Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

IZVEŠTAJA O REVIZIJI INFORMACIONE TEHNOLOGIJE

Elektronski sistem javnih nabavki e-nabavke

Priština, avgust 2023

Nacionalna Kancelarija Revizije Republike Kosova je najviša institucija ekonomske i finansijske kontrole i o njenom radu odgovara Skupštini Republike Kosova.

Naša misija je da preko kvalitetnih revizija jačamo polaganje odgovornosti u javnoj upravi za efektivno, efikasno i ekonomično korišćenje nacionalnih resursa. Izveštaji Nacionalne Kancelarije Revizije na direktan način promovišu polaganje odgovornosti javnih institucija pošto oni pružaju održivu osnovu za zahtevanje odgovornosti od strane menadžera svake budžetske organizacije. Tako mi povećavamo poverenje u trošenju javnih fondova i odigravamo aktivnu ulogu u obezbeđivanju interesa poreskih platiša i ostalih interesnih strana u povećanju javne odgovornosti.

Ova revizija je izvršena u skladu sa Međunarodnim standardima vrhovnih revizorskih institucija (MSVRI 30001[1]) i sa Vodičem o reviziji informacionih sistema (GUID 51002[2]) kao i sa evropskim dobrim praksama.

Revizije informacionih tehnologija preduzete od Nacionalne kancelarije revizije su ispitivanje i pregled sistema Informacione tehnologije i odgovarajućim kontrolama da bi imalo bezbednost o principima zakonitosti, efikasnosti[3],ekonomičnosti[4],i efektivnosti[5], sistema Informacione tehnologije i odgovarajućih kontrola.

Generalna Revizorka je odlučila o sadržaju ovog Nacrta izveštaja revizije učinka „ Elektronski sistem javnih nabavki e-nabavke", u konsultaciji sa Pomoćnicom generalne revizorke, Myrvete Gashi Morina, koja je nadgledala reviziju.

Tim koji je realizovao ovaj izveštaj:

Samir Zymberi, Direktor odeljenja revizije

Arbërore Sheremeti, Vođa tima

Saranda Husaj Baraliu, Član tima

Gazmend Lushtaku, Član tima

[1] MSVRI 3000 - Standardi i uputstva o reviziji učinka zasnovane na Standardima revizije MOVRI-a i praktičnom iskustvu.

[2] GUID 5100 - Vodič o reviziji informacionih sistema izdat od INTOSAI

[3] Efikasnost - Princip efikasnosti podrazumeva postizanje maksimuma od raspoloživih resursa. To se odnosi na vezu između angažovanih resursa i datih rezultata u smislu kvantiteta, kvaliteta i vremena.

[4] Ekonomičnost - princip ekonomičnosti podrazumeva minimiziranje troškova resursa. Korišćeni resursi trebaju biti raspoloživi na vreme, u pravoj količini i kvalitetu i sa najpovoljnijom cenom.

[5] Efektivnost - Princip efektivnosti podrazumeva postizanje unapred određene ciljeve i postizanje očekivanih rezultata.

SADRŽAJ

Opšti pregled 4
1 Uvod 6
2 Cilj i oblasti revizije 8
3 Nalazi revizije 9
3.1 Upravljanje, rad i podugovaranje e-nabavke 10
3.2 Kontrole unosa i bezbednost „e-nabavke“. 14
4 Zaključci 20
5 Preporuke 21
Prilog I. Dizajn revizije 23
Rizične oblasti i pokazatelji problema revizije 23
Opis sistema 24
Uloga i odgovornosti za elektronski sistem e-nabavke 24
Kriterijumi revizije 26
Metodologija revizije 28
Relevantni dokumenti 28
Prilog II. Potvrdno pismo entiteta 29

Spisak skraćenica

UO	Ugovorni organ
CAN	Centralna agencija za nabavke
ARBK	Agencija za registraciju biznisa
ACR	Agencija za civilnu registraciju
PAK	Poreska administracija Kosova
LJR	Ljudski resursi
BDP	Bruto domaći proizvod (u Izveštaju o napretku za Kosovo)
CBK	Centralna banka Kosova
BRK	Budžet Republike Kosovo
RKJN	Regulatorna komisija za javne nabavke
MFRT	Ministarstvo finansija, rada i transfera
MUP	Ministarstvo unutrašnjih poslova
BO	Budžetske organizacije
EO	Ekonomski operater
PEFA	Public Expenditure and Financial Accountability (javni rashodi i finansijska odgovornost)
PIP	Sistem javnih investicija
RKS	Republika Kosovo
SIMFK	Informacioni sistem za finansijsko upravljanje Kosova
IT	Informaciona tehnologija
NKR	Nacionalna kancelarija za reviziju

Opšti pregled

Razvoj sistema javnih nabavki je jedan od strateških prioriteta Vlade Republike Kosovo kao deo nacionalnih strukturnih reformi i u okviru reforme javne uprave. Upotreba informacionih tehnologija za javni sektor, a posebno za sistem nabavki, jeste pokretački element za povećanje efikasnosti i efektivnosti tokom implementacije Zakona o nabavkama. Regulatorna komisija za javne nabavke je odgovorna za razvoj, rad i opšti nadzor sistema javnih nabavki na Kosovu, uključujući elektronski informacioni sistem "e-nabavke".

Uzimajući u obzir značaj ovog sistema, Nacionalna kancelarija za reviziju je izvršila reviziju informacionih tehnologija, kako bi ocenila da li je Regulatorna komisija za javne nabavke efikasno upravljala IT poslovima, kako bi se obezbedilo da elektronski sistem „e-nabavke“ kontinuirano podržava proces javnih nabavki i održava njegov integritet.

Rezultati revizije pokazuju da je elektronski sistem e-nabavki pomogao povećanju efikasnosti, efektivnosti i transparentnosti razvoja aktivnosti javnih nabavki. Međutim, uočeni su nedostaci u procesima informacionih tehnologija koji utiču na kontinuirano očuvanje stabilnosti i integriteta ovog sistema.

Upravljanje, rad i podugovaranje e-nabavke treba poboljšati[6]**.** RKJN nema dovoljno IT profesionalnih ljudskih resursa i ne postoji odgovarajuća podela dužnosti postojećih IT službenika. Kao rezultat toga, obavljanje ključnih zadataka za funkciju sistema obavljaju eksterni ekonomski operateri, rizikujući stvaranje zavisnosti od trećih strana. Takođe, ne postoji elektronski registar/sistem problema i incidenata koji se dešavaju, kako bi se kategorizovali i identifikovali najčešći problemi i mogućnost njihovog tretmana.

Uočeni nedostaci u upravljanju i IT poslovanju mogu dovesti u opasnost da ova institucija ne bude u mogućnosti da realizuje sve zakonom definisane zadatke, odgovornosti i ciljeve, čime bi se ugrozio kontinuitet rada ovog sistema.

Potreban je dalji razvoj kontrola unosa i bezbednosti e-nabavke[7]**.** U modulima sistema e-nabavke nisu uspostavljene potrebne kontrole ili ograničenja, kao ni veze sa osnovnim sistemima Republike Kosovo, kako bi se sprečila obrada netačnih podataka, a posebno podataka korisnika.

Politika bezbednosti informacija nije bila potpuna u pogledu elektronskog upravljanja računima. Nevažeći ili fiktivni nalozi nisu identificirani za deaktiviranje ili zatvaranje, dok su lozinke retko menjali korisnici. Takođe, umesto službenih e-mail, korisnici su koristili privatne e-mail, a osim toga, isti e-mail je korišćen za otvaranje više naloga, izlažući akreditive korisnika drugim ljudima. Oko 50% korisnika nije poštovalo uslove korišćenja sistema elektronskih nabavki, kao ni administrativna uputstva za službene elektronske račune.

[6] Detaljni nedostaci su predstavljeni u Poglavlju 3-3.1 Upravljanje, rad i podugovaranje „e-nabavke“; strana 11

[7] Detaljni nedostaci su predstavljeni u Poglavlju 3-3.2 Kontrole unosa i bezbednost "e-nabavke"; strana 16

Pored toga, elektronski računi i aktivnosti koje se obavljaju sa ovih naloga nisu praćene ni od strane ugovornih organa koji imaju obavezu održavanja svojih korisnika, niti od strane RKJN kao vlasnika ove platforme.

Nepotrebno otvaranje korisnika, nedostatak zatvaranja pasivnih korisnika kao i nedostatak praćenja korisničkih naloga, između ostalog, slabi performanse platforme e-nabavke, povećava rizik od pretnji bezbednosti informacija, kao i povećava mogućnost zloupotrebe naloga za aktivnosti van pravila javnih nabavki.

Stoga smo dali 13 preporuka Regulatornoj komisiji za javne nabavke (u saradnji sa relevantnim institucijama Republike Kosovo), u cilju rešavanja pitanja vezanih za kontinuiranu podršku procesa javnih nabavki kao i održavanje integriteta ovog sistema. Lista preporuka je predstavljena u Poglavlju 5 ovog izveštaja.

Odgovor entiteta

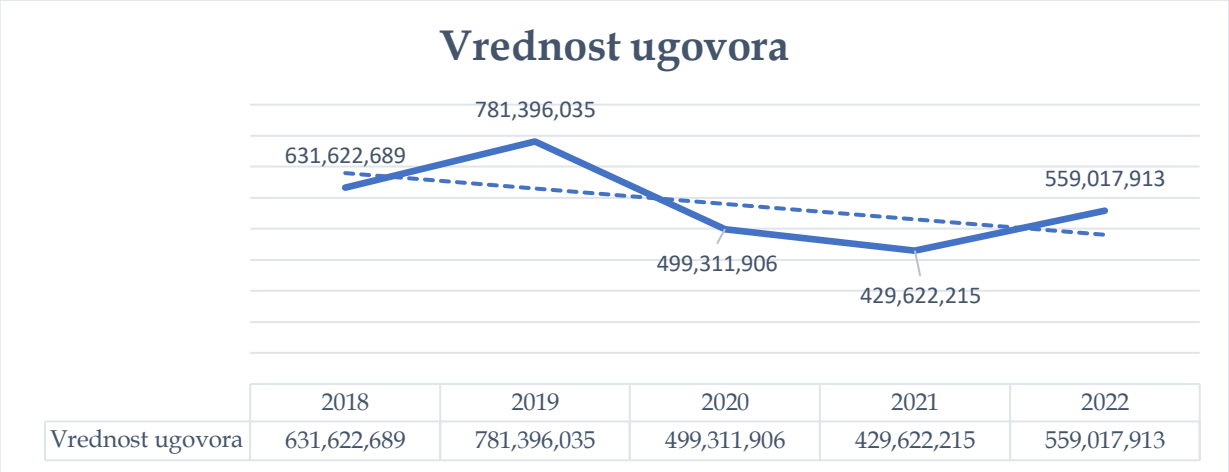
Regulatorna Komisija za Javne Nabavke se saglasila sa nalazima i zaključcima revizije i obavezala se da će adresirati date preporuke.

