Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

Izveštaj Revizije
Informacione Tehnologije

Informacioni Sistem Carine Kosova - ASYCUDA World

Priština, decembar 2024

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

Nacionalna Kancelarija Revizije je nezavisna institucija koja pomaže Generalnom Revizoru u obavljanju njegovih/njenih dužnosti. Naša misija je da efikasno doprinesemo odgovornosti javnog sektora kroz kvalitetne revizije, promovišući javnu transparentnost i dobro upravljanje, i promovišući ekonomičnost, efektivnost i efikasnost vladinih programa za dobrobit svih. Na ovaj način uvećavamo poverenje u trošenje javnih sredstava i igramo aktivnu ulogu u obezbeđivanju interesa poreskih obveznika i drugih interesnih strana za povećanje javne odgovornosti. Generalni Revizor izveštava Skupštini za vršenje dužnosti i ovlašćenja definisanih Ustavom, Zakonom, podzakonskim aktima i međunarodnim standardima revizije javnog sektora.

Ova revizija je obavljena u skladu sa Međunarodnim Standardima Vrhovnih Revizorskih Institucija (SNISA 3000[2]) i Uputstva za Reviziju Informacionih Sistema (GUID 5100[3]).

Revizije informacione tehnologije koje sprovodi Nacionalna Kancelarija Revizije su provera i pregled Informacione Tehnologije i određenih kontrola kako bi se stekla sigurnost o principu zakonitosti, efikasnosti[4], ekonomičnosti[5], i efektivnosti[6] sistema informacione tehnologije i određenih kontrola.

Generalna Revizorka je odlučila u vezi sa ovom revizijom „ Informacioni Sistem Kosovske Carine – ASYCUDA World „ uz konsultaciju Pomoćnika Generalne Revizorke Myrvete Gashi Morina koja je nadgledala reviziju.

1 Zakon 05_L_055 o Generalnom Revizoru i Nacionalnoj Kancelariji Revizora Kosova
2 SNISA 3000 – Standardi i uputstva za reviziju učinka na osnovu Standarda Revizije ONISA -e i praktično iskustvo
3 GUID 5100 – Priručnik za reviziju informacionih sistema izdat od INTOSAI
4 Efikasnost – Načelo efikasnosti podrazumeva uzimanje maksimuma od raspoloživih resursa, radi se o povezanosti među angažovanih resursa i datih rezultata u smislu količine, kvaliteta i vremena
5 Ekonomičnost - Načelo ekonomičnosti podrazumeva minimizovanje cene resursa. Korišteni resursi trebaju biti raspoloživi s vremenom, potrebnoj količini i kvalitetu i najboljom cenom.
6 Efektivnost – Načelo efektivnosti podrazumeva postizanje određenih objektiva i postizanje očekivanih rezultata.

Tim koji je realizovao ovaj izveštaj:

Samir Zymberi, Direktor Odeljenja revizije;
Poliksena Berisha , Vođa tima;
Gazmend Lushtaku, član tima;
Besim Lezi, Član Tima; i
Naim Neziri, Član tima.

ZYRA KOMBËTARE E AUDITIMIT – Adresa:Rr. Ahmet Krasniqi nr. 210, Lagjja Arbëria,
Prishtinë 10000, Kosovë
Tel: +383(0) 38 60 60 04/1011
http://zka-rks.org

Tabela sadržaja

Lista skraćenica

NISP	Napredni Informacioni Sistem Putnika (Advanced Pasanger Information System)
PP	Privremen Prijem (Admission Temporaire -Temporary Admission)
CSAW	Carinski Sistem (ASYCUDA World)
EU	Evropska Unija
TRPK	Tehnike revizije uz pomoć kompjutera (Computer assisted audit techniques)
KFP	Kancelarija za Fiskalnu Pomoć (Customs and Fiscal Assistance Office)
CESST	Centralno Evropski Sporazum o Slobodnoj Trgovini (Central European Free Trade Agreement)
OATPP	Odeljenje Akcize, Tarife, Porekla i Procedura
CK	Carina Kosova
OGD	Operativna i Granična Direkcija
PIS	Pravo Intelektualne Svojine
OCS	Odeljenje Carinskih Sistema
DZU	Direkcija Zajedničkih Usluga
JCD	Jedinstveni Carinski Dokument
DSZ	Direkcija Sprovođenja Zakona
SUS	Sistem Upravljanja Sadržaja (Enterprise Content Management)
ERP	Elektronska Razmena Podataka (Electronic Data Interchange)
MOVS	Međunarodna Organizacija Vazdušnog Saobraćaja (International Air Transport Association)
MOCA	Međunarodna Organizacija Civilne Avijacije (International Civil Aviation Organisation)
ICSI	Integrisani Carinski Sistem Informacija (Integrated Customs Information System)
SIP	Softver Intelektualnih Prava (Software for Intellectual Rights)
EK	Evropska Komisija
SSZ	Sistem Sprovođenja Zakona (Law Enforcement System)
MJA	Ministarstvo Javne Administracije
ME	Ministarstvo Ekonomije
MFRT	Ministarstvo Finansija, Rada i Transfera
MIPT	Ministarstvo Industrije, Preduzetništva i Trgovine

STO	Svetska Trgovačka Organizacija
OEO	Ovlašćen Ekonomski Operator
KJI	Ključna Javna Infrastruktura (Public Key Infrastructure)
PON	Plan Oporavka od Nesreće
PKP	Plan Kontinuiteta Poslovanja
URI	AW Upravljanje Rizikom i Izbor (AW Risk- Management & Selectivity)
GIR	Godišnji Izveštaj Revizije
SAW	Sektor ASYCUDA World
SREP	Sistematska Razmena elektronskih podataka (Systematic Electronic Exchange of Data)
SPO	Sektor Procedura i Ovlašćenja
SPIT	Sektor Podrške Informacione Tehnologije
SRM	Sektor Rizika i Monitoringa
ITK	Integrisana Tarifa Kosova
DMT	Drumski Međunarodni Transport (Transports Internationaux Routiers)
PDV	Porez na Dodatnu Vrednost
KUNTR	Konferencija Ujedinjenih Nacija za Trgovinu i Razvoj (UN Trade and Development)
SCO	Svetska Carinska Organizacija (WCO World Customs Organisation)
PZJ	Proširen znakovni jezik (Extensible Markup Language)

Opšti Sažetak

Carina Kosova je agencija za upravljanje prihodima u okviru Ministarstva Finansija, Rada i Transfera. Prihodi prikupljeni od strane Carine doprinose oko 60% ukupnih prihoda prikupljenih za budžet Republike Kosovo. Carina Kosova ima široku misiju, počev od zaštite države, privrede i građana.

U cilju što efikasnije realizacije svoje misije, Carina Kosova je digitalizovala svoje procese razvojem i primenom informacionih sistema. ASYCUDA World je osnovni sistem Carine Kosova, koji se proteže na carinarnice, kapije, granične prelaze i slobodne zone. Glavna uloga ovog sistema je upravljanje carinskim procedurama za carinjenje robe, kao i upravljanje svim vrstama budžetskih prihoda, odnosno oko 1,5 milijardi evra godišnje koje trenutno prikuplja Carina Kosova.

Nacionalna Kancelarija Revizije je sprovela reviziju Informacione Tehnologije da proceni da li sistem ASYCUDA World omogućava Carini Kosova da sprovede elektronske carinske procese na tačan, bezbedan i pouzdan način.

Carina Kosova je kontinuirano razvijala sistem ASYCUDA World kako bi osigurala digitalizaciju carinskih procesa i poboljšala sigurnost i tačnost podataka i procesa koji se sprovode kroz ovaj sistem i sigurnost samog sistema. Takođe je implementirala sporazum za sistem ASYCUDA, koji se odnosi na promociju rodne ravnopravnosti.

Kosovska carina ima nedostatke u politici ugovaranja, pošto se nije bavila zaštitom bezbednosti informacija u sporazumima-ugovorima koje imaju sa spoljnim stranama, stoga u slučaju incidenata sajber bezbednosti odgovornost strana u projektu za sistem ASYCUDA nije definisano.

Kontrole koje se sprovode za zaštitu informacione bezbednosti u Carini Kosova ne garantuju u dovoljnoj meri integritet, poverljivost i dostupnost sistema, pošto politike bezbednosti informacija nisu ažurirane, postoje nedostaci u organizaciji strukture osoblja, koncentracija i sukob odgovornosti u vezi sa bezbednošću

informacija i nedostacima u upravljanju pristupom informacionim sistemima. Kao i nedostatak obuke za podizanje svesti osoblja u vezi sa bezbednošću informacija.

Carina nije obezbedila dovoljne mehanizme za kontinuitet poslovanja, nedostaje plan i struktura za operacionalizaciju plana, kao i pisane procedure za kontinuitet poslovanja. U nedostatku ovih mehanizama, kontinuitet poslovanja je ugrožen u slučaju bilo kakve katastrofe, gubitka, oštećenja podataka i sistema, kao i otpuštanja ključnih kadrova.

