim tehnologijama **identifikovani** i da su u Planu tretmana rizika identifikovane ranjivosti i prijetnje, te da je napravljen plan tretmana u cilju njihovog popravljanja.

Osim toga, izvršena je interna provjera, u skladu sa Procedurom interne provjere (PR 03), o čemu je sastavljen Izvještaj sa interne provjere (OB 3.3 od 03.07.2019. godine), gdje su između ostalog vršene provjere procesa Upravljanje rizicima i sigurnosti informacija (PR 06) i Upravljanje rizicima i prilikama (PR 14). U Izvještaju je konstatovano da neusaglašenosti ne postoje. Registar rizika i Plan tretmana rizika (OB 6.1) su definisani i dostavljeni direktoru na upoznavanje i saglasnost (br. 01-5000 od 04.07.2019. godine), a Plan tretmana rizika je dostavljen rukovodiocima organizacionih cjelina u Sektoru za IT na dalje postupanje i realizaciju. Registar poslovnih prilika i rizika sa tretmanom (OB 14.1) je definisani kod predstavnika rukovodstva. Direktor Fonda i direktor IT su upoznati sa registrom i planom tretmana (saglasnost br. 01-5026 od 04.07.2019. godine).

Na osnovu navedenog utvrđeno je da je Fond za zdravstveno osiguranje Crne Gore u prethodnom periodu, **vršio** preispitivanje rezultata analize rizika, u skladu sa članom 39 Uredbe o mjerama informacione bezbjednosti.

Preporuka je realizovana.

Preporuka broj 6

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da se u Fondu za zdravstveno osiguranje Crne Gore ne vrši blagovremeno ažuriranje i ukidanje korisničkih naloga.

Neblagovremenim ukidanjem korisničkih naloga, naročito kod prekida radnog odnosa postoji rizik neovlašćenog pristupa softveru.

Fondu za zdravstveno osiguranje **preporučeno je** da unaprijedi mjere za bezbjednost informacionog sistema kroz procedure i bolju kontrolu logičkog pristupa sistemu i aplikacijama.

Utvrđeno činjenično stanje za preporuku br. 6:

Fond za zdravstveno osiguranje Crne Gore je u cilju realizacije date preporuke **unaprijedio** mjere za bezbjednost informacionog sistema i uspostavio procedure i bolju kontrolu logičkog pristupa sistemu i aplikacijama i **donio** dokument Uputstvo za upravljanje korisničkim nalozima i lozinkama (UP 6.3).

Utvrđeno je da su ranije važeća dokumenta Politika korisničkih šifri (br. 04-2751/4 od 10.04.2017. godine) i Politika udaljenog pristupa (br. 04-2751/3 od 10.04.2017. godine) u sklopu postupka uvođenja ISO standarda inkorporirana u Uputstvo za upravljanje korisničkim

[10] Preporuka broj 4, preporuka broj 6, preporuka broj 8 i preporuka broj 2, na stranama broj 15, 18, 21 i 13 ovog Izvještaja.

nalozima i lozinkama sa datumom primjene od 14.11.2018. godine. Ovim uputstvom definisani su tipovi lozinki, korisnička prava, kompleksna i generalna uputstva pri kreiranju šifri, načini promjene lozinki, preispitivanje prava pristupa i ukidanja datih prava.

Internom provjerom o kojoj je sačinjen Izvještaj sa interne provjere od 03.07.2019. godine (OB 3.3), izvršena je između ostalog i provjera procesa Upravljanje korisničkim nalozima i lozinkama. U Izvještaju su konstatovane sledeće neusaglašenosti:

- zahtjevi za otvaranje, ažuriranje ili ukidanje korisničkog naloga se uvijek ne dostavljaju na obrascu OB 6.2
- obavještenja o realizaciji zahtjeva se ne dostavljaju korisnicima i podnosiocu u pisanoj formi ili putem maila
- preispitivanje prava pristupa aplikaciji Fonda putem korisničkih naloga nije vršena u 2019. godini
- korisnici nisu u potpunosti upoznati sa uputstvima pri kreiranju šifri i standardima za zaštitu šifri.