1 Uvod

Javne nabavke[8] su ključni aspekt u javnoj upravi, koji je vezan za sistem javnih finansija i ima društvene i ekonomske rezultate. Kao takav, to je ključna determinanta efektivnosti vlade i kvaliteta javnih usluga i infrastrukture. Dakle, javne nabavke se odnose na to kako javne vlasti troše javni novac, kada kupuju robu, radove ili usluge na tržištu [9].

Značajan deo državnog budžeta se troši kroz aktivnosti javnih nabavki. Tržište javnih nabavki na Kosovu tokom 2021. godine je procenjeno na 5,65% bruto domaćeg proizvoda (BDP), [10]dok je u 2022. godini procenjeno na 6,50% BDP-a [11]. Tokom 2022. godine potpisano je 10.290 javnih ugovora u vrednosti od 559.017.913 eura [12].

*Slika 1 **Vrednost** potpisanih javnih ugovora 2018-2022 2*



	2018	2019	2020	2021	2022
Vrednost ugovora	631,622,689	781,396,035	499,311,906	429,622,215	559,017,913

Glavni izvor finansiranja za 2021. za javne tendere je bio iz budžeta Kosova sa oko 80%, iz sopstvenih prihoda sa blizu 19% i 0,4% je finansirano iz donacija [13].

Funkcionisanje sistema javnih nabavki predstavlja suštinsko pitanje upravljanja javnim finansijama za javnu administraciju na Kosovu. Pravi sistem javnih nabavki omogućava najefikasnije i razumno korišćenje javnih sredstava, omogućavajući značajne uštede u Konsolidovanom budžetu Kosova, kao i značajno doprinoseći borbi protiv korupcije, zloupotreba i istovremeno ekonomskom razvoju Kosova. Stoga je Vlada Kosova u martu 2016. godine odlučila da se elektronska nabavka primenjuje na centralizovane nabavke, dok je od januara 2017. godine elektronska nabavka postala obavezna za sve budžetske organizacije [14].

[8] Javna nabavka je proces koji se bavi nabavkom dobara, pružanjem usluga i izvođenjem radova, korišćenjem javnih sredstava, u skladu sa važećim zakonima o nabavkama.

[9] Važno je da se novac poreskih obveznika troši efektivno donoseći najbolju korist zemlji.

[10] Izveštaj o napretku za Kosovo 2021, 2020

[11] Godišnji izveštaj o učinku, KRPP-2022

[12] Godišnji izveštaj o učinku, KRPP-2021

[13] Godišnji revizorski izveštaj, 2021

[14] Nacionalna strategija javnih nabavki 2017-2021 , Strategija-za-javne nabavke.pdf (rks-gov.net)

Sve publikacije u elektronskim nabavkama su transparentne, javne i dostupne svim zainteresovanim stranama, uključujući potpisane ugovore i dokumentaciju o oceni eliminisanih i dodeljenih ponuda (odluke GA o oceni ponuda i standardna pisma za uspešne i eliminisane ponuđače).

Platforma za elektronske nabavke je i 2022. godine jedan od najčešće korišćenih sistema na nivou vlade, koji koriste preduzeća, građani i zainteresovane strane.

Tabela 1 : Aktivnosti iz sistema elektronskih nabavki 2018-2022

Godine	Ponude dostavljene	Ugovorni organ	Ekonomski operateri	KORISNICI	Razvoj procedura	Potpisani ugovori
2022	29.000	208	14,440	36.000	11,140	9,042
2021	24,600	201	12.000	32,000	6,900	6.200
2020	25,500	197	9,450	24,800	6,657	5,389
2019	100% preko platforme	190	7,650	20,500	7,627	5,630
2018	97% preko platforme	190	6,000	16.000	6,781	5,174

Upotreba informacionih tehnologija za javni sektor, a posebno za sistem nabavki, je pokretački element za povećanje efikasnosti i efektivnosti tokom implementacije zakona o nabavkama.

2 Cilj i oblasti revizije

Cilj ove revizije je da proceni da li je RKJN efikasno upravljala IT operacijama, kako bi se osiguralo da elektronski sistem "e-nabavke" kontinuirano podržava proces javnih nabavki i održava njegov integritet.

Ovom revizijom, cilj nam je da pružimo relevantne preporuke RKJN-u i drugim korisnicima sistema u cilju poboljšanja njihovog pristupa u vezi sa upravljanjem sistemskim uslugama.

Oblasti revizije su IT upravljanje, podugovaranje, sigurnost informacija, kontrola aplikacija i IT operacije. Ove oblasti uključuju sledeća revizijska pitanja:

Oblasti revizije	Pitanja revizije
1. IT upravljanje, poslovanje i podugovaranje	1. Organizaciona struktura/ljudi i resursi
	2. Upravljanje kontinuitetom rada sistema e-nabavke
	3. Upravljanje problemima i incidentima
	4. Upravljanje promenama; i ugovor o nivou usluge (SLA)
2. Kontrole aplikacija i IT sigurnost	5. Ulazni podaci i veze sa drugim sistemima
	6. Upravljanje privilegijama
	7. Poverljivost
	8. Mehanizmi sledivosti

Delokrug ove revizije je RKJN, sa posebnim fokusom na odeljenje elektronske nabavke, koje je odgovorno za obezbeđivanje nesmetanog rada i funkcionisanja usluga koje nudi e-nabavka;

Ova revizija je obuhvatila period od 1. januara 2017. do 30. juna 2023. godine, odnosno od trenutka kada su elektronske nabavke postale obavezne za sve budžetske organizacije, sa fokusom na najnovija dešavanja sistema i odeljenja, odnosno u poslednje dve godine.

Detaljna metodologija primenjena tokom ove revizije, pitanja i kriterijumi revizije su predstavljeni u Dodatku I.

3 Nalazi revizije

U ovom poglavlju predstavljena su pitanja iz revizije elektronskog sistema javnih nabavki koja se odnose na njegovu podršku i efikasnost. Pitanja su strukturirana u dva dela.

Prvi deo je predstavljen u poglavlju 3.1. pokriva pitanja vezana za IT upravljanje, poslovanje i podugovaranje, koje je potrebno poboljšati kako bi se osiguralo da elektronski sistem e-nabavke kontinuirano podržava proces javnih nabavki.

Slika 2 predstavlja broj pitanja i njihovo rangiranje prema oblastima upravljanja, poslovanja i podugovaranja "e-nabavke"

Drugi deo je predstavljen u poglavlju 3.2, pokriva identifikovana pitanja vezana za kontrolu unosa i sigurnost u aplikaciji, koja utiču na integritet ovog sistema kako bi se osiguralo da se tačni podaci obrađuju u ovom sistemu i od strane ovlaštenih osoba.

Na slici 3 prikazan je broj pitanja i njihovo rangiranje prema oblastima ulaznih kontrola i sigurnosti u sistemu "e-nabavke"

3.1 Upravljanje, rad i podugovaranje e-nabavke

Najključniji element upravljanja IT-om su ljudski resursi, koji osiguravaju da se IT-u dodeli dovoljno resursa za postizanje potreba organizacije. IT operacije su opisane kao svakodnevni zadaci uključeni u vođenje i podršku informacionih sistema institucije. Tokom podugovaranja, institucija mora da obezbedi da je u mogućnosti da nastavi IT usluge u slučaju da podizvođači više nisu u mogućnosti da pružaju ove usluge.[15] U nastavku smo predstavili nalaze kao rezultat neefikasnosti u ove tri oblasti informacione tehnologije.

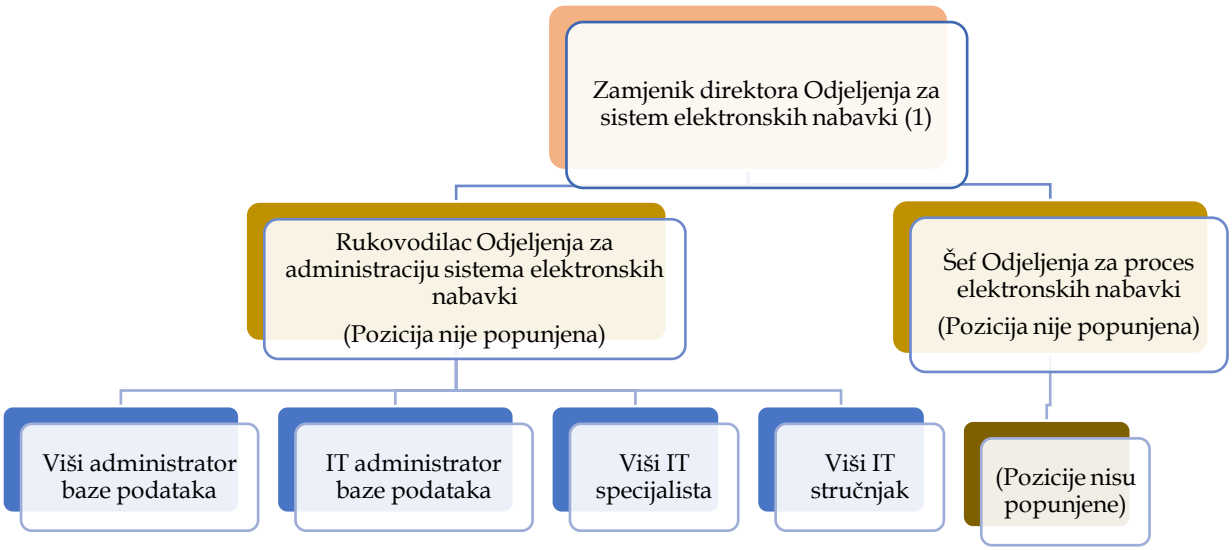
1. RKJN nema kompletnu organizacionu strukturu i jasnu podelu uloga i odgovornosti u IT

Da bi se omogućilo efikasno funkcionisanje sistema e-nabavki, odeljenje sistema elektronskih nabavki mora imati odvojene uloge i odgovornosti ljudskih resursa kako bi ispunilo svoju misiju. RKJN mora imati plan za postizanje sadašnjih i budućih zahteva kako bi zadovoljio svoje potrebe za najefikasnije funkcionisanje sistema e-nabavke. [16]

U organizacionoj strukturi RKJN-a, odeljenje elektronskog sistema nabavke je jasno pozicionirano i njime upravlja direktor odeljenja koji je direktno odgovoran predsedniku Upravnog odbora RKJN-a [17].

