Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

Izveštaj o Reviziji Informacionih Tehnologija

PLATFORMA ZA ONLINE USLUGE E-KOSOVA

Priština, avgust 2025.

Generalni revizor Republike Kosova je najviša institucija ekonomske i finansijske kontrole, kojoj Ustav i Zakon[1] garantuju funkcionalnu, finansijsku i operativnu nezavisnost.

Nacionalna kancelarija za reviziju je nezavisna institucija, koja pomaže Generalnom revizoru u obavljanju njegovih/njenih dužnosti. Naša misija je da kroz kvalitetnih revizija na efektivan način doprinesemo odgovornosti javnog sektora, promovišući javnu transparentnost i dobro upravljanje, i podstičući ekonomiju, efektivnost i efikasnost vladinih programa za dobrobit svih. Na taj način povećavamo poverenje u trošenje javnih fondova i igramo aktivnu ulogu u obezbeđivanju interesa poreskih obveznika i drugih zainteresovanih strana u povećanju javne odgovornosti. Generalni revizor je odgovoran Skupštini za vršenje dužnosti i nadležnosti utvrđenih Ustavom, Zakonom, podzakonskim aktima i međunarodnim standardima revizije javnog sektora.

Ova revizija je izvršena u skladu sa Međunarodnim standardima vrhovnih revizorskih institucija (SNISA 3000[1]) i Vodiča o reviziji informacionih sistema (GUID 5100[2]).

Revizije informacionih tehnologija preduzete od Nacionalne kancelarije revizije su ispitivanje i pregled sistema Informacionih tehnologija i odgovarajućih kontrola kako bi se stekla bezbednost o principima zakonitosti, efikasnosti[3], ekonomičnosti[4] i[5] efektivnosti sistema informacionih tehnologija i odgovarajućih kontrola.

Generalni revizor je odlučio u vezi sa ovim revizorskim izveštajem "Platforma za online usluge e-Kosova" u konsultaciji sa Pomoćnikom Generalnog revizora Myrvete Gashi Morina, koja je nadgledala reviziju.

Tim koji je realizovao ovaj izveštaj:

Samir Zymberi, Direktor odeljenja revizije;
Poliksena Berisha, Vođa tima;
Gazmend Lushtaku, Član tima;
Atdhe Gashi, Član tima; i
Gëzim Krasniqi, Član tima.

NACIONALNA KANCELARIJA REVIZIJE - Adresa: Ul. Ahmet Krasniqi br. 210, Naselje Arbëria, Priština 10000, Kosovo.
Tel: +383(0) 38 60 60 04/1011
http://zka-rks.org

[1] Zakon 05_L_055 o Generalnom revizoru i Nacionalnoj kancelariji revizije Republike Kosova.

1 SNISA 3000 - Standardi i uputstva za reviziju učinka bazirani na ONISA standardima revizije i praktičnim iskustvima.

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

3 Efikasnost - Princip efikasnosti podrazumeva izvlačenje maksimuma iz raspoloživih resursa. Radi se o povezanosti između angažovanih resursa i rezultata datih u smislu kvantiteta, kvaliteta i vremena.

4 Ekonomija - Princip ekonomije podrazumeva minimiziranje troškova resursa. Resursi korišćeni moraju biti dostupni na vreme, u odgovarajućoj količini i kvalitetu i po najboljoj ceni.

5 Efikasnost - Princip efektivnosti podrazumeva postizanje unapred utvrđenih ciljeva i postizanje očekivanih rezultata.

TABELA SADRŽAJA

Spisak skraćenica

ACR	Agencija za civilnu registraciju
AID	Agencija za informaciono društvo
CAAT	Tehnike revizije pomoću računara (Computer assisted audit techniques)
DDos	Distribuirani napad uskraćivanja usluge (Distributed Denial of Service)
KIJU	Kosovski institut za javnu upravu
IRK	Institucije Republike Kosova
ISO/IEC	Međunarodna organizacija za standardizaciju/Međunarodna elektrotehnička komisija (International Organization for Standardization/International Electrotechnical Commission)
RKV	Regionalna kompanija za vodosnabdevanje
MONTI	Ministarstvo obrazovanja, nauke, tehnologije i inovacija
MFRT	Ministarstvo finansija, rada i transfera
MUP	Ministarstvo unutrašnjih poslova
DCP	Državni centar za podatke
ISDSPP	Informacioni sistem Departmana za socijalnu politiku i porodicu
SBV	Sloj bezbedne veze (Secure Socket Layer)
IT	Informacione tehnologije

Opšti rezime

Vlada Kosova je kreirala platformu "e-Kosova" kao jedan od razvoja za poboljšanje pružanja javnih usluga i povećanje efikasnosti uprave. Ova platforma namerava da olakša pristup građanima i biznisima javnim uslugama putem elektronskih usluga, smanjujući troškove i potrebu za fizičkim prisustvom na šalterima.

Platforma e-Kosova je jedan od sistema od nacionalnog značaja, klasifikovan i na nivou zemlje po značaju koji ima, kojim upravlja Agencija za informaciono društvo. Trenutno pruža oko 230 javne usluge elektronskim putem i služi kao jedinstvena porta za pristup uslugama iz različitih institucija, doprinoseći transparentnosti i modernizaciji javne uprave.

Nacionalna kancelarija revizije izvršila je reviziju Informacionih tehnologija sa fokusom revizije na usluge ove platforme: "Dodaci za decu", "Porez na imovinu", "Subvencija za knjige" i modul "Elektronska plaćanja" kako bi procenila da li sprovođenje platforme e-Kosova omogućava građanima realizaciju efikasnih elektronskih usluga na tačan, bezbedan i pouzdan način.

Platforma e-Kosova je obeležila značajan napredak u digitalizaciji javnih usluga, poboljšavajući pristup, transparentnost i efikasnost u njihovom pružanju građanima i institucijama. Preduzeti su koraci za postavljanje tehničkih zaštitnih mehanizama i čuvanje podataka i revizijskih tragova, koji sačinjavaju važnu osnovu za održivi razvoj platforme. Međutim, kako bi se pružio bezbedni i pouzdani rad, neophodno je adresirati postojeće nedostatke u unutrašnjim kontrolama, posebno u aspektima koji se vežu na ugovaranje, razvoj sistema, kao i kontrolu podataka i bezbednost informacija.

Agencija za informaciono društvo nije postavila dovoljne standarde za upravljanje ugovorima, izbegujući nejasnoće u odgovornostima za bezbednost informacija. U ugovorima za razvoj i održavanje ove platforme nije isticano dovoljno klauzule o zaštiti podataka i reagovanju na bezbednosne incidente. Razvijena je hitna u***sluga na platformi e-Kosova na neplaniran način i van standardnih postupaka za dokumentovanje razvoja softvera i tehničkog projektovanja.*** Usluga je razvijena ubrzanim odlučivanjem, bez odgovarajuće dokumentacije, jasnih tehničkih kriterijuma i aktivnog ugovora o subvencionisanju knjiga, ugrožavajući kvalitet rešenja i ispunjavanje njihovih funkcionalnih ciljeva.

AID ne garantuje dovoljno bezbedno informaciono okruženje zbog nedostatka ažurnih politika i operativnih uputstva za upravljanje pristupima i incidentima. Postoje zastarele politike i nedovoljne mere za podizanje svesti osoblja, dok nedostaje kompletna regulatorna infrastruktura koja adresira zaštitom informacija na održiv način.

AID nije spremna da povrati usluge u vanrednim slučajevima ili katastrofama, ugrožavajući kontinuitet elektronskih državnih operacija. Nedostaje dokumentovani i testirani plan oporavka od katastrofe; ne postoje funkcionalni rezervni centri, dok su postojeće rezervne kopije nedovoljne za bezbedan i blagovremeni oporavak.

Nedostatak funkcionalnih i tehničkih kontrola u aplikacijama platforme e-Kosova stvorio je rizike za tačnost podataka i integritet usluga. Evidentirani su nedostaci u povezivanju sistema za verifikaciju kriterijuma, obradi podataka bez tehničkih validacija, kao i nedovoljnim kontrolama koje su rezultirale dvostrukim apliciranjima i ponovljenim plaćanjima.

Platforma e-Kosova se suočava sa nedostacima u kontrolama aplikacije, koji ugrožavaju integritet, tačnost i bezbednost podataka. Za usluge kao "Dodaci za decu" i "Subvencionisanje knjiga", nedostatak povezivanja sistema za verifikaciju kriterijuma kao "prebivalište" dozvolio je korist bez ispunjavanja potrebnih uslova. Povezivanje službe za dečije dodatke sa unutrašnjim sistemom MFRT-a dovelo je do duplih apliciranja i poteškoća u upravljanju plaćanjima. Nedostatak ažuriranja stanja plaćanja u realnom vremenu i slabe kontrole u modulu plaćanja dopustili su da se ista plaćanja izvršavaju više puta, stvarajući finansijske posledice za građane.

Iako platforma obezbeđuje jedinstvene i identifikacione tragove za svaku transakciju, nedostatak aktivnog i periodičnog praćenja kao posledica ograničenih ljudskih kapaciteta i nedostatka standardizovanih postupaka ograničava sposobnost blagovremene identifikacije neovlašćenih intervencija i sumnjivih aktivnosti.

Stoga, gore identifikovani rizici pokazuju da Agencija za informaciono društvo, Ministarstvo finansija, rada i transfera, kao i Ministarstvo obrazovanja, nauke i inovacija koji administriraju i pružaju usluge putem platforme e-Kosova imaju potrebe za dodatna poboljšanja, kako bi se obezbedila zaštita podataka i neprekidno funkcionisanje digitalizovanih usluga. U vezi sa tim, dali smo ukupno 15 preporuka, od kojih 13 preporuka za Agenciju za informaciono društvo i 2 preporuke za Agenciju za informaciono društvo u koordinaciji sa Ministarstvom finansija, rada i transfera i Ministarstvom obrazovanja, nauke, tehnologije i inovacija. Spisak preporuka je prikazan u Poglavlju 5 ovog izveštaja.

Odgovor entiteta uključenih u reviziju

Ministarstvo unutrašnjih poslova, Agencija za informaciono društvo i Ministarstvo finansija, rada i transfera saglasili su se sa nalazima i zaključcima revizije, kao i obavezali da će adresirati date preporuke.

1 Uvod

Platforma e-Kosova je glavna državna platforma gde se javne usluge koje se nalaze u kancelarijama i fizičkim šalterima institucija pružaju elektronskim putem građanima, biznisima i samim zaposlenima u javnoj upravi.

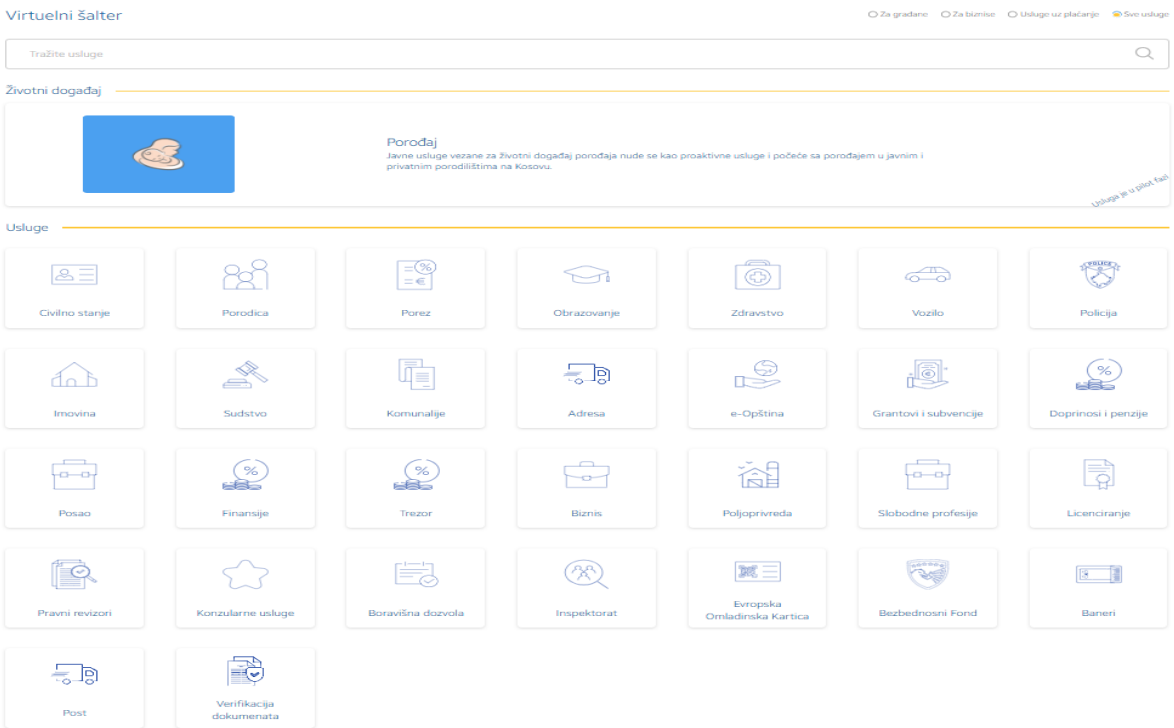
Do sada ova platforma pruža oko 230 usluge u elektronskoj formi, od 658 centralnih usluga i 100 lokalnih usluga za svaku opštinu, koje se pružaju fizičkim i elektronskim putem.

Platforma e-Kosova upravlja se i administrira od Agencije za informaciono društvo. AID je osnovana kao izvršna agencija vlade u okviru ministarstva odgovornog za javnu upravu, ili ispred najvišeg organa državne uprave postavljenog od Vlade i koji je sada Ministarstvo unutrašnjih poslova.