Za navedene neusaglašenosti predložene su adekvatne korektivne mjere sa navedenim odgovornim licem i rokom za realizaciju mjera, koje su realizovane u toku vršenja revizije. Takođe je dostavljen Izvještaj o realizaciji mjere IA-9 o izvršenom preispitivanju prava pristupa aplikaciji FZO (br. 04-6379 od 28.08.2019. godine) o godišnjem preispitivanju.

Utvrđeno je da se administratorske i posebne lozinke čuvaju u zapečaćenim kovertama u sefu u kancelariji pomoćnika direktora za IT, u skladu sa Uputstvom za upravljanje korisničkim nalozima i lozinkama.

Izvršen je uvid u registrator evidencije korisničkih naloga, i konstatovano je da je evidencija uredna, za razliku od prethodnog perioda kad je vršena revizija IS FZO 2017. godine. I dalje postoji problem oko zatvaranja korisničkih naloga, jer zahtjeve za zatvaranje korisničkih naloga služba za kadrovske poslove ne dostavlja blagovremeno. Takođe, umjesto na propisanom Obrascu zahtjeva za pristup informacionom sistemu Fonda (OB 6.2) koji je sastavni dio Uputstva za upravljanje korisničkim nalozima i lozinkama, zahtjevi za otvaranje, ažuriranje i zatvaranje korisničkih naloga sa detaljima o promjenama koje je potrebno izvršiti, uglavnom stižu email-om od nadležnih sektora.

Izvršen je uvid u spisak zaposlenih koji su primljeni na rad u periodu od 01.01.2017. do 09.07.2019. godine, kao i spisak zaposlenih koji su otišli iz Fonda u periodu od 01.01.2017. do 09.07.2019. godine. Takođe, za pristup informacionom sistemu, u skladu sa svojim nadležnostima, kreirani su korisnički nalozi za pojedine službenike iz Ministarstva zdravlja, Ljekarske i Farmaceutske komore.

Izvršen je validacijski test u cilju utvrđivanja da li sistem od korisnika zahtjeva promjenu lozinke pri prvom logovanju. Kreiran je probni korisnički nalog za koji je prilikom prvog logovanja sistem zatražio promjenu šifre. Utvrđeno je da sistem zahtijeva postavljanje jake šifre, što je u skladu sa Uputstvom o kreiranju korisničkih naloga i lozinki. Takođe je utvrđeno da postoji kontrola datuma, tako da se korisnički nalog može kreirati unaprijed, ali se ne može koristiti prije datuma naznačenog u sistemu.

Preporuka je realizovana.

Preporuka broj 7

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da zaposleni u Fondu za zdravstveno osiguranje jedni drugima znaju korisnička imena i šifre, kao i da šifre od kreiranja nisu promijenjene, pa ih je lako pretpostaviti, te da zaposleni nisu svjesni odgovornosti koju zahtijeva njihovo radno mjesto.

Postoji **rizik** od zloupotrebe i neovlašćenog pristupa podacima.

Fondu za zdravstveno osiguranje **preporučeno je** da vrši redovnu edukaciju zaposlenih u smislu obaveze čuvanja i zaštite tajnih podataka kojima po opisu radnog mjesta imaju pristup, kao i da preduzmu mjere na uvođenju lične izjave o prihvatanju odgovornosti za zaposlene.