Prema propisu, broj zaposlenih u ovom odeljenju trebalo bi da bude 8 (osam), dok je trenutno broj zaposlenih pet (5), gde su po aktima imenovanja: zamenik direktora odjeljenja, viša administratorka baze podataka, IT administrator baze podataka, viši IT specijalista i viši IT stručnjak, dok su tri (3) nepopunjene radne pozicije, od kojih su dve rukovodeće. U nastavku smo prikazali trenutno stanje popunjenih i nepopunjenih radnih mesta.

Slika 4 : Sistematizacija kadrova u službi javnih nabavki prema ugovorima o radu



[15] Priručnik za reviziju informacionih tehnologija, IT upravljanje, IT operacije i podugovaranje

[16] Priručnik za reviziju informacionih tehnologija, Poglavlje 2, IT upravljanje

[17] Uredba br. 01/2020 o unutrašnjoj organizaciji i sistematizaciji radnih mesta Regulatorne komisije za javne nabavke, https://krppcms.rksgov.net//uploads/RREGULLORE_Nr_012020_81dd85b299.pdf

Kao što se vidi iz gornje slike, odeljenje e-nabavke nema popunjena sva radna mesta predviđena i odobrena Zakonom o budžetu, kao i pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mesta, u kom slučaju radna mesta direktora odeljenja je sa zamenom, dok dve pozicije rukovodilaca uopšte nisu popunjene. Dok je službenik za bezbednost informacija imao ključnu ili suštinsku ulogu u IT procedurama, RKJN nije uspostavio ovu poziciju u propisima ili u okviru organizacione šeme.

Prema ugovorima o radu/imenovanjima, u Odeljenju za elektronske procese nabavki nema zaposlenog. Međutim, u praksi smo primetili da je celokupno osoblje odeljenja za elektronske nabavke angažovano na pružanju usluge pomoći (putem telefonskih linija, e-maila ili direktnih kontakata) svim korisnicima platforme za elektronske nabavke. Dvoje zaposlenih kao administratori baze podataka koji pripadaju drugom sektoru kontinuirano su angažovani na obavljanju ove funkcije, što onemogućava obavljanje primarnih poslova definisanih ugovorom.

Takođe, viši IT stručnjak ima gotovo iste dužnosti i odgovornosti kao i direktor sektora e-nabavke, a osim toga, odgovornosti službenika za informatičku sigurnost prema procedurama su delegirane na ove službenike. Ova situacija je stvorila i sukob pozicija i odgovornosti ili čak njihovo dupliranje. Dok je informatičar zadužen za administraciju sistema, u praksi on obavlja zadatak administratora baze podataka. Dakle, prema aktu o imenovanju imaju jedno radno mesto, dok u praksi obavljaju i druge poslove.

Takođe, dve važne stručne pozicije za administraciju infrastrukture i jedna stručna pozicija za bazu podataka i primenu prvobitno su pokrivene od strane donatora, a nastavljene su ugovorima za posebne usluge.

Za popunjavanje pozicije službenika za informacionu sigurnost, do sada nisu učinjeni napori da se takav službenik angažuje. Vredi napomenuti da bi ovaj službenik bio odgovoran za identifikaciju pretnji, procenu ranjivosti, utvrđivanje rizika, implementaciju strategija kontrole kako bi se smanjio rizik od potencijalnih sajber napada kako unutar tako i izvan budžetske organizacije.

Nedostatak stručnih pozicija nastao je kao posledica odlaska kadrova, dok je nepopunjenost mesta direktora odeljenja i rukovodioca odeljenja nastala kao rezultat neprijavljivanja kandidata na ovim internim konkursima za kretanje unutar kategorije, a nisu raspisali eksterni konkurs. Nepravilna podela zadataka i odgovornosti nastala je kao posledica nedostatka kadrova, u kom slučaju je postojeće osoblje moralo pokrivati sve informatičke poslove, kao i za ostale poslove angažovano je osoblje iz drugih odeljenja koji su bili pokriveni ugovorima za posebne usluge.

Nedostatak dovoljnih stručnih resursa može rizikovati da RKJN neće biti u stanju da sprovede sve zadatke, odgovornosti i ciljeve definisane zakonom. Takođe, nepravilno razdvajanje dužnosti može dovesti do neidentifikacije potencijalnih rizika kao što su zloupotreba imovine, neovlašćeno otkrivanje ili zloupotreba informacija, neovlašćeni pristup, smanjena odgovornost, itd.

2. *RKJN nema strategiju da osigura kontinuitet sistema e-nabavke*

Institucija mora imati dobro definisano vlasništvo nad sistemom, kao i dovoljnu dokumentaciju o tome kako bi mogla da nastavi sa radom u okviru kritične funkcije ako izvođači ili prodavci nisu u mogućnosti da pruže

uslugu. Institucija mora imati strategiju da osigura kontinuitet sistema e-nabavke bilo sa internim ljudskim kapacitetima ili drugim izvođačima u slučaju neuspeha pružaoca usluga. [18]

RKJN je utvrdio vlasništvo nad sistemom i pružio dovoljno dokaza da je sistemska dokumentacija kompletna uključujući proces razvoja sistema kao i dizajn sistema, kao što je dokumentacija o prihvatanju izvornog koda, sistemska dokumentacija, promena u sistemu, infrastrukturna dokumentacija, dijagrami, itd.

Međutim, RKJN nema nikakvu strategiju niti interne kapacitete da nastavi sa radom sistema e-nabavke u dužem vremenskom periodu, budući da je kontinuirano obezbeđivala eksterne izvođače kako za održavanje tako i sa pojedinačnim konsultantima-ugovaračima za pružanje određenih usluga, čije bi odsustvo onemogućilo svakodnevni rad sistema i ključno je za osiguranje kontinuiteta njegovog rada.

Prema zvaničnicima RKJN-a, napori ili strategije su kontinuirano uloženi da se izbegne stvaranje zavisnosti od trećih strana, u početku potpisivanjem kratkoročnih ugovora sa EO sa ciljem da RKJN poveća svoje resurse. Takođe, svaki novi ugovor o održavanju imao je manje ugovorenih usluga, ali većinu ovih poslova i dalje su pokrivali pojedinačni spoljni izvođači.

Što se tiče razvoja internih kapaciteta, strategija RKJN-a je bila da obuči osoblje sa redovnim ugovorima gde su im pružene različite obuke kao što su informaciona bezbednost, COBIT, ITIL, itd., tako da je u budućnosti moguće obezbediti kontinuitet usluga koje pružaju treća lica, uključujući i prenos znanja od ovih strana u ugovorima, međutim, nije bio u mogućnosti da ispuni ovaj cilj.

Uprkos činjenici da je RKJN preduzela mere u vezi sa vlasništvom i dokumentacijom sistema, nedostatak internih kapaciteta za razvoj ugovorenih usluga je rizikovao stvaranje zavisnosti od trećih strana.

3. RKJN nije dovoljno efikasan u upravljanju problemima u sistemu

Organizacija mora uspostaviti mehanizme za otkrivanje i dokumentovanje stanja koji mogu dovesti do identifikacije incidenta, ovi mehanizmi imaju za cilj da spreče pojavu sličnih incidenata ili problema u budućnosti. Organizacija mora imati sistem upravljanja incidentima/problemima u kojem se prijavljuju svi incidenti koji se dogode.[19]

RKJN je izradio nacrt politike i procedure za upravljanje incidentima, koji prilično dobro opisuje kako se nositi sa IT sigurnosnim incidentima. U okviru ove procedure, slučajevi incidenata u informacionoj bezbednosti moraju biti prijavljeni službeniku za bezbednost informacija. Međutim, trenutno u ovoj instituciji nijedan službenik nije zadužen za ove dužnosti . Isto tako, takva pozicija nije predviđena pravilnikom o unutrašnjoj organizaciji. Shodno tome, u nedostatku službenika za informatičku sigurnost, postupak upravljanja incidentima informacione sigurnosti je delimično primenjiv.

[18] Priručnik za reviziju informacionih tehnologija, poglavlje 5, Podugovaranje

[19] ISACA – CISA Review Manual 27th Edition, 4.8 Problem and Incident Management.

Zadaci i odgovornosti Odeljenja za procese elektronskih nabavki uključuju, između ostalog, informacije u vezi sa problemima u sistemu elektronskih nabavki koje se upućuju službenicima help deska, kao i pripremu izveštaja o predmetnim aktivnostima. RKJN prati proces oko zahteva koji dolaze službenicima help desk-a, a u zavisnosti od prirode zahteva/problema neki se rešavaju unutar help deska dok se drugi prenose radi rešavanja IT službenicima, službenicima za pravila ili nadzorom, ali ne postoji pisana procedura o ovom procesu i upravljanju help deska uopšte.