U 2013. godini Skupština Republike Kosova je usvojila Zakon 04/L-145, na osnovu člana 65. (1) Ustava Republike Kosova, o vladinim organima informacionog društva, koji utvrđuje AID kao glavnog organa za razvoj i sprovođenje usluga u oblasti informacione i komunikacione tehnologije u svim institucijama Republike Kosova.

Pored usluga koje su razvijene na ovoj platformi, takođe su povezane putem Platforme za interoperabilnost (interakcije) i direktna povezivanja i druge elektronske usluge, koje se upravljaju od drugih institucija, ali pružaju svoje usluge putem e-Kosova kao jedinstvenu elektronsku portu za građane.

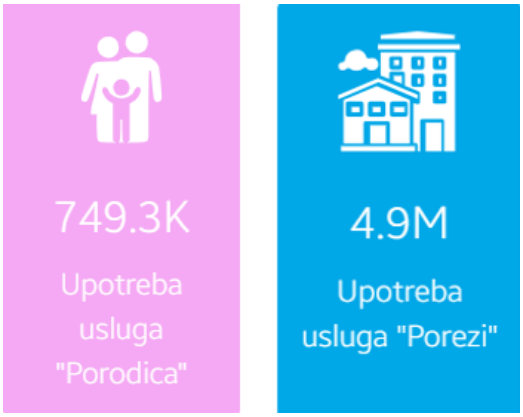
Usluge koje se pružaju u e-Kosova podeljene su u 25 kategorija, koje su prikazane na slici u nastavku.



Slika 1. Kategorije usluga u e-Kosova

Ove usluge olakšavaju administrativne procese i pružaju brži i lakši pristup građanima. Među najčešće korišćenim kategorijama usluga na ovoj platformi su Porodica i Porezi. U kategoriji porodice najviše se koristi usluga dečijih dodataka, dok se u kategoriji poreza usluga poreza na imovinu.

Najčešće korišćene usluge na platformi e-Kosova, koje se karakterišu značajnim mesečnim finansijskim obrtom, su "Dodaci za decu" i "Porez na imovinu". Porez na imovinu je usluga integrisana spoljnim krajnjim sistemom, koji, osim što se široko koristi od građana, sadrži i komponentu plaćanja, povećavajući tako osetljivost na moguće rizike. Takođe, usluga Subvencionisanja školskih udžbenika je uključena zbog pitanja koja su postavljena/povezana sa Platformom e-Kosova, tokom procesa revizije. Stoga je Nacionalna kancelarija revizije orijentisala svoj delokrug revizije u ovim kategorijama usluga, da bi adresirala ključna pitanja funkcionisanja platforme e-Kosova, i planirala je da se naredna revizija u oblasti informacionih tehnologija fokusira na sistem poreza na imovinu.



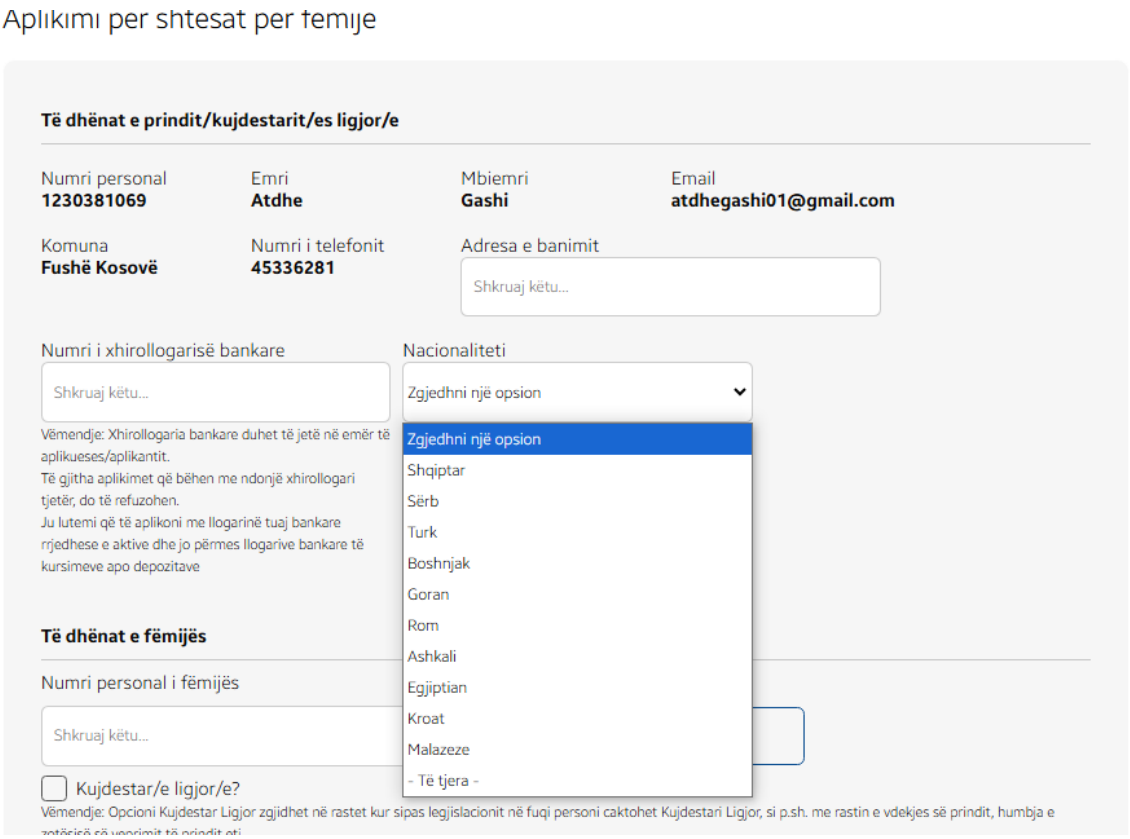
Slika 2. Korišćenje usluga u e-Kosova

Stoga ćemo u nastavku detaljnije tretirati ove usluge, analizirajući procese.

Dodaci za decu

Program Dodataka za decu je dizajniran da se sprovodi na gradualan način, uključujući starosnu grupu od 0-16 godina.

Roditelji ili zakonski staratelji mogu da apliciraju za dečje dodatke putem elektronske platforme e-Kosova. Apliciranje se vrši online sledeći korake u nastavku, kao i što je prikazano na slici 3:



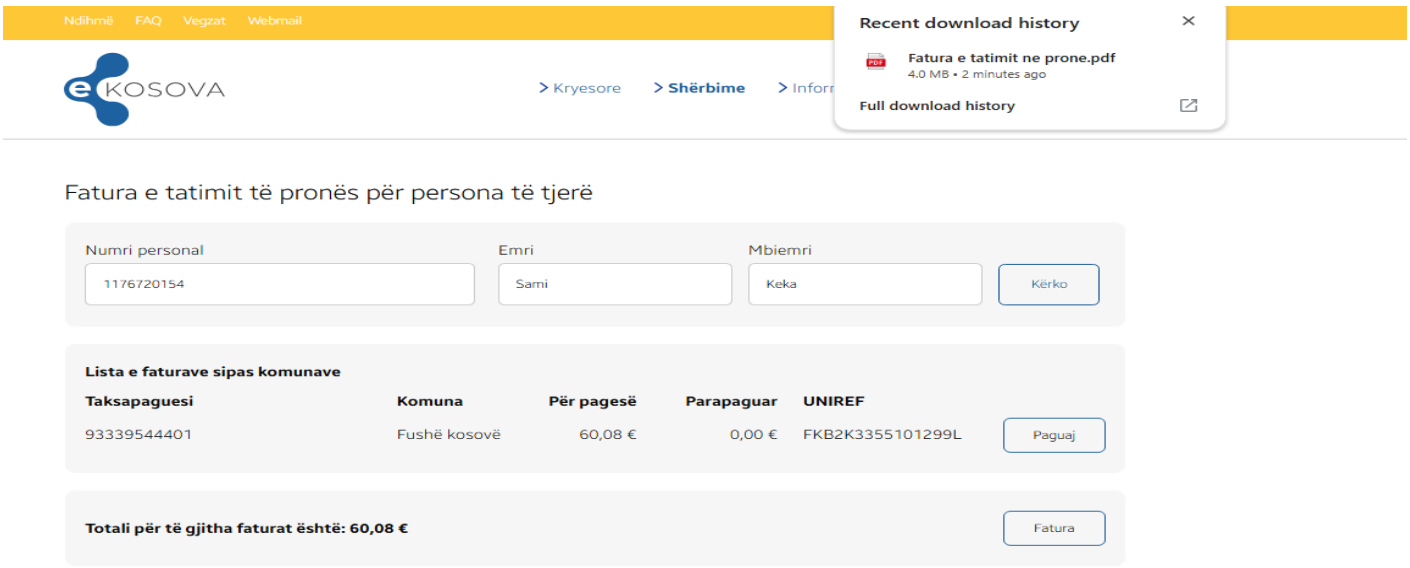
Slika 3. Apliciranje za dečje dodatke

Isplate dodataka vrše se svakog meseca, obično dana 25. ili sledećeg radnog dana, na bankovni račun roditelja ili staratelja koji je aplicirao. Rok za apliciranje za dečje dodatke je otvoren od dana 01 do 10 svakog meseca (apliciranje se vrši samo jednom, a zatim se dodatak primenjuje svakog meseca do ispunjavanja kriterijuma).

Porez na imovinu

Porez na imovinu na Kosovu je godišnja obaveza koja se primenjuje na nepokretnu imovinu, uključujući zemljište i zgrade. Ovaj porez je važan izvor prihoda za opštine i koristi se za finansiranje lokalnih javnih usluga.
Porez se sprovodi na sve nepokretne imovine, uključujući zemljišta i zgrade, bez obzira na njihovu upotrebu (stambene, poslovne, poljoprivredne itd.).

Na slici u nastavku prikazan je način kako se može preuzeti račun za porez na imovinu.

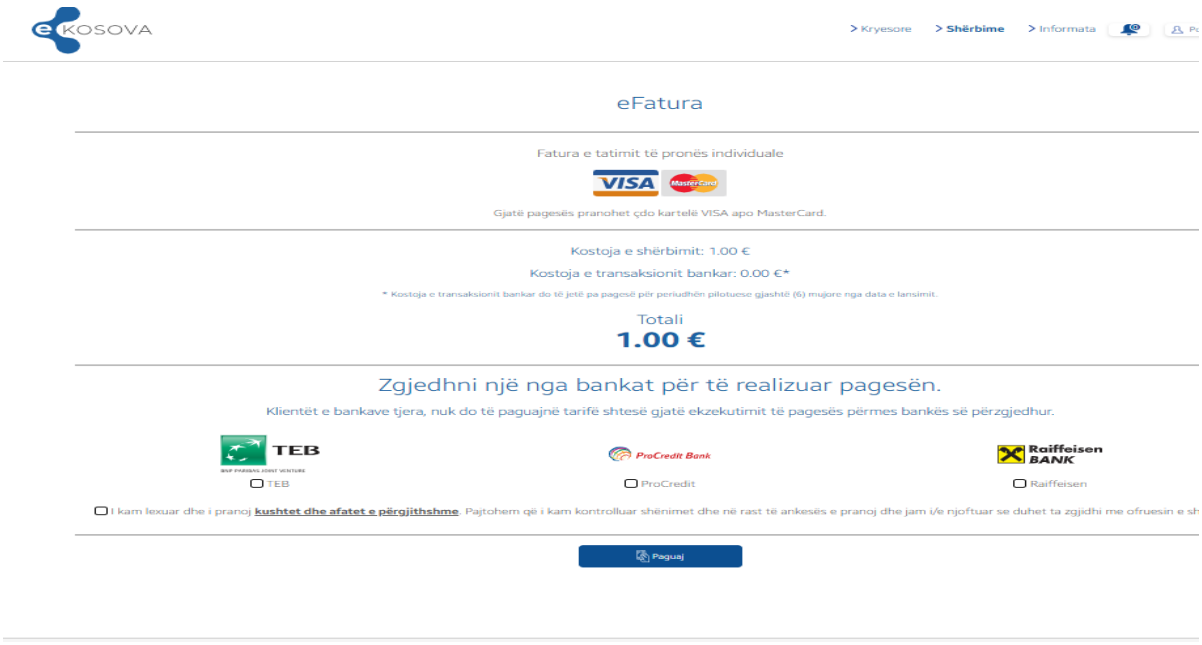


Slika 4. Zakon o porezu na imovinu

Elektronska plaćanja putem e-Kosova

Komponenta eKosovaPaymentGateway predstavlja web aplikaciju koja se koristi kao posrednik između e-Kosova i sistema različitih banaka u svrhu pokretanja i kontrole plaćanja, što je jedan od najosetljivijih modula za građane i bezbednost informacija.

Sve usluge koje realizuju plaćanja koriste ovaj modul. Nakon klika na opciju "Plati" na bilo kojoj usluzi koja sadrži plaćanje, otvara se modul plaćanja kao na slici u nastavku.



Slika 5. eRačun za realizaciju elektronskog plaćanja u eKosova

Kao što je prikazano na slici 4, modul za Elektronska plaćanja prikazuje sve podatke o plaćanju, uključujući i informacije o "Bankama koje obrađuju".

Bezbednost podataka u e-Kosova

Mehanizmi koji su implementirani za pružanje bezbednosti u svim komponentama platforme e-Kosova su putem firewall-a, čuvanje tragova revizije i mehanizama za autentifikaciju.

2 Cilj i oblasti revizije

Cilj ove revizije je da se proceni da sprovođenje platforme e-Kosova omogućava građanima realizaciju efikasnih elektronskih usluga na tačan, bezbedan i pouzdan način.

Ovom revizijom nameravamo da pružimo relevantne preporuke za MUP, AID i odgovorne subjekte kako bi poboljšale informacioni sistem u vezi sa informacionom bezbednošću i razvojem i kontrolom aplikacije.

