CRNA GORA
DRŽAVNA REVIZORSKA INSTITUCIJA
Broj: 40114/19-033-120/29
Podgorica, 24.05.2019. godine.

KONAČNI IZVJEŠTAJ

O KONTROLNOJ REVIZIJI INFORMACIONOG SISTEMA
FONDA PENZIJSKOG I INVALIDSKOG OSIGURANJA CRNE GORE

Podgorica, maj 2019. godine

SADRŽAJ

I OPŠTI DIO

1. Pravni osnov za vršenje revizije 3

2. Vrsta, predmet i cilj revizije 3

3. Djelatnost subjekta revizije i informacioni sistem Fonda PIO 4

II UTVRĐENO ČINJENIČNO STANJE 6

III ZAKLJUČAK 16

I OPŠTI DIO

1. PRAVNI OSNOV ZA VRŠENJE REVIZIJE

Pravni osnov za vršenje kontrolne revizije informacionog sistema Fonda penzijskog i invalidskog osiguranja Crne Gore (u daljem tekstu: Fond PIO) 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 24. januara 2019. godine (broj: 40114/19-033-120/3) u sastavu: g. Radule Žurić (rukovodilac Kolegijuma) i dr Milan Dabović (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 kontrola realizacije preporuka sadržanih u Konačnom izvještaju o reviziji Godišnjeg finansijskog izvještaja Fonda penzijskog i invalidskog osiguranja Crne Gore za 2016. godinu (broj: 40113/17-031-143/29 od 13.10.2017. godine), u daljem tekstu: Izvještaj o reviziji Fonda penzijskog i invalidskog osiguranja Crne Gore.

Cilj revizije je 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. Polazni materijali za vršenje revizije bili su izvještaji subjekta revizije o sprovedenim radnjama u cilju realizacije preporuka, i to:

– Plan aktivnosti Fonda PIO za realizaciju preporuka u roku od 60 dana (Dopis broj: 40114/18-033-40/2 od 02.02.2018. godine), u daljem tekstu: Plan aktivnosti za realizaciju preporuka,

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

- Preduzete radnje Fonda PIO u roku od 6 mjeseci, po datim preporukama u skladu sa članom 15 Zakona o Državnoj revizorskoj instituciji (Dopis broj: 40114/18-033-40/3 od 17.04.2018. godine), u daljem tekstu: Izvještaj o realizaciji preporuka, i
- Preduzete aktivnosti Fonda PIO u cilju realizacije preporuka na obavještenje o vršenju kontrolne revizije (Dopis broj: 40114/19-033-120/14 od 01.03.2019. 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 penzijskog i invalidskog osiguranja Crne Gore.

3. DJELATNOST SUBJEKTA REVIZIJE I INFORMACIONI SISTEM FONDA PIO

3.1. Djelatnost subjekta revizije

Shodno Zakonu o penzijskom i invalidskom osiguranju, Fond je institucija koja vrši javna ovlašćenja prilikom rješavanja o pravima i obavezama iz penzijskog i invalidskog osiguranja. Osnovne funkcije Fonda su: efikasno, racionalno i zakonito ostvarivanje prava iz PIO, obračun i isplata prava u nacionalnom pravu i primjenom međunarodnih sporazuma o socijalnom osiguranju; utvrđivanje postojanja i uzroka invalidnosti i tjelesnog oštećenja; pružanje stručne pomoći pri ostvarivanju prava; donošenje nacrta budžeta Fonda; vođenje evidencije i analiza podataka o osiguranicima i korisnicima prava; vođenje evidencije i analiza podataka o zaradama, odnosno osnovicama osiguranja na koje su uplaćeni doprinosi, kao i preduzimanje mjera za utvrđivanje njihove ispravnosti; vođenje evidencije o visini uplaćenog doprinosa za osiguranike, kao i o visini penzija; organizovanje poslova za sprovođenje penzijskog i invalidskog osiguranja i obezbjeđenje informatičke tehnologije na zakonom propisan način.

Fond PIO je javni fond koji je osnovan u cilju efikasnog finansiranja unapređenja sistema penzijskog i invalidskog osiguranja. Fond PIO se do 2010. godine tretirao kao vanbudžetski fond, a od 01.01.2010. godine uključen u Konsolidovani račun Državnog trezora.

Zakonom o penzijskom i invalidskom osiguranju ("Službeni list Republike Crne Gore", br. 054/03, 039/04, 061/04, 079/04, 081/04, 029/05, 014/07, 047/07, Službeni list Crne Gore", br. 012/07, 013/07, 079/08, 014/10, 078/10, 034/11, 039/11, 040/11, 066/12, 036/13, 038/13, 061/13, 006/14, 060/14, 060/14, 010/15, 044/15, 042/16, 055/16) je otpočela reforma sistema penzijskog i invalidskog osiguranja, kroz uvođenje višestubnog sistema penzijskog i invalidskog osiguranja, tako da penzijsko i invalidsko osiguranje u Crnoj Gori obuhvata:

1) obavezno penzijsko i invalidsko osiguranje na osnovu tekućeg finansiranja;
2) obavezno penzijsko osiguranje na osnovu individualne kapitalizovane štednje;
3) dobrovoljno penzijsko osiguranje na osnovu individualne kapitalizovane štednje.