Kontrole aplikacije implementirane u ASYCUDA ne osiguravaju da se samo ispravni i validni podaci postavljaju i ažuriraju u sistemu. Budući da se neki procesi i dalje sprovode manuelno, kao što je obračun koeficijenta za određivanje cene nakon ponovne procene; procena rizika kroz kriterijume koji su postavljeni samo u tekstualnom obliku, ne ostavljajući mogućnost merenja.

Ne potvrđuje polja za registraciju ličnog/poslovnog broja i žiga u odsustvu veza sa drugim sistemima. Kao i dizajn nekih od modula za korisnike sektora za procenu rizika i naknade nije jednostavan i pogodan za korisnika.

Stoga, rizici identifikovani u politikama ugovaranja, bezbednosti informacija, kontinuitetu poslovanja i kontrolama primene, ukazuju na to da Carini Kosova, koja administrira i koristi sistem ASYCUDA, treba poboljšanja kako bi podaci u ovom sistemu bili zaštićeni i digitalizovani carinski procesi da ne bi bili prekinuti. S tim u vezi, dali smo 13 preporuka za Carinu Kosova. Lista preporuka je predstavljena u Poglavlju 5 ovog izveštaja.

Odgovor entiteta

Carina Kosova se složila sa nalazima i zaključcima revizije i obavezala se da će primeniti date preporuke.

UVOD

01

1. Uvod

Carina Kosova (CK) je razvijena na osnovu standarda EU i finansira se iz Budžeta Kosova, ona je glavna u doprinosu u pogledu prikupljanja prihoda i zaštite svojih građana od zabranjene i ograničene robe.

Informacioni sistem koji je razvila Konferencija Ujedinjenih Nacija za Trgovinu i Razvoj (UNCTAD), ASYCUDA World je osnovni sistem Carine Kosova, kreiran u avgustu 2011. godine i pušten u rad u septembru 2012. godine.

Ovo je najveći UNCTAD-ov program tehničke saradnje koji pokriva 102 zemlje širom sveta, uključujući Kosovo, Bosnu i Hercegovinu i Albaniju u našem regionu. Ukupni troškovi za implementaciju (sprovođenje) samo ASYCUDA sistema iznose 1.350.158 USD, bez opreme i infrastrukture. Sistem se proteže na carinarnice, kapije, granične prelaze i slobodne zone.

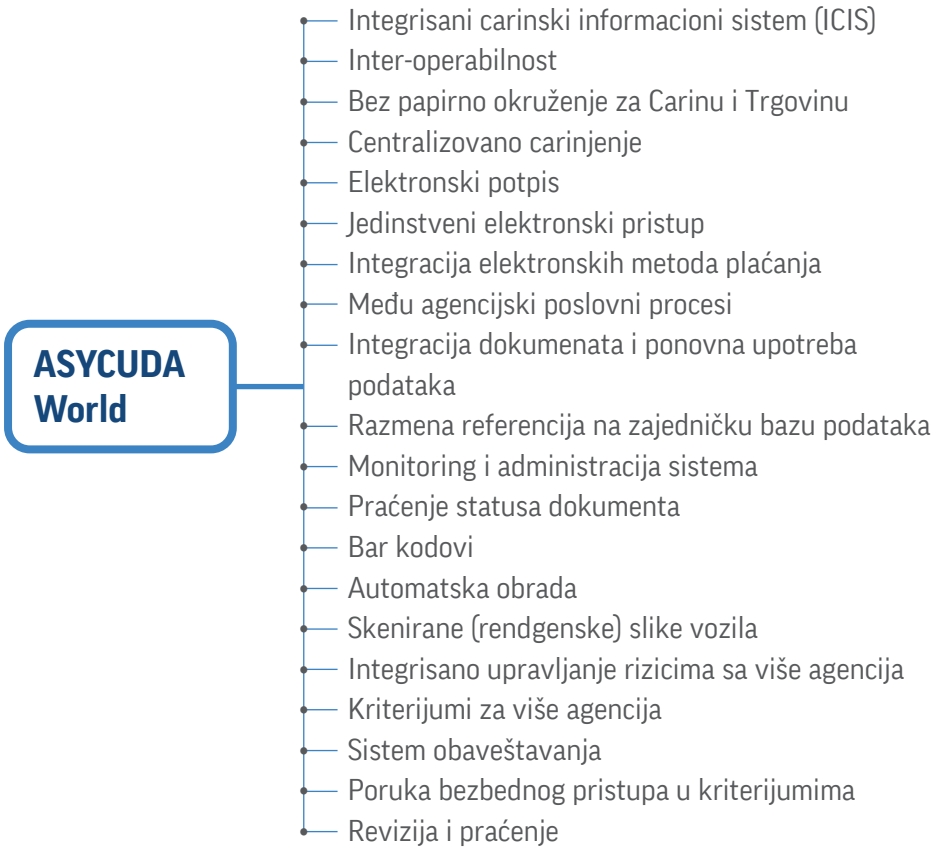
Automatizovani sistem carinskih podataka – ASYCUDA World (AW) je kompjuterizovani sistem upravljanja carinom koji pokriva većinu spoljnotrgovinskih procedura. AW se bavi carinskim manifestima[7] i deklaracijama, zajedno sa računovodstvenim, tranzitnim i carinskim postupcima suspenzije. AW generiše trgovinske podatke koji se mogu koristiti za statističku ekonomsku analizu. ASYCUDA koristi međunarodne kodove i standarde koje su razvili ISO (Međunarodna Organizacija za Standardizaciju), SCO (Svetska Carinska Organizacija) i Ujedinjene Nacije. ASYCUDA obezbeđuje elektronsku razmenu podataka (ERP) između trgovaca i carine koristeći preovlađujuće standarde, kao što je XML. U Carini Kosova ova platforma je u funkciji od 2012. godine sa svim svojim modulima i od tada do 2023. godine, preko ovog sistema, CK je uspela da prikupi preko

7 Carinski manifest je službeni dokument koji se koristi u carinskim postupcima da opiše teret robe koja se transportuje iz jedne zemlje u drugu. Ovaj dokument sadrži detaljne informacije o robi, uključujući njenu vrstu, količinu, vrednost, poreklo i odredište.

11 milijardi evra[8] uključujući automatske potvrde u realnom vremenu, koje od 45 minuta u 2011, sada traje 3 sekunde.

Najvažniji aspekti ovog sistema su sažeti u nastavku, a to su:

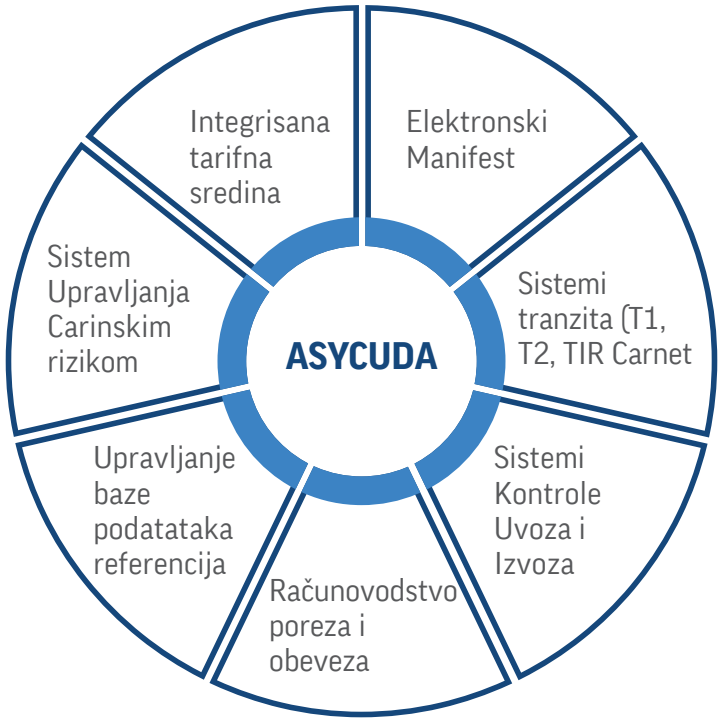
Figura 1. Najbitniji Aspekti sistema AW



Glavne funkcije integrisanog sistema upravljanja AW Carina, kroz koje se razvijajucarinski procesi, a koje su obuhvaćene tokom revizije su:

8 Interni dokument CK-a sa podacima iz carinskih sistema - Zahtev za odobrenje carinskih sistema kao državnih informaciono-komunikacionih sistema od strateškog značaja.

Figura 2. Glavne Funkcije ASYDUCA World



02

VIZIJE

CILJI OBLASTI

2. Cilj i oblasti revizije

Cilj ove revizije je da se oceni da li sistem ASYCUDA World omogućava Carini Kosova da primeni tačne, sigurne i poverljive elektronske procese.