Da bismo odgovorili na cilj revizije, fokusirali smo se na oblast bezbednosti informacija i kontrole aplikacija, kao i na pitanja koja se vežu sa politikama ugovaranja i kontinuiteta biznisa odabirajući oblasti revizije kao u nastavku:

Tabela 2: Oblasti i pitanja revizije

Oblasti revizije	Pitanja revizije
1. **Ugovaranje**	1. Bezbednost
2. Kupovina i razvoj	2. Analiziranje, prioritizacija i upravljanje zahtevima
3. Informaciona bezbednost i sajber bezbednost	3. Komunikacije i upravljanje operacijama
	4. Sistem za otkrivanje i zaštitu od upada
4. Plan kontinuiteta biznisa - Plan oporavka (povratka) od katastrofa[6]	5. Politika i plan organizacije o kontinuitetu biznisa
5. Kontrole aplikacija	6. Kontrole ulaza
	7. Kontrola obrade
	8. Kontrole odlaznih podataka
	9. Bezbednosne kontrole aplikacija

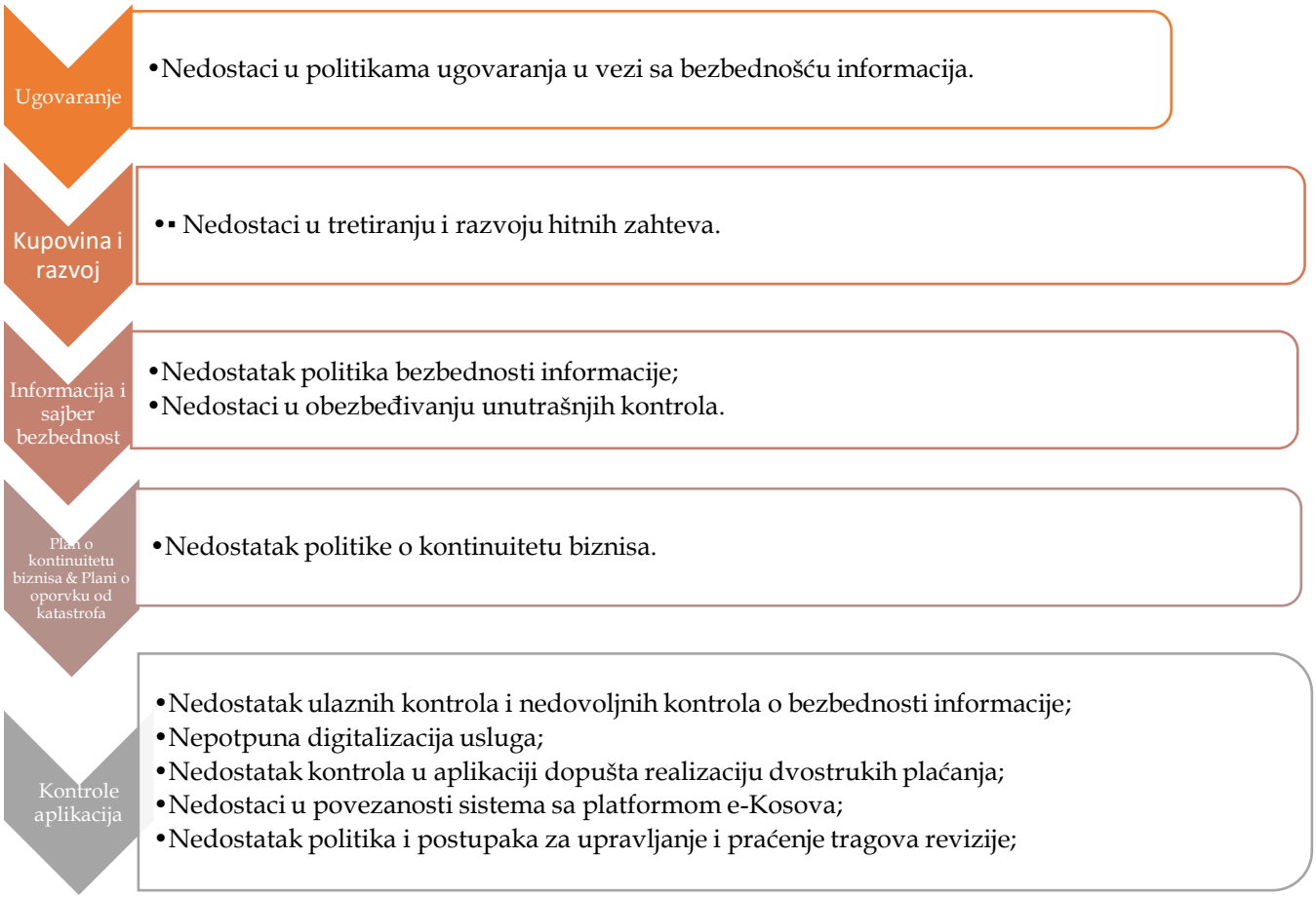
Delokrug ove revizije je Ministarstvo unutrašnjih poslova, odnosno Agencija za informaciono društvo i departmani odgovorni za administriranje, upravljanje i bezbednost platforme e-Kosova. Takođe, uključene su i odgovarajuće jedinice unutar Ministarstva finansija, rada i transfera, odnosno Departmana za porez na imovinu i upravljanje socijalnim šemama, koje administriraju odgovarajućim uslugama na platformi e-Kosova, kao što su usluge poreza na imovinu i dečji dodatak. Revizija je pokrila period od januara 2024. godine do završetka revizije, razmatrajući funkcionisanje i pružanje ovih usluga putem platforme **e-Kosova.** Za sistem poreza na imovinu vrši se još jedna posebna revizija. Pored toga, NKR je u 2023. godini objavila izveštaj o reviziji informacionih tehnologija "Upravljanje projektima za sisteme informacionih tehnologija u Agenciji za informaciono društvo", gde je deo platforme e-Kosova uključen u reviziju u vezi sa razvojem i upravljanjem projektom.

6 PKB & POK - Plan o kontinuitetu biznis & Plan o oporavku od katastrofa.

3 Nalazi revizije

Platforma e-Kosova pružanjem oko 230 elektronskih usluga postigla je značajan napredak u digitalizaciji javnih usluga za građane. Međutim, pored razvoja, identifikovani su i neki nedostaci koji zahtevaju poboljšanje, a koji su predstavljeni u ovom poglavlju izveštaja.

Nalazi revizije povezuju se na politike ugovaranja, zahteve za razvoj, kontrole i administriranje bezbednosti informacija, plana o kontinuitetu biznisa i kontrole aplikacije platforme e-Kosova. Nalazi su strukturisani prema oblastima i pitanjima revizije.



Slika 6. Struktura pitanja revizije platforme e-Kosova

Prvi deo prikazan u poglavlju 3.1 pokriva identifikovana pitanja a koja imaju potrebe za poboljšanje koja se vežu sa ugovaranjem informacionih sistema (1).

Drugi deo koji je prikazan u poglavlju 3.2 pokriva identifikovana pitanja koja se vežu sa razvojem i kupovinom (2).

Treći deo koji je prikazan u poglavlju 3.3 pokriva identifikovana pitanja koja se vežu za informacije i sajber bezbednost (3-4).

Četvrti deo koji je prikazan u poglavlju 3.4 pokriva identifikovana pitanja koja se vežu za plan kontinuiteta biznisa i plan oporavka od katastrofe (5).

Peti deo koji je prikazan u poglavlju 3.5 pokriva identifikovana pitanja koja se vežu za kontrole aplikacija (6-10).

3.1 Politike ugovaranja

Organizacije moraju imati neke politike koje utvrđuju koje funkcije se mogu ugovoriti i koje funkcije moraju se razviti u prostorijama organizacije. Ugovaranje usluga u organizaciji zahteva blisko praćenje i podleže zahtevima privatnosti i bezbednosti.[7]

Ugovorni procesi, AID razvijaju se prema zakonodavstvu na snazi, ali postoje nedostaci u uključivanju bezbednosti informacija tokom ugovaranja.

Slika 7. Politika ugovaranja (Sistem, politike i bezbednost informacija)

1. Ugovor ne adresira na dovoljan način aspekte bezbednosti informacija

> *Bezbednosni zahtevi organizacije moraju biti istaknuti od ugovarača na odgovarajući način. Sporazum sa spoljnim stranama koji uključuje pristup, obradu, komunikaciju ili upravljanje informacijama ili strukturom za obradu informacija organizacije, ili unos proizvoda ili usluga u sistem za obradu informacija, u skladu je sa svim odgovarajućim bezbednosnim zahtevima.*[8]

Analiza ugovora i prateće dokumentacije pokazuje da u sadržaju ugovora nije adresiran deo o bezbednosti informacija. Elementi vezani za bezbednost informacija pomenuti su u tenderskom dosijeu, ali ne i u osnovnom ugovoru.

Štaviše, nisu uključene klauzule koje utvrđuju kako će se čuvati privatnost podataka i koji su odgovorni u slučaju kompromitacije informacija ili bilo kakvog bezbednosnog incidenta.

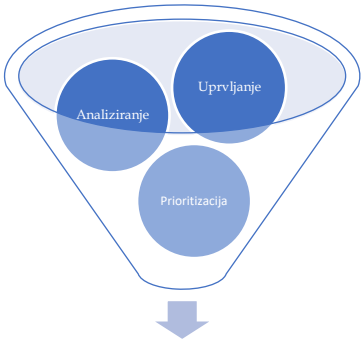
[7] Priručnik o reviziji informacionih tehnologija, Politike ugovaranja.
[8] Priručnik o reviziji informacionih tehnologija - Ugovaranje, bezbednost.

Na osnovu postojeće dokumentacije i trenutne prakse, glavni fokus sporazuma je tehnički i funkcionalni aspekt sistema. Dok zbog nedostatka standardizovanih politika, bezbednosti informacije nije dato adekvatna važnost u sporazumu. Za ugovaranje, AID se poziva na zakon o nabavkama, u kojem nije predviđena posebna politika o bezbednosti informacija, već je opisana samo u opštem obliku.

Nedostatak tretmana bezbednosti informacija i nedostaci u politikama ugovaranja ugrožavaju bezbednost ugovorenih sistema i u slučaju bilo kakvog incidenta bezbednosti informacija nema mogućnosti identifikovati odgovornost ugovornih strana, kao i praćenje i izveštavanje o incidentu.

3.2 Kupovina i razvoj

Razvoj, kupovina i spoljnje ugovaranje, obezbeđuju da upravljanje zahtevima, analiziranje i prioritizacija, kontinuirano podržavaju ispunjavanje potreba korisnika na optimalan način za razvoj usluga na platformi e-Kosova.[9]



Slika 8. Upravljanje razvojnim zahtevima

2. Nedostaci u tretiranju hitnim zahtevima za digitalizaciju usluga za subvencionisanje knjiga na platformi e-Kosova i usluga nije u potpunosti elektronska

AID mora analizirati, utvrđivati prioritete i upravljati zahtevima kako bi se obezbedilo da su potrebe korisnika ispunjene na optimalan način i sa efektivnim troškom.[10] *Transakcije aplikacija se izvršavaju u skladu sa očekivanim ponašanjem.* [11]

AID za razvoj elektronskih usluga na platformi e-Kosova, pored planiranih usluga, takođe razvija usluge sa hitnim ili ubrzanim zahtevima koji se tretiraju izvan standardnih postupaka i planskog dokumenta.

U 2023. godini u ubrzanom obliku razvijena je "Služba za subvencionisanje knjiga na zahtev MONTI". Ovaj zahtev je podnesen bez tehničkih specifikacija i izvan uobičajenih postupaka planiranja. Štaviše, u to vreme, AID nije imala aktivan ugovor za održavanje i razvoj platforme e-Kosova, pa su nedostajali potrebni dokumenti i analize kako bi se obezbedio kvalitet ove usluge.

[9] Priručnik o reviziji informacionih tehnologija, Razvoj, kupovina i spoljnje ugovaranje.
[10] Priručnik o reviziji informacionih tehnologija - Kupovina i razvoj.
[11] Priručnik o reviziji informacionih tehnologija - Kontrole aplikacije, kontrole obrade.

Tehnički detalji i kriterijumi za ovu uslugu diskutovani su samo na verbalnim sastancima i nisu dokumentovani. I u 2024. godini, ova usluga je aktivirana na neposredan način putem zahteva bez neke promene iz prethodne godine.

AID ne prati standardizovane postupke za hitne zahteve, jer ne postoji pismeni proces za njihov tretman. Dok su zahtevi za razvoj usluge došli bez oslanjanja na tehničku analizu od stručnog osoblja ministarstva istraživanja, u ovom slučaju od MONTI.

Bez preliminarnih analiza i jasnih kriterijuma, usluga digitalizacije možda neće ispuniti potrebe građana. U ovom slučaju imala su korist lica kojima ne pripadaju ili nisu se kvalifikovala za subvencionisanje knjiga.

Štaviše, usluga za subvencionisanje knjiga na platformi e-Kosova nije potpuno elektronska. Sve ostale informacije nakon apliciranja građana tretiraju se izvan ove platforme, ručno od završne institucije (MONTI).

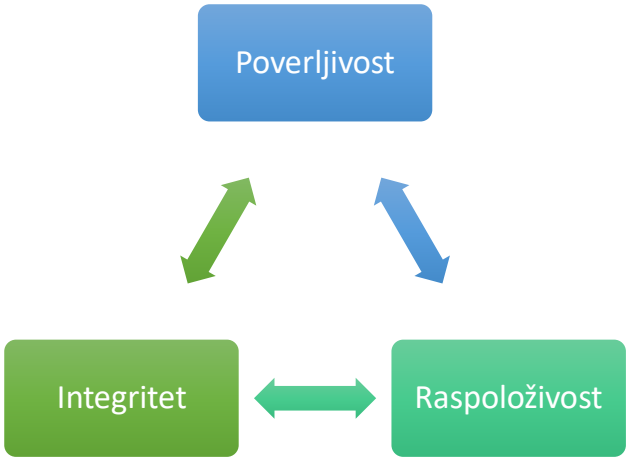
Nedostatak analiza za razvoj usluge i nedostatak adekvatne saradnje između AID kao sprovodilac i MONTI kao istraživačke jedinice i utvrđivanja kriterijuma učinilo je da razvoj elektronske usluge bude neefektivan i nije se postigla njegova potpuna digitalizacija nepružajući potpune i tačne informacije.