Osim toga, ne postoji elektronski registar/sistem problema i incidenata koji se dešavaju, kako bi se kategorizovali, identifikovali najčešći problemi koji se javljaju i mogućnost njihovog rešavanja kroz uputstva, promene u sistemu u cilju povećanja efikasnosti rad ili fokusirane obuke zasnovane na najčešćim problemima korisnika sistema e-nabavki.

Od uvođenja elektronskog sistema nabavke, RKJN je primao zahteve za rešavanje problema e-nabavke od korisnika putem e-maila, telefonskih linija i direktnog fizičkog obrasca, iako je 2018. godine pripremljen predlog sa procesom rešavanja ovih zahteva, ali nije primenjen.

Iz izveštaja ovog odeljenja u proseku se sedmično javlja oko 200 zaheva koji se odnose na moguće probleme u sistemu e-nabavki koje upućuju naručioci ili ekonomski operateri, dok značajan broj telefonskih poziva[20] nije obuhvaćen ovim izveštajem iz razloga što su više bili informativni saveti za pozivaoce.

Nepostojanje elektronskog registra ili sistema može imati nekoliko posledica. To može dovesti do nerešenih problema, kašnjenja u odgovoru, neidentifikacije uzroka ili ponavljajućih problema, kao i do povećanog obima posla i smanjene efikasnosti ovog odeljenja.

4. RKJN nema proceduru za upravljanje promenama u sistemima informacionih tehnologija

Sve promene u informacionim sistemima moraju pratiti definisanu proceduru upravljanja promenama, uključujući i one hitne, koje moraju biti odobrene pre implementacije u operativnom okruženju. [21] *Takođe, RKJN mora imati detaljan ugovor o nivou usluge zajedno sa svim zahtevima i mora kontinuirano da prati da li se ugovorne aktivnosti sprovode.*

RKJN je izradio, ali nije odobrio nacrt dokumenta od 2018. godine, čija je svrha da definiše politiku i proces za razvoj softvera RKJN platforme za e-nabavke i svih drugih platformi i softvera u okviru RKJN-a. Ova procedura naglašava softverske zahteve i aktivnosti, ali takođe ističe korake za druge promene platforme e-nabavke tokom objavljivanja i razvoja. Međutim, ovaj dokument ne uključuje proces hitnih promena.

Iako ova politika nije odobrena, procesi koje sledi RKJN zasnivaju se na ovoj politici u vezi sa promenama koje je izvršio u svojim sistemima. Takođe, za promene u aplikacijama, ugovori uključuju ključne elemente sporazuma na nivou usluge, uključujući prakse koje će se slediti za

[20] Tokom posmatranja procesa u roku od 30 minuta bilo je šest telefonskih poziva, ako je ova stopa kontinuirana onda se ispostavlja da je u proseku 300 telefonskih poziva nedeljno.

[21] ISACA-CISA – Priručnik za reviziju, 26. izdanje, 2016. – Poglavlje 4, Operacije, održavanje i podrška informacionih sistema.

upravljanje promenama, kao i za eskalirane incidente i druge probleme. Međutim, primetili smo da ovi elementi nisu specificikovani kod pojedinačnih pružalaca IT usluga.

RKJN je locirao (hostovao) glavne (proizvodne) hardverske i softverske komponente elektronskog sistema nabavke u prostorima Data centra u Agenciji za informaciono društvo (u daljem tekstu AID). U međuvremenu, u prostorijama Data centra Ministarstva finansija, rada i transfera (u daljem tekstu MFRT) nalaze se (hostovane) hardverske i softverske rezervne komponente sistema elektronskih nabavki. Dakle, rad i funkcionisanje sistema elektronskih nabavki zavisi od rada i funkcionisanja infrastrukture Centra podataka kojim administriraju AID-Ministarstvo unutrašnjih poslova (u daljem tekstu MUP) i DTI-MFRT.

Zbog važnosti funkcionisanja sistema i sporazuma u funkciji pružanja usluga i upravljanja elektronskim sistemom nabavki, RKJN je od 2017. godine sa MFRT i 2018. godine sa AID-MUP, pripremio Memorandume o razumevanju i sporazum na nivou Službe sa potrebne elemente, ali ti sporazumi još nisu potpisani. Prema rečima zvaničnika RKJN, uprkos održanim sastancima sa ovim institucijama, do sada nisu dobili odgovor od ovih institucija.

Nedostatak procedure upravljanja promenama povećava rizik od odstupanja od definisanog plana, dozvoljavajući neovlaštene, neproverene i nedovoljne promene koje mogu da utiču na rad sistema ili da nemaju uspeha u identifikovanju grešaka tokom faze testiranja. Takođe, nedostatak sporazuma između organizacije i pružalaca usluga povećava rizik da RKJN neće pravilno definisati i pratiti rad, potpuno funkcionisanje i dostupnost sistema e-nabavke.

3.2 Kontrole unosa i bezbednost „e-nabavke“.

Ciljevi kontrole pristupa su provera valjanosti i autentičnosti priprema izvornih podataka, autorizacije i radnji pristupa kako bi aplikacija prihvatila tačne, pouzdane i potpune podatke. Dok se informacijska bezbednost može definisati kao sposobnost sistema da zaštiti informacije i sistemske resurse u skladu sa uslovima poverljivosti i integriteta. Upravljanje korisničkim nalozima i praćenje njihovih aktivnosti među najvažnijim su elementima bezbednosti informacija. U ovim tačkama, naša revizija je istakla sledeće nedostatke:

5. *Kontrole unosa u aplikaciji nisu dovoljne za sprečavanje obrade netačnih podataka*

Institucija mora imati dobro osmišljena, dokumentovana i implementirana pravila validacije u input interakciji. Aplikacija treba pravilno odbaciti nevažeće podatke. Kriterijumi valjanosti se ažuriraju na odgovarajući i ovlašten način i postoje sveobuhvatne kontrole kao što su pravila registracije i ovlašćenja u slučaju mogućnosti bitnih kontrola pristupa. [22]

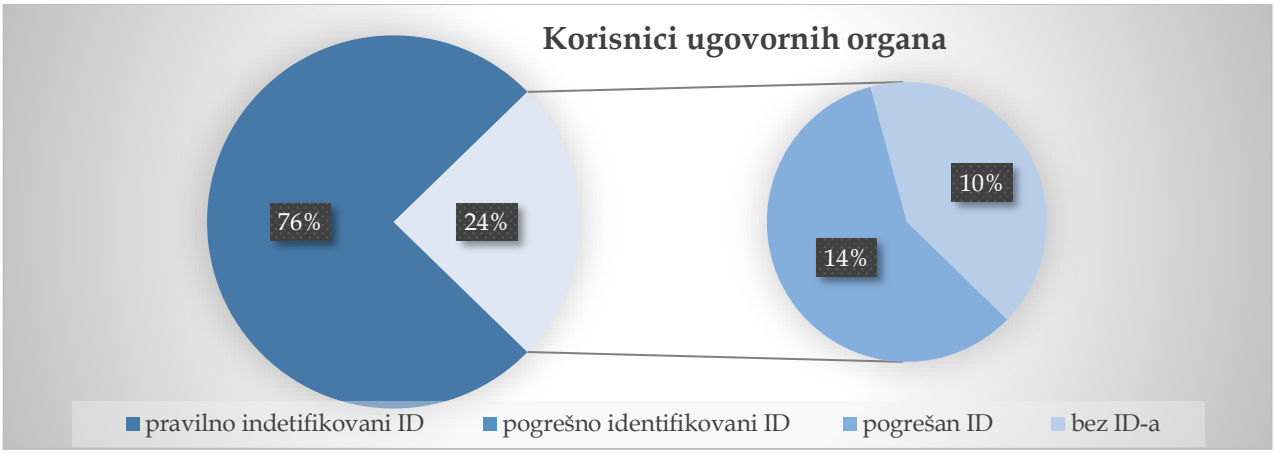
Uzimajući u obzir da je elektronski sistem javnih nabavki jedan od najčešće korišćenih sistema u institucijama Republike Kosovo, kontrole unosa za registraciju podataka, posebno korisnika, treba da odbace nevažeće podatke. Testirali smo modul registracije sa svim njegovim komponentama za ekonomske operatere i ugovorne organe. Obavezna polja u ovom modulu su ime, prezime,

[22] Priručnik za reviziju informacionih tehnologija (ZKA, 2022) – Poglavlje 8, Kontrole aplikacija, Kontrole pristupa

identifikacioni br. (ID ili fiskalni broj), email, itd. Međutim, u ovim oblastima nisu uspostavljene kontrole ili ograničenja neophodna za sprečavanje obrade netačnih podataka.

Kao rezultat toga, u nedostatku postavljanja potrebnih ograničenja, samo od aktivnih korisnika naručilaca od ukupno 17.600 identifikovali smo 4.100 ID-ova grešaka, od čega oko 1.700 naloga koji nemaju ID korisnika koji posluju u okviru ugovornih organa. Pored toga, sistem je dozvolio da se u polje ID registruju i drugi znakovi koji nisu brojevi, što bi u principu trebalo da bude broj. Na donjoj slici, prikazali smo procenat ID-ova grešaka u odnosu na ukupne ID-ove koji su registrovani za organe za kontakt.

Slika 5 predstavlja procenat ID greške u odnosu na ukupan ID aktivnih organa za kontakt do marta 2023.



Takođe, modul za registraciju ekonomskih operatera ne radi ispravno da pravi razliku između rezidentnih i nerezidentnih EO, što bi izbeglo pogrešnu registraciju poslovnih brojeva barem za rezidentne EO.

Takođe je nedostajalo kontrola u unosu podataka u polju za registraciju e-pošte. Identifikovali smo najmanje 50 korisničkih naloga registrovanih na mejlove koji ne zadovoljavaju standarde i stoga su neupotrebljivi nalozi. Kao rezultat toga, ovi korisnici da bi se prijavili na ovu platformu moraju otvoriti druge dodatne račune, učitavajući bazu podataka nevažećim informacijama.

Štaviše, u poljima koja sadrže tekst kao što su ime, prezime itd., dozvoljena je obrada znakova kao što su: ". , ; ! @ <>“, koji smanjuju mogućnost sprečavanja mogućih sajber napada.