Utvrđeno činjenično stanje za preporuku br. 7:

U skladu sa preporukom koja je data, Fond za zdravstveno osiguranje Crne Gore je **vršio** edukaciju zaposlenih u smislu bezbjedonosnih pravila radi obezbjeđivanja podataka kojima ta lica imaju pristup kroz dokumenta koja je **donio:** Politiku upravljanja kvalitetom i sigurnosti informacija (POL 01) i Politike sigurnosti (POL 02), zatim upoznavanje sa Uputstvom za upravljanje korisničkim nalozima i lozinkama (UP 6.3) i potpisivanje sporazuma o povjerljivosti i zajedničkom čuvanju i neotkrivanju podataka.

Politika sigurnosti, koju su zaposleni u obavezi da poštuju, između ostalog obuhvata pitanja koja se bave:

- sigurnošću personalnih računara koja se odnosi na obradu čuvanje i korišćenje podataka i instalaciju programskih paketa uz zaštitu od destruktivnih programa
- korišćenjem programskih paketa sa licencom
- primjerenom upotrebom informatičkih resursa u smislu profesionalnog, etičkog i zakonitog korišćenja računarskih resursa
- korišćenjem interneta uz zaštitu od neovlašćenog pristupa unutrašnjoj mreži ili podacima
- zaštitom od malicioznog koda
- korišćenjem mobilnih uređaja i odgovornošću za čuvanje podataka na njima
- postupanjem sa dokumentima – politika "čistog stola i čistog ekrana"
- zaštitom podataka i informacija od kopiranja na prenosive medije.

Uputstvom za upravljanje korisničkim nalozima i lozinkama zaposleni su upoznati sa načinom kreiranja jakih šifri i da poslovne šifre ne smiju nikom govoriti jer su osjetljive, povjerljive i poslovne informacije. Osim toga, o novim uslovima korisničkih šifri, periodu njihovog važenja i vremena dozvoljene neaktivnosti, svi zaposleni u Fondu su obaviješteni elektronskom poštom predstavnika rukovodstva od 14.03.2018. godine.

Svim zaposlenima u Fondu poslato je obavještenje (elektronska pošta predstavnika rukovodstva od 15.11.2018. godine), da u vezi sigurnosti podataka i informacija u pravno-formalnom dijelu je potrebno da potpišu sporazum o povjerljivosti, i da potpisane sporazume dostave lično ili putem pošte, sa rokom dostavljanja 23.11.2018. godine.

Izvršen je uvid u potpisane sporazume koji se nalaze kod predstavnika rukovodstva. Slučajnim izborom na nivou uzorka je utvrđeno je da su sporazume potpisali svi zaposleni u Fondu, u dva

primjerka, od kojih jedan zadržava zaposleni a drugi se čuva u Sektoru za IT i razmjenu podataka u IISZ. Sporazumi su zavedeni, a sve ih je u ime Fonda potpisao direktor.

Preporuka je realizovana.

Preporuka broj 8

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Procedura za Backup Fonda za zdravstveno osiguranje nije usklađena sa Uredbom o mjerama informacione bezbjednosti (članovi 18, 19 stav 2).

Nevršenjem izrade rezervne kopije podataka u skladu sa Uredbom vezano za skladištenje podataka postoji **rizik** od narušavanja bezbjednosti, povjerljivosti, cjelovitosti i dostupnosti podataka.

Fondu za zdravstveno osiguranje **preporučeno je** da Proceduru za backup IZIS uskladi sa Uredbom o mjerama informacione bezbjednosti, čl.18 u smislu:

- vrste skladištenja podataka koje se vrše (dnevno, sedmično, mjesečno i godišnje)
- vremena čuvanja godišnje uskladištenih podataka
- označavanja uskladištenih podataka
- vođenja evidencije informatičkih medija na kojima su podaci uskladišteni.

Utvrđeno činjenično stanje za preporuku br. 8:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, Fond za zdravstveno osiguranje Crne Gore je **izmijenio** Proceduru za backup IZIS i izradio Uputstvo za bekap (UP 6.4), doneseno 12.02.2019, koje je **usaglašeno sa** Uredbom o mjerama informacione bezbjednosti u smislu člana 18 i 19 stav 2.