Ovaj način organizovanja i postavljanja usluga negativno utiče na efektivnost, bezbednost i pouzdanost usluga pruženih građanima, kao i na unapređenje i povezivanje ove platforme sa drugim sistemima.

Beleška: Finansiranje/subvencionisanje školskih udžbenika je revidirano od tima za finansijsku reviziju, a nalazi vezani za ovo pitanje, uključujući finansijski uticaj, prikazani su u Izveštaju o reviziji za godišnje finansijske izveštaje Ministarstva obrazovanja, nauke, tehnologije i inovacija za 2024. godinu.

3.3 Bezbednost informacija

Bezbednost informacija je jedan od osnovnih aspekata upravljanja IT-a kako bi se obezbedila dostupnost, poverljivost i integritet podataka. Za bolje upravljanje bezbednošću informacija, institucija mora stvoriti mehanizme koji omogućavaju upravljanje rizicima vezanim za bezbednost, preduzimanje odgovarajućih mera i garanciju da su informacije dostupne, upotrebljive, potpune i beskompromisne.[12]



Slika 9. Principi bezbednosti informacija

3. AID funkcioniše bez politike bezbednosti informacija koja je ukinuta, a nije ažurirana i odobrena.

AID mora se obezbediti da postoje utvrđene politike za bezbednost informacija i da su usvojene, saopštene i sprovedene u organizaciji. Politike se moraju pregledavati na redovan način ili kada postoje značajne izmene u organizaciji, tehnologiji ili primenjivim zakonima.[13] Politike i postupci moraju formirati održivo upravljačko okruženje za unutrašnje i spoljašnje komunikacije.[14]

AID je 2010. godine izradila politike bezbednosti informacija koje su u to vreme ispunjavale zahteve organizacije, sa kojima je politika funkcionisala do 2021. godine. Ove politike su ukinute odlukom Vlade. Međutim, oni i dalje nastavljaju da koriste ukinute politike kao praksu, u nedostatku njihovog ažuriranja. Oni nisu izradili ni postupke za bezbednost informacija i funkcionišu bez ikakve regulatorne podrške. Stoga, događaji koji su se desili u AID i u oblasti informacione bezbednosti na globalnom nivou od 2010. do 2021. godine nisu se odrazili u odgovarajućim politikama o bezbednosti informacija. Stoga, AID nema usvojenu i efikasnu politiku i na snazi o bezbednosti informacija. Iako nedostaju politike i postupci, Kancelarija premijera i MUP, uz podršku spoljnih institucija i aktera, izradili su Strategiju o elektronskoj vladavini 2023-2027. Njen cilj je da ubrza e-upravljanje na Kosovu putem poboljšanja postojećeg sistema, dodavanjem novih funkcija i korišćenjem modernih praksi i tehnologija. Pored toga, AID je preduzela zaštitne mere, tehničke aplikacije i konfiguracije u informacionim sistemima za bezbednosnu zaštitu od sajber pretnji.

[12] Priručnik o reviziji informacionih tehnologija, bezbednost informacija.
[13] ISO/IEC 27002:2022. - Politika o bezbednosti informacija.
[14] Priručnik o reviziji informacionih tehnologija - Informacije i sajber bezbednost, komunikacije i upravljanje operacijama.

AID bila na čekanju je obezbeđivanja pravne osnove i krajem 2024. godine usvojen je Zakon o uspostavljanju pravnog osnova za donošenje podzakonskih akata od strane Vlade i ministara[15] koji takođe predviđa donošenje Uredbe o bezbednosti informacija.

Bezbednosna politika ukinuta i neažuriana, kao i nedostatak novih uputstva o bezbednosnim praksama, ostavlja zaposlene neinformisane i nesposobne da na efektivan način zaštite organizaciju i čini organizaciju ranjivijom na sajber napade i strategiju i bilo koje druge inicijative za sajber bezbednost manje efektivne.

4. AID ima nedostatke u unutrašnjim kontrolama

Organizacija mora obezbediti da se upadi otkriju i da će se otkriti i suzbiti.[16] Organizacija mora obezbediti da postoje odgovarajuće mere za sprečavanje, otkrivanje i oporavak od pretnji štetnog koda kroz politike, tehničke kontrole i osveščivanje korisnika. [17] Agencija za informaciono društvo treba da vodi računa o bezbednosti i zaštiti elektronske i infrastrukture i podataka i koordinira aktivnosti za bezbednost usluga IT-a.[18]

Tehničke bezbednosne aplikacije od strane AID se sprovode na nivou namenske zaštitne opreme, koja je konfigurisana da obezbedi naprednu zaštitu od smetnji. Takođe, realizuje izveštaje o incidentima sajber bezbednosti u AID-ovoj IT infrastrukturi u pisanom obliku. Međutim, AID nema pisanu proceduru za sprečavanje ometanja.

Pored nedostatka postupaka, ne postoje dokumenti koji preciziraju koji portovi servera ili platformi su dozvoljeni ili zabranjeni za pristup. Iako je pristup na portama utvrđen prema tehničkim i softverskim zahtevima institucija.

Takođe, oni ne realizuju specifičnu dokumentaciju za zaštitu od smetnji, ali informacije o nivou pristupa se čuvaju u odgovarajućim uređajima koji upravljaju bezbednošću. Ista praksa se realizuje i za platformu e-Kosova.

Štaviše, osveščivanje osoblja u vezi sa bezbednošću informacija je niska, AID nije realizovala kampanje osveščivanja o bezbednosti informacija, niti ima plan i izdvojene resurse za obuku ljudskih resursa u vezi sa ovim delom. Međutim, AID aktivnost osveščivanja o bezbednosti informacija adresirala je na reaktivan način putem informativnih obaveštenja i e-mailova, posebno u slučajevima kada su evidentirani pokušaji phishinga (elektronska prevara koja se koristi u kategoriji sajber napada za dobijanje osetljivih informacija) ili drugi bezbednosni incidenti. U tim slučajevima preduzete su neposredne mere za informisanje osoblja i minimiziranje rizika. Takođe, Kosovski institut za javnu upravu (KIJU) je odgovoran za pružanje obuka, uključujući i oblast informacione bezbednosti, koja je u okviru svojih programa za podizanje kapaciteta javne uprave.

Ovi nedostaci u unutrašnjim kontrolama za bezbednost informacija su i kao uzrok nedostatka resursa AID-a, stoga je sve mere bezbednosti orijentisala na tehničke bezbednosne aplikacije.

Nedostatak postupaka za zaštitu od smetnji i kontrolu pristupa informacionom sistemu povećava rizik od zloupotrebe pristupa i korišćenja neovlašćenih pristupa, kao i neevidentiranju

[15] Zakon br. 08/L-276 o izmenama i dopunama posebnih zakona za uspostavljanje pravnog osnova za donošenje podzakonskih akata od strane Vlade i ministara.
[16] Priručnik o reviziji informacionih tehnologija - Informacija i sajber bezbednost, Sistem o otkrivanju i zaštite od upada.
[17] ISO 27001 - Kriterijumi za zaštitu od štetnog koda (malware).
[18] Uredba (VRK) br. 02/2016. o koordinaciji između Agencije za informaciono društvo i organizacionih struktura/Službenika za informacione i komunikacione tehnologije u institucijama Republike Kosova.

blagovremene intervencije i neidentifikaciju odgovornosti u slučajevima incidenata bezbednosti informacija.

3.4 Plan kontinuiteta biznisa - Plan oporavka od katastrofe

Organizacija mora imati i plan kontinuiteta kako bi obezbedila i kontinuitet pružaoca usluga za njihovu delatnost ili da preuzme to od neku drugu kompaniju.
Ako se oporavak od katastrofe kritične funkcionalne oblasti ugrozi, ugroziće se kontinuitet biznisa (delatnosti).[19]

Slika 10. Kontinuitet biznisa

5. AID nema efektivnu politiku za kontinuitet biznisa

Organizacija mora imati organizacione politike o kontinuitetu biznisa, koje sadrže dužnosti i odgovornosti, svrhu, kriterijume / principe raspodele resursa, zahteve za obuku, raspored održavanja, raspored testiranja, backup planove (čuvanje rezervnih kopija), kao i nivoe odobrenja.[20] *Organizacija mora imati plan za održavanje i obnavljanje operacija biznisa, kako bi se obezbedila dostupnost informacija na zahtevanom nivou i u utvrđeno vreme nakon prekida ili neuspeha procesa biznisa.*[21] *Rezervne kopije aplikacija i baza podataka vrše se u skladu sa standardnim operativnim procedurama i moraju se čuvati u tajnosti na osnovu zakona.*[22]

[19] Priručnik o reviziji informacionih tehnologija, PKB - POK.
[20] Priručnik o reviziji informacionih tehnologija - PKB - POK, Politika i plan organizacije o kontinuitetu biznisa.
[21] ISO 27001 - Upravljanje kontinuitetom biznisa.
[22] Uredba (VRK) br. 02/2016. o koordinaciji između Agencije za informaciono društvo i organizacionih struktura/Službenika za informacione i komunikacione tehnologije u institucijama Republike Kosova.

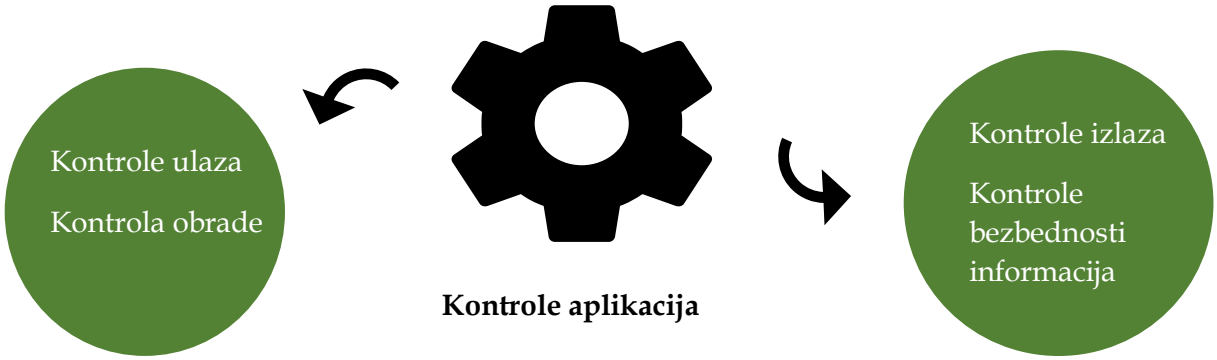
AID nema politike i postupke za kontinuitet biznisa i oporavak od katastrofe, oni se baziraju na Administrativno uputstvo o upravljanju bezbednošću informacija 2010. godine koje je ukinuto za realizaciju rezervne kopije (backup). Štaviše, oni nemaju neki drugi centar za kontinuitet biznisa i oporavak od katastrofe, ili čak drugu istu hardversku infrastrukturu za testiranje i puštanje u funkciji rezervne kopije u slučaju potrebe. AID je u kontinuirano uložila napore za stvaranje centra za kontinuitet biznisa preduzimajući i radnje, posebno poslednjih godina. Do trajnog rešenja, oni realizuju stvaranje rezervne kopije (backup) na redovnim osnovama za infrastrukturu gde se postavila platforma e-Kosova, dok je mogu vratiti na primarnu infrastrukturu koja je u upotrebi i ne može se realizovati redovno testiranje rezervne kopije.

Uzrok nedostatka politika i postupaka za kontinuitet biznisa je nedostatak Centra za kontinuitet biznisa i oporavak od katastrofe i nedostatak infrastrukture. Iako je nedostatak ovog centra kao posledica nedostatka upravljanja resursima zasnovano na riziku kao rezultat lošeg IT upravljanja u AID. Međutim, ove godine je potpisan ugovor o obezbeđivanju infrastrukture koja c□e omoguc□iti implementaciju rešenja za kontinuitet poslovanja, a stvoren je i pravni osnov za izdavanje podzakonskih akata.

U slučaju katastrofe, postoji značajan rizik da se sistemi oštete, podaci izgube i kao posledica, operacije ovih državnih platformi, uključujući i e-Kosova, neće uspeti da rade/funkcionišu.

3.5 Kontrole aplikacija

Kontrole aplikacija su: kontrola nad funkcijom ulaza, obrade, izlaza i bezbednosti. Oni uključuju metode kako bi se obezbedilo da: samo potpuni, tačni, vredni i pouzdani podaci se postavljaju i ažuriraju u informacionom sistemu, obrada realizuje tačnu dužnost, a rezultat obrade ispunjava očekivanja i podaci se čuvaju.[23]



6. Nedostatak restriktivnih kriterijuma prilikom provere ulaska na platformi e-Kosova za uslugu dečjeg dodatka

Pravila validnosti moraju biti dobro izrađena i sprovedena u interakciji ulaza (inputa); različite metode za unos podataka moraju se dokumentovati; nevažeći podaci moraju se odbaciti na odgovarajući način od aplikacije; kriterijumi validnosti se ažuriraju na odgovarajući i ovlašćeni način; moraju postojati sveobuhvatne kontrole kao pravila registracije u slučaju mogućnosti osnovnih kontrola ulaska; postoje kontrole za ulaze aplikacije.[24] Agencija podržava i koordinira aktivnosti između IRK-a kako bi važne baze podataka/registri međusobno komunicirali.[25]

Na elektronskoj platformi e-Kosova postavljena je usluga "Dodaci za decu", koja se upravlja od Ministarstva finansija, rada i transfera (MFRT), na osnovu odluke Vlade u 2024. godini. Za dobijanje ovog dodatka postavljen je kriterijum starosti i broja dece, gde će za porodice koje imaju do dvoje dece uzrasta od 0-16 godina, finansijska podrška biti 20 evra mesečno za svako dete, a za porodice koje imaju troje ili više dece uzrasta od 0-16 godina, podrška će biti 30 evra mesečno za svako dete. Takođe u ovoj odluci je utvrđeno da će imati koristi od finansijske podrške sva deca do 16 godina koja imaju državljanstvo Kosova i koja su rezidentni stanovnici Republike Kosova. Međutim, ovaj kriterijum se ne primenjuje na platformi e-Kosova, kako bi se istovremeno sprečila korist od nerezidentnih stanovnika, stoga trenutno sistem tehnički dozvoljava apliciranje i korišćenje finansijske podrške i za decu koja nisu rezidentni stanovnici i koja žive van Republike Kosova.