Zakonom o penzijskom i invalidskom osiguranju uređuje se obavezno penzijsko i invalidsko osiguranje na osnovu tekućeg finansiranja, dok penzijsko osiguranje na osnovu individualne kapitalizovane štednje i dobrovoljno penzijsko osiguranje na osnovu individualne kapitalizovane štednje uređeno je posebnim zakonom.

Obaveznim penzijskim i invalidskim osiguranjem, na osnovu tekućeg finansiranja, osiguranicima se, po osnovu rada, zavisno od dužine ulaganja i visine osnovice na koju je plaćen doprinos za penzijsko i invalidsko osiguranje, uz primjenu načela uzajamnosti i solidarnosti, obezbjeđuju prava za slučaj starosti, invalidnosti i tjelesnog oštećenja, a članovima njihovih porodica pravo za slučaj smrti osiguranika, odnosno korisnika prava.

3.2. Informacioni sistem Fonda PIO

Informacioni sistem Fonda PIO je uveden u produkcionu upotrebu 2009. godine.
Informacioni sistem Fonda PIO sa implementacijom elemenata poslovnog informacionog sistema se sastoji iz dvije grupe međusobno povezanih softverskih rješenja:

Grupa I: Core aplikacija sa modulima:
- Matična evidencija penzionera
- Evidencija aktivnih osiguranika
- Isplata prava
- Kancelarijsko poslovanje

Grupa II: Poslovni aplikativni softver:
- Finansijko poslovanje
- Obračun zarada
- Kadrovska služba
- Osnovna sredstva

Fond PIO se nalazi na ukupno 12 lokacija. Broj zaposlenih u Fondu PIO je 207, od kojih 199 u svom radu koriste računar. Broj zaposlenih koji koriste isti računar je 5. Broj zaposlenih u Sektoru za informacione tehnologije u oblasti penzijskog i invalidskog osiguranja je 28. Broj zaposlenih koji imaju korisnički nalog za aplikaciju je 162, a 5 zaposlenih ima administratorski nalog za aplikaciju. Broj računara je 203, a izlaz na internet ima 156 računara. Broj servera u produkciji je 12, a broj servera na kojima je postavljen sistem za izvještavanje je 6. Svi računari u Fondu PIO su povezani na centralni antivirus server na kojem se vrši ažuriranje i kontrola antivirusa na svim radnim stanicama u Fondu PIO. Ažuriranje se vrši automatski, server preuzima svakodnevno nove definicije virusa, dok se ostale radne stanice ažuriraju preko servera.

Sistem je napravljen sa najvećim mogućim stepenom redudanse. Server sala koja se nalazi na centralnoj lokaciji u Podgorici bežično je povezana prema područnim jedinicama. Prostor u kojem se nalaze računari za vođenje baze podataka i centralni računar informacionog sistema (serveri), mrežna ili komunikaciona oprema informacionog sistema, organizuje se kao administrativna zona. Po područnim jedinicama oprema je smještena u komunikacionim rek ormanima.

Instalaciju, konfiguraciju i monitoring rada servera, rutera, switch-eva vrše zaposleni u Sektoru za informacione tehnologije u oblasti penzijskog i invalidskog osiguranja.

II UTVRĐENO ČINJENIČNO STANJE

Revizija koju je sprovela Državna revizorska institucija 2017. godine, ukazala je na postojanje propusta u radu Fonda penzijskog i invalidskog osiguranja 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 Godišnjeg finansijskog izvještaja Fonda penzijskog i invalidskog osiguranja Crne Gore za 2016. godinu.**

Preporuka broj 1

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond PIO nema usvojenu strategiju za informacione tehnologije (u daljem tekstu: IT strategija), niti bilo kakav drugi strateški dokument koji uređuje ovu oblast.

Bez usvojene IT strategije koja treba biti sastavni dio strateškog planiranja za period 3-5 godina, postoji **rizik** da informacione tehnologije Fonda PIO ne mogu u odgovarajućoj mjeri doprinijeti ostvarivanju i razvoju poslovnih ciljeva Fonda PIO, ni u sistemskom (hardver i softver), ni u razvojnom (izbor i realizacija projekata), ni u kadrovskom (struktura i znanje) smislu.

Fondu PIO **preporučeno je** da preduzme aktivnosti na izradi i usvajanju strateškog dokumenta (IT strategija), kojim bi se planirao razvoj i upravljanje informacionom infrastrukturom, sistemima, komunikacijama, računarskim aplikacijama, bazama podataka i kontinuiranom obukom zaposlenih. U sklopu realizacije strateškog dokumenta potrebno je osigurati stabilno finansiranje IT projekata kroz detaljno planiranje budžeta za razvoj, nabavku i održavanje.

Utvrđeno činjenično stanje za preporuku br. 1:

U skladu sa preporukom koja je data, Fond je izradio i dostavio Plan aktivnosti za realizaciju preporuka, kojim je planirano da strategija bude napisana do 10.05.2018. godine, a zatim je u Izvještaju nakon obavještenja o vršenju kontrolne revizije izvijestio DRI da je donesena IT strategija Fonda PIO za period 2018 – 2022. godina.

Kontrolnom revizijom utvrđeno je da je Fond PIO **donio** IT strategiju za period 2018-2022. godina (br. 01-1451 od 05.06.2018. godine).