Ovom revizijom želimo da ponudimo relevantne preporuke Carini Kosova, na način da se poboljša sistem informacija u vezi sa sigurnošću informacija i kontrole aplikacije.

Kako bi dali odgovore na cilj revizije, fokusirani smo na oblast bezbednosti informacije i kontrole aplikacije, kao i pitanja u vezi politika ugovaranja i kontinuiteta biznisa izabravši oblasti revizije kao u nastavku:

Tabela 2: Revizijske oblasti i pitanja

Oblasti revizije	Pitanja revizije
1. Ugovaranje	1. Politike Ugovaranja
	2. Bezbednost
2. Bezbednost Informacije i Kibernetička Bezbednost	3. Politike bezbednosti informacije
	4. Sigurnosna Struktura IT-a.
	5. Bezbednost IT-a Ljudskih Resursa
	6. Kontrole Pristupa
3. Plan Kontinuiteta Poslovanja –	7. Struktura Funkcije Kontinuiteta Poslovanja
4. Plan Oporavka od Nesreće[9]	
5. Kontrola Aplikacije	8. Kontrola Uvoda
	9. Kontrola prerade

Delokrug ove revizije je Carina Kosova i relevantna odeljenja za IT upravljanje, sistem ASYCUDA i carinske funkcije. Revizija obuhvata period od 2022. do 2024. godine.

9 PKP & PON – Plan Kontinuiteta Poslovanja& Plan Oporavka od Nesreće

03

ANALAZI VIZIJE

3. Nalazi revizije

Sistem Asycuda World koji je razvio UNCTAD i koristi Carina Kosova predstavlja važnu inovaciju u oblasti carinske administracije, modernizacije carinskih procedura i upravljanja na efikasniji i održiviji način. Ovaj sistem je dizajniran da pojednostavi i optimizuje procese koji se odnose na spoljnu trgovinu, uključujući carinske deklaracije, tranzitne operacije i obračun tereta. Preko ovog sistema podaci se čuvaju i upravljaju i izvršavaju procesi koji se odnose na vrednost od oko 60% državnih prihoda koji se prikupljaju putem digitalizovanih procedura koje obezbeđuje AW.

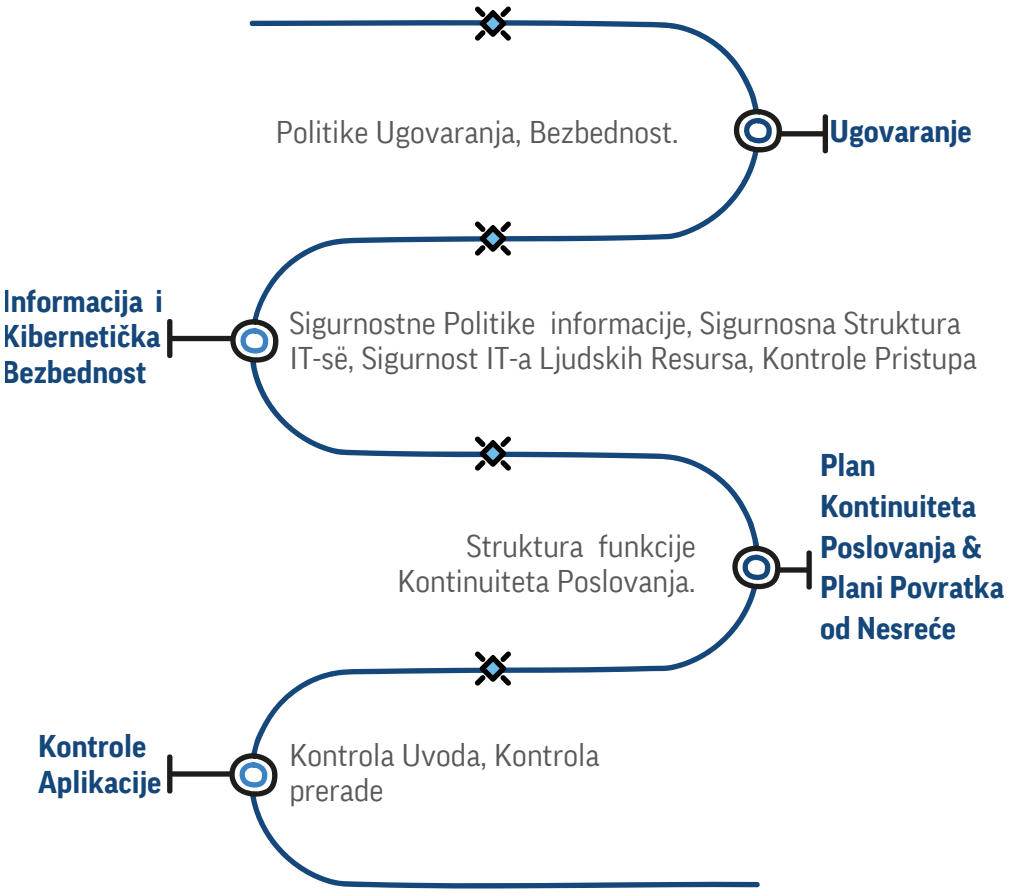
Jedna od glavnih prednosti ovog sistema je upotreba međunarodnih standarda, koji povećavaju nivo usklađenosti i saradnje između država i međunarodnih institucija. Sistem takođe podržava elektronsku razmenu podataka (ERP) sa CK, omogućavajući nesmetan protok informacija između uključenih strana. Ovo povećava tačnost podataka i eliminiše potrebu za fizičkim dokumentima, doprinoseći čistijem i ekološki prihvatljivijem procesu.

Pored toga, AW je dizajniran da digitalizuje i optimizuje procese, što direktno utiče na smanjenje vremena i troškova povezanih sa međunarodnom trgovinom. Ovo olakšava trgovinu i povećava poverenje preduzeća i trgovinskih partnera u efikasnost carinskih institucija.

U zaključku, implementacija AW sistema predstavlja važan korak ka modernizaciji globalne trgovine i jačanju lokalnih ekonomija, odnosno finansijske i administrativne održivosti.

Međutim, uporedo sa razvojem ovog sistema, postoje i nedostaci koji su prikazani u ovom poglavlju. Nalazi revizije se odnose na politiku ugovaranja i aktivnosti strana odgovornih za administraciju, bezbednost informacija i plan kontinuiteta poslovanja i kontrole primene ASYCUDA World Sistem u CK. Nalazi su strukturirani prema oblastima revizije i pitanjima.

Figura 3. Struktura pitanja revizije CK



Prvi deo predstavljen u poglavlju 3.1 pokriva identifikovana pitanja koja su potrebna za poboljšanje u vezi sa ugovaranje informacionih sistema (1).

Drugi deo koji je predstavljen u poglavlju 3.2 pokriva identifikovana pitanja vezana za informacionu i sajber bezbednost (2-5).

Treći deo koji je predstavljen u poglavlju 3.3 pokriva identifikovana pitanja u vezi sa planom kontinuiteta poslovanja i planom oporavka od nesreće (6).

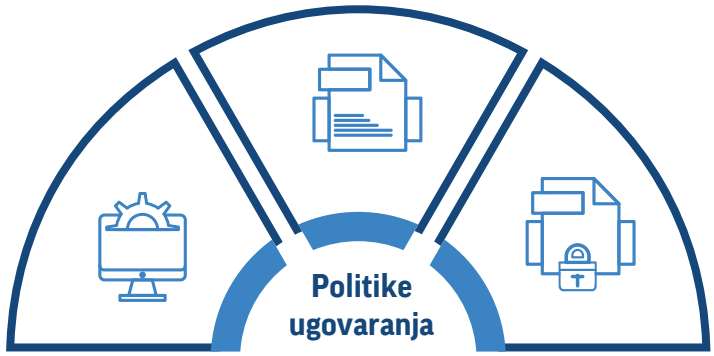
Četvrti deo koji je predstabljen u poglavlju 3.4 pokriva identifikovana pitanja u vezi sa kontrolama aplikacija (7-11).

3.1. Politike ugovaranja

Organizacije treba da imaju neke politike koje određuju koje funkcije se mogu ugovarati, a koje se moraju razvijati u prostorijama organizacije. Ugovaranje usluga organizaciji zahteva pažljivo praćenje i podleže zahtevima privatnosti i bezbednosti.

CK razvija ugovorne procese u skladu sa zakonima na snazi, ali postoje nedostaci u uključivanju bezbednosti informacija tokom ugovaranja.