Nedostatak primene ovog kriterijuma kao restriktivne kontrole u sistemu, na platformi e-Kosova i koji je utvrđen odlukom br. 55-5/2024., koji obavezuje sve građane rođene van Kosova ili koji su kasnili više od tri meseca da apliciraju za dodatak da se podvrgnu procesu verifikacije na platformi e-Kosova, MFRT to upravlja ručno, što se realizuje u fizičkom obliku putem pošte.

[23] Priručnik o reviziji informacionih tehnologija, Kontrola aplikacija.
[24] Priručnik o reviziji informacionih tehnologija - Kontrole aplikacija, kontrole ulaza.
[25] Uredba (VRK) br. 02/2016. o koordinaciji između Agencije za informaciono društvo i organizacionih struktura/Službenika za informacione i komunikacione tehnologije u institucijama Republike Kosova.

Platforma e-Kosova ne sprovodi kriterijum prebivališta kao restriktivnu kontrolu sistema jer nema tačne podatke o prebivalištu građana izvan Kosova i nedostaje funkcionalna povezanost sa sistemima koji mogu da verifikuju ove informacije. AID je naglasila da nema neki mehanizam za verifikaciju prebivališta, jer nema pristup tačnim podacima iz registra ACR-a.

Elektronska usluga za dečji dodaci na platformi e-Kosova dopušta mogućnost pružanja dečjih dodataka i građanima koji ne pripadaju ovoj službi. To je zato što u aplikaciji nema postavljenih dovoljno ulaznih kontrola u nedostatku kriterijuma na platformi i mehanizma za verifikaciju prebivališta. Ali ova kontrola se realizuje ručno od MFRT.

7. Modul plaćanja na e-Kosova dozvoljava realizaciju dvostrukih plaćanja.

Transakcije aplikacije se izvršavaju u skladu sa očekivanim ponašanjem. [26] Transakcije aplikacije moraju se izvršiti na kontrolisan i pouzdan način, obezbeđujući da se usklade sa pravilima biznisa, parametrima konfiguracije i predviđenim scenarijima obrade. [27]

Za elektronske usluge koje se pružaju na platformi e-Kosova, građani mogu realizovati plaćanja putem modula za plaćanje na ovoj platformi. Ovaj modul je povezan sa bankarskim platformama i realizuje plaćanje u realnom vremenu i bezbedno, bezbednost je na nivou bankarskih bezbednosnih mehanizama. Međutim, tokom verifikacije 120,233 transakcija/uzoraka za različita plaćanja realizovana od građana preko platforme e-Kosova u ovom modulu, naišli smo na 1,112 duplih platnih transakcija, za različite usluge kao što su: policijske kazne, voda za RKV Priština, Sertifikat o pravima na individualnoj nepokretnoj imovini, Sertifikat o pravima na poslovnoj nepokretnoj imovini, Otpad u opštini Priština, KESCO, HidroDrini, Katastar, porez na imovinu. Za dalje analize odabrani su uzorci službi Policije Kosova i Opštine Priština. Iz kojih smo dobili i dodatne dokaze koji potvrđuju postojanje dvostrukih plaćanja, žalbi građana i zahteva za refundiranje.

Uzrok za dvostruka plaćanja na platformi e-Kosova je neotpisivanje duga u trenutku plaćanja u realnom vremenu na platformi e-Kosova i dozvoljavanje izvršenja iste uplate nekoliko puta zaredom bez ikakvog prethodnog obaveštavanja građanina i bez potvrde o izvršenju prve uplate. Kao rezultat toga, građani su više puta platili istu uplatu za usluge na platformi e-Kosova.

8. Proces prijave za dečji dodatak između dva sistema nije u potpunosti sinhronizovan i digitalizovan.

Organizacija mora imati izrađene postupke kako bi se obezbedilo da je potpunost i tačnost rezultata aplikacija procenjena pre upotrebe rezultata iz dalje obrade, uključujući obradu krajnjih korisnika i kontrole potpunosti i tačnosti da budu efektivne. [28]

Na elektronskoj platformi e-Kosova vrši se samo apliciranje za dečje dodatke na digitalizovan način. MFRT prihvata ove aplikacije u svom sistemu na mesečnim osnovama putem ručnog interfejsa od IT službenika u MFRT, koji to realizuje pozivanjem svih aplikacija za svaki mesec i sinhronizirajući ih u MFRT sistemu, Informacionom sistemu Departmana za socijalne i porodične politike (ISDSPP). Ali, povezanost nema dovoljno kontrola, a tokom sinhronizacije podataka imamo slučajeve dupliranja za dečje dodatke. Oni se sprečavaju i identifikuju kroz MFRT sistem, ISDSPP, a ti spiskovi

[26] Priručnik o reviziji informacionih tehnologija - Kontrole aplikacija, kontrole obrade.
[27] Korišćenje COBIT uputstva (posebno DSS05 i BAI09) za kontrolu procesa i obezbeđivanje pouzdanosti obrade transakcija.
[28] Priručnik o reviziji informacionih tehnologija - Kontrole aplikacije, kontrole izlaznih podataka.

se filtriraju od dupliranja. Dakle, sve informacije nakon apliciranja građanina se tretiraju izvan platforme e-Kosova, sve do faze odobravanja i odbijanja koja se realizuje od odgovornog službenika MFRT-a na ovoj platformi.

AID nije obaveštena da postoje dupliranja jer komunikacija između sistema nije u potpunosti digitalizovana, rezultirajući do prekida između njih. Povezanost je realizovana uvozom podataka preko sinhronizacionog fajla, u nedostatku servisa za povezanost u ISDSPP sistemu. U AID, službenici su istakli da ne postoji nijedno dvostruko apliciranje od e-Kosova i to smo verifikovali tokom testiranja na aplikaciji, kao i potvrđeno je i nakon verifikacije uzoraka primljenih iz baze podataka e-Kosova, da tako nešto nije dozvoljeno. Ali to se dešava tokom procesa sinhronizacije podataka između dva sistema.

Platforma e-Kosova i sistem ISDSPP nemaju potpunu međusobnu povezanost i na realno vreme, jer postoje prekidi u komunikaciji. Kao posledica toga, dešavaju se dupliranja aplikacija za dečje dodatke.

9. Služba poreza na imovinu ne prikazuje realno stanje fakture nakon plaćanja.

Organizacija mora imati izrađene procedure kako bi se osiguralo da je potpunost i tačnost rezultata aplikacije procenjena pre upotrebe rezultata iz dalje obrade, uključujući obradu krajnjeg korisnika, i kontrole potpunosti i tačnosti da bi bile efikasne.[29]

Platforma e-Kosova je povezana sa sistemom poreza na imovinu (kao krajni sistem) iz kojeg dobija podatke za prezentaciju izjava o dugu, a u slučaju plaćanja, ta uplata se prosleđuje u sistem poreza na imovinu. Međutim, sistem poreza na imovinu ne koristi podatke o plaćanju da odražava račun poreza na imovinu. Dakle, kada građanin izvrši uplatu poreza na imovinu, sistem poreza na imovinu ne koristi vrednost koju je prihvatila e-Kosova, već čeka podatke koje Trezor šalje za prihod primljen na račun Trezora.

Stoga, iako je uplata izvršena i pojavljuje se na platformi kao završena, faktura za plaćanje ostaje ista i još uvek se pojavljuje u sistemu kao dug, omogućavajući da se ista uplata ponovo izvrši. Ovo čeka prijem informacija iz Trezora i to se dešava kontinuirano.

Takođe, u slučajevima kada građani izvrši uplatu poslednjeg dana roka posle radnog vremena, ta uplata se registruje u sistemu poreza na imovinu nekoliko dana nakon njenog prihvatanja kako je unesena na račun Trezora, zanemarujući podatak o tačnom datumu plaćanja koji šalje platforma e-Kosova, iako je definicija člana za plaćanje definisana Zakonom o porezu na imovinu. Kao rezultat toga, građanin je kažnjen primenom kamate i kazne. To stvara dodatne troškove i prisiljava građana da podnese žalbe u fizičkom obliku kako bi dokazao vreme plaćanja u zakonskom roku.

MFRT to opravdava Uredbom o prihodima trezora i ne uzima u obzir član Zakona o porezu na imovinu u vezi sa plaćanjem i rokom plaćanja.

10. AID ima nedostatak politika i procedura za upravljanje i praćenje revizijskih tragova

Mora postojati dovoljno revizijskih tragova koji obuhvataju modifikacije, ovlašćene registracije kritičnih transakcija; revizijski tragovi se periodično pregledavaju kako bi se pratile nenormalne aktivnosti; revizijski

[29] Priručnik za reviziju informacionih tehnologija – Kontrole aplikacija, kontrole izlaznih podataka.

tragovi se održavaju i čuvaju na odgovarajući način; Jedinstveni i sekvencijalni brojevi ili identifikatori moraju biti definisani za svaku transakciju.[30]

Platforma e-Kosova čuva revizijske tragove unutar sistema i unutar baze podataka. Revizijski tragovi su zaštićeni od modifikacija i pristupi za njihovo praćenje su odvojeni u skladu sa standardima za održavanje bezbednosti informacija. Iz uzoraka dobijenih od preko 2 miliona zapisa o sledljivosti i analiziranih kroz radne alate za reviziju (CATs), procenili smo da su jedinstveni i sekvencijalni identifikacioni brojevi sledljivosti nemodifikovani i pravilno zaštićeni.

Međutim, iako je AID kreiralo revizijske tragove za platformu e-Kosova i odvojio pristup revizijskim tragovima od korisničkih pristupa, oni ne vrše redovno praćenje revizijskih tragova, nemaju politiku ili proceduru za upravljanje i praćenje revizijskih tragova koji bi odredili vreme i dužnosti zvaničnika odgovornih za praćenje revizijskih tragova. Međutim, oni vrše praćenje samo u slučaju sumnjivih aktivnosti i izveštaja o mogućim incidentima.

Nedostatak resursa, a posebno ljudskih resursa, onemogućio je AID-u da redovno prati revizijske tragove, dok su u pogledu procedura oni bili deo bezbednosne politike koja je sada ukinuta.

Nedostatak jasne politike i procedure za periodično praćenje i pregled revizijskih tragova, kao i njihovo redovno praćenje od strane AID za platformu e-Kosova, ograničava mogućnost i povećava rizik da se blagovremeno identifikuju netačne ili neovlašćene aktivnosti. Iako nisu pronađeni konkretni incidenti tokom perioda revizije. Ovo ugrožava integritet, pouzdanost i sigurnost informacionog sistema i može dovesti do gubitka podataka, neovlašćenog uplitanja ili institucionalne odgovornosti za neaktivnost.

[30] Priručnik za reviziju informacionih tehnologija – Kontrole aplikacija, kontrole bezbednosti aplikacija.

4 Zaključci

Platforma e-Kosova je ostvarila važne korake ka digitalizaciji javnih usluga, pružajući važan alat za olakšavanje pristupa građana i institucija različitim administrativnim procesima, istovremeno poboljšavajući transparentnost i efikasnost. Međutim, još uvek postoje izazovi u integraciji sistema, bezbednosti informacija, kontroli podataka koja utiče na njihovu pouzdanost, kao i kontinuitet poslovanja koji utiče na bezbednost podataka.

Ugovaranje
Ugovor ne uključuje dovoljno zahteve i mere za bezbednost informacija, kao što su: klauzula o zaštiti podataka i odgovornosti stranaka u projektu u slučaju incidenata. Fokus ugovora je samo na tehničkim aspektima, dok je bezbednost takođe zaostala zbog nedostatka specifičnih politika i zakonodavstva, ostavljajući bezbednost informacionog sistema ne dovoljno adresiranom.

Nabavka i razvoj
AID obrađuje hitne zahteve za e-usluge bez odgovarajuće dokumentacije i planiranja. Usluga subvencionisanja knjiga razvijena je bez aktivnog ugovora i bez jasnih tehničkih kriterijuma, bez praćenja standardnih procedura. To je dovelo do neefikasnih usluga i rizika od lošeg upravljanja koristima.

Informaciona bezbednost i kibernetička bezbednost
AID nastavlja da radi sa ukinutim i zastarelim politikama bezbednosti informacija, bez pisanih procedura koje definišu kako upravljati pristupom i sprečiti upade. Ova situacija ostavlja zaposlene ne informisanim i organizaciju najranjivijom na kibernetičke napade, što negativno utiče na efikasnost bezbednosnih mera i strategija.
Međutim, AID je sprovelo tehničke zaštitne mere i napredne mehanizme za sprečavanje upada, ali nedostatak specifične dokumentacije i svest osoblja o bezbednosti informacija povećava rizik od zloupotrebe, neovlašćenog pristupa i neblagovremene identifikacije bezbednosnih incidenata.