IT strategija prikazuje tranziciju od postojećeg IT stanja ka željenom, uz detaljno prikazivanje svih izdataka, kako za razvoj, licence, održavanje, tako i za kontinuiranu obuku zaposlenih u Sektoru za informacione tehnologije. IT strategija daje presjek postojećeg stanja i nešto čemu Fond teži kada je IT u pitanju. U strategiji su predstavljena postojeća hardverska i softverska rješenja koja se koriste u informacionom sistemu Fonda PIO, zatim je dat prikaz novih tehnologija i predlozi unapređenja hardverske infrastrukture i softvera, prepoznata je potreba za kontinuiranom obukom zaposlenih u Sektoru za informacione tehnologije za rad sa novim tehnologijama. U IT strategiji je takođe data procjena finansijskih sredstava neophodnih za modernizaciju informacionog sistema Fonda.

Fond PIO je na osnovu procijenjenih sredstava u IT strategiji za modernizaciju hardvera i sistemskog softvera, u skladu sa planom (nacrta) budžeta za 2019. godinu, uputio zahtjev Ministarstvu finansija za budžetsku potrošnju za 2019. godinu. Razmatrajući zahtjev za budžetska sredstva koja se tiču nabavki vezanih za informacione tehnologije, Ministarstvo finansija uputilo je Fond PIO na potrebnu saglasnost nadležnog Ministarstva javne uprave.

Fond PIO se obratio Ministarstvu javne uprave dopisom br. 01-2414 od 10.10.2018. godine. Dopisom (br. 01-051/18-4591/3 od 28.11.2018. godine) Ministarstvo javne uprave, poštujući smjernice za davanje saglasnosti za modernizaciju informacionog sistema, sagledao je sve bitne aspekte postojećeg stanja i planiranih aktivnosti.

Uz saglasnost sa inicijativom za unapređenje informacionog sistema Fonda PIO, u cilju praćenja kvaliteta i nadzora nad kompleksnim i složenim procesom unapređenja, Ministarstvo javne uprave predložilo je formiranje radnog tima u čijem će radu između ostalih učestvovati i dva predstavnika Ministarstva javne uprave.

Za ovu godinu, za modernizaciju informacionog sistema Fond PIO je obezbijedio budžetska sredstva u iznosu od 793.200,00€.

Preporuka je realizovana.

Preporuka broj 2

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da se u Fondu PIO ne vrši ažurna kontrola zatvaranja korisničkih naloga u skladu sa dokumentom Korišćenje i sigurnost računarskog sistema Fonda PIO (br. 01-1181/10 od 30.11.2012. godine), kojim se propisuje procedura korišćenja računara jedinstvenog računarskog sistema Fonda PIO od strane korisnika, a koji između ostalog sadrži Uputstvo o kreiranju i gašenju korisničkih naloga u IT sistemu i potrebne obrasce. Otvaranje korisničkih naloga i dodjela korisničkih prava vrši se na pismeni zahtjev pomoćnika direktora organizacione jedinice zaposlenog prema obrascu (Prilog 5), dok se zatvaranje korisničkih naloga (usled prestanka radnog odnosa ili zbog povrede radnih obaveza) vrši preko Kadrovske službe Fonda PIO koja obavještava Sektor za informacione tehnologije putem obrasca (Prilog 6), ali Sektor za informacione tehnologije informacije o prestanku radnog odnosa od Kadrovske službe nije dobijao redovno, iako je u navedenom dokumentu definisana ova procedura, već su sami dolazili do saznanja da je nekim licima prestao radni odnos.

Nepoštovanjem procedure zatvaranja korisničkog naloga, postoji **rizik** od neovlašćenog pristupa sistemu (softveru i bazama podataka), čime se narušava bezbjednost informacionog sistema.

Fondu PIO **preporučeno je** da u potpunosti poštuje pravila i procedure koje je usvojio, a koja se odnose na ažuriranje zatvaranja korisničkih naloga.

Utvrđeno činjenično stanje za preporuku br. 2:

U skladu sa preporukom koja je data, Fond PIO je, kako je navedeno u Planu aktivnosti za realizaciju preporuka, imenovao službenika iz Odsjeka za ljudske resurse, koji je zadužen da obavještava Sektor za informacione tehnologije o svakoj promjeni koja se tiče radnog statusa

zaposlenih. Za sve zaposlene kojima je između dvije revizije prestao radni odnos, iz Odsjeka za ljudske resurse su dostavljena obavještenja Sektoru za informacione tehnologije (elektronska pošta pomoćniku direktora Sektora za informacione tehnlogije od 19.12.2017. godine i od 15.01.2018. godine, dopisi pomoćniku direktora Sektora za informacione tehnlogije od 24.12.2018. godine i od 20.02.2019. godine, svi se odnose na po jednog službenika). Izvršen je uvid u informacioni sistem i utvrđeno je da su nalozi za ova četiri službenika neaktivni.

Kontrolnom revizijom je utvrđeno da se zatvaranje korisničkih naloga vrši **ažurno**.

Preporuka je realizovana.

Preporuka broj 3

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond PIO nije vršio procjenu efikasnosti mjera fizičke zaštite shodno članu 9 Uredbe o mjerama informacione bezbjednosti ("Službeni list Crne Gore", br. 058/10 od 08.10.2010, 055/15 od 30.09.2015), s obzirom da je Plan fizičke zaštite iz maja 2017. godine (br. 04-1374 od 19.05.2017. godine).

Nevršenje procjene efikasnosti mjera fizičke zaštite prostora u kojem se nalaze serveri, mrežna i komunikaciona oprema dovodi do **rizika** po bezbjednost informacionog sistema Fonda PIO.