U tom cilju u Uputstvu za bekap su pored dnevnog skladištenja baze podataka, definisani sedmično, mjesečno i godišnje skladištenje podataka. Takođe je definisano čuvanje godišnje uskladištenih podataka na 12 mjeseci. Utvrđeno je da se vrši označavanje uskladištenih podataka kao i da se vodi evidencija.

U skladu sa Uputstvom, za čuvanje uskladištenih podataka Fond je obezbijedio bezbjednu lokaciju – sef u kancelariji direktora Sektora za IT i razmjenu podataka IISZ-a i sef u banci.

Takođe, internom provjerom o kojoj je sačinjen Izvještaj sa interne provjere od 03.07.2019. godine (OB 3.3), izvršena je između ostalog i provjera procedure backup-a (UP 6.4). U Izvještaju je konstatovano par neusaglašenosti koje se odnose na prostor za čuvanje backupa koji nije bio obezbijeđen u momentu provjere, predložene su korektivne mjere koje su realizovane u toku vršenja revizije.

Preporuka je realizovana.

Preporuka broj 9

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje ne vrši šestomjesečnu provjeru upotrebljivosti sigurnosne kopije podataka, što nije u skladu sa članom 20 Uredbe o mjerama informacione bezbjednosti.

Nevršenjem provjere rezervne kopije podataka postoji **rizik** od nemogućnosti obnavljanja rada servera baze podataka.

Fondu za zdravstveno osiguranje **preporučeno je** da najmanje svakih šest mjeseci vrši provjeru upotrebljivosti sigurnosne kopije podataka, uz provjeru postupka povraćaja baza podataka uskladištenih na informatičkom mediju, tako da vraćeni podaci nakon izvršene provjere budu cjeloviti, povjerljivi i dostupni za upotrebu, u skladu sa članom 20 Uredbe o mjerama informacione bezbjednosti.

Utvrđeno činjenično stanje za preporuku br. 9:

U cilju realizacije date preporuke **vršeno** je testiranje - provjera upotrebljivosti sigurnosne kopije podataka. U Fondu je smatrano da realizacija ove preporuke zavisi od postojanja paralelnog sistema tj. Disaster Recovery site-a, na kojem bi se vršila provjera postupka povraćaja baze podataka, tako da vraćeni podaci budu cjeloviti, povjerljivi i dostupni za upotrebu, te da će realizacija ove preporuke biti moguća nakon realizacije preporuke br. 3. Kako se ove provjere mogu vršiti na testnim sistemima, iz Fonda su u toku vršenja revizije, 01.08.2019. godine, uspješno izvršili provjeru upotrebljivosti sigurnosne kopije podataka, što je **u skladu** sa članom 20 Uredbe o mjerama informacione bezbjednosti.

U skladu sa Uputstvom za backup (UP 6.4), tačka 3.6 Provjera backup-a podataka, provjera upotrebljivosti sigurnosne kopije podataka vršena je tako što su na testnom sistemu pokrenuta tri izvještaja koji su potpuno nezavisni jedan od drugog i vezani su za pojedinačne softverske module. Ista tri izvještaja pokrenuta su sa produkcije, izvršeno je upoređivanje navedenih izvještaja i potvrđeno da nema odstupanja ili neslaganja. Provjera je urađena bez uočenih nepravilnosti ili prepreka u sprovođenju procedura, o čemu je sačinjen Izvještaj provjere backup-a OB 6.4 (broj: 04-5063 od 01.08.2019. godine), testiranje je bilo uspješno.

Preporuka je realizovana.

Preporuka broj 10

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da se podaci Integralnog zdravstvenog informacionog sistema pri prenosu kroz sistem ne kriptuju, što nije u skladu sa članom 22 Uredbe o mjerama informacione bezbjednosti.

Kada podaci nisu kriptovani postoji **rizik** pristupa i zloupotrebe od strane neovlašćenih lica.