Plan kontinuiteta biznisa – Plan oporavka od katastrofe
AID nema efikasnu politiku za kontinuitet biznisa i oporavak od katastrofe, jer nedostaju neophodne procedure i infrastruktura, uključujući sekundarni funkcionalni centar. Uprkos svim naporima da se uspostavi ovaj centar i ostvare rezervne kopije, one nisu dovoljne da se obezbedi brz i siguran povratak operacija u slučaju vanrednih situacija, što ugrožava funkcionisanje kritičnih državnih sistema.

Kontrole aplikacija
Na platformi e-Kosova identifikovani su nedostaci u kontroli aplikacija, kao što su kontrola pristupa, integracija sistema i bezbednost informacija. Nedostatak dolaznih kontrola i automatske kontrole kriterijuma stvorio je mogućnosti korišćenja bez kriterijuma, posebno u uslugama "Dečji dodaci" i "Subvencija školskih udžbenika", gde su u službi "Subvencija knjiga" identifikovani konkretni slučajevi. Platforma takođe ne omogućuje potpunu digitalizaciju i ima problema sa sinhronizacijom podataka između sistema u realnom vremenu. Kao rezultat toga, zabeležene su duple aplikacije i ponovljene isplate građana, što šteti njima i kredibilitetu platforme. Nedostatak politika i procedura za praćenje i upravljanje revizijskim tragovima, u kombinaciji sa nedostatkom dovoljnog broja osoblja, povećava rizik od kršenja integriteta, sigurnosti i funkcionalnosti sistema.

Ovi problemi ukazuju na hitnu potrebu da se poboljšaju kontrole, integracija, digitalizacija i bezbednost platforme, kako bi se garantovalo pouzdano i efikasno pružanje javnih elektronskih usluga.

5 Preporuke

Preporučujemo Ministarstvu unutrašnjih poslova i Agenciji za informaciono društvo, Ministarstvu finansija, rada i transfera, kao i Ministarstvu obrazovanja, nauke, tehnologije i inovacija da:

1. **Politike ugovaranja**, MUP i AID, pre pokretanja razvoja bilo kog projekta informacionih tehnologija, moraju da se bave zahtevima bezbednosti informacija sa svim svojim elementima u svim razvijenim ugovorima o informacionim tehnologijama, uključujući očuvanje privatnosti podataka i određivanje odgovornosti strana u projektu na osnovu standardnih politika bezbednosti informacija.

2. **Upravljanje zahtevima,** AID za izradu "hitnih" zahteva treba da osmisli proceduru koja vodi tretiranje zahteva i njegovom dokumentovanju, da analizira i razvije sve neophodne elemente razvoja koji se odnose na tačnost, potpunost i bezbednost informacija.

   2.1. Kontrole obrade u aplikaciji za subvenciju za knjige AID i MONTI u koordinaciji, za aktiviranje usluge subvencionisanja knjiga, mora da izradi uslove sa tehničkim specifikacijama i definiše neophodne kriterijume koji ograničavaju aplikacije samo na građane koji imaju pravo na dobijanje subvencije i digitalizuju ceo proces do odobrenja/odbijanja i prihvatanja subvencije preko platforme e-Kosova, takođe definisanje uloga za odobravanje, odbijanje i praćenje usluge.

3. **Politika bezbednosti informacija,** MUP i AID treba da ažuriraju politike i procedure za zaštitu bezbednosti informacija.

4. **Unutrašnje kontrole za bezbednost informacija,** AID kako bi se osigurale procedure za sprečavanje smetnji i upravljanje pristupom određenim portovima platformi i serverske infrastrukture.

   4.1. AID da sprovede dokumentaciju o postupcima za zaštitu od intervencija.

   4.2. AID da obezbedi plan za svest o ljudskim resursima u vezi sa bezbednošću informacija i da fokusira svoje resurse na obuku i svest osoblja u vezi sa bezbednošću informacija.

5. **Plan kontinuiteta biznisa,** Rukovodstvo AID-a treba odmah ponovo proceniti rizike i orijentisati resurse među ostalim dešavanjima u kontinuitetu biznisa, počevši od uspostavljanja Centra za kontinuitet poslovanja i oporavak od katastrofe.

   5.1. AID mora da izradi, odobri i sprovede politike, procedure i plan kontinuiteta biznisa.

6. **Kontrole pristupa u aplikaciji za uslugu dečjeg dodatka**, AID za povezivanje usluge dečjeg dodatka sa registrima građana za prebivalište i omogućavanje realizacije usluge u potpunosti u elektronskom obliku. AID, na platformi e-Kosova, treba da primeni najprikladniji mehanizam za identifikaciju rezidentnih stanovnika Kosova, koristeći podatke iz svih relevantnih institucija u zemlji.

7. **Kontrole aplikacije za platni modul,** AID za ažuriranje izjava o dugovima za usluge građana u e-Kosova u realnom vremenu i instaliranje kontrolnih mehanizama u platnom modulu koji obaveštavaju građane o realizaciji uplate, čime se izbeglo duplo plac□anje.

8. **Odlazne kontrole u aplikaciji za uslugu dečjeg dodatka,** AID i MFRT radi sprovođenja odgovarajućih kontrola interkonekcije između sistema e-Kosova i SIDPSF i sprovođenja sigurne interkonekcije koja ne dozvoljava umnožavanje podataka ostvarivanjem potpune digitalizacije procesa putem e-Kosova. Podaci koje šalje platforma treba da se obrađuju kroz sistem, a ne manuelno.

9. **Odlazne kontrole u aplikaciji za uslugu poreza na imovinu,** MFRT da koriste podatke o plaćanju građana izvršene putem platforme e-Kosova, koja ih prima putem veze sa AID na ovu platformu, kako bi precizno sproveli zakon o porezu na imovinu koji se odnosi na plaćanje. U cilju komunikacije sa institucijama Republike Kosovo u realnom vremenu i prikazivanja stanja računa i u realnom vremenu za uplatu koju je izvršio građanin.

   9.1. AID da spreči dvostruko plaćanje u modulu "Plaćanja" na platformi e-Kosova, obaveštavajući građanina da je ova uplata već jednom izvršena.

10. **Bezbednosne kontrole u aplikaciji – praćenje revizijskih tragova,** AID da obezbedi politike i procedure za upravljanje i praćenje revizijskih tragova u informacionim sistemima i da definiše zadatke za praćenje tragova na redovnoj osnovi uz obezbeđivanje neophodnih resursa.

Prilog I. Dizajn revizije

Područja rizika i pokazatelji problema revizije

Platforma e-Kosova je jedan od najvažnijih sistema u zemlji, klasifikovan na nacionalnom nivou, zbog značaja koji ima u pružanju javnih usluga elektronskim putem, koji ima za cilj da administraciju učini pristupačnijom, transparentnijom i efikasnijom. Razvijen je i upravlja od strane Agencije za informaciono društvo (AID) i ima za cilj da smanji zavisnost od fizičkih šaltera državnih institucija.

Revizija ove teme je važna s obzirom na preporuke i pitanja koja su identifikovana u IT reviziji koju je prethodno sproveo NAO, [31]s obzirom na to da je e-Kosovo glavna platforma za digitalizaciju državnih usluga, bezbednost i integritet su ključna pitanja za ovu platformu i poverenje građana.

Takođe, tokom predstudijske faze, nakon pregleda dokumenata koji se odnose na IT sisteme i usluge za građane, kao i obavljenih razgovora sa nadležnim službenicima za platformu e-Kosova, utvrdili smo da, uprkos napretku postignutom u digitalizaciji javnih usluga, e-Kosova se i dalje suočava sa nekim važnim izazovima, a to su:

- Nedostatak adresiranja pitanja bezbednosti informacija u ugovorima platforme e-Kosova, kao i nedostatak politike bezbednosti informacija, pošto propis o bezbednosti informacija sa kojim posluju od 2010. godine, sada nije na snazi. To čini bezbednost informacija i kibernetička bezbednost ovog sistema ranjivijim. Kao nedostatak procedura i njihovih ažuriranja u odnosu na najnovija tehnološka dostignuća u okviru ADI-a, ostavio je bez zaštitnih mera za bezbednost informacija i kibernetičku bezbednost. Kao što su: Praćenje tragova aktivnosti u informacionom sistemu, praćenje tragova za kibernetičku bezbednost radi prevencije i detekcije upada. Nedostatak podele uloga i odgovornosti pristupa i odgovornosti u sistemu. Lista mogućih rizika i plan za upravljanje njima. Postupak reagovanja na bezbednosne incidente u oblasti informacija. Kao i nedostatak liste kritične infrastrukture i plana kontinuiteta biznisa.

    - Nedostatak mehanizama za zaštitu bezbednosti informacija ugrožava podatke servisa na e-Kosova. Postaje osetljiviji u slučaju obrade podataka koji se odnose na plaćanja. E-Kosova ima mnogo usluga koje sadrže modul za plaćanje, stoga nedostatak ovih mehanizama čini modul plaćanja ranjivijim na moguće kibernetičke napade.

- Ograničena međusobna povezanost sa drugim državnim sistemima, što dovodi do ručne verifikacije i kašnjenja u ažuriranju podataka za neke usluge. Najčešće korišćene usluge sa najčešćim cirkulacijom finansijskih sredstava na redovnom mesečnom nivou koje su na vrhu liste usluga u e-Kosova identifikovane su sa problemima sledeće prirode:

[31] Upravljanje projektima za sisteme informacionih tehnologija u Agenciji za informaciono društvo – Izveštaj o IT reviziji (2023.)

- **Dečji dodaci,** u odsustvu povezanosti sa sistemima identifikacije prebivališta, čak i građani koji ne žive na Kosovu mogu da primaju dečji dodatak bez ispunjavanja ovog kriterijuma. To se dešava zbog nedostatka interakcije sistema i verifikacije njihovog prebivališta.
- **Porez na imovinu,** podaci službe za porez na imovinu dolaze sa interkonekcijom na platformi e-Kosova, stoga je potrebno testirati bezbednost ove interkonekcije s obzirom na to da smo tokom pred-studijske faze utvrdili da postoji vrlo malo dokumentacije za bezbednost informacija o međusobnom povezivanju usluga. Ova usluga je najviše korišćena od strane građana i ima element plaćanja koji ga čini još ranjivijim, stoga ova usluga ima nedostatke u mehanizmima bezbednosti informacija.

- Nedostatak digitalizacije za neke usluge, posebno za ranjive grupe, kao što su starije osobe i osobe sa zdravstvenim problemima. Važna usluga identifikovana tokom pred-studije je potreba za fizičkim prisustvom za nastavak penzija, gde penzioneri moraju da se lično pojave u kancelarijama za socijalni rad. Ovo pokazuje potrebu za većom analizom tokom digitalizacije procesa i prioritizacije i upravljanja potrebama za digitalizacijom usluga za građane, od strane donosioca odluka za razvoj zahteva.

Ispitivanje pokazatelja identifikovanog problema iz različitih izvora, sastanci sa licima odgovornim za identifikaciju problema na platformi e-Kosova, kao i naše procene na osnovu Aktivnog priručnika za reviziju IT-a[32] za identifikaciju najrizičnijiih oblasti iz prihvaćene dokumentacije usmeravaju nas na glavni problem: platforma e-Kosova ima nedostatke u razvoju i ugovaranju informacionog sistema, u organizovanju bezbednosti informacija i kontrole aplikacije.

[32] Aktivni priručnik revizije – je platforma koju su razvili ITWG/EUROSAI i WGITA/INTOSAI, a koja se koristi za identifikaciju najrizičnijiih oblasti, definisanje pitanja, kriterijuma i metodologije rada tokom procesa revizije IT-a.

Opis sistema

3.1. Ministarstvo unutrašnjih poslova

Misija Ministarstva unutrašnjih poslova je da obezbedi vladavinu zakona i javnu bezbednost na celoj teritoriji Republike Kosovo.

Ministarstvo, pored toga što je odgovorno za izgradnju, održavanje i unapređenje bezbednosti za sve građane zemlje, takođe priprema i sprovodi politike za administraciju i komunikaciju sistema, kao jedna od ključnih institucija koja upravlja elektronskim podacima u smislu kvantiteta, kvaliteta i značaja. Ministarstvo posluje preko svojih 8 agencija i organa, uključujući Agenciju za informaciono društvo (AID) i 13 departmana i divizija.

AID je osnovano kao izvršna agencija vlade u okviru ministarstva nadležnog za javnu upravu, odnosno na najvišem organu državne uprave koju je osnovala Vlada i koja je sada Ministarstvo unutrašnjih poslova.

Skupština Republike Kosova je 2013. godine usvojila Zakon 04/L-145, zasnovan na članu 65. (1) Ustava Republike Kosovo, o Vladinim organima informacionog društva, koji definiše AID glavni organ za razvoj i sprovođenje usluga u oblasti informaciono-komunikacionih tehnologija u svim institucijama Republike Kosovo. Strukture odgovorne za informaciono društvo u institucijama Republike Kosovo u skladu sa ovim zakonom su AID i odgovarajuća organizaciona struktura ili službenik za upravljanje IKT u IRK. Definisani su i nadležni organi za razvoj usluga informacionog društva u institucijama Republike Kosovo, njihove nadležnosti, odgovornosti, organizacija i funkcionisanje.