Takođe, elektronski sistem nabavke prima podatke od PAK-a, međutim primetili smo da postoje nedostaci u interfejsima aplikacije jer podaci dobijeni od PAK-a pre njihove konačne obrade mogu da se menjaju i obrađuju u aplikaciji e-nabavke uključujući i fiskalni broj.

RKJN nije posvetio dovoljno pažnje testiranju aplikacije za validaciju određenih polja kako bi sprečio netačne registracije. Prema njima, primarni fokus je da sistem bude funkcionalan i da se procesi izvršavaju bez prepreka. Takođe, nedostatak povezanosti sa osnovnim sistemima Republike Kosovo je uticao da ovaj sistem prihvati netačne podatke.

Dozvoljavanje evidentiranja netačnih podataka utiče na performanse sistema nepotrebnim povećanjem njegovih kapaciteta, ne održava integritet baze podataka i utiče na netačan pregled

prilikom sastavljanja statistike. Netačni podaci ili mešanje znakova u sistemskim poljima prilikom registracije korisnika takođe povećava rizik od pristupa neovlaštenih osoba sa strane.

6. E-nabavke nemaju veze sa drugim državnim sistemima

U aplikaciji e-nabavke treba da postoje dodatne kontrole kao što su ovlašteni registri kako bi se sprečilo unošenje netačnih podataka.[23] *Kroz proces registracije, korisnici kreiraju svoj virtuelni identitet (nalog) u sistemu koji je povezan sa njihovim fizičkim identitetom i identitetom organizacije (ugovarača ili ekonomskog operatera) koji predstavljaju u sistemu.*[24]

Elektronski sistem nabavke od 1. januara 2017. godine je obavezan da se koristi od strane svih institucija Republike Kosovo za razvoj svih aktivnosti javnih nabavki, stoga interakcija između sistema elektronske nabavke i drugih relevantnih IT sistema vlade treba realizovati u cilju povećanja efikasnosti i transparentnosti ovog sistema.

Do sada, ovaj sistem razmenjuje podatke samo sa PAK-om, čija razmena je omogućila povećanje efikasnosti prilikom registracije ekonomskih operatera. Međutim, e-nabavka nije predvidela potrebne veze za dobijanje drugih informacija u PAK-u, na primer, kao što je overa poreskih dugova, što je kriterijum za razvoj aktivnosti nabavke.

Sistem elektronskih nabavki prikuplja i čuva lične podatke potrebne za identifikaciju korisnika. Međutim, ovaj sistem više nije povezan sa ARC sistemom, a zbog nepostojanja ove veze svi podaci za korisnika moraju se popunjavati ručno, stvarajući prostor za obradu netačnih podataka**.** Kao rezultat toga, najmanje 11% virtualnog identiteta korisnika (naloga) ne odgovara njihovom fizičkom identitetu.

Takođe, elektronski sistem javnih nabavki nema veze ni sa SIMFK sistemom, što bi povećalo efikasnost posebno korisnika SIMFK sistema, korišćenjem potpisanog ugovora kao i broja ugovora, koji je jedinstven, iz e-nabavke koji bi koristili za bilo koje plaćanje u vezi sa ugovorom. Veza sa SIMFK-om bi takođe pomogla u drugim procesima kao što je Deklaracija o dostupnosti ili zalogu sredstava, s obzirom da aktivnost nabavke ne može početi bez ovog koraka. Faktusirana vrednost i plaćena vrednost su takođe korisne informacije ako se uspostavi ova veza. Dakle, to su tačke koje bi omogućile bolju efikasnost rada službenika za nabavke.

Interkonekcije sa ovim elektronskim sistemima u početku nisu bile predviđene i nisu preduzete inicijative za njihovu realizaciju. Iako su pokrenute inicijative sa SMFK-om i postoji dogovor za realizaciju ove veze, još uvek nema razmene informacija.

Prema rečima zvaničnika u RKJN-u, sa ulaskom u rad okvira interoperabilnosti koji sprovodi AID, predviđeno je da će se izvršiti neophodne razmene. Obrazloženo je da u slučaju nedostatka dostupnosti drugih sistema može doći do neuspeha svakog procesa nabavke uopšte.

[23] Priručnik za reviziju informacionih tehnologija (ZKA, 2022) – Poglavlje 8, Kontrole aplikacija, Kontrole pristupa

[24] Uredba br. 001_2022 o javnim nabavkama

Međutim, međupovezanost između osnovnih sistema IRK-a izbegava moguće netačnosti i zloupotrebe procesa nabavke. Dok je registracija korisnika ručnim označavanjem njihovih podataka bez veze između sistema stvorila prostor da korisnici registruju više netačnih podataka i smanjila efikasnost rada korisnika ovog sistema.

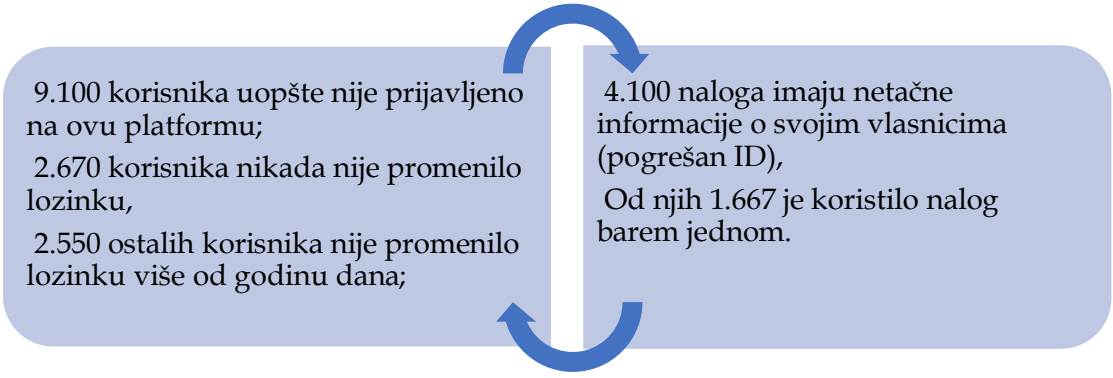
7. *Postoje nedostaci u upravljanju nalozima u elektronskom sistemu javnih nabavki*

Svi korisnici informacionih sistema treba da imaju jedinstvene i personalizovane naloge (ID korisnika), koji se koriste samo za individualnu upotrebu. Lozinku naloga administratora treba da zna samo jedna osoba, da se čuva u bezbednim prostorijama i da može da koristi sistem kada administrator nije dostupan. Nalozi sa potpunim pristupom treba da se prate u kontinuitetu.[25]

RKJN je, u okviru politike informacione bezbednosti, odobrila i politiku uslova korišćenja i prihvatljivosti za korisnike elektronskog sistema javnih nabavki. Uputstva koja se daju korisnicima ovog sistema uključuju različita uputstva, međutim ne uključuju uputstva o odgovarajućim okolnostima za zatvaranje ili deaktivaciju naloga. Štaviše, uputstva ne preciziraju kako da se pregledaju nalozi da bi se identifikovali potencijalni slučajevi nevažećih ili fiktivnih naloga.

Od podataka o svim aktivnim korisnicima ugovornih organa do marta 2023. godine na platformi za elektronske nabavke registrovano je 16.700 korisnika. Na donjoj slici smo prikazali nedostatke koji su proizašli iz analize korisnika.

Slika 6: Analiza naloga aktivnih korisnika ugovornih organa..



Slična situacija je i sa aktivnim korisnicima ekonomskih operatera, od 15.153 korisnika koliko je bilo registrovano na ovoj platformi, najmanje 1.421 korisnik je imao pogrešan ID, najmanje 1.519 korisnika je koristilo isti ID više od jednog puta i za različite kompanije.

Pored toga, korisnički nalozi nisu imali postavljeni standard za njihovo imenovanje. To može izazvati poteškoće u njihovoj identifikaciji i praćenju.

Na osnovu ovih podataka dolazimo do zaključka da korisnički nalozi nikada nisu pregledani od strane ugovornih organa koji imaju obavezu da održavaju svoje korisnike, kao ni od strane RKJN-a kao vlasnicu ove platforme. Isto tako, sistem nije konfigurisao mogućnost promene akreditiva

[25] Familija standarda ISO / IEC 27000 Međunarodne organizacije za standardizaciju (ISO) i Međunarodne elektrotehničke komisije (IEC); Administrativno uputstvo (MJU) br. 02/2015 o službenim elektronskim nalozima;

nakon određenog perioda kako je to poželjno standardima informacione bezbednosti. Drugi razlog za nekorišćenje naloga je otvaranje naloga greškom od strane ugovornih organa i njihovo nezatvaranje nakon identifikacije greške, a takođe i nezatvaranje naloga kada službenici menjaju posao ili prelaze u druge institucije. Shodno tome, najmanje 50% korisnika nije poštovalo uslove korišćenja elektronskog sistema nabavki, kao ni administrativna uputstva o službenim elektronskim nalozima.

Nepotrebno otvaranje korisničkih naloga, nedostatak zatvaranja pasivnih korisničkih naloga kao i nedostatak praćenja korisničkih naloga, između ostalog, slabi rad platforme za elektronske nabavke, povećava rizik od pretnji po bezbednost informacija i povećava mogućnost zloupotrebe naloga za aktivnosti van pravila javnih nabavki.

8. Proces otvaranja korisničkih naloga u e-nabavci nije efikasan

Sistem elektronskih nabavki primenjuje odgovarajuće tehničke mere za zaštitu korisnika i njihovih ličnih podataka. Ove tehničke mere se sastoje od aktivacije e-maila, Tajnih pitanja, principa lozinke, zaštite robota („captcha"). Svaki korisnik treba da obezbeđuje službeni e-mail koji služi za komunikaciju sa sistemom. [26]

Za otvaranje naloga u sistemu elektronskih nabavki, ključni element za čuvanje akreditiva i poverljivosti je email. Prema administrativnom uputstvu (bivše Ministarstvo javne uprave sada MUP) br. 02/2015 o službenim elektronskim nalozima, službeni nalozi – su oni nalozi koje koriste korisnici državnih IT sistema za pristup elektronskim uslugama. I prema ovom uputstvu za korišćenje elektronskih usluga trebaju da koriste službeni nalog.