Fondu za zdravstveno osiguranje **preporučeno je** da uspostavi sistem kriptovane zaštite podataka u prenosu podataka informacionim i telekomunikacionim sistemom, u skladu sa članom 22 Uredbe o mjerama informacione bezbjednosti.

Utvrđeno činjenično stanje za preporuku br. 10:

U skladu sa preporukom koja je data, Fond za zdravstveno osiguranje je **uspostavio** sistem kriptovane zaštite podataka u prenosu podataka informacionim i telekomunikacionim sistemom, kroz Trustpoint sistem na osnovu tenderskog postupka iz septembra 2018. godine. Sva komunikacija iz filijala ka Fondu se kriptuje, transportni linkovi su kriptovani, što je **u skladu** sa članom 22 Uredbe o mjerama informacione bezbjednosti.

Preporuka je realizovana.

Preporuka broj 11

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje nema politiku bezbjednosti informacija i plan IT bezbjednosti.

Nepostojanje politike bezbjednosti informacija i plana IT bezbjednosti, povećava se **rizik** od unutrašnjih ili spoljašnjih, namjernih ili slučajnih prijetnji po informacije koje se nalaze u sistemu zdravstva.

Fondu za zdravstveno osiguranje **preporučeno je** da izradi politiku bezbjednosti informacija koja treba da sadrži: prava pristupa informacijama, način kontrole njihove primjene, definiše kontrole koje štite od neautorizovanog pristupa informacionim vrijednostima i uputstvo za zaposlene u skladu sa zahtjevima bezbjednosti informacija, kao i plan IT bezbednosti koji uključuje taktičke planove, klasifikaciju podataka, tehnološke standarde, sigurnost i kontrolne politike i upravljanje rizikom.

Utvrđeno činjenično stanje za preporuku br. 11:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, utvrđeno je da je Fond za zdravstveno osiguranje **donio** Politiku upravljanja kvalitetom i sigurnosti informacija (POL 01) i Politike sigurnosti (POL 02), koje zajedno sa procedurama i uputstvima obuhvataju oblasti predviđene politikom bezbjednosti informacija i planom IT bezbjednosti.

Politika upravljanja kvalitetom i sigurnosti informacija (POL 01) sadrži načela za poboljšavanje Sistema upravljanja kvalitetom i sigurnosti informacija, sa ciljem optimalnog poslovanja, zaštite povjerljivih informacija i daljeg uspješnog razvoja.

Politike sigurnosti (POL 02), koju su zaposleni u obavezi da poštuju, između ostalog obuhvata pitanja koja se bave:

- procjenom sigurnosnog rizika (3.1) sa ciljem identifikacije prijetnji informacionom sistemu i njegovih ranjivosti
- klasifikacijom podataka (3.3) s obzirom na njihovu povjerljivost, pouzdrnost i raspoloživost,
- zahtjevima za fizičku sigurnost informatičkih resursa (3.5) klasifikovanjem u kategorije: područje otvoreno za javnost, područje koje nije otvoreno za javnost ali je otvoreno za zaposlene u IT Fonda i područje koje je otvoreno samo ovlašćene zaposlene,

- zahtjevima za sigurnost računarskih sistema i mreže (3.6) sa podešavanjima koja bilježe sve događaje o pristupu povjerljivim ili osjetljivim podacima ili programima,
- pristupom resursnim elementima informacionog sistema (3.8),
- postupcima u slučajevima incidenata (3.16), i drugi.

Preporuka je realizovana.

Preporuka broj 12

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje nema uspostavljena bezbjedonosna interna pravila za zaposlene, u skladu sa članom 32 Uredbe o mjerama informacione bezbjednosti.

Nepostojanjem bezbjedonosnih internih pravila za zaposlene postoji **rizik** od narušavanja informacione bezbjednosti podataka kojima zaposleni imaju pristup.