Dužnosti i odgovornosti AID-a:

- Predlaže i koordinira sve politike u vezi sa razvojem IKT-a u institucijama Republike Kosovo;
- Priprema strategiju elektronske uprave i njen akcioni plan za odobrenje od strane Vlade i prati njeno sprovođenje;
- Rukovodi i nadzire sprovođenje projekata IKT-a u institucijama Republike Kosovo;
- Podržava razvoj informacionih tehnologija, promoviše investicije u oblasti informacionog društva, razvoj sistema obuke u oblasti informacionih tehnologija, te koordinira, vodi i nadzire procese i mehanizme elektronske uprave u oblasti IT infrastrukture, širenja internet usluga. Vrši akumulaciju, administraciju, širenje i čuvanje podataka u Državnom elektronskom centru za podatke;
- Podrška razvoju bezbednosti i zaštite elektronske komunikacije i infrastrukture podataka, kao i borbi protiv kibernetičkog kriminala. Takođe upravlja i štiti intelektualnu svojinu i prava u vezi sa bazama podataka i softverom, koji su vlasništvo države, kao i štiti lične podatke u elektronskoj formi, u skladu sa važećim zakonodavstvom i pomaže pristup javnim informacijama u elektronskom obliku;
- U saradnji sa KIJA-om, identifikuje potrebe za elektronskom obukom informacionog društva za zaposlene u institucijama Republike Kosovo;
- Razmatra uslove za planirane projekte i prati njihovu realizaciju u skladu sa politikama i strategijom elektronske uprave;

- Koordinira aktivnosti za bezbednost elektronskih usluga.

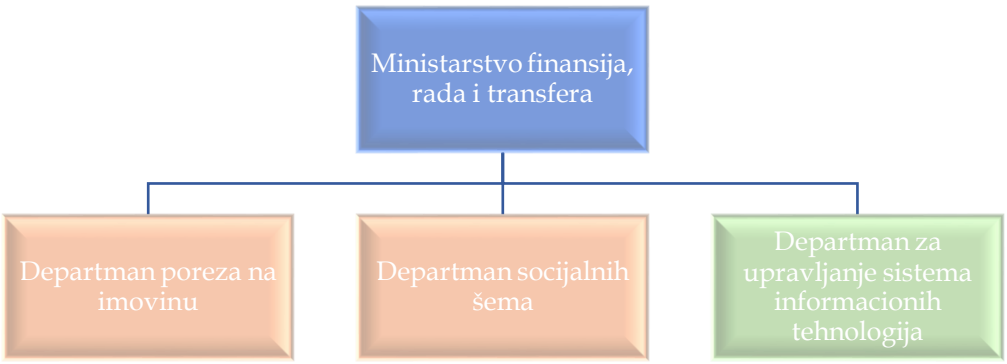
AID je organizovalo odgovornosti za razvoj ovih funkcija u pet direkcija, koje su predstavljene sa sledećom slikom:

Slika 7. Organizacija AID-a

Ministarstvo finansija, rada i transfera (MFRT), na osnovu Uredbe[33] o oblastima administrativne odgovornosti kancelarije premijera i ministarstava, ima nadležnosti za: pripremu, izradu, odobravanje, sprovođenje, procenu i nadzor javnih politika, izradu pravnih akata, izradu i usvajanje podzakonskih akata, utvrđivanje obaveznih standarda u oblasti javnih finansija i upravljanja porezima. U oblasti oporezivanja imovine, Ministarstvo obezbeđuje sprovođenje poreskog zakonodavstva i nadzire pravila za trošenje javnog novca, doprinoseći održivom fiskalnom i ekonomskom upravljanju.
Za dečje dodatke, MFRT obezbeđuje obračun i izvršenje socijalnih programa, uključujući koristi koje se odnose na porodične dodatke i dečje dodatke, u skladu sa važećim zakonodavstvom. To podrazumeva da ministarstvo ima centralnu funkciju u garantovanju finansijske podrške građanima, uključujući porodice sa decom, kao i na platformi e-Kosova upravlja i administrira podacima o uslugama koje ima ulogu i odgovornost, stoga je odgovorno i za veće usluge, kao što su služba poreza na imovinu i usluga dečjeg dodatka. MFRT ima 8 Agencije i 18 departmane, koji uključuju Departman za porez na imovinu, Departman za socijalne šeme i Departman za upravljanje sistemima informacione tehnologije.

[33] **Uredba (VRK) broj 06/2020 o oblastima administrativne odgovornosti Kancelarije premijera i ministarstava**

Nadležnosti ovih departmana će se fokusirati samo na usluge koje se pružaju putem platforme e-Kosova, a ne na osnovne sisteme kao što je porez na imovinu, već samo na uslugu u okviru e-Kosova, a ne na osnovni sistem poreza na imovinu.



Slika 8. Organizacija departmana MFRT-a koja su uključena u oblast delovanja

Delokrug i pitanja revizije

Obim ove revizije biće Agencija za informaciono društvo i nadležni departmani za administraciju, upravljanje i bezbednost platforme e-Kosova. Ministarstvo finansija, rada i transfera sa nadležnim departmanima za porez na imovinu i upravljanje socijalnim programima koji upravljaju relevantnim uslugama u e-Kosova za porez na imovinu i dečji dodatak.

U AID: Direkcija za racionalizaciju administrativnih procesa; Direkcija za razvoj i politike e-uprave; Direkcija za administraciju i razvoj elektronskih sistema; Direkcija za centralne službe i bezbednost; i Direkcija državne mreže.

U MFRT-u: Departman za porez na imovinu; Departman za socijalne šeme; i Departman za upravljanje sistemima informacione tehnologije.

Fokus revizije će biti informaciona bezbednost i kontrola aplikacija za sistem informacione tehnologije, platformu e-Kosova. Revizija će obuhvatiti period od januara 2024. godine do završetka revizije.

Pitanja o reviziji

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

1. *Da li su zahtevi za bezbednost informacija u ugovornim dokumentima za e-Kosova adresirani i da li su oni u skladu sa bezbednosnom politikom AID-a?*
2. *Kako AID identifikuje, određuje prioritete i upravlja svojim zahtevima za platformu e-Kosova?*
3. *Da li je unutrašnja i vanjska komunikacija informacionog sistema u e-Kosova bezbedna?*
4. *Da li je neovlašćeni pristup i umnožavanje ili uvid u osetljive informacije onemogućeno u e-Kosova?*

5. *Da li postoji efikasna politika kontinuiteta poslovanja u AID?*
6. *Da li se procenjuje da li su podaci uneseni prilikom pristupa aplikaciji validni u bazi podataka i od strane ovlašćenog osoblja na platformi e-Kosova?*
7. *Da li aplikacija e-Kosova obezbeđuje integritet, validnost i pouzdanost transakcija tokom ciklusa obrade podataka?*
8. *Da li je obezbeđeno da je izlaz informacija na e-Kosova potpun i tačan pre dalje upotrebe i da li se čuva na odgovarajući način?*
9. *Da li su informacije u aplikaciji e-Kosova bezbedne od zloupotrebe?*

Kriterijumi revizije[34]

Kriterijumi koji se koriste u ovoj reviziji su izvedeni iz Aktivnog priručnika za reviziju IT-a[35]; Međunarodni standardi za bezbednost informacija[36], kao i Uredba o koordinaciji između AID-a i IRK-a[37].

U cilju procene identifikacije potreba i adresiranja zahteva bezbednosti informacija u ugovoru o razvoju sistema e-Kosova utvrđeni su sledeći kriterijumi:

- Bezbednosni zahtevi organizacije moraju biti istaknuti od strane ugovarača na odgovarajući način.[38]

  Sporazum sa spoljnim stranama koji uključuje pristup, obradu, komunikaciju ili upravljanje informacijama ili strukturom za obradu informacija organizacije, ili uvođenje proizvoda ili usluga u sistem za obradu informacija, u skladu je sa svim relevantnim bezbednosnim zahtevima.[39]

U cilju procene identifikacije potreba i odgovora na uslove za nabavku i izradu ugovora za razvoj sistema e-Kosova, utvrđeni su sledeći kriterijumi:

- AID mora analizirati, odrediti prioritete i upravljati zahtevima kako bi se osiguralo da su potrebe korisnika zadovoljene optimalno i efektivno.[40]

Da bi se procenilo da AID ima mehanizme za informacionu bezbednost i kontinuitet biznisa, utvrđeni su sledeći kriterijumi:

- AID mora da obezbedi da postoje definisane politike za bezbednost informacija i da su usvojene, saopštene i sprovedene u organizaciji.

[34] Za više informacija konsultovati ISSAI 300, Criteria, p.7
[35] Priručnik za reviziju informacione tehnologije je proizvod EUROSAI-t (WGITA) radnih grupa za informacione tehnologije (WGITA), kao i INTOSAI razvojne inicijative (IDI) za definisanje pravila i standarda revizije informacionih tehnologija.
[36] Sistem upravljanja bezbednošću informacija ISO/IEC 27000/01.
[37] Uredba (VRK) br. 02/2016 za koordinaciju između Agencije informacionog društva i organizacione strukture/zvaničnici informacione i komunikacione tehnologije u institucije Republike Kosova.
[38] Priručnik za reviziju informacionih tehnologija – ugovaranje, bezbednost.
[39] ISO 27001 – Politike bezbednosti informacije.
[40] Priručnik za reviziju informacionih tehnologija – Nabavka i razvoj.

Politike treba redovno pregledavati ili kada postoje značajne promene u organizaciji, tehnologiji ili važećim zakonima.[41]
Politike i procedure treba da formiraju stabilno upravljačko okruženje za unutrašnje i vanjske komunikacije.[42]

- Organizacija mora osigurati da se upadi otkriju i da će biti otkriveni i boriti.[43]
  Organizacija mora da obezbedi odgovarajuće mere za sprečavanje, otkrivanje i oporavak od pretnji zlonamernog koda kroz politike, tehničke kontrole i svest korisnika.[44]
  Agencija za informaciono društvo treba da vodi računa o bezbednosti i zaštiti elektronske i podatkovne infrastrukture i koordinira aktivnosti za bezbednost IT usluga.[45]

- Organizacija mora imati organizacione politike o kontinuitetu biznisa, koje sadrže dužnosti i odgovornosti, svrhu, kriterijume/principe raspodele resursa, zahteve za obuku, raspored održavanja, raspored testiranja, rezervne planove, kao i nivoe odobrenja.[46]
  Organizacija mora imati plan za održavanje i obnavljanje biznisa, kako bi se osigurala dostupnost informacija na potrebnom nivou i u određeno vreme nakon prekida ili neuspeha procesa biznisa. Ovaj plan treba da identifikuje rizike sa kojima se suočava organizacija, identifikuje kritičnu poslovnu imovinu, identifikuje uticaje incidenata, razmotri sprovođenje dodatnih preventivnih kontrola i dokumentuje planove kontinuiteta biznisa uz rešavanje bezbednosnih zahteva. Mora osigurati da plan uključuje identifikaciju i odobravanje odgovornosti, utvrđivanje prihvatljivog gubitka, sprovođenje procedura oporavka i restauracije, dokumentovanje procedura i redovno testiranje.[47]
  Državni registri i elektronske usluge IRK-a moraju biti hostovani u CDP-u ili u njihovim centrima za podatke, ali pod uslovom da imaju rezervnu kopiju (backup) u CDP-u. Rezervne kopije aplikacija i baza podataka vrše se u skladu sa standardnim operativnim procedurama i moraju se čuvati u poverenju prema zakonu.[48]

41 ISO/IEC 27002:2022 – Politike za bezbednost informacije.
42 Priručnik za reviziju informacione tehnologije - Informacije i kibernetička bezbednost, komunikacije i upravljanje operacijama.
43 Priručnik za reviziju informacione tehnologije – Sistem za zaštitu od kibernetičke informacije i bezbednosti, detekcije i upada.
44 ISO 27001 – Kriterijumi za zaštitu od zlonamernog koda (malware).
45 Uredba (VRK) br. 02/2016 za koordinaciju između Agencije informacionog društva i organizacione strukture/zvaničnici informacione i komunikacione tehnologije u institucije Republike Kosova.
46 Priručnik za reviziju informacione tehnologije – PVB-PRF, Politika i plan kontinuiteta biznisa organizacije.
47 ISO 27001 – Upravljanje kontinuitetom biznisa.
48 Uredba (VRK) br. 02/2016 za koordinaciju između Agencije informacionog društva i organizacione strukture/zvaničnici informacione i komunikacione tehnologije u institucije Republike Kosova.

Da bi se procenilo da postoje mehanizmi kontrole aplikacija za platformu e-Kosova, koji omogućavaju siguran, logičan (softverski) i pouzdan pristup informacionom sistemu, utvrđeni su sledeći kriterijumi:

- Pravila validnosti moraju biti dobro dizajnirana, dokumentovana i sprovedena u ulaznoj interakciji; moraju biti dokumentovani različiti načini unosa podataka; nevažeći podaci moraju biti pravilno odbačeni od strane aplikacije; kriterijumi validnosti se ažuriraju na odgovarajući i ovlašćeni način; sveobuhvatne kontrole kao što su pravila registracije i ovlašćenja treba da postoje u slučaju da su moguće osnovne kontrole ulaska; Postoje odgovarajuće kontrole i dokumentacija za unose aplikacije.[49]

- Za ulazne podatke u aplikaciji mora postojati jasan i kompaktan sistem za rukovanje greškama predstavljanjem vrste problema kako bi se preduzele korektivne mere za bilo koju vrstu greške. Greške moraju biti ispravljene na odgovarajući način pre obrade transakcija. Registracije treba periodično pregledati i preduzeti neophodne korektivne mere.[50]

  Agencija podržava i koordinira aktivnosti između IRK-a kako bi relevantne baze podataka/registri međusobno komunicirali.[51]

- Aplikacija mora imati postavljene nivoe autorizacije transakcija i mora se sprovoditi kroz različite kontrole; trebalo bi da postoji precizna podela zadataka za unos podataka; Imati kompenzacione kontrole za slučajeve u kojima podela zadataka nije moguća.[52]

- Transakcije aplikacije moraju biti izvršene u skladu sa očekivanim ponašanjem.[53]

  Transakcije aplikacije moraju biti izvršene na kontrolisan i pouzdan način, osiguravajući da su u skladu sa poslovnim pravilima, parametrima konfiguracije i očekivanim scenarijima obrade.[54]

- Organizacija mora imati uspostavljene procedure kako bi se osiguralo da je potpunost i tačnost rezultata aplikacija procenjena pre upotrebe rezultata iz dalje obrade, uključujući obradu krajnjeg korisnika; omogućiti praćenje rezultata aplikacije; rezultat treba pregledati za razumnost i tačnost; kontrole kompletnosti i tačnosti da budu efikasne.[55]

- Mora postojati dovoljno revizijskih tragova koji obuhvataju modifikacije, ovlašćene registracije kritičnih transakcija; revizijski tragovi se periodično pregledavaju kako bi se pratile nenormalne aktivnosti; revizijski tragovi se održavaju i čuvaju na odgovarajući način; Jedinstveni i sekvencijalni brojevi ili identifikatori moraju biti definisani za svaku transakciju.[56]

[49] Priručnik za reviziju informacione tehnologije – kontrole aplikacije, kontrole pristupa.
[50] Priručnik za reviziju informacione tehnologije – kontrole aplikacije, kontrole pristupa.
[51] Uredba (VRK) br. 02/2016 za koordinaciju između Agencije informacionog društva i organizacione strukture/zvaničnici informacione i komunikacione tehnologije u institucije Republike Kosova.
[52] Priručnik za reviziju informacione tehnologije – kontrole aplikacije, kontrole pristupa.
[53] Priručnik za reviziju informacione tehnologije – kontrole aplikacije, kontrole izrade.
[54] Korišćenje COBIT smernica (posebno DSS05 i BAI09) za kontrolu procesa i obezbeđivanje pouzdanost obrade transakcija.
[55] Priručnik za reviziju informacione tehnologije – kontrole aplikacije, kontrole izlaznih podataka.
[56] Priručnik za reviziju informacione tehnologije – kontrole aplikacije, kontrole bezbednosti aplikacija.