Fondu PIO **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, s obzirom da je Plan fizičke zaštite od 19.05.2017. godine.

Utvrđeno činjenično stanje za preporuku br. 3:

U skladu sa preporukom koja je data, kako je navedeno u Planu aktivnosti za realizaciju preporuka i Izvještaju nakon obavještenja o vršenju kontrolne revizije, Fond PIO je formirao Komisiju koja je izvršila procjenu efikasnosti mjera fizičke zaštite i sačinila Izvještaj (br. 01-618/2 od 28.03.2018. godine).

Kontrolnom revizijom utvrđeno je da je direktor Fonda PIO donio Rješenje o imenovanju Komisije za procjenu efikasnosti mjera fizičke zaštite (br. 01-618 od 22.02.2018. godine) koja ima zadatak da postupi po preporukama Državne revizorske institucije i izvrši procjenu mjera fizičke zaštite u skladu sa članom 9 Uredbe o mjerama informacione bezbjednosti, da do 01.04.2018. godine, a po izvršenoj provjeri, sačini zapisnik u kojem će konstatovati postojeće stanje, kao i da najmanje jednom godišnje vrši navedenu procjenu. Komisija je izradila Izvještaj, kojim je navedeno u Izvještaju o reviziji Fonda penzijskog i invalidskog osiguranja Crne Gore konstatovala i preporučila da se u cilju efikasnijeg sprovođenja plana fizičke zaštite vodi evidencija ulazaka neovlašćenih lica uz navođenje razloga ulaska u administrativnu zonu.

U postupku kontrolne revizije održan je sastanak sa Komisijom za procjenu efikasnosti mjera fizičke zaštite na kojem je utvrđeno da Komisija nema prateća dokumenta u vezi izrade Izvještaja, kao i da nije bilo bezbjedonosnih incidenata iznutra i da nije bilo narušavanja fizičke bezbjednosti spolja, pa da ne postoje izvještaji o tome; zatim da nije bilo kadrovskih promjena

pa ni potrebe za ažuriranjem spiskova lica ovlašćenih za pristup zoni A (Prilog 3 dokumenta Korišćenje i sigurnost računarskog sistema Fonda PIO) i zoni B (Prilog 4 istog dokumenta). Nema izmjena lokacija na kojima se čuvaju uskladišteni podaci, kao ni izmjene u vezi kriptovanja podataka u prenosu kroz sistem. Takođe, nije vršeno testiranje fizičke zaštite servera i ne postoje izvještaji o periodičnom fizičkom testiranju. Što se tiče provjere koja se odnosi na skladištenje podataka, ona se vrši mjesečno sinhronizacijom podataka, kada se vrši testiranje isplate penzija, a za to je zadužen glavni voditelj projekta. Odnedavno je uvedena dupla sinhronizacija sistema, radi ažuriranja podataka na sistemu za izvještavanje. O testiranju ispravnosti kopije podataka su elektronskom poštom dostavljeni izvještaji službenika zaduženog za ove poslove, od 06.03.2018. godine, 01.10.2018. godine i 27.03.2019. godine, kojima informiše pomoćnika direktora Sektora za informacione tehnlogije o izvršenim testiranjima, što je u skladu sa članom 20 Uredbe o mjerama informacione bezbjednosti.

Osim toga, direktor Fonda PIO je donio Rješenje o imenovanju Komisije za procjenu efikasnosti mjera fizičke zaštite (br. 01-30 od 11.01.2019. godine), u istom sastavu, radi vršenja povjerenog zadatka kontinuirano, najmanje jednom godišnje. Komisija je izradila Izvještaj (br. 01-30/12 od 15.04.2019. godine) u kome navodi da je ustanovila i izvršila provjeru mjera informacione bezbjednosti. Dostavljena je i prateća dokumentacija na osnovu koje je sačinjen Izvještaj:

- Zapisnik sa sastanka komisije za procjenu efikasnosti mjera fizičke zaštite održanog 25.03.2019. godine (br. 01-30/8 od 11.04.2019. godine), u kojem je konstatovano da pitanja u vezi procjene, navedeno je 11 pitanja, treba uputiti pomoćniku direktora Sektora za informacione tehnologije, te da će neposrednu kontrolu i provjeru izvršiti dva člana Komisije;
- Dopis Komisije pomoćniku direktora Sektora za informacione tehnologije sa 10 pitanja (br. 0502-30/9 od 11.04.2019. godine);
- Odgovor pomoćnika direktora Sektora za informacione tehnologije (br. 04-30/10 od 12.04.2019. godine);
- Dopis Komisije pomoćniku direktora Sektora za informacione tehnologije (br. 0502-30/7 od 11.04.2019. godine), za omogućavanje ulaska članova Komisije u administrativne zone radi provjere faktičkog stanja (predsjedavajući Komisije je lice koje je ovlašćeno za ulazak u zone A i B, dok članovi Komisije nisu ovlašćeni);
- Zapisnik Komisije o provjeri faktičkog stanja (br. 01-30/11 od 1215.04.2019. godine);
- Evidencija ulazaka lica koja nisu na listi ovlašćenih lica za pristup zoni A, sa 11 registrovanih ulazaka u periodu februar 2018 – april 2019. godine;
- Evidencija ulazaka lica koja nisu na listi ovlašćenih lica za pristup zoni B, sa devet (9) registrovanih ulazaka u periodu septembar 2018 – april 2019. godine;
- Lista ovlašćenih lica za pristup zoni A (br. 04-95 od 19.01.2017. godine);
- Lista ovlašćenih lica za pristup zoni B (br. 04-101 od 19.01.2017. godine);
- Plan fizičke zaštite (br. 04-1374 od 19.05.2017. godine).