Međutim, sa spiska korisnika, za ugovorne organe javnih institucija, identifikovali smo najmanje 4.600 korisnika koji su za otvaranje naloga u ovom sistemu koristili privatne/neslužbene naloge.

Štaviše, imajući u vidu da zvanične elektronske naloge ne mogu da pozajmljuju ili koriste druga lica, u 64 slučaja smo utvrdili da su u istom mejlu poslati akreditivi više od jednog korisnika (ukupno je bilo 408 takvih korisnika). Bilo je slučajeva da su akreditivi 96 korisnika za istu organizaciju poslati na službeni elektronski nalog.

Ovo se desilo kao rezultat nepoštovanja pravila korišćenja sistema kao i nedostatka svesti o značaju bezbednosti informacija o korišćenju i čuvanju akreditiva od strane glavnih službenika nabavke u relevantnim institucijama. Isto tako, nedostatak uspostavljanja mehanizama u sistemu da se samo jedan mejl može koristiti za aktivan nalog omogućio je službenicima u institucijama da otvore više od jednog naloga sa istim mejlom.

Izlaganje korisničkih akreditiva drugim licima krši princip poverljivosti, povećavajući rizik od izlaganja i zloupotrebe informacija. Isto tako, to omogućava neovlašćenim službenicima da obavljaju radnje u sistemu u ime drugih lica, ne poštujući zakone i principe javnih nabavki.

[26] Uredba br. 001/2022 o javnim nabavkama; član 3. Zahtevi za korisnike sistema elektronskih nabavki

9. Ne postoji praćenje aktivnosti korisnika

Aplikacija i baza podataka treba da imaju tragove revizije koji obuhvataju promene, zamene i ovlašćene registre (logove) za kritične transakcije; Tragove revizije treba periodično pregledati kako bi se pratile neobične aktivnosti i treba ih pravilno održavati i štititi; Jedinstveni i sekvencijalni brojevi ili identifikatori treba da budu dodeljeni svakoj transakciji. [27]

Proveravanjem tabela kao i testova u aplikaciji, tragovi revizije su zabeležili svaku promenu koja se dogodila, uključujući i to koji su podaci ili polja promenjena, kada su promenjena, šta je promenjeno i ko je izvršio promene. Isto tako, iz kontrolisanih tabela, svaki događaj evidentiran u aplikaciji je povezan sa jedinstvenim sekvencijalnim brojem koji je sačuvao svoju doslednost. Ovo je uticalo da sistem održi svoj integritet i da tragovi revizije budu potpuni.

Međutim, u RKJN-u, preventivni mehanizmi za otkrivanje bilo kakve neobične aktivnosti nisu dovoljni. RKJN ne prati aktivnosti ekonomskih operatera ugovorenih za održavanje aplikacije, kao ni korisnika koji imaju pun pristup kao aplikaciji tako i bazi podataka.

Pregled tragova aktivnosti u sistemu se ne vrši redovno. Tragovi se prate samo sa posebnim zahtevima, u slučaju bilo kakvih žalbi od strane ugovornih organa ili ekonomskih operatera. Štaviše, osoblje zaduženo za praćenje tragova prema proceduri za logovanje i praćenje, ima pun pristup ovim tragovima i prati sebe, dakle to je sukob praćenja i nadzora njihovih aktivnosti. Isto tako, nisu izradili izveštaje o aktivnostima evidentiranim u dosijeima elektronskog sistema nabavki.

Nedostatak adekvatnog alata za praćenje aktivnosti korisnika bio je među uzrocima nepraćenja korisnika, posebno onih sa punim pristupom sistemu, kao i ekonomskih operatera ugovorenih za održavanje sistema.

Nedostatak praćenja i tretiranja događaja aktivnosti u određenim vremenskim periodima, predstavlja rizik da se greške i zloupotrebe ne identifikuju na vreme ili da se one uopšte ne identifikuju.

[27] Priručnik za reviziju informacionih tehnologija (NKR, 2022) – Poglavlje 8, Kontrole aplikacija, Kontrole bezbednosti aplikacija; Familija standarda ISO/IEC 27000 Međunarodne organizacije za standardizaciju (ISO) i Međunarodne elektrotehničke komisije (IEC);

4 Zaključci

Upravljanje, poslovanje i podugovaranja „e-nabavki“

Bez obzira da li je odeljenje elektronske nabavke u RKJN-u dobro i jasno pozicionirano, za potpuno funkcionisanje odeljenje treba da bude popunjeno planiranim radnim mestima. Nedostatak dovoljnih resursa dovodi do toga da RKJN rizikuje da ne bude transparentna i odgovorna, takođe rizikuje da ne postigne definisane ciljeve i ispunjavanje potreba za adekvatno funkcionisanje sistema e-nabavke.

KRPP nije kreirala strategiju za obezbeđivanje kontinuiteta poslovanja, jer je nedostatak razvoja internih kapaciteta i obavljanja važnih/vitalnih zadataka za funkciju sistema sa spoljnim ugovaračima rizikovao da RKJN postane zavisna od trećih lica, i takođe postoji interni rizik od gubljenja znanja o aplikaciji za e-nabavke, onemogućavajući nastavak njenog korišćenja u dužem vremenskom periodu.

RKJN, u nedostatku elektronskog registra/sistema problema i incidenata koji se dešavaju, nije uspeo da vrši kategorizaciju i identifikaciju najčešćih problema kako bi ih rešio putem vodiča, promena u sistemu i povećala efikasnost rada ili fokusirane obuke na osnovu problema za korisnike sistema e-nabavke.

Kontrole unosa i bezbednost e-nabavki

U sistemu elektronskih javnih nabavki nisu dovoljno dizajnirane kontrole unosa tako da se obrađuju samo tačni podaci. Isto tako, ne postoji veza sa drugim vladinim sistemima koji bi omogućili evidenciju vrednih podataka i povećali efikasnost rada, a nedostaju i dovoljne radnje koje se odnose na ostvarivanje veza. Kao rezultat toga, sistemski moduli, polja za evidenciju dozvoljavaju postavljanje specijalnih znakova koji mogu ugroziti bezbednost aplikacije i mogu dozvoliti pristup neovlašćenim licima spolja. Shodno tome, mogućnost unošenja neadekvatnih podataka u sistem e-nabavki onemogućava tačan pregled registrovanih lica ili korisnika u ovom sistemu.

Politike bezbednosti informacija koje je RKJN usvojila nisu bile potpune u pogledu upravljanja nalozima. Preko 50% naloga koji su figurirali kao aktivni uopšte nije bilo aktivirano, umesto zvaničnih naloga koristili su privatne naloge i štaviše isti mejl je korišćen za otvaranje više naloga, dok su lozinke retko menjali korisnici i štaviše, nije bilo praćenja njihovih naloga i aktivnosti. Kao rezultat toga, jedan deo korisnika ovog sistema nisu poštovali uslove korišćenja i principe javnih nabavki, povećavajući rizik od izlaganja informacijama, zloupotrebe naloga i sajber pretnji sistemu e-nabavki. Shodno tome, upravljanje nalozima u ovom sistemu je slabo i prilično osetljivo.

5 Preporuke

Regulatorna komisija za javne nabavke treba da obezbedi:

1. **Organizaciona struktura.** Napraviti jasnu podelu dužnosti i odgovornosti za sve IT pozicije, obezbeđujući da ne postoji sukob odgovornosti i da se obezbedi da su raspoloživi svi neophodni mehanizmi, uključujući službenika za bezbednost informacija da bi se primenile interne IT procedure;

2. **Kontinuitet funkcionisanja.** Izraditi odgovarajuće strategije za obezbeđivanje kontinuiteta elektronskog sistema javnih nabavki.

3. **Upravljanje incidentima.** Izraditi proceduru za upravljanje Šalterom za informacije. Takođe, razmisliti o kreiranju registra/sistema za upravljanje zahtevima/problemima koji se adresiraju ovoj diviziji.

4. **Upravljanje promenama.** Razmotriti i usvojiti proceduru upravljanja promenama, uključujući i one hitne, za celokupnu infrastrukturu informacionih tehnologija i obezbediti da se ova procedura sprovodi u kontinuitetu.

   4.1. U saradnji sa **javnim institucijama Republike Kosovo** koje pružaju IT usluge kako bi se obezbedio kontinuirano funkcionisanje ovog sistema, potpisati ugovore o pružanju usluga.

5. **Valjanost ulaznih podataka.** Obezbediti da su u sistemu e-nabavki postavljena adekvatna ograničenja i kontrole, kako bi se izbegle greške prilikom obrade ulaznih podataka u aplikaciji, a posebno postaviti kontrole koje zabranjuju obradu posebnih znakova koji mogu ugroziti bezbednost sistema.

6. **Povezivanje sistema.** RKJN, zajedno sa **relevantnim javnim institucijama Republike Kosovo**, da preduzme neophodne mere za interakciju između njihovih sistema, kako bi oni imali usklađivanje između podataka, da spreče unošenje netačnih podataka i povećati efikasnost rada.

7. **Upravljanje privilegijama.** Pregledati politiku upravljanja nalozima sa delom za zatvaranje i praćenje naloga u sistemu i takođe izvršiti neophodne izmene u sistemu javnih nabavki za promenu lozinke svakog naloga najmanje jednom u šest meseci i razmotriti mogućnost standardizacije svih elektronskih naloga u ovaj sistem.

   7.1. U saradnji sa **javnim institucijama Republike Kosovo**, oni treba da pregledaju naloge i da zatvore/pasivizuju naloge koji se ne koriste.

8. **Poverljivost.** Stvoriti potrebne mehanizme tako da sistem ne prihvata više od jednog aktivnog naloga u mejlu i takođe preduzeti neophodne mere za zatvaranje svih naloga koji ne pripadaju odgovornim licima.