Figura 4. Politike ugovaranja (Sistem, politike i bezbednost informacije)



1. Carina Kosova ima nedostatke u svojim politikama ugovaranja za razvoj i održavanje sistema ASYCUDA

Organizacija mora implementirati organizacione politike ugovaranja.[10] Izvođač mora da istakne bezbednosne zahteve organizacije na odgovarajući način u sporazumima sa spoljnim stranama.[11]
Carina Kosova mora da sprovede potpisani sporazum uključujući i član koji predviđa promociju rodne ravnopravnosti uz učešće zaposlenih žena u projektu.[12]

CK za razvoj AW sistema je 2011. godine potpisao ugovor sa UNCTAD-om u kojem su definisani uslovi za razvoj ovog sistema, ali iz analize dokumenata[13] i intervjua sa službenicima, uočili smo da CK to nije postigla da u ovom sporazum rešava zahteve za bezbednost informacija tako što ga ne uključuje u uslove osnovnog ugovora koji je zaključen 6. maja 2011. Za ugovaranje, se odnosi na zakon o nabavkama i procedure predviđene ovim zakonom, koji nije predviđena je posebna politika za bezbednost informacija, ali je opisana samo u opštem obliku. U 2Z017. godini, CK je izradila politike, procedure i standarde za bezbednost informacija, koje trenutno koristi, ali je nastavio da se ne bavi bezbednosnim pitanjima čak ni u tekućim ugovorima za održavanje i unapređenje AW sistema. Službenici odgovorni za AW sistem su ovaj nedostatak objasnili pristupom izvođača samo razvojnom okruženju, a ne stvarnom, ali smo primetili da baza podataka sadrži i stvarne podatke.

Međutim, CK je uspela da primeni zahteve za rodnu ravnopravnost, koji su predviđeni sporazumom sa UNCTAD-om. U sektoru ASYCUDA, koji se sastoji od tri službenika, dva su muška i jedna žena.

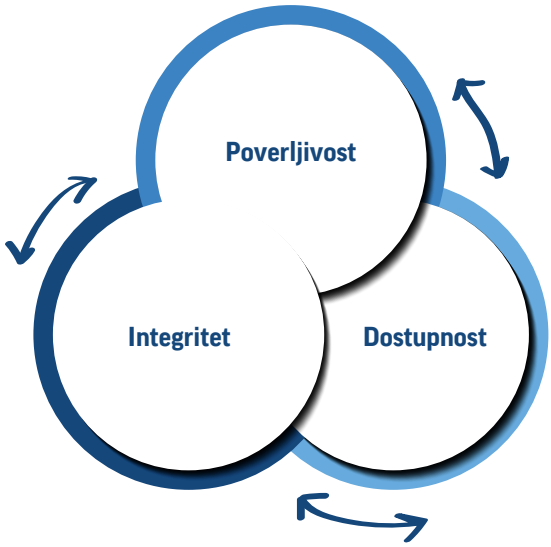
Nedostatak tretmana informacione bezbednosti i nedostaci u politikama ugovaranja informacione bezbednosti ugrožavaju bezbednost ugovorenih sistema i u slučaju bilo kakvog incidenta bezbednosti informacija ne postoji mogućnost da se identifikuje odgovornost strana u ugovoru, kao i praćenje i izveštavanje incident.

10 Priručnik Revizije Informacione Tehnologije - Ugovaranja, Bezbednost
11 ISO 27001 – Politike Bezbednosti Informacije.
12 Dodatak 2 Sporazum Između Carine Kosova i Konferencije Ujedinjenih Nacija za Trgovinu i Razvoj (UNCTAD), Mart 2023.
13 Ugovor potpisan između Vlade Republike Kosovo i Specijalizovane Agencije Ujedinjenih Nacija, UNCTAD; Ugovori o radu; Odluke direktora o premeštaju.

3.2. Bezbednost Informacije

Informaciona bezbednost je jedan od osnovnih aspekata IT upravljanja kako bi se osigurala dostupnost, poverljivost i integritet podataka. Za bolje upravljanje bezbednošću informacija, institucija mora da stvori mehanizme koji će omogućiti upravljanje bezbednosnim rizicima, preduzimajući odgovarajuće mere i garantujući da su informacije dostupne, upotrebljive, potpune i beskompromisne.[14]

Figura 5. Načela bezbednosti informacije



14 Priručnik revizije informacione tehnologije, Bezbednost Informacije.

2. Carina Kosova nema ažuriranu bezbednosnu politiku

Kosovska carina mora da dokumentuje, odobri i saopšti odgovarajuće politike i procedure za usmeravanje poslovanja i IT operacija kako bi ostvarila svoj mandat. Politike bezbednosti informacija moraju pokrivati sve operativne rizike i biti u stanju da razumno zaštite svu kritičnu informacijsku imovinu od gubitka, oštećenja i zloupotrebe. Sistem upravljanja bezbednošću informacija i druge interne politike, procedure ili primenljiva pravila moraju da obezbede da su u skladu sa najnovijim razvojem organizacije i da se redovno revidiraju.[15]

CK ima politiku bezbednosti informacija, ali ova bezbednosna politika nije ažurirana. U skladu sa Administrativnim uputstvom br. 02/2010 MAP-a, za upravljanje bezbednošću informacija, CK je 2017. godine izradio politike, procedure i standarde za bezbednost informacija, koji se trenutno koriste, ali ova politika još uvek nije ažurirana. Stoga, razvoj CK-a i informacione bezbednosti na globalnom nivou od 2017. do 2024. godine nije uključen u ovu politiku.

Razlog za ne ažuriranje ove politike i drugih politika koje se odnose na carinske procedure i IT je planiranje njihovog ažuriranja nakon stupanja na snagu Kodeksa br. 08/L-247 Carine i akcize u cilju prilagođavanja. Stoga su sada u procesu napredovanja da se prilagode novom Carinskom Zakonu.

Zastarela bezbednosna politika i nedostatak novih smernica o bezbednosnim praksama ostavlja zaposlene ne informisanim i nesposobnim da efikasno zaštite organizaciju i čini organizaciju ranjivijom na sajber napade.

15 Priručnik Revizije Informacione Tehnologije -Informacije i Kibernetičke Informacije, Politike bezbednosti informacije i ISO 27000.

3.Nedostaci u strukturi IT bezbednosti i podele odgovornosti, kao i uticaj na upravljanje revizorskim tragovima u informacionom sistemu CK-a.

Kosovska carina treba da ima jasne IT dužnosti i odgovornosti u vezi sa Politikom Informacione Bezbednosti, ne bi trebalo da postoji sukob odgovornosti ili nesklad u aktivnostima bezbednosti informacija (poziva se na ISO 27000). [16]

Tokom perioda revizije, analize dokumenata za organizaciju IT u Carini i intervjua sa odgovornim službenicima, primetili smo da Carina Kosova nije uspela da stvori jasnu strukturu bezbednosti informacija. Carinski IT službenici koji administriraju bazu podataka imaju pun pristup bazi podataka i aplikaciji ASYCUDA World, takođe imaju potpun pristup evidenciji revizorskog traga. Dok oni rade analizu revizorskih tragova u slučaju bilo kog zahteva, kao što je bio slučaj spoljne revizije. Pored toga, u IT odeljenju je naglašen fokus odgovornosti i puna zavisnost od službenika sa administrativnim pristupom svim sistemima i bazama podataka u vlasništvu CK-a.

Takođe, u organizacionoj strukturi usvojenoj 2016. godine, zajedno sa njenim dodatkom koji detaljno opisuje dužnosti i odgovornosti svakog sektora CK i ažuriran 2019. godine, uključio je odredbe za sektor sistema, bezbednosti i infrastrukture. Međutim, on ne definiše na specifičan način odgovornost za praćenje bezbednosti informacija, niti definiše specifičnu ulogu za praćenje revizorskih tragova u okviru informacionih sistema i baza podataka.

Takođe, tokom revizije, odnosno fizičkog osmatranja na carinskim punktovima, uočeno je da nakon što carinski agenti popune beleške u sistemu ASYCUDA i stigne kamion, uvoz za provere u crvenom kanalu mora da bude fizički pregledan od strane carinika, koji ovaj zadatak obavlja sam, a ne sa svojim kolegama u vidu komisije, iako nam je tokom opisa carinskih procesa u intervjuima predstavljeno da se ovaj proces odvija timski. Takođe, rukovodstvo CK-a se uverilo da ovaj proces sprovodi više službenika, a ne jedan službenik, uprkos činjenici da je uputstvom broj 17/2015 predviđeno da ovaj proces realizuje jedan službenik.

16 Priručnik Revizije Informacione Tehnologije – Informacije i Kibernetičke Bezbednosti , Struktura bezbednosti Struktura IT-je.

Nedostatak definisane strukture informacione bezbednosti izazvao je sukob odgovornosti u pristupima službenika u njenim sistemima i nije uspeo da klasifikuje nivo informacione bezbednosti. Potpuni pristup revizorskom tragu koji se daje administratoru baze podataka i aplikacija, oslanjajući se samo na jednog službenika, stvara značajne rizike. To uključuje mogućnost neovlašćenih promena, grešaka ili zloupotrebe podataka, kao što je zaobilaženje ili brisanje revizorskih tragova, što ugrožava integritet sistema.

Dok realizacija fizičke kontrole robe ugrožava transparentnost procesa i tačnost procene.