Kontrolnom revizijom je utvrđeno da Fond PIO 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, **u skladu** sa članom 9 Uredbe o mjerama informacione bezbjednosti.

Preporuka je realizovana.

Preporuka broj 4

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond PIO nema uspostavljena bezbjedonosna pravila u skladu sa članom 32 Uredbe o mjerama informacione bezbjednosti, radi obezbjeđivanja informacione bezbjednosti podataka kojima zaposleni imaju pristup, odnosno kako postupaju sa njima. Bezbjedonosna pravila podrazumjevaju interna pravila za zaposlene i edukaciju i stručno usavršavanje zaposlenih. Zaposleni u Fondu PIO u ugovorima nemaju klauzulu o povjerljivosti.

Ne uspostavljanjem bezbjedonosnih pravila za zaposlene mogu nastati operativni **rizici** poslovanja Fonda PIO koji se tiču neovlašćenog pristupa podacima i zloupotrebe podataka, što za posledicu može imati uništavanje podataka ili narušavanje ispravnog rada cijelog informacionog sistema Fonda PIO.

Fondu PIO **preporučeno je** da u skladu sa članom 32 Uredbe o mjerama informacione bezbjednosti uspostavi bezbjednosna pravila i edukaciju zaposlenih radi obezbjeđivanja informacione bezbjednosti podataka kojima ta lica imaju pristup, odnosno koja postupaju sa njima.

Utvrđeno činjenično stanje za preporuku br. 4:

U skladu sa preporukom koja je data, kako je navedeno u Planu aktivnosti za realizaciju preporuka i Izvještaju nakon obavještenja o vršenju kontrolne revizije, Fond PIO je u cilju edukacije zaposlenih, sačinio (novembar 2017. godine), a zatim i inovirao (mart 2019. godine) dokument Prava i obaveze korisnika IT sistema Fonda PIO, u kojem su opisana bezbjedonosna pravila kao i obaveze kojih se zaposleni moraju pridržavati u radu sa sistemom. U okviru dokumenta se nalazi Potvrda o preuzimanju prava i obaveza korisnika IT sistema Fonda i klauzule o povjerljivosti, koju su potpisali svi zaposleni.

Kontrolnom revizijom je utvrđeno da je ovaj dokument preko rukovodilaca organizacionih jedinica Fonda dostavljen svim zaposlenima na upoznavanje, koji su se na taj način edukovali u smislu bezbjedonosnih pravila. Kontrolom izabranog uzorka utvrđeno je da su zaposleni potpisali Potvrdu o upoznavanju sa dokumentom prava i obaveze korisnika IT sistema Fonda i klauzula o povjerljivosti, te da se ona čuva u Sektoru za informacione tehnologije. Fondu je u postupku revizije sugerisano da je potrebno da sve potvrde imaju djelovodni broj, pa je uvedena nova procedura kojom se potpisane potvrde o preuzimanju prava i obaveza korisnika IT sistema Fonda i klauzule o povjerljivosti, dostavljaju Sektoru za opšte i pravne poslove, koje će se ovjeravati i biti stavljane u personalne dosijee zaposlenih.

Kontrolnom revizijom je utvrđeno da je Fond PIO uspostavio bezbjednosna pravila i edukaciju zaposlenih radi obezbjeđivanja informacione bezbjednosti podataka kojima ta lica imaju pristup, odnosno koja postupaju sa njima, **u skladu** sa članom 32 Uredbe o mjerama informacione bezbjednosti.

Preporuka je realizovana.

Preporuka broj 5

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da u Fondu PIO ne postoji plan za oporavak od katastrofe (Disaster Recovery).

Postoji **rizik** od potencijalnog negativnog uticaja u slučaju prirodnih katastrofa i sl. koji mogu dovesti do većeg incidenta na informacionom sistemu i podacima, čime bi bili ugroženi poslovni procesi i osnovna funkcija Fonda PIO.

Fondu PIO **preporučeno je** da završi projekat Disaster Recovery u Bijelom Polju, za kritične servise s obzirom da je Disaster Recovery Data centar u funkciji[2].

Utvrđeno činjenično stanje za preporuku br. 5:

U skladu sa preporukom koja je data, kako je navedeno u Planu aktivnosti za realizaciju preporuka i Izvještaju nakon obavještenja o vršenju kontrolne revizije, Fond PIO će projekat Disaster Recovery u Bijelom Polju završiti u sklopu modernizacije IT sistema Fonda, za koju su za 2019. godinu obezbijeđena budžetska sredstva.

Disaster Recovery tj. oporavak od katastrofe, čine procesi, politike i procedure povezane sa pripremom za oporavak ili obnovu tehnološke infrastrukture od kritične važnosti nakon havarije. Kontrolnom revizijom je utvrđeno da je IT strategijom 2018-2022 planirano da se Plan oporavka od katastrofe u potpunosti realizuje do januara 2021. godine.

Realizacija preporuke je planirana i oročen termin realizacije, odnosno obezbjeđenja plana oporavka od katastrofe.