- Podaci o aplikaciji moraju biti zaštićeni u skladu sa bezbednosnim standardima i priručnikom za reviziju IT-a. Efikasne logičke i fizičke kontrole pristupa, kao što je definisano u domainu o bezbednosti informacija, moraju se sprovesti kako bi se osigurala autentifikacija, autorizacija i praćenje pristupa. Takođe, aplikacija mora imati dokumentovani plan oporavka od katastrofe, uključujući sigurne mehanizme za backup-a i oporavak, prema domenu na PVB/PRF. Planovi za bezbednost i oporavak treba redovno testirati kako bi se osigurao kontinuitet biznisa i zaštita informacije.[57]

Metodologija revizije

Da bismo odgovorili na pitanja revizije i podržali zaključke revizije, primenićemo sledeću metodologiju:

U cilju procene identifikacije potreba i odgovora na zahteve bezbednosti informacije iz ugovora o platformi e-Kosova, biće realizirano:

- Pregled ugovornih dokumenata. Pregled prvobitnog ugovora za razvoj platforme e-Kosova, važećeg ugovora o održavanju i unapređenju platforme e-Kosova, kao i tenderskog dosijea sa konkretnim uslovima. Takođe, revizija politika i procedura AID-a za bezbednost informacije.

U cilju procene identifikacije potreba i adresiranja i prioritizacije zahteva građana u ugovorima o platformi e-Kosova, realizira se:

- Pregled zahteva da bi se utvrdilo da li uključuju autora, datum, prioritet, troškove, rizik i druge elemente. Pregledajte i analizirajte zahteve ili komentare na zahteve vlasnika biznisa – Vlade, donosioca odluka ili zainteresovanih strana kako bi se utvrdilo da li su svi stavovi prikupljeni i sažeti za odgovarajuću analizu (prihvatanje, odlaganje, odbijanje, itd.). Pregled matrice sledljivosti da bi se utvrdilo da li su odobreni zahtevi dodeljeni razvojnim projektima i da li se prate do završetka kada se sprovode. Pregled kriterijuma za određivanje prioriteta zahteva kako bi se procenilo da li uključuju elemente kao što su troškovi, osnovne potrebe građana, hitna pitanja i novi zahtevi.

Da bi se procenilo da postoje mehanizmi za informacionu bezbednost i kontinuitet biznisa platforme e-Kosova, realizira se:

- Analiziranje politika i procedure organizacije da li odgovaraju potrebama građana upoređujući ih. Verifikacija načina na koji organizacija dokumentuje svoje procedure i kako ih čine dostupnim svim korisnicima. Intervjuisanje osoblja različitih nivoa kako bi se ispitalo da li su sve procedure za obrađivanje podataka poznate zaposlenima. Provera koliko često se pregledaju i ažuriraju procedure za obrađivanje podataka i komunikacija. Pregled strategije kibernetičke bezbednosti, ako postoji, i osigurati da pokriva zaštitu kritičnih sredstava.
- Verifikacija propisa za tretman fizičkih intervencija u prostorima u kojima se nalazi oprema. Analiziranje izveštaja o incidentima. Kao i identifikovanje da organizacija ima jasnu politiku za sprečavanje neovlašćenog pristupa.

[57] Priručnik za reviziju informacione tehnologije – kontrole aplikacije, kontrole bezbednosti aplikacija.

- Pregled dokumenata kako bi se procenili da li su politike usklađene sa opštim politikama IT- a i adresiraju zahteve kontinuiteta biznisa. Vođenje intervjua sa osobljem kako bi se videlo koliko često se ažuriraju politike. Proverite politike o tome kako su odobrene i da li su ažurne, kao i proceniti da li su ove politike razumljive osoblju.

Da bi se procenilo da platforma e-Kosova ima mehanizme kontrole aplikacija koji omogućavaju bezbedan, logičan i pouzdan pristup informacionom sistemu, realizira se:

- Analiziranje pravila, zahteva, dokumentacije o aplikaciji i intervjuisanje nadležnih osoba poslovnih procesa kako bi se utvrdilo koja pravila važenja treba obezbediti u poslovnom procesu koji se procenjuje. Pregledajte da li su pravila validnosti dobro izrađena i dokumentovana. Provera da li su provere validnosti za dolazne podatke na mestu, izvršenje aplikacije u okruženju za testiranje, i testiranje različitih interakcija za dolazne podatke.
- Tretiranje grešaka u aplikaciji sa svojim programerom ili administratorom. Verifikacija i potvrda da li postoje politike i procedure za tretiranje transakcijama koje ne uspevaju u proveri modifikacije i validnosti. Verifikacija da li sistem daje poruke za bilo koju vrstu greške (na nivou polja ili transakcije), poruke koje ne mogu da odgovaraju validnosti ili modifikacije. Verifikacija kako aplikacija funkcioniše ako su podaci odbijeni dolaznim proverama. Provera da li su elementi podataka prijavljeni ili da li su automatski popunjeni.
- Inspekcija i potvrda da li dizajniranje sistema obezbeđuje ovlašćenu listu za upotrebu. Verifikacija kroz inspekciju liste ovlašćenja, da su nivoi ovlašćenja dobro definisani za svaku grupu transakcija. Procena da li su pravila ovlašćenja za postavljanje podataka, modifikacija, prihvatanje, odbijanje i zloupotreba su dobro izrađeni i definisani. Ako postoji tabela za podelu zadataka, način na koji se distribuiraju glavni zadaci i radne funkcije, kao i dozvoljene transakcije, a zatim analiziramo listu korisnika i listu privilegija korisničkih pristupa.
- Usluge koje se nude na platformi su identifikovane i grupisane prema važnosti usluge koju nudi. Pregledati dokumentaciju platforme da bi se proverili da li je odgovarajuća, obezbeđuje integritet i pouzdanost tokom ciklusa obrade transakcija.
- Kontrolna lista dolaznih podataka se kreira ako postoji bilo kakav prethodni pregled za pružene usluge. Identifikacija da li je za određene usluge sistem e-Kosova povezan sa osnovnim sistemima i potvrđuje podatke iz krajnjeg sistema. Procena da li su odlazne informacije nakon obrade u sistemu e-Kosova tačne i potpune i da li su prikazane identifikovane greške.
- Analiziranje i pregled politika i procedura za održavanje revizijskih tragova i kako ih verifikovali. Verifikacija revizijskih tragova i drugih dokumenata kako bi se proverilo da li je revizijski trag efikasno uspostavljen. Identifikacija ko su lica ovlašćena da opozove ili izbriše revizijske tragove. Obezbeđivanje da je pristup revizijskim tragovima ograničen i da im mogu pristupiti samo ovlašćena lica. Procena da li su tragovi zaštićeni od modifikacija i da li postoje jedinstveni identifikatori za svaku transakciju. Procena da li platforma e-Kosova ima neophodan integritet i kredibilitet.
- Pregled i analiziranje dokumentacije platforme da biste videli da li su informacije o platformi sigurne protiv zloupotrebe. Intervjuisanje IT osoblja da vidimo kako oni razumeju bezbednosne mehanizme sprovedene u aplikaciji.

Relevantni dokumenti

Zakoni
Zakon br. 04/L-145 za vladine o udruženju informisanja

Ovaj Zakon utvrđuje nadležne institucije, funkcije i njihovu odgovornost u vezi razvoja i sprovođenja informativne tehnologije u institucijama Republike Kosova, osnivanje Agencije za Udruženje Informacije, kao i konsolidacija funkcija i odgovornosti u oblasti sprovođenja informacione tehnologije i komuniciranje (ITK).

Zakon (06/L-005) - o porezu na nepokretnu imovinu
Ovim zakonom utvrđuje se porez na nepokretnu imovinu kao i pravila i osnovne procedure za upravljanje nepokretnom imovinom od strane opština i Ministarstva za finansije. Odredbe ovog zakona su obavezujuće za sve institucije i njihove odgovarajuće jedinice koje su odgovorne za sprovođenje ovog zakona, za lica koja su obveznici poreza na imovinu, kao i za druga lica koja su dužna da izvrše zakonske obaveze u smislu odredaba utvrđenih ovim zakonom.

Uredbe
Uredba broj 02/2016 za koordinaciju između Agencije informacionog društva i organizacione strukture/zvaničnici informacione i komunikacione tehnologije u institucije Republike Kosova

Sa ovim uredbe odlučuju se standardi, način funkcionisanje i koordinacija aktivnosti između Agencija za Informaciono Društvo i struktura zvaničnici IKT-a i IRK.
Nadzornik za sprovođenje ove uredbe je AID.

Uredba (MJU) broj 02/2015 o standardima, softuerima i harduere

Cilj ove uredbe je određivanje standarda za korišćenje softvera i hardvera od strane službenika institucija Republike Kosova.
Ova uredba je takođe definisala nabavku, instalaciju i korišćenje licenci koje koriste IRK.

Uredba br. 06/2018 za upravljanje projekta u oblasti informacione tehnologije i komunikacije

Svrha ove Uredbe je određivanje standarda i uredbi jedinstveni za institucije Republike Kosovo u vezi iniciranja, planiranja, egzekutivan, upravljanja kontrole, kao i zatvaranja procesa upravljanja projekata u oblasti Informacioni Tehnologije i Komuniciranja (u daljem tekstu: ITK).

Uredba (VRK) br. 06/2020 o oblastima administrativne odgovornosti Kancelarije premijera i ministarstava
Ova uredba određuje oblasti administrativne odgovornosti Kancelarije premijera i Ministarstava u Vladi Republike Kosovo =.

Uredba (KP) br. 02/2023 o unutrašnjoj organizaciji i sistematizaciji radnih mesta u Ministarstvu finansija, rada i transfera

Ova Uredba ima za cilj da definiše unutrašnju organizaciju i sistematizaciju radnih mesta u Ministarstvu finansija, rada i transfera.

Prilog II. Pismo potvrde

Republika e Kosovës

Republika Kosova-Republic of Kosovo

Qeveria - Vlada - Government

Ministria e Financave, Punës dhe Transfereve

Ministarstvo Finansija, Rada i Transfera - Ministry of Finance, Labour and Transfers

DATË/A:	22.08.2025
REFERENCË:	/ 2024
PËR/ZA/TO:	z. Samir Zymberi, Drejtor i Departamentit të Auditimit të Teknologjisë Informative, Zyra Kombëtare e Auditimit
NGA/OD/FROM:	z. Arton Ahmeti, Sekretar i Përgjithshëm i Ministrisë së Financave, Punës dhe Transfereve
TEMA/SUBJEKAT/SUBJECT:	Letër konfirmimi për pajtueshmërinë me gjetjet e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit Platforma e Shërbimeve online e-Kosova

I nderuar z. Zymberi,

Përmes kësaj, konfirmojmë se:

- Kemi pranuar draft Raportin e Zyrës Kombëtare të Auditimit për raportin e auditimit të teknologjisë së informacionit Platforma e Shërbimeve online e-Kosova (në tekstin e mëtejmë "Raporti");
- Lidhur me të gjeturat dhe rekomandimet e dhëna pajtohemi, dhe nuk kemi ndonjë koment shtesë për përmbajtjen e Raportit;
- Ju njoftojmë se brenda 30 ditëve nga pranimi i Raportit përfundimtar, do t'ju dorëzojmë një plan të veprimit për zbatimin e rekomandimeve të dhëna, i cili do të përfshijë edhe afatet kohore dhe stafin përgjegjës për zbatimin e tyre.

Me respekt,

Arton Ahmeti

Sekretar i Përgjithshëm i Ministrisë së Financave, Punës dhe Transfereve

1

Republika e Kosovës

Republika Kosova-Republic of Kosovo

Qeveria –Vlada-Government

Ministria e Punëve të Brendshme-Ministarstvo Unutrašnjih Poslova-Ministry of Internal Affairs

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit **Platforma e shërbimeve online e-Kosova,** dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data: 31.07.2025

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **Platforma e shërbimeve online e-Kosova** (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.

Ministri//Kryetari//Kryeshefi Ekzekutiv/Drejtori i Përgjithshëm

z. Xhelal Svecla
Ministër në detyrë i Punëve të Brendshme

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