4. Nedostatak svesti i obuke o bezbednosti informacija za zaposlene u CK-a

Carina Kosova mora da obezbedi da svi zaposleni (uključujući izvođače ili korisnike osetljivih podataka) budu kvalifikovani za održavanje podataka, korišćenje resursa, razumevanje dužnosti i odgovornosti. Od regrutovanja do prestanka radnog odnosa, osoblje mora da održava bezbednost informacija. Kada se ugovor o radu prekine, njihov pristup se mora prekinuti. Periodične obuke za osvežavanje znanja o odgovarajućim veštinama i znanjima takođe treba ponuditi zaposlenima čija je uloga u organizaciji značajna za Bezbednost Informacija i Kibernetiku.[17]

Tokom pregleda na carinskim punktovima utvrdili smo da službenici Carine nisu dovoljno upoznati sa informatičkom bezbednošću. Primetili smo da svoje lozinke drže izloženim u radnim prostorima, lako dostupnim trećim licima, a da nisu svesni održavanja pristupa i bezbednosti informacija.

Iako su obaveštenja o bezbednosti informacija poslata e-poštom iz IT Odeljenja svim službenicima, obuka o bezbednosti informacija nedostaje. Obrazloženje zvaničnika za otkrivanje lozinki bila je teška politika složenosti lozinki i često menjanje lozinki, kao i veliki broj lozinki koje koriste za različite sisteme.

17 Priručnik Revizije Informacione Tehnologije – Informacije i Kibernetička Sigurnost , Sigurnost IT-je i Ljudskih Resursa.

Nepravilna zaštita pristupa sistemu ugrožava podatke i pristup neovlašćenih lica. Takođe, rizikuje realizaciju bilo kog važnog carinskog procesa kroz taj pristup neovlašćenih lica i njihova ne identifikacija.

5. Carina Kosova nema proceduru za kontrolu pristupa korisnika informacionom sistemu

Politika pristupa informacionim sistemima u Carini Kosova treba da obezbedi osnovu za kontrolu mešanja u informacije. Funkcija bezbednosti informacija prati efektivnost kontrole operacija upravljanja korisničkim nalogom na vreme i izveštava o efikasnosti i efektivnosti operacije.[18] Dodela i korišćenje privilegija u okruženju informacionog sistema mora biti ograničeno i kontrolisano, odnosno privilegije se dodeljuju na osnovu potrebe za korišćenjem, privilegije se dodeljuju tek nakon formalnog procesa autorizacije. [19]

Carinici i carinski agenti koji su eksterni korisnici i koji imaju pristup registraciji carinskih podataka, za realizaciju carinskih procesa, imaju pristup AW sistemu koji implementira CK. Medutim, CK nema pisanu proceduru za kontrolu pristupa informacionim sistemima, pošto to nisu smatrali razumnim, pošto je komunikacija putem e-pošte za omogućavanje i promenu pristupa bila jednostavnija, procedura po njima bi izazvala kašnjenje, stoga nemaju odredeni proces za obezbedivanje pristupa informacionom sistemu, ali u praksi koriste tri metode.

Prvi metod za popunjavanje obrasca za pristup računarskim sistemima i aplikacijama. Ovaj metod se koristio od 2004-2020, ali pošto je doveo do kašnjenja zbog zavisnosti potpisa od upravnika sektora, onda je ovaj metod eliminisan i oni su nastavili da koriste drugi metod.

Drugi način promene pristupa se donosi odlukom generalnog direktora, koji potpisuje premeštaj osoblja u različite sektore i različite pozicije, a ova odluka se šalje sektoru za administraciju AW sistema. Na osnovu ove odluke sprovode promene u carinskim sistemima, uključujući i AW sistem.

18 Priručnik Revizije Informacione Tehnologije – Informacije i Kibernetička Sigurnost, Kontrola pristupa.
19 ISO 27001 – Kontrole pristupa.

Treći način promene pristupa vrši se na zahtev rukovodioca sektora, u carinskim ispostavama ili graničnim prelazima, koji šalje e-mail sa relevantnim informacijama za promenu pristupa carinskih službenika.

Ova tri metoda se koriste samo za interne korisnike – carinske službenike, dok carinski agenti podnose zahtev preko Udruženja Lokalnih i Međunarodnih Špeditera Kosova kako je definisano u sporazumu iz 2015. godine.

Takođe, zbog nepostojanja procedure za kontrolu pristupa carinskim sistemima, pregledi pristupa listi korisnika se ne sprovode redovno u informacionom sistemu. Najosetljiviji deo liste korisnika je lista korisnika carinskih agenata (5250 korisnika sa pristupom carinskim agentima), koji i pored promena nastavljaju da koriste naloge svojih kolega, uključujući i one koji nisu u radnom odnosu.

Proces upravljanja pristupom putem zahteva poslatih e-poštom prema njima je brži. Što se tiče redovnog pregleda pristupa, oni nisu smatrali da je to potrebno jer je svaki zahtev za obezbeđivanje i uklanjanje pristupa ispunjen. Iako prema standardima za bezbednost informacija, pregled pristupa korisnika mora se vršiti najmanje jednom godišnje. Dok prema CK za pristupe carinskih agenata postoji sporazum iz 2015. godine između CK i Udruženja Domaćih i Međunarodnih Špeditera Kosova koji definiše formu pristupa carinskih agenata i prema kojem je njihov pristup omogućen.

Nedostatak procedure za kontrolu pristupa korisnika informacionom sistemu povećava rizik od zloupotrebe pristupa i korišćenja neovlašćenog pristupa, kao i stvara nesigurnost zbog nepostojanja pregleda liste korisnika i jasnog procesa za odobravanje i uklanjanje pristupa.

3.3. Plan kontinuiteta poslovanja – Plan oporavka od nesreće

Organizacija takođe mora imati plan kontinuiteta kako bi osigurala kontinuitet pružaoca usluga za aktivnost ili to preuzela od druge kompanije. Ako je oporavak od katastrofe kritične funkcionalne oblasti ugrožen, kontinuitet poslovanja će biti ugrožen. Ako uloge i odgovornosti nisu jasne i razumljive od strane relevantnog osoblja, čak i najbolji plan sukcesije takođe može postati neefikasan.[20]

Slika 6. Kontinuitet poslovanja

20 Priručnik revizije informacione tehnologije PVB – PRF.

6. Carina Kosova nema plan za kontinuitet poslovanja

Kosovska Carina mora da pokrije sve kritične oblasti organizacije u grupi. Dužnosti i odgovornosti Uslovi za članove grupe.[21] Testovi plana kontinuiteta poslovanja treba da osiguraju da su svi članovi tima za oporavak i drugo relevantno osoblje svesni planova i svoje odgovornosti za kontinuitet poslovanja i bezbednost informacija i da znaju svoju ulogu kada se plan pozove.[22]

CK nema posebnu politiku, proceduru ili priručnik za plan kontinuiteta poslovanja, ali je sistem ASYCUDA konfigurisan tako da se baza podataka replicira u realnom vremenu preko platforme Oracle ActiveDataguard. CK ima dva data centra koja su međusobno povezana optičkim vlaknom, replikacija se vrši preko VMware platforme, takođe imaju replikaciju preko Storage-to-Storage platforme (3PAR8400 – 3PAR8200).

Takođe, nisu odredili konkretnu strukturu odgovornih lica koja je u funkciji za realizaciju plana kontinuiteta poslovanja, u slučaju bilo kakve nesreće ili vanredne situacije koja bi izazvala poremećaj procesa u informacionom sistemu, s obzirom da ne postoji i konkretan plan kontinuiteta poslovanja koji bi definisao ovu strukturu.

Iako je CK prilagodila implementaciju AW sistema na osnovu zakonodavstva Carine Kosova, oslanjajući se i na sopstvene opšte procedure, koje je napisala, ne može u potpunosti da podrži kontinuitet poslovanja u njima, s obzirom da su ove procedure zastarele i da su nije ažuriran tokom razvoja i unapređenja sistema.

Svaki proces koji se sprovodi kroz ASYCUDA sistem je u skladu sa carinskim zakonodavstvom Kosova, tako da su ovi procesi brojni i složeni. Oni nemaju specifične dijagrame za sve procese i radove, jer je sistem prilagođen u zavisnosti od carinskog zakonodavstva na snazi.

Osoblje Carine Kosova je deo vladinih radnih grupa i carinski podaci se čuvaju u objektima Vlade. Međutim, preduzete su i tehničke radnje za kontinuitet

21 Priručnik Revizije Informacione Tehnologije - – PVB – PRF - Struktura Funkcije Kontinuiteta Poslovanja
22 ISO 27001 – Struktura funkcije kontinuiteta poslovanja.

poslovanja kroz replikaciju i skladištenje podataka na dve različite lokacije. Što se tiče strukture ona nije definisana u nedostatku plana, ali službenici IT redovno vode računa o nadzoru rezervne kopije. Što se tiče ažuriranja procedura, dobili smo i informaciju od interne revizije da su predložili izradu i ažuriranje procedura koje objašnjavaju carinske procese i one informacionog sistema, ali još nisu uspeli da ih sprovedu.