Preporuka broj 6

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da Fond PIO nije vršio preispitivanje procjene rizika. Naime, u toku vršenja prethodne revizije Fond je kreirao Plan aktivnosti (br. 04-1375, od 19.05.2017. godine) u kojem su detaljno opisani i navedeni rizici koji bi mogli uticati na rad informacionog sistema Fonda PIO i dovesti do eventualne nedostupnosti sistema, što je u skladu sa članom 38 Uredbe o mjerama informacione bezbjednosti. S obzirom da se rizik može prihvatiti ukoliko bi nastala šteta bila manja od štete koja bi nastala usled nesprovođenja određene aktivnosti, radi se na smanjivanju rizika sprovođenjem i primjenom mjera definisanih u Planu aktivnosti.

Nevršenjem preispitivanja procjene **rizika**, mogu nastati negativni efekti na poslovanje, finansijsko stanje i ostvarivanje poslovnih ciljeva.

Fondu PIO **preporučeno je** da se rezultati analize rizika redovno preispituju, saglasno potrebama Fonda PIO, uslovljeni unutrašnjim ili vanjskim potrebama u skladu sa članom 39 Uredbe o mjerama informacione bezbjednosti.

[2] Disaster Recovery Data centar u Bijelom Polju je projekat realizovan na osnovu Strategije za obezbjeđenje podataka u slučaju katastrofe za potrebe državnih organa i organa uprave u Crnoj Gori (Strategije implementacije Disaster Recovery-ja) u cilju smanjenja rizika od potencijalnih negativnih uticaja u slučaju prirodnih katastrofa, seizmičkih pomjeranja i drugih uticaja koji bi doveli do gubitka podataka smještenih na centralnoj lokaciji.

Utvrđeno činjenično stanje za preporuku br. 6:

U skladu sa preporukom koja je data, kako je navedeno u Planu aktivnosti za realizaciju preporuka i Izvještaju nakon obavještenja o vršenju kontrolne revizije, Fond PIO je formirao Komisiju koja je izvršila preispitivanje procjene i analizu rizika u skladu sa članom 39 Uredbe o mjerama informacione bezbjednosti i sačinila Zapisnik (br. 01-617/2 od 30.03.2018. godine).

Kontrolnom revizijom je utvrđeno da je direktor Fonda PIO donio Rješenje o imenovanju Komisije za upravljanje rizikom informacione bezbjednosti (br. 01-617 od 22.02.2018. godine) koja ima zadatak da postupi po preporukama Državne revizorske institucije i izvrši preispitivanje procjene rizika informacione bezbjednosti u skladu sa članom 39 Uredbe o mjerama informacione bezbjednosti; da do 01.04.2018. godine, a po izvršenoj provjeri sačini zapisnik u kojem će konstatovati postojeće stanje; kao i da redovno vrši preispitivanje analize rizika. Komisija je izradila Zapisnik u kojem je konstatovala da Plan aktivnosti u momentu preispitivanja ispunjava svoju funkciju preduzimanja organizacionih i drugih neophodnih mjera u cilju izbjegavanja radnji koje bi mogle izazvati rizik, kao i sprovođenja aktivnosti nakon nastanka rizika. Komisija je takođe ustanovila da rizici koji su navedeni u Planu aktivnosti i dalje postoje i da se nisu desili novi događaji koji bi doveli do novih rizika.

U postupku kontrolne revizije održan je sastanak sa Komisijom za upravljanje rizikom informacione bezbjednosti na kojem je utvrđeno da Komisija nema prateća dokumenta u vezi izrade Zapisnika. Što se tiče nestanka električne energije nisu vršili testiranja s obzirom da se (često) dešava da dođe do njenog nestanka, pa na taj način utvrđuju da UPS-ovi rade. O ovim incidentima ne pišu izvještaje, a nisu vršili ni testiranja ispada električne energije koji su duži od 8 sati. Protivpožarni aparati i klima uređaji se redovno servisiraju.

Takođe, direktor Fonda PIO je donio Rješenje o imenovanju Komisije za upravljanje rizikom informacione bezbjednosti (br. 01-30/2 od 11.01.2019. godine), u istom sastavu, radi kontinuiranog vršenja povjerenog zadatka. Komisija je izradila Izvještaj (br. 01-30/3 od 29.03.2019. godine) u kojem je za svaki rizik iz Plana aktivnosti utvrdila trenutno stanje i navela osam aktivnosti (preporuka) za njihovo poboljšanje:

1. Potrebno je zaljučiti ugovor o održavanju velikog UPS-a APC MGE Galaxy 5000 sa ovlašćenim serviserom čime bi bilo pokriveno njegovo servisiranje u skladu sa preporukama proizvođača.
2. Potrebno je zaključiti ugovor o održavanju novog agregata sa ovlašćenim serviserom nakon isteka garantnog roka.
3. Preporučuje se čuvanje i skladištenje arhivske građe u skladu sa Uredbom o načinu i čuvanju javne registrature i arhivske građe (“Sl. list Crne Gore” br. 03/14).
4. Potrebno je zaključiti ugovor o održavanju Sistema za dojavu požara sa ovlašćenim serviserom.
5. Preporučuje se da se izvrši instalacija obezbijeđenog klima-uređaja prije početka ljeta.
6. Preporučujemo se da na udaljenoj lokaciji, osim godišnjeg full bekapa, čuva i mjesečni bekap (mjesečni full bekap).