Fondu za zdravstveno osiguranje **preporučeno je** da uspostavi bezbjedonosna interna pravila za zaposlene radi obezbjeđivanja informacione bezbjednosti podataka kojima ta lica imaju pristup, u skladu sa članom 32 Uredbe o mjerama informacione bezbjednosti.

Utvrđeno činjenično stanje za preporuku br. 12:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, utvrđeno je da je Fond za zdravstveno osiguranje **donio** Politiku upravljanja kvalitetom i sigurnosti informacija (POL 01) i Politike sigurnosti (POL 02), čime je uspostavio interna pravila za zaposlene što je **u skladu** sa članom 32 Uredbe o mjerama informacione bezbjednosti.

Politika upravljanja kvalitetom i sigurnosti informacija (POL 01) obezbjeđuje i garantuje, između ostalog, ostvarivanje visokog nivoa sigurnosti informacija, kao i permanentno i plansko usavršavanje zaposlenih i razvoj svijesti o potrebi sigurnosti informcija.

Politike sigurnosti (POL 02) se između ostalog odnose na:
- Obuku korisnika (3.4) u cilju unapređenja svijesti korisnika o važnosti sigurnosti informacija,
- Sigurnost personalnih računara (3.10) radi sprječavanja sigurnosnih rizika,
- Korišćenje programskih paketa (3.11) u skladu sa zakonom i licencnim pravima,
- Zaštitu od malicioznog koda (3.14),
- Upravljanje medijima sa podacima (3.22) po kojem zaposlenima nije dozvoljeno korišćenje prenosnih medija u privatnom vlasništvu.

Utvrđeno je da je u prethodnom periodu vršena edukacija zaposlenih održavanjem radionice čija je glavna tema bila sigurnost podataka i informacija, a u sklopu uvođenja ISO 27001 i ISO 9001. Zaposleni su takođe, putem elektronske pošte i internog portala upoznati sa politikama i uputstvima koje se odnose na sigurnost podataka i informacija.

Preporuka je realizovana.

Preporuka broj 13

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Odsjek za operativu ima sistematizovanih 10 radnih mjesta od kojih je 8 popunjeno, a samo pet službenika radi na poslovima IT bezbjednosti Fonda, PZZ, SZZ, ZHMP i ZTK u čijem sistemu ima ukupno 3.111 računara (2.118 je bilo 2017.godine kada je data preporuka).

Postoji **rizik** od propusta u radu koji u značajnom mogu ugroziti bezbjednost sistema i podatke koji se nalaze u njemu usled povećanja obima posla nastalog zbog privremenih spriječenosti za rad i povremenog odsustva dijela zaposlenih.

Fondu za zdravstveno osiguranje **preporučeno je** da nastavi aktivnosti na jačanju kadrovskog kapaciteta i potencijala IT stručnjaka u Fondu za zdravstveno osiguranje Crne Gore.

Utvrđeno činjenično stanje za preporuku br. 13:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, utvrđeno je da je Fond za zdravstveno osiguranje **donio** Proceduru za upravljanje obukama (PR 02) od 01.09.2018. godine. Ovom procedurom se definiše postupak za utvrđivanje potreba, planiranja i realizacije obuke zaposlenih u Sektoru za IT i razmjenu podataka u IISZ, kako bi se obezbijedila neophodna kompetentnost zaposlenih čiji rad utiče na kvalitet i učinak procesa integrisanog sistema za upravljanje kvalitetom i sigurnosti informacija (IMS – Integral Management System).

Procedura se odnosi na internu i eksternu obuku svih zaposlenih u Sektoru, kao i obuke za novozaposlene i honorarno angažovane radnike. Planom obuke (OB 2.1) definišu se prioriteti potrebnih obuka koje mogu biti:

A – zakonska obaveza, zahtjev korisnika, ugroženo odvijanje procesa, poboljšanje efektivnosti i efikasnosti procesa, ili
B – opšte stručno usavršavanje zaposlenih.