U slučaju nesreće, gubitka podataka, oštećenja sistema ili odlaska ključnog osoblja, nedostatak sveobuhvatnog plana kontinuiteta poslovanja predstavlja značajan rizik za poslovanje. Ovo uključuje nedostatak definisane strukture za sprovođenje takvog plana i nedostatak pisanih procedura za carinske aktivnosti koje se sprovode kroz sistem ASYCUDA, koji upravlja kritičnim carinskim podacima i procesima. Ovi nedostaci ugrožavaju sposobnost carine da održi neprekidne operacije tokom vanrednih situacija

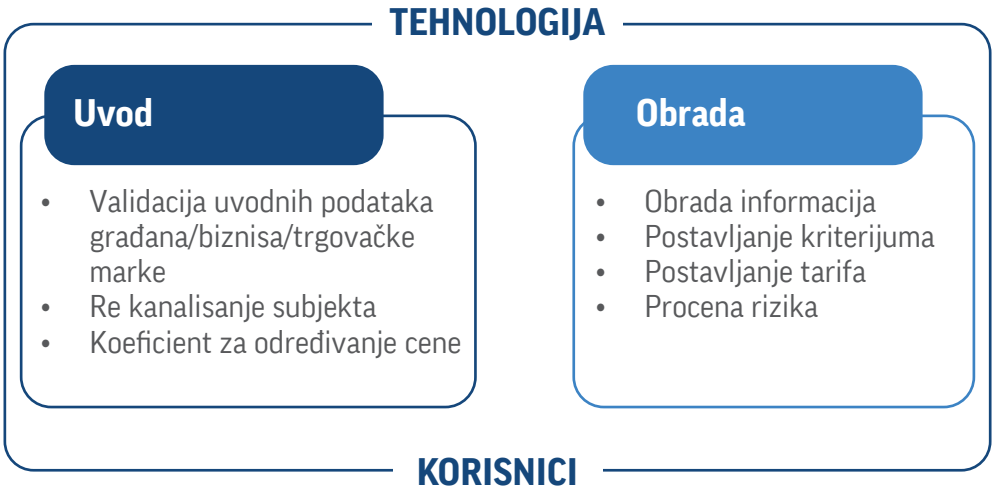
3.4. Kontrola aplikacije

Kontrole aplikacije su: kontrola funkcionisanja ulaza, obrade i izlazne funkcije. Oni uključuju metode koje osiguravaju da: samo potpuni, tačni i validni podaci se unose i ažuriraju u informacioni sistem, obrada obavlja ispravan zadatak i da rezultat obrade ispunjava očekivanja, a podaci se čuvaju.[23]

Sistem **ASYCUDA World,** koji koristi Carina Kosova, uključuje seriju automatizovanih i manuelnih kontrola sa ciljem da se obezbedi integritet i bezbednost carinskih podataka. Generalno, ove kontrole pomažu da se olakša rad sistema i obezbedi usklađenost sa propisima, ali postoje nedostaci u kontrolama unosa i obrade u AW informacionom sistemu.

23 Priručnik Revizije Informacione Tehnologije, Kontrole aplikacije

Slika 7. Model uvod-obrada podataka informacioni sistem AW



7. Obračun koeficijenta za određivanje cene u ASYCUDA vrši se manuelno

Pravila validacije moraju biti dobro osmišljena i primenjena u ulaznoj interakciji (input) ; ne validni podaci moraju biti pravilno odbačeni od strane aplikacije; trebaju postojati sveobuhvatne kontrole kao što su pravila registracije i autorizacije u slučaju mogućnosti suštinskih kontrola pristupa; postoje odgovarajuće kontrole i dokumentacija za unose aplikacija.[24]

Tokom procesa carinjenja roba koja prolazi kroz proces kontrole se ocenjuje prema ciljanju kriterijuma rizika, koji kanališu subjekat u kanal visokog rizika (crveni kanal), srednjeg rizika (žuti kanal) i niskog rizika (zeleni kanal). Stavke u crvenom kanalu podležu fizičkim proverama, stavke u žutom kanalu podležu dokumentarnim proverama, a stavke u zelenom kanalu prolaze bez provere. Zatim, Sektor u centrali za ocenjivanje subjekata koji se nalaze u žutom kanalu analizira izvornu dokumentaciju i ocenjuje adekvatnost cene iskazane u Jedinstvenom Carinskom Dokumentu (JCD) od strane stranaka prema relevantnim članovima Carinski Kodeks Kosova za ocenjivanje.

24 Priručnik Revizije Informacione Tehnologije – Kontrole Aplikacije, Kontrole ulaza.

U momentu kada carinski službenik utvrdi da se cena deklarisana u JCD-u treba promeniti nakon poređenja sa internim i eksternim izvorima cena, pomenuti moraju ručno da izračunaju koeficijent utvrđivanja cene (opis 45 u JCD-propisu) van sistema, tada moraju da unesu u sistem ASYCUDA bez ikakvih provera unosa u sistem, da proveri tačnost podataka kako bi se u JCD generisala cena robe promenjena/procenjena od Carina.

Sistem ASYCUDA ne omogućava izračunavanje koeficijenta za automatsko određivanje cene unutar sistema, jer to nije zahtevano od strane poslovne jedinice i nije dat primer kako se to realizuje.

Pošto carinski službenik manuelno izračunava koeficijent za određivanje cene, može doći do greške prilikom obračuna i neispravne vrednosti.

8. Ponovno kanalisanje materijala iz zelenog kanala u crveni kanal

Treba dokumentovati različite metode unosa podataka; nevažeći podaci moraju biti pravilno odbačeni od strane aplikacije; kriterijumi validnosti se ažuriraju na odgovarajući i ovlašćen način; sveobuhvatne kontrole kao što su pravila registracije i ovlašćenja treba da budu na mestu u slučaju mogućnosti suštinskih kontrola pristupa; postoje odgovarajuće kontrole i dokumentacija za unose aplikacija.[25] *Trebalo bi da postoje dokumentarne i fizičke provere robe koja izlazi u crvenom kanalu (ekipe za posmatranje), kao i kontrola dokumentacije u žutom kanalu.*[26]

Carinik (može biti i vođa smene/vođa jedinice), 15 minuta nakon što sistem kanališe materijal u zeleni kanal, može da ga vrati u crveni kanal ako utvrdi da su potrebni dodatni pregledi i postoje informacije koje su potrebne. da se potvrdi. Bez posedovanja dokumentacije o razlogu za ponovno kanalisanje, ili mogućnosti kontrole od strane sistema u slučaju greške u ponovnom kanalisanju predmeta.

25 Priručnik revizije Informacione Tehnologije -Kontrole Aplikacije, Kontrole ulaza.
26 Carina Kosova – Identifikacija rizika za Carinu Kosova 2023.

U testiranim slučajevima, carinik ili lice koje je vratilo predmet u crveni kanal ne daje nikakav komentar ili opravdanje za ovu akciju. Za ovu radnju ne postoji procedura koja obavezuje carinika da napiše komentar, ali sistem takođe nema polje za komentar, da napiše razlog za ponovno kanalisanje. Iako standardi za kontrolu unosa u aplikaciji predlažu verifikaciju i dokumentovanje postavljanja podataka u sistem.

Ovo utiče na nedostatak pregleda rizičnih slučajeva za sektor upravljanja rizicima, kao i na transparentnost i odgovornost za rad službenika na carinskom punktu. To takođe donosi nedostatke u izveštajima o stanju za donošenje odluka od strane menadžmenta.

9.Sistem ASYCUDA ne potvrđuje podatke za lične/poslovne brojeve i trgovačke marke

Aplikacija mora propisno odbaciti nevažeće podatke; kriterijumi validacije su ažurirani na odgovarajući način i verifikovani u odnosu na osnovne zapise podataka[27]. Uključujući lični broj i poslovni broj. Takođe, identifikacija žigova se mora izvršiti tokom faze carinjenja u JCD odeljku 31 JCD a, tako da nakon registracije žiga, AW sistem upozorava da li se radi o zaštićenoj trgovačkoj marki.[28]

Prilikom registracije deklaracije od strane carinskih službenika, videli smo da u svim slučajevima registracije ličnog i poslovnog broja oni opisuju broj u ručnom obliku i on nije verifikovan bazom podataka matične knjige ili poslovni registar.

Lični broj i poslovni broj su podaci Agencije Civilne Registracije i Agencije za Registrovanje Biznisa, dok Carina nije uspostavila vezu za neke od polja koje koristi sistem ASYCUDA, iako nam je predočila pismeni ugovor sa Agencijom za Registraciju Biznisa, tehnički priključak nije implementiran u sistemu.