7. Postojeći Plan aktivnosti potrebno je tabelarno prikazati sa svim ključnim elementima za upravljanje rizikom u skladu sa Smjernicama za uspostavljanje i sprovođenje procesa upravljanja rizicima u subjektima javnog sektora izdatim od strane Ministarstva finansija decembra 2018. godine.
8. Potrebno je da se svaki incident evidentira u pisanoj formi.

Dostavljena je prateća dokumentacija na osnovu koje je sačinjen Izvještaj, koju čine Plan aktivnosti, Mišljenje komisije za upravljanje rizkom informacione bezbjednosti sa akcionim planom u kom su navedene četiri aktivnosti (br. 01-617/3 od 30.03.2018. godine), Zapisnik sa sastanka Komisije i pomoćnika direktora za IT od 26.03.2019. godine.

Dostavljena je i dokumentacija kojom se potvrđuje provjera svih navoda u Izvještaju:

- račun za uslugu serisiranja protivpožarnih (PP) aparata od 12.06.2018. godine;
- račun za usluge PP preventive za servisiranje sistema za dojavu požara i servis protivprovalne centrale (od 15.06.2018. godine) sa zapisnicima od 07.06.2018. godine i od 08.06.2018. godine;
- računi za čišćenje klima uređaja od 10.05.2018. godine i 12.06.2018. godine;
- komunikacija člana Komisije sa službenikom koji je nadležan za praćenje rada antivirus servera elektronskom poštom od 29.03.2019. godine, sa informacijom o stanju antivirus servera i računom-potvrdom o nabavljenoj licenci za antivirus softver od 22.03.2019. godine;
- komunikacija člana Komisije sa službenikom koji je nadležan za hardversku infrastrukturu elektronskom poštom od 28.03.2019. godine sa informacijom o otkazivanju pojedinih hard diskova, dopisom pomoćnika direktora Sektora za informacione tehnologije upućenog direktoru Fonda PIO o potrebi hitne nabavke (br. 04-2850 od 18.09.2018. godine) i računima za nabavke hard diskova od 07.08.2018. godine, 18.09.2018. godine, 25.09.2018. godine i 13.11.2018. godine;
- komunikacija člana Komisije sa službenikom koji je nadležan za izvršavanje Procedure za skladištenje podataka elektronskom poštom od 29.03.2019. godine, u vidu izvještaja.

Osim toga, Komisija je putem neposrednog intervjua sa koordinatorom za rizike utvrdila da je, po pitanju uspostavljanja registra rizika u Fondu PIO, u skladu sa članom 13 stav 1 Zakona o sistemu unutrašnjih finansijskih kontrola u javnom sektoru ("Sl. list Crne Gore" br. 73/08, 20/11, 30/12 i 34/14), donesena: Odluka o uspostavljanju registra rizika broj 01-2743/3 od 17.10.2016. godine na nivou Fonda kao cjeline, Rješenje o imenovanju lica zaduženog za koordinaciju uspostavljanja i sprovođenja procesa upravljanja rizicima broj 01-2743/2 od 17.10.2016. godine, kao i odluke o uspostavljanju registra rizika po organizacionim jedinicama na nivou Sektora broj 01-2889 od 07.11.2016. godine; da su tri predstavnika Fonda PIO prisustvovala Seminaru na temu "Upravljanje rizicima u javnom sektoru" u organizaciji Centralne jedinice za harmonizaciju pri Ministarstvu finansija Crne Gore, te da druga dokumenta koja se bave pitanjem registra rizika još uvijek nijesu donesena.

Komisija je takođe konstatovala da Plan aktivnosti u momentu preispitivanja ispunjava svoju funkciju preduzimanja organizacionih i drugih neophodnih mjera u cilju izbjegavanja radnji koje bi mogle izazvati rizik, kao i sprovođenja aktivnosti nakon nastanka rizika. Komisija je takođe ustanovila da rizici koji su navedeni u Planu aktivnosti i dalje postoje i da se nisu desili novi događaji koji bi doveli do novih rizika.

Kontrolnom revizijom je utvrđeno da Fond PIO rezultate analize rizika redovno preispituje, saglasno svojim potrebama, uslovljeno unutrašnjim ili vanjskim potrebama, **u skladu** sa članom 39 Uredbe o mjerama informacione bezbjednosti.

Preporuka je realizovana.

Preporuka broj 7

Prethodnom revizijom izvršenom od strane DRI **utvrđeno je** da u Fondu PIO ne postoji pisana procedura za postupanje na osnovu Izvještaja o preminulima koji se dobija sinhronizacijom baze podataka Fonda PIO i Centralnog registra stanovništva (CRS), kojom bi bili precizno definisani postupci i vremenski rokovi. Rješenje o prestanku prava donosi se u Sektoru za penzijsko i invalidsko osiguranje u područnoj jedinici koja je odgovorna za taj predmet, a obustavu prava vrši Odsjek za obračun i isplatu, na osnovu dostavljenog rješenja područne jedinice.

Postojećom međusektorskom komunikacijom dolazi do **propusta** u donošenju rješenja o prestanku prava na penziju i obustavi isplate prava na istu.

Fondu PIO **preporučeno je** da donese proceduru za postupanje po izvještajima o preminulima dobijenim iz CRS-a, kojom bi bili precizno definisani vremenski rokovi za kontrolu lica koja su preminula dosta davno, a konstanto se pojavljuju u mjesečnim izvještajima o preminulima dobijenim iz CRS-a.