Izvršen je uvid u planove obuke za 2018 i 2019. godinu. Utvrđeno je da su planom obuka za 2018. godinu bile planirane ukupno tri obuke, koje su i realizovane. Polaznici obuka za upoznavanje sa standardima ISO 9001 i ISO 27001 (17.04.2018. godine) i obuka za razmjenu iskustava iz ICT oblasti (INFOFEST 2018, 01.10 - 05.10.2018) su bili zaposleni u Sektoru za IT i razmjenu podataka u IISZ. Predstavnik rukovodstva je pohađao trodnevnu obuku za korišćenje naprednih alata za izvještavanje Bussiness inteligence (BI).

Plan obuka za 2019. godinu predviđa šest obuka od kojih je do sada pet realizovano. U cilju upoznavanja sa iskustvima, planovima i izazovima, za predstavnika rukovodstva realizovane su trodnevna posjeta Hrvatskom Zavodu za zdravstveno osiguranje i dvodnevna posjeta Zavodu za zdravstveno osiguranje Slovenije. Trodnevna razmjena iskustava iz ICT oblasti sa kolegama iz regiona (YU INFO 2019) realizovana je za pomoćnika direktora za IT i predstavnika rukovodstva, dok je samostalni savjetnik iz Odsjeka za operativu pohađao četvorodnevni kurs za Red Hat System Administration sertifikat. Trodnevna obuka za Oracle BI je organizovana za sve zaposlene u Sektoru za IT, dok će u oktobru biti realizovan INFOFEST 2019 - razmjena iskustava iz ICT oblasti sa kolegama iz zemlje i regiona.

Kako jačanje kadrovskog kapaciteta i potencijala IT stručnjaka u Fondu za zdravstveno osiguranje osim obuka predviđa i zapošljavanje novih kadrova, ono nije realizovano iz razloga što je u prethodnom periodu bilo više konkursa za koje prijavljeni kandidati nisu ispunjavali tražene uslove konkursa. Osim toga, u poslednjih par godina Fond ne dobija saglasnost Ministarstva finansija za popunjavanje upražnjenih radnih mjesta, zbog odluke Vlade koja se odnosi na ograničavanje zapošljavanja u javnom sektoru. Rezultat toga je i činjenica da su Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Fonda za zdravstveno osiguranje, iz decembra 2018. godine, u Sektoru za IT i razmjenu podataka IISZ ukinuta dva radna mjesta.

Preporuka je djelimično realizovana.

Preporuka broj 14

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje nema politiku bezbjednosti informacija sa davaocima usluga.

Nepostojanjem politike bezbjednosti informacija sa davaocima usluga postoji **rizik** od narušavanja funkcionisanja informacionog sistema.

Fondu za zdravstveno osiguranje **preporučeno je** da definiše politiku bezbjednosti informacija sa davaocima usluga, radi obezbjeđivanja ispravnog i bezbjednog funkcionisanja informacionog sistema.

Utvrđeno činjenično stanje za preporuku br. 14:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, utvrđeno je da je Fond za zdravstveno osiguranje **donio** Politiku sigurnosti (POL 02) od 01.09.2018. godine, kojom je u dijelu 3.2 definisan rad sa spoljnim partnerima i dobavljačima, čime je definisana politika bezbjednosti informacija sa davaocima usluga.

Precizno je definisana obaveza davaoca usluga tj. spoljnih partnera koji moraju preuzeti obavezu brige za sigurnost informacionog sistema Fonda za zdravstveno osiguranje Crne Gore i informacionih resursa koji su u vlasništvu IT Fonda, a u skladu sa Sigurnosnom politikom IT Fonda i aktima koji iz nje proizilaze.