Takođe, tokom provera koje su vršili carinski službenici, videli smo da sistem ASYCUDA ne obaveštava o slučajevima zaštićenih žigova, ali imaju poseban sistem

27 Priručnik Revizije Informacione Tehnologije – Kontrole Aplikacije, Kontrole ulaza
28 Carina Kosova- Identifikacija Rizika za Carinu Kosova 2023.

(INES) koji navodi zaštićene žigove iz CK i liste u dokumente kojima se ručno verifikuje da li je roba zaštićena trgovačka marka.

Štaviše, podaci o žigovima registrovanim u sistemu INES koje koristi CK nemaju tehničku mogućnost za uspostavljanje veze sa sistemom ASYCUDA. Osnovni sistem koji čuva ove INES podatke je ograničen i ograničava mogućnosti razmene podataka sa AW sistemom.

Nedostatak ovih veza za proveru valjanosti podataka može dovesti do namernih ili nenamernih grešaka i da se ne verifikuje u realnom vremenu. U slučajevima ulaska bilo koje robe bez provere žiga zaštićenog od CK, to bi prouzrokovalo štetu marki i građaninu. Kao i, nepoštovanje sporazuma sa spiskom trgovaca koji CK ima za zaštitu trgovačke marke.

10. Moduli za postavljanje kriterijuma i određivanje naknada u sistemu ASYCUDA nisu pogodni i jednostavni za korisnika

Aplikacija mora ispravno identifikovati greške u transakcijama. Mora postojati odgovarajući mehanizam za rukovanje greškama u obradi.[29] *Službenici iz relevantnog sektora u kontinuitetu trebaj se baviti ažuriranjem procene rizika, primanju informacija i procesovanje u sistem ASYCUDA World, koje se zatim mogu čitati u obliku kriterijuma tokom faze provere, kao i svaki korisnik AW , takođe na osnovu ovih kriterijuma (nivoi rizika) da se subjekat ponovno kanalizuje od strane samog sistema AW Žutog Kanala, Plavog, Zelenog i Crvenog Kanala.* [30]

Modul za postavljanje kriterijuma u ASYCUDA-i nije lak za korišćenje, odgovorni službenici sektora rizika moraju biti pažljivi da razumeju baze podataka i sintaksu programskih jezika, pošto postavljanje kriterijuma u ASYCUDA zahteva specifično znanje. Stoga smo tokom prezentacije ovog modula shvatili da zbog načina na koji je modul dizajniran, dolazi do sintaksnih grešaka pri postavljanju kriterijuma, što je rezultiralo i kriterijumima u realnom sistemu.

29 Priručnik Revizije Informacione Tehnologije – Kontrole aplikacije Kontrole prerade.
30 . Carina Kosova – Identifikacija rizika za Carinu Kosova 2023.

Takođe, modul za postavljanje stopa nije prilagođen korisniku, službenici moraju da napišu formule za izračunavanje u svakom prostoru za promenu stope. Dok u slučaju promene mnogih tarifa, sistem ASYCUDA ne dozvoljava da se zameni sve tarife odjednom u automatskom obliku, već moraju da izvrše promenu jednu po jednu za svaku, što oduzima vreme i ostavlja mogućnosti za greške, gde se tokom izvršenja prikazuju slučajevi grešaka.

Realizacija ovih modula je urađena u ovom obliku jer je ASYCUDA gotov sistem i opcije koje nudi su generalizovane za sve AW korisnike u svim zemljama sveta u kojima se koristi. Carinski službenici su tvrdili da je modul kriterijuma rizika razmatran na konferenciji UNCTAD-a nakon što je zatražena promena, ali CK nije uputila nikakav službeni pismeni zahtev po ovom pitanju.

Promena i postavljanje kriterijuma i stopa u postojećem obliku u sistemu AW utiče na efikasnost rada ova dva sektora i svih korisnika AW koji koriste kriterijume i stope, dopuštajući mogućnost greške u podacima koje evidentiraju relevantni sektori i negativno utiče u funkcionisanju sistema.

11. Sistem ASYCUDA ne vrši procenu rizika na automatski i merljiv način

Službenici iz relevantnog sektora moraju kontinuirano da ažuriraju procenu rizika, primaju informacije i obrađuju ih u sistemu ASYCUDA World, koji se potom mogu pročitati u obliku kriterijuma tokom faze ispitivanja, kao i svaki korisnik AW, da na osnovu ovih kriterijuma (nivoi rizika) subjekti se ponovo kanališu iz samog AW sistema u Žuti, Plavi, Zeleni i Crveni kanal.[31]

Sektor rizika u okviru Carine Kosova, na osnovu internog istraživanja, prošlosti uvoza i onih ekonomskih operatera, određuje kriterijume koji se moraju uzeti u obzir tokom procesa ocarinjenja za određene kategorije.

31 . Carina Kosova – Identifikacija rizika za Carinu Kosova 2023.

Kriterijume u sistem unosi sektor rizika u tekstualnom obliku, svi kriterijumi su napisani kao tekst sa određenim poljem i carinik čita ove kriterijume i mora da uporedi kriterijume sa dokumentima koje je stranka predstavila u carini proces ocarinjenja. Sve se to radi manuelno uz komentar carinika, koji tekstom formulisanim u formi zapisnika popunjava polje „akt inspekcije". Ali da ne postoji određeni parametar kojim bi se u automatskom, merljivom obliku u realnom vremenu saopštio nivo rizika od primene tih kriterijuma, koji kriterijumi su primenjeni, a koji nisu sa tačnom statističkom cifrom.

CK nema postupak kojim se utvrđuje način procene rizika i definisanje kriterijuma koji bi pomogli u razvoju ovog procesa i u sistemu. Takođe, nije definisana podela dužnosti i nedostatak formalnog odobrenja u procesu definisanja kriterijuma.

Nedostatak formalnog odobrenja i nejasna podela odgovornosti u određivanju kriterijuma rizika mogu uticati na doslednost donošenja odluka, stvarajući mogućnosti za neujednačen tretman slučajeva i izazove u rešavanju prioriteta rizika. Takođe, ova situacija može ograničiti potpuni pregled (povratne informacije) i efikasan period za sektor rizika na definisanim kriterijumima, čineći proces njihovog praćenja i analize izazovnijim. Ovo može uticati na efikasnost donošenja odluka i alokacije resursa.

ZAKLJUČI

04

4. Zaključci

Carina Kosova je ostvarila značajan napredak ka digitalizaciji carinskih procesa, poboljšanju efikasnosti i transparentnosti u upravljanju svojim operacijama. Ovaj napredak je postignut implementacijom sistema ASYCUDA World, koji omogućava automatizaciju značajnog dela carinskih procedura, smanjenje birokratije i ubrzanje procesa. Sistem omogućava elektronsku registraciju i obradu carinske dokumentacije, kao i razmenu podataka u realnom vremenu između carinskih agenata, ekonomskih operatera i drugih relevantnih institucija. Korišćenjem ovog sistema, Carina Kosova je uspela da poboljša praćenje tokova robe. Međutim, digitalizacija je i dalje proces koji traje, a izazovi kao što su dalje prilagođavanje kriterijuma rizika, puna integracija sektora i pružanje tehnološke podrške zahtevaju stalnu posvećenost da se postigne pun nivo digitalizacije

Ugovaranje

Carina Kosova iako je postigla da primeni sporazum za sistem ASYCUDA u vezi sa razvojem, unapređenjem i održavanjem sistema, kao i preko ovog projekta postigla da sprovede i zahtev UNCTAD za promovisanje polne jednakosti. Carina Kosova nije postigla da preko sporazuma jasno odredi odgovornosti i zadatke stranaka u procesu zaštite i obezbeđenja informacije ostavivši bezbednost informativnog sistema ne adresiran i ugrožen.

Informacija i kibernetička bezbednost

Kosovska carina ima nedostatke u kontroli bezbednosti informacija u odsustvu jasne IT bezbednosne strukture. Uz nizak nivo svesti zaposlenih o bezbednosti informacija, nedostaje procedura za kontrolu pristupa korisnika i postoji politika bezbednosti informacija koja se ne ažurira. Koja je kontinuirano izložena riziku održavanja sigurnosti informacija od oštećenja, promena i gubitka bez mogućnosti identifikacije i prevencije na vreme.

Plan kontinuiteta poslovanja – Plan oporavka od nesreće

Carina Kosova nema efikasnu politiku za kontinuitet poslovanja u organizaciji kao što je nedostatak plana kontinuiteta poslovanja, struktura koja će omogućiti sprovođenje plana i pisane carinske procedure koje se sprovode kroz sistem ASYCUDA.