Utvrđeno činjenično stanje za preporuku br. 7:

U skladu sa preporukom koja je data, Fond PIO je u Izvještaju o realizaciji preporuka izvijestio DRI da je donio Proceduru za postupanje sa podacima o činjenici smrti korisnika prava iz penzijskog i invalidskog osiguranja (br. 01-1057 od 13.04.2018. godine).

Kontrolnom revizijom utvrđeno je da je Fond PIO **donio** Proceduru za postupanje sa podacima o činjenici smrti korisnika prava iz penzijskog i invalidskog osiguranja kojom se uređuje postupanje sa podacima o činjenici smrti korisnika prava iz penzijskog i invalidskog osiguranja, koji se dobijaju sinhronizacijom baze podataka Fonda PIO i CRS-a, kao i definisanje rokova za postupanje po istim.

- Ovlašćeno lice Sektora za informacione tehnologije, svakog mjeseca, nakon obračuna prava iz penzijskog i invalidskog osiguranja, pokreće računarsku proceduru ka CRS-a, za sve korisnike koji se isplaćuju na teritoriji Crne Gore. Procedura će poslati upit ka CRS-a po JMBG za svakog navedenog korisnika prava. Odgovor od CRS se smješta u bazu podataka Fonda PIO, na osnovu kojih se generiše izvještaj: Spisak korisnika koji imaju isplatu po osnovu prava iz penzijskog i invalidskog osiguranja sa podacima o činjenici smrti.
- Izvještaj se do 23. u mjesecu dostavlja pomoćniku direktora Sektora za sprovođenje osiguranja na dalju nadležnost.
- Pomoćnik direktora Sektora za sprovođenje osiguranja, izvještaje sa podacima o činjenici smrti, odmah prosleđuje putem elektronske pošte načelnicima Područnih jedinica Fonda PIO na dalje postupanje.
- Načelnici područnih jedinica, u okviru svoje mjesne nadležnosti, vrše uvid u spise predmeta i provjeravaju, da li se u istim nalaze dokazi o činjenici smrti za lica, za koja u navedenim izvještajima postoji podatak o činjenici smrti, kao i da li je već donijeto rješenje o prestanku prava iz penzijskog i invalidskog osiguranja usled smrti.
- Za korisnike prava iz penzijskog invalidskog osiguranja, za koje se utvrdi da u spisima predmeta ne postoji izvod iz matičnog registra umrlih, načelnici područnih jedinica odmah upućuju MUP-a CG, Područnoj jedinici za građanska stanja i lične isprave, zahtjev za dostavljanje izvoda iz knjige umrlih.

- U područnoj jedinici se pokreće postupak po službenoj dužnosti i donosi rješenje o prestanku prava iz penzijskog i invalidskog osiguranja, nakon dostavljanja izvoda iz matične knjige umrlih od strane MUP-a. Rješenje se odmah dostavlja Odsjeku za obračun i isplatu prava na realizaciju.
- U slučaju kada MUP na dostavi izvod iz matičnog registra umrlih, područna jedinica, u roku od **15 dana** od dana dostavljanja izvještaja sa podacima o činjenici smrti, donosi rješenje o obustavi isplate prava iz penzijskog i invalidskog osiguranja, i rješenje odmah dostavlja Odsjeku za obračun i isplatu prava, na realizaciju, a istovremeno se upućuje urgencija MUP-a, za dostavljanje izvoda iz matičnog registra umrlih, radi donošenja rješenja o prestanku prava iz penzijskog i invalidskog osiguranja.

Na osnovu dostavljenih Izvještaja sa podacima o činjenici smrti za 2018. godinu i 2019. godinu, izabranim uzorkom utvrđeno je da **nema nepravilnosti od kad je usvojena pomenuta procedura.**

U prethodnom periodu nije bilo tehničkih problema u pogledu konekcije sa CRS-om, koji bi uslovili kašnjenje u dostavljanju izvještaja.

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 Milan Dabović (predsjednik Senata – član Kolegijuma), na sjednici održanoj 24. maja 2019. godine, usvojio je:

KONAČNI IZVJEŠTAJ
o kontrolnoj reviziji informacionog sistema
Fonda penzijskog i invalidskog osiguranja Crne Gore

ZAKLJUČAK

Aktivnostima i radnjama koje je Fond penzijskog i invalidskog osiguranja Crne Gore preduzeo i cilju realizacija preporuka DRI **otklonjen je najveći dio nedostataka**, odnosno od ukupno **sedam (7)** izdatih preporuka DRI, koje su bile predmet kontrolne revizije:

- **realizovano je** **6** preporuka
- **započeta realizacija** **1** preporuka.

Preporuka koja nije još realizovana odnosi se na oporavak od katastrofe (Disaster Recovery). Državni revizori su konstatovali da je učinjeno znatno poboljšanje u odnosu na prethodnu reviziju.

Subjekat revizije dužan je u roku od dvije (2) godine izvjestiti DRI o realizaciji započete preporuke, koju je neophodno u potpunosti realizovati, s obzirom na njen značaj i rok do kojeg je IT strategijom Fonda PIO planirano da se realizuje Disaster Recovery rješenje.

Rukovodilac Kolegijuma

Radule Žurić
Član Senata DRI