   8.1. RKJN u saradnji sa **javnim institucijama Republike Kosovo** da obezbede da, posebno glavni službenici za javne nabavke, kao i svi drugi službenici koji otvaraju naloge u ovom sistemu koriste sistem u potpunosti u skladu sa pravilima javnih nabavki.

9. **Praćenje tragova revizije.** Obezbediti da se evidencija tragova revizije redovno pregleda radi moguće manipulacije i neovlašćenog pristupa njima.

9.1. Pripremiti periodične izveštaje o aktivnostima korisnika, posebno sveobuhvatne izveštaje o aktivnostima ekonomskih operatera kao i korisnika sa punim pristupom sistemima i bazama podataka.

Prilog I. Dizajn revizije

Rizične oblasti i pokazatelji problema revizije

Međunarodni izveštaji cenili su puštanje u funkciju e-nabavki. Međutim, prema izveštaju o ocenjivanju PEFA za Kosovo, naglašava se da ne postoji automatska veza između PIP, ISUFK-a i elektronskih nabavki. Dok je u izveštaju o napretku za Kosovo u 2020. godini ocenjeno da treba uložiti dodatne napore da se obezbedi interoperabilnost između sistema elektronskih nabavki i drugih relevantnih IT sistema Vlade. Ovaj izveštaj za 2021. godinu ocenjuje da je proširenje modula elektronskih nabavke poboljšano i povećane su veze između ovog sistema i informacionog sistema upravljanja finansijama na Kosovu za kontrolu obaveza i pravilno sprovođenje budžeta. Međutim, potrebno je više napora da se obezbedi interoperabilnost između sistema elektronskih nabavki i drugih relevantnih vladinih IT sistema kako bi se povećala transparentnost, uključujući praćenje plaćanja.

Dok, u Strategiji za upravljanje javnim finansijama 2022-2026, kao i tokom faze pre studije, analizirana je dokumentacija, izveštaji i intervjui sa službenicima u RKJN-u, kao i drugi izveštaji, i pored gore navedenih problemi, takođe su istaknuti sledeći problemi:

- RKJN se suočava sa nedostatkom ljudskih kapaciteta za održavanje sistema e-nabavke, i takođe opis radnih zadataka nije u skladu sa obavljenim radom.
- RKJN zavisi od trećih lica, kako od kompanije koja je razvila i održava sistem, a takođe i od pojedinačnih ugovarača.
- Politike izrađene za upravljanje incidentima i problemima se ne sprovode u potpunosti.
- Ne postoji dovoljno praćenje EO za održavanje sistema od strane RKJN-a.
- Nisu urađeni testovi propustnosti kako bi se obezbedilo da ovaj sistem ima optimalnu bezbednost od mogućih sajber napada. Takođe nema službenika za bezbednost informacija.

Na osnovu gore identifikovanih pitanja, kao i naših procena zasnovanih na aktivnom Priručniku za IT reviziju da bismo identifikovali najrizičnije oblasti, fokusiraćemo reviziju na pitanja koja uključuju sledeće elemente:

- Upravljanje ljudskim kapacitetima
- Upravljanje kontinuitetom usluga
- Upravljanje bezbednošću informacija
- Upravljanje promenama
- Upravljanje incidentima i problemima
- Upravljanje nivoima usluga
- Upravljanje ulaznim podacima

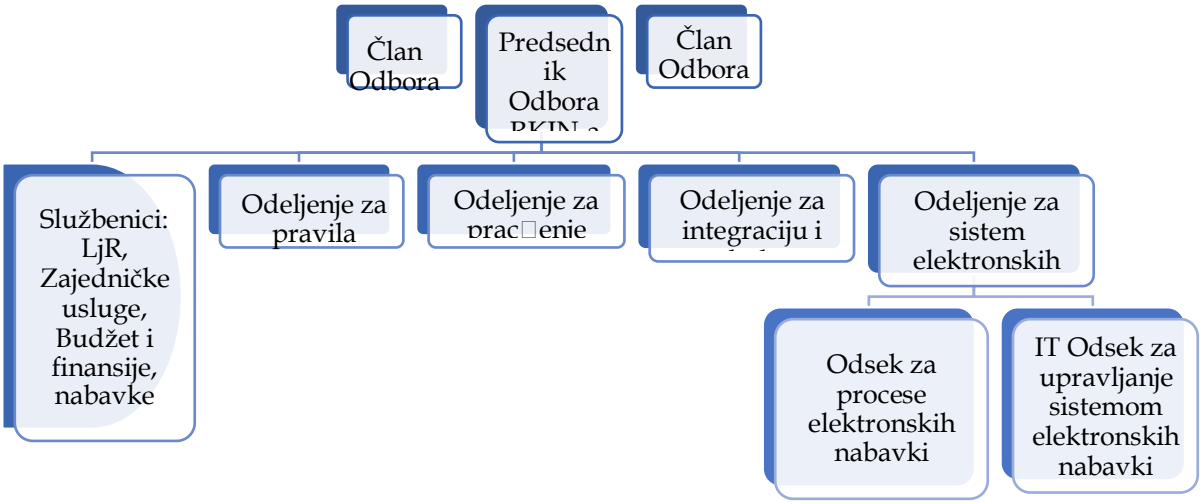
Pokazatelji gore navedenih problema dovode nas do formulisanja problema revizije na sledeći način: institucija nije efikasno upravljala IT operacijama kako bi obezbedila da elektronski sistem javnih nabavki „E-Nabavke“ može kontinuirano da podržava usluge nabavki i da očuva svoj integritet. .

Opis sistema

RKJN, u skladu sa Zakonom o javnim nabavkama Kosova br. 04/L-042, odgovorna je za razvoj, funkcionisanje i opšti nadzor sistema javnih nabavki na Kosovu. Jedna od funkcija koja je RKJNU-u propisana zakonom je da razvije elektronski informacioni sistem na celom Kosovu kako bi se poboljšalo objavljivanje obaveštenja koje zahteva ovaj zakon i da se objavi tenderska dokumentacija.

Organizacionu strukturu Regulatorne komisije za javne nabavke čine Odbor RKJN-a[28], predsednik odbora, odeljenja i odseci.

Slika 3 *Organizaciona struktura RKJN-a.*



Uloga i odgovornosti za elektronski sistem e-nabavke

Odeljenje za sistema elektronskih nabavki ima zadatak da vodi i upravlja svim IT uslugama koje su deo sistema elektronskih nabavki. U okviru ovog odeljenja spadaju IT odsek za upravljanje sistemom elektronskih nabavki i Odsek za procese elektronskih nabavki. Broj zaposlenih u ovom odeljenju je četiri zaposlenih sa punim radnim vremenom.

[28] https://krppcms.rks-gov.net//uploads/RREGULLORE_Nr_012020_81dd85b299.pdf

Upravni odbor

Da nadgleda sistem javnih nabavki u Republici Kosovo;
Priprema i usvaja strategiju i akcioni plan sistema javnih nabavki Republike Kosovo;
Da donosi i usvaja uredbe sekundarnog zakonodavstva za sistem nabavke i rada RKJN-a.
Predsednik odbora zastupa RKJN i potpisuje dokumenta u ime RKJN-a;

Predsednik Odbora RKJN-a

Predsednik zastupa, rukovodi i organizuje rad RKJN-a-a i ima opštu odgovornost za učinak svakodnevnih poslova.
Potpišite dokumente u ime RKJN-a, potpisuje sve odluke donete od strane Odbora. RKJN neće izdati nijedan službeni dokument koji nije potpisan od strane predsednika.
Odgovoran je za upravljanje finansijskim sredstvima RKJN-a;

Odeljenje za sistem elektronskih nabavki

Obezbeđuje neprekidan rad i funkcionisanje usluga koje pruža platforma za elektronske nabavke;
Vodi i upravlja na dnevnoj osnovi celokupnom IT osobljem odgovornim za upravljanje i podršku elektronskom sistemu nabavki koje sprovodi RKJN;
Analizira i procenjuje na dnevnoj osnovi funkcionisanje, rad i učinak sistema elektronskih nabavki koji se primenjuje u RKJN, uključujući analizu i usvajanje predloga za unapređenje, modifikaciju, popravku i ažuriranje modula i funkcionalnosti sistema elektronskih nabavki;
Detaljno planira i priprema 6 (šest) mesečnih i godišnjih planova ažuriranja, ispravke i unapređenja sistema elektronskih nabavki za hardverski i softverski deo sistema;
Priprema i ažurira politiku bezbednosti i standardne operativne procedure platforme e-nabavke koje će sprovoditi IT osoblje;
Daje savete rukovodstvu RKJN-a u vezi sa bilo čim koje se odnosi na sistem elektronskih nabavki.
Sarađuje sa svim zainteresovanim stranama i u vezi sa platformom sistema elektronskih nabavki;

IT odsek za upravljanje sistemom elektronskih nabavki

Upravlja i održava u kontinuitetu infrastrukturu platforme za elektronske nabavke, kako bi obezbedio neprekidan rad i funkcionisanje usluga koje pruža platforma;
Proverava tehničke greške, nemogućnost korišćenja platforme, nefunkcionisanje platforme za potrebne slučajeve i vremenske periode i kad god se to desi.
Sprovodi politike i procedure i uredbe o IT bezbednosti; upravljanje aplikacijom; upravljanje bazom podataka; planiranje kontinuiteta poslovanja; plan upravljanje rizikom/akcioni plan; planiranje oporavka od incidenata; politika pravljenja rezervnih kopija (Backup); arhivsku politiku.
Priprema planove za unapređenje i ažuriranje platforme za elektronske nabavke za hardverski i softverski deo kad god je to potrebno;

Odsek za procese elektronskih nabavki

Pruža pomoć, objašnjenja i konsultantske usluge o korišćenju platforme za elektronske nabavke, uključujući rešavanje tehničkih problema;
Pruža usluge putem telefonskih linija, e-maila itd. svim korisnicima platforme za elektronske nabavke, kao deo UO i EO, i savetuje ih o odgovarajućim radnjama kako bi sledili standardne procedure;
Prati i evidentira probleme koji se najčešće javljaju i služe za otklanjanje grešaka na platformi, uključujući identifikaciju situacija koje zahtevaju hitnu pažnju;
Informiše o problemima koji se ponavljaju i priprema izveštaje o ovim aktivnostima.