- Pristup resursima informacionog sistema može biti omogućen samo uz pisanu saglasnost ovlašćenog lica.
- Za pristup informacionom sistemu je potrebno potpisati ugovor o poslovnoj saradnji koji uključuje tehničku specifikaciju komunikacione veze, raspoložive servise, lozinku za pristup, kontakt osobe koje su odgovorne za vezu, kao i druge potrebne informacije. Ugovor mora uključiti i sve odredbe sigurnosne politike i obavezu čuvanja tajnosti podataka.

Eksterni pristup informacionom sistemu Fonda se omogućava odobravanjem VPN (Virtual Private Network – virtuelna privatna mreža) konekcije na osnovu pisanog zahtjeva.

Preporuka je realizovana.

Preporuka broj 15

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond za zdravstveno osiguranje ne zahtijeva potpisivanje sporazuma o povjerljivosti sa zaposlenima iz partnerskih kompanija.

Postoji **rizik** da korisnici sistema iz partnerskih kompanija vrše neovlašćeni uvid ili izmjenu podataka u bazi osiguranika.

Fondu za zdravstveno osiguranje **preporučeno je** da sa korisnicima sistema iz partnerskih kompanija potpisuje izjave o povjerljivosti.

Utvrđeno činjenično stanje za preporuku br. 15:

U skladu sa preporukom koja je data i u sklopu uvođenja standarda, utvrđeno je da je Fond za zdravstveno osiguranje **donio** Politiku sigurnosti (POL 02) od 01.09.2018. godine, kojom je u dijelu 3.2 definisan rad sa spoljnim partnerima i dobavljačima. Uvođenjem Politike sigurnosti Fond je obezbijedio pravno-formalnu zaštitu podataka i informacija kroz zaključivanje sporazuma o povjerljivosti sa partnerskim kompanijama koje dolaze u posjed povjerljivih i drugih informacija iz Fonda, odnosno sa kojima Fond razmjenjuje povjerljive i druge informacije.

Revizijom je **utvrđeno** da je Fond potpisao ugovore o čuvanju i povjerljivosti informacija sa davaocima usluga. Izvršen je uvid u sve ugovore koji su potpisani sa kompanijama koje su spoljni saradnici. Dokumentacija je uredna i nalazi se kod predstavnika rukovodstva.

Preporuka je realizovana.

III ZAKLJUČAK

Na bazi sprovedene kontrolne revizije i utvrđenog činjeničnog stanja, a u skladu sa članom 12 Zakona o Državnoj revizorskoj instituciji i članom 45 Poslovnika Državne revizorske institucije, nadležni Kolegijum DRI u sastavu: Radule Žurić (član Senata - rukovodilac Kolegijuma) i dr Branislav Radulović (član Senata – član Kolegijuma), na sjednici održanoj 18. septembra 2019. godine, usvojio je:

KONAČNI IZVJEŠTAJ
o kontrolnoj reviziji informacionog sistema
Fonda za zdravstveno osiguranje Crne Gore

ZAKLJUČAK

Aktivnostima i radnjama koje je Fond za zdravstveno osiguranje Crne Gore preduzeo i cilju realizacija preporuka DRI **otklonjen je najveći dio nedostataka**, odnosno od ukupno **petnaest (15)** izdatih preporuka DRI, koje su bile predmet kontrolne revizije:

- **realizovano je** **13** preporuka
- **djelimično realizovana** **1** preporuka
- **nije realizovana** **1** preporuka.

Preporuka koja nije realizovana, preporuka broj 3, odnosi se na oporavak od katastrofe (Disaster Recovery), dok se djelimično realizovana preporuka, preporuka broj 13, odnosi na kadrovske kapacitete Fonda koje je potrebno ojačati i popuniti u skladu sa važećim Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Fonda za zdravstveno osiguranje Crne Gore.

Subjekat revizije je dužan da u roku od šest mjeseci izvjesti DRI o realizaciji preporuke broj 3 i preporuke broj 13.

Rukovodilac Kolegijuma

Radule Žurić
Član Senata DRI