Pitanja revizije

Da bismo odgovorili na cilj revizije, postavili smo sledeća pitanja revizije:

1. *Da li je RKJN obezbedila dovoljno ljudskih resursa da obezbedi adekvatno funkcionisanje sistema e-nabavke?*
2. *Da li je RKJN dovoljno sigurna da se sistem e-nabavke i druge ugovorene usluge mogu nastaviti i u slučaju raskida ugovora sa EO?*
3. *Da li su zahtevi korisnika dovoljno podržani i da li su uspostavljene politike za upravljanje promenama?*
4. *Da li su kontrole aplikacije dizajnirane da prihvataju samo valjane podatke?*
5. *Da li je efikasan i bezbedan proces pružanja i obustave kontrole pristupa korisnicima e-nabavke?*

Kriterijumi revizije

Kriterijumi revizije koji su korišćeni u ovoj reviziji proizilaze iz domaćih zakona i uredbi, međunarodnih standarda tehnologije/informacionih sistema, ciljeva kontrole informacija i tehnologije kao i dobre prakse iz oblasti informacionih tehnologija kao i standarda koji se bave upravljanjem bezbednošću informacija.

Da bi se procenilo da li je RKJN efikasno upravljala ljudskim kapacitetima, nivoima i kontinuitetom usluga e-nabavke, mi ćemo koristiti sledeće kriterijume:

- Za omogućavanje efikasnog funkcionisanja sistema e-nabavke, odeljenje za sistem elektronskih nabavki treba da bude jasno pozicionirano unutar organizacije i takođe da ima odvojene uloge i odgovornosti ljudskih resursa kako bi ispunilo svoju misiju;
- RKJN treba da ima plan za ispunjavanje sadašnjih i budućih zahteva da ispuni svoje potrebe za što efikasnije funkcionisanje sistema e-nabavke;
- KRPP treba da ima detaljan ugovor o nivou usluge zajedno sa svim zahtevima i takođe treba da u kontinuitetu prati da li se aktivnosti ugovora sprovode;
- RKJN treba da ima dobro definisano vlasništvo nad sistemom, kao i dovoljno dokumentovanje načina da bi bila u stanju da nastavi sa radom u okviru kritične funkcije ako ugovarači ili prodavci nisu u mogućnosti da pružaju uslugu.
- RKJN treba da ima strategiju da obezbedi kontinuitet sistema e-nabavke bilo sa unutrašnjim ljudskim kapacitetima ili drugim ugovaračima u slučaju neuspeha pružaoca usluga.

Da bi se osiguralo da je IT odsek uspostavio politike upravljanja promena i incidentima, postavljeni su sledeći kriterijumi:

- KRPP treba da uspostavi mehanizme za otkrivanje i dokumentovanje uslova koji mogu dovesti do identifikacije incidenta, ovi mehanizmi imaju za cilj sprečavanje pojave sličnih incidenata ili problema u budućnosti;
- IT odsek treba da ima dokumentovane procedure za otkrivanje i evidentiranje nepravilnih uslova. Uspostavljeni mehanizmi treba da najmanje identifikuju incidente kao što su neovlašćeni pristup korisnika, upadi (bezbednost), propusti na mreži (operativni), slaba

funkcionalnost programa (pružanje usluga) ili nedostatak veština krajnjih korisnika (obuka), itd.;

- RKJN treba da ima sistem upravljanja incidentima/problemima gde se prijavljuju svi incidenti koji su se desili;
- Svaka promena u informacionim sistemima treba da prati definisanu proceduru upravljanja promenama, koja treba da bude odobrena pre sprovođenja u operativnom okruženju. Proces upravljanja promenama treba da obezbedi da se promene evidentiraju, ocenjuju, ovlašćuju, daje im se prioritet, planiraju, testiraju, implementiraju, dokumentuju i pregledaju u skladu sa dokumentovanim i odobrenim procedurama upravljanja promenama. Takođe, RKJN treba da ima i da sprovodi proceduru za vanredne promene.

Da bi se procenilo da li je RKJN efikasno upravljala bezbednošću informacija, mi ćemo koristiti sledeće kriterijume:

- Treba da postoji politika pristupa koja obezbeđuju osnovu za kontrolu pristupa informacijama i obezbeđuju poverljivost svakog korisničkog naloga, i takođe ova politika treba da se primenjuje;
- Svi korisnici informacionih sistema treba da imaju jedinstvene i personalizovane naloge (ID korisnika), koji se koriste samo za individualnu upotrebu;
- Lozinku naloga administratora treba da zna samo jedna osoba, da se čuva u bezbednim prostorijama i da bude u stanju da koristi sistem kada administrator nije dostupan;
- Nalozi sa punim pristupom moraju se stalno pratiti;
- Sistem elektronskih nabavki sprovodi odgovarajuće tehničke mere za zaštitu korisnika i njihovih ličnih podataka. Ove tehničke mere se sastoje od aktivacije e-maila, tajnih pitanja, principa lozinke, zaštite robot („captcha“). Svaki korisnik treba da obezbedi jedan službeni e-mail koji služi za komunikaciju sa sistemom.

Da bi se procenilo da li su kontrole aplikacije dizajnirane tako da prihvataju samo valjane podatke i čuvaju obrađene promene, postavljeni su sledeći kriterijumi[29]:

- U aplikaciji E-nabavka treba da postoje dodatne kontrole kao što su ovlašćeni registri za sprečavanje unošenja netačnih podataka.
- Aplikacija i baza podataka moraju imati tragove revizije koji obuhvataju promene, ovlašćene zamene i evidencije (logove) za kritične transakcije;
- Tragove revizije treba periodično pregledati kako bi se pratile neobične aktivnosti i treba ih pravilno održavati i štititi;
- Svakoj transakciji treba dodeliti jedinstveni i sekvencijalni brojevi ili identifikator;

[29] Priručnik za reviziju informacionih tehnologija kao proizvod radnih grupa informacionih tehnologija EUROSAI (WGITA) kao i Inicijative za razvoj INTOSAI (IDI) – Poglavlje 8, Kontrole aplikacija.

Metodologija revizije

Naš pristup reviziji koristi različitost tehnika za dobijanje dokaza i bezbednosti revizije. Biće analizirani dokumenti, relevantno zakonodavstvo, biće intervjuisane odgovorne strane, i takođe biće sprovedene testiranja i osmatranja na terenu[30].

Analize će obuhvatiti:

- Zakonski i regulatorni okvir koji se primenjuje na sistem e-nabavki;
- Zakonski i regulatorni okvir u vezi sa IT-om (zakoni, uredbe, administrativna uputstva);
- Organogram RKJN-a;
- Interne politike i procedure za razvoj, promene i upravljanje sistemom;
- Priručnici za aplikacije i module;
- Intervjui sa osobljem RKJN-a;
- Testiranje sistema za modul upravljanja pristupom;
- Izveštaji o radu IT-a/ Izveštaji o incidentima/problemima koji nastaju;
- Struktura interakcije podataka sa drugim sistemima;
- Unutrašnja i spoljašnja pravila koja se odnose na klasifikovane i poverljive informacije;
- Zaključeni ugovori sa spoljnim licima;
- itd.

Relevantni dokumenti

- *Zakon o javnim nabavkama Republike Kosovo br. 04/L-042 izmenjen i dopunjen Zakonom br. 04/L-237, Zakonom br. 05/L-068 i Zakonom br. 05/L-092*
- *Nacionalna strategija za javne nabavke 2017-2021*
- *Vodič br. -001/2023 za javne nabavke*
- *Uredba br.001/2022 o javnim nabavkama*
- *Plan učinka RKJN-a*
- *Godišnji izveštaj o učinku RKJN-a*
- *Politike i procesi razvoj softvera*
- *Politike bezbednosti elektronske platforme*
- *Upravljanje incidentima u bezbednost informacija*
- *Plan kontinuiteta poslovanja*
- *Politike korišćenja i uslovi podobnosti*
- *Politike prijavljivanja i praćenja*

[30] Metodologija koja će se koristiti detaljno, nalazi se u matrici revizije.

Prilog II. Potvrdno pismo entiteta

Republika e Kosovës
Republika Kosova-Republic of Kosovo

KOMISIONI RREGULLATIV I PROKURIMIT PUBLIK
REGULATIVNA KOMISIJA ZA JAVNE NABAVKE
PUBLIC PROCUREMENT REGULATORY COMMISSION

REPUBLIKA E KOSOVËS-REPUBLIKA KOSOVA-REPUBLIC OF KOSOVO
ZYRA KOMBËTARE E AUDITIMIT
NACIONALNA KANCELARIJA REVIZIJE / NATIONAL AUDIT OFFICE
- 1. 08. 2023

Njësia Org. Jedin. Org. Unit	Shif.klasif. Klasif. Kod Class. Code	Nr. Prot. Br. Prot. Prot. No.	Nr.i faqeve Br. Stranica No. Pages
06	47	1311	1

REPUBLIKA E KOSOVËS
REPUBLIKA KOSOVA
REPUBLIC OF KOSOVA
KRPP - RKJN - PPRC
Nr. 541 2023
Dt. 01 08 2023

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit **"Sistemi elektronik i prokurimit publik e-prokurimi"**, dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data: Prishtinë 26/07/2023

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **"Sistemi elektronik i prokurimit publik e-prokurimi"** (në tekstin e mëtejmë "Raporti");
- pajtohem me të gjeturat dhe rekomandimet dhe nuk kam ndonjë koment për përmbajtjen e Raportit; si dhe
- brenda 30 ditëve nga pranimi i Raportit final, do t'ju dorëzoj një plan të veprimit për implementimin e rekomandimeve, i cili do të përfshijë afatet kohore dhe stafin përgjegjës për implementimin e tyre.

Osman VISHAJ

Kryetar i Komisionit Rregullativ të Prokurimit Publik

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

Nacionalna Kancelarija Revizije | Naselje Arbëria | Ul. Ahmet Krasniqi, 210 | 10000 Priština

Republika Kosovo