Kontrola aplikacije

Carina Kosova je kontinuirano razvijala sistem ASYCUDA World za digitalizaciju carinskih procesa. Međutim, nisam uspeo da se uverim da su podaci uneseni u sistem tačni, jer se podaci za obračun koeficijenta za utvrđivanje cene obrađuju manuelno. Takođe, ne garantuje da su to validni i pouzdani podaci jer ne može da validira sve podatke koji se nalaze u sistemu čak ni u slučajevima kada su to provereni podaci iz postojećih baza podataka zbog načina na koji su postavljeni kriterijumi za procenu rizika u ovom sistemu. CK sistem ne uspeva da ima merljiv pregled prezentacije rizika. Takođe, ovaj sistem nije lak za korisnika, ne nudi jednostavne opcije korišćenja, posebno za module naknada i rizika, pa kao rezultat ima slučajeva da se pojave greške u sistemu.

PREPORUKE

05

5. Preporuke

Preporučujemo Carini Kosova da:

1. Politike ugovaranja , pre pokretanja razvoja svakog projekta informacione tehnologije, treba se u svim ugovorima informacione tehnologije adresirati zahtevi za obezbeđivanje informacije.

2. Politika bezbednosti informacije da obnovi politike i procese radi zaštite bezbednosti informacije.

3. Struktura bezbednosti informacione tehnologije, podela odgovornosti i upravljanje tragova revizije, da izvrši podelu zadataka i odgovornosti u sistemu informacija i da ograniči radnje svih uloga po standardima za čuvanje informacija sigurnim, podelivši ulogu administratora baze podataka i administratora sistema od uloge službenika za bezbednost informacije. Ograničiti i nadgledati privilegije pristupa na redovnoj osnovi bez izazivanja sukoba odgovornosti i održavanja integriteta podataka.

3.1 Da izvrši pregled postupka obrade carinskih deklaracija u sistemu ASYCUDA World od strane službenika za kontrolu fizičke robe, kako bi se izvršila preciznija i transparentnija fizička kontrola.

4. Svest o informacionoj bezbednosti i obuka za službenike Carine Kosova, da održe obuku za sve carinske službenike u vezi sa bezbednošću informacija i da preispitaju mogućnosti pristupa informacionim sistemima kroz formu svih sistema sa pristupom jedinstvenom prijavom. (single sign on).

5. Kontrola pristupa korisnika u informacionom sistemu, da sprovede proceduru kontrole pristupa kroz koju mora da utvrdi proces odobravanja i uklanjanja pristupa informacionom sistemu, kao i redovnog pregleda pristupa.

5.1 Razmotriti sporazum iz 2015. između Carine Kosova i Udruženja Lokalnih i Međunarodnih Špeditera Kosova koji definiše formu pristupa carinskih agenata i razmotriti pristupe carinskih agenata.

6. Plan kontinuiteta poslovanja, izraditi i odobriti plan kontinuiteta poslovanja, definisati strukturu sa ulogama i odgovornostima za sprovođenje plana. Kao i da izradi dokument sa pisanim carinskim procedurama sa procesima koji se sprovode kroz sistem ASYCUDA World.

7. Izračunavanje koeficijenta utvrđivanja cena u ASYCUDA World, da se automatizuje proces izračunavanja koeficijenta utvrđivanja cena iz sistema ASYCUDA World, tako da carinski službenici ne moraju da obavljaju ovaj proces manuelno.

8. Pre kanalisanje predmeta u sistemu ASYCUDA World, da se stvori obavezno polje u sistemu, da carinski službenik, uključujući i šefa smene ili jedinice, pruži obrazloženje ili komentar u sistemu za postupanje prilikom vraćanja slučaja sa zelenog kanala na crveni kanal.

9. Validacija podataka u sistemu ASYCUDA World, da zaključi ugovore sa relevantnim institucijama koje su vlasnici osnovnih baza podataka (Agencija za Civilnu Registraciju i Kosovska Agencija za Registraciju Biznisa) i da kreira tehnička rešenja za razmenu podataka sa sistemom ASYCUDA World za njihovu verifikaciju sa osnovnim bazama podataka.

10. Jednostavni moduli za korisnika, za ažuriranje sistema jednostavnijim modulima za korisnika, pronalaženje najpogodnijeg oblika koji olakšava korišćenje modula korisnicima u sektoru rizika i naknada.

11. Procena rizika i definisanje kriterijuma, da se primeni interni pravilnik za procenu rizika i definisanje kriterijuma. Takođe, u sistemu ASYCUDA trebalo bi da bude moguće kreirati kontrolnu listu za postavljanje kriterijuma, tako da sektor rizika, kao i menadžment, imaju mogućnost da u realnom vremenu dobijaju informacije i statistike, analiziraju ih i preduzimaju odgovarajuće radnje na osnovu izvršene analize.

DODATAK

Dodatak I. Dizajn revizije

Rizične oblasti i pokazatelj problema u reviziji

Carina Kosova ima širu misiju, počev od zaštite države, privrede i građana. Dakle, misija Carine Kosova se može podeliti u dve glavne kategorije:

1. Za ekonomska pitanja - Naplata carine: Carinska taksa; porez na dodatu vrednost; Akciza za Konsolidovani budžet Kosova. Kontrola uvoza i izvoza, zaštita privrede; zaštita trgovačke marke i dr., kao i tačna statistika o spoljnoj trgovini.
2. Za bezbednost - Borba protiv nelegalnih aktivnosti. Povećana bezbednost kroz prisustvo na graničnim prelazima; Borba protiv graničnog kriminala; Borba protiv trgovine drogom itd. Zaštita stanovništva i životne sredine, sprečavanje krijumčarenja oružja i eksplozivnih materija.

Imajući u vidu ulogu i značaj CK, Nacionalna kancelarija Revizije (NKR) u svom godišnjem izveštaju i Evropska Komisija (EK) u Izveštaju o Kosovu, daju joj poseban prostor.

U Izveštaju za Kosovo EK, istaknut je napredak CK i značaj IT sistema, kao i napredak koji je CK ostvarila sa digitalizacijom procesa.

Takođe, NKR je u Godišnjem Revizorskom Izveštaju (GRI) za 2022. godinu identifikovala da je bilo slučajeva da nije bilo potpunog usklađivanja carinskih dažbina u ITK-u sa sistemom ASYCUDA. To je zato što Carina nije uspela da ažurira listu tarifnih kodova i podšifara između dva sistema, nije imala kompletnu listu carinskih tarifa ažuriranu u sistemu AW.

Zbog svoje važnosti, budući da ova tema zahteva poseban tretman, jer se odnosi na reviziju sistema informacionih tehnologija, NKR je smatrala neophodnom posebnu reviziju od strane sektora performansi, odnosno IT, za tretman bezbednosti i tačnosti informacija sistema CK-a.

Tokom faze pred-studije, nakon pregleda dokumentacije koja se odnosi na IT sisteme i carinske procese i intervjua sa odgovornim službenicima CK, identifikovali smo sledeće nedostatke:

- CK ima nedostatke u organizaciji, strukturi i politici informacione bezbednosti;
- CK nije adresirala pitanja bezbednosti informacija u sporazumu o razvoju, a zatim i u kasnijim ugovorima o održavanju i unapređenju
- Bezbedan pristup sa višestrukom autentifikacijom se ne koristi u sistemu ASYCUDA World u CK.
- Sistem ASYCUDA World ima nedostatak veza sa drugim sistemima, zbog čega se neke od registracija vrše ručno, kao što je registracija ličnog broja.
- CK, iako koristi INES sistem za registraciju trgovačke marke, nije u mogućnosti da identifikuje zaštićenu marku, zbog nepovezanosti ovog sistema sa ASYCUDA World i LES ECM sistemima.

Istovremeno, ova revizija se sprovodi u okviru LOTA programa IDI, koji ima za cilj razvoj VRI u IT reviziji, upotrebi IT i Strategiji.

Razmatranje indikatora problema identifikovanih iz različitih izvora, održani sastanci sa osobama odgovornim za identifikaciju problema u informacionim sistemima u CK, kao i iz naših procena na osnovu Priručnika za aktivnu IT reviziju[32] za identifikaciju najviše rizika iz primljene dokumentacije nas orijentiše na glavni problem: CK ima nedostatke u organizaciji bezbednosti informacija i kontrole aplikacija.

32 Aktivni Priručnik – je platforma razvijena od ITWG/ EUROSAI i WGITA/ INTOSAI, za identifikaciju rizičnih oblasti, određivanje pitanja, kriterijuma i metodologije rada tokom procesa revizije IT-je.

1.1. Opis sistema

1.1.1. Ministarstvo Finansija, Rada i Transfera

Ministarstvo Finansija, Rada i Transfera (MFRT), na osnovu Uredbe [33] o oblastima administrativne nadležnosti kabineta premijera i ministarstava, ima nadležnost za: pripremu, izradu, odobravanje, sprovođenje, evaluaciju i nadzor javnih politika, izrada zakonskih akata, izrada i usvajanje podzakonskih akata, utvrđivanje obaveznih standarda u oblasti upravljanja javnim finansijama, interne kontrole i revizije za javni sektor, računovodstvenih i standarda finansijskog izveštavanja za privatni sektor i javna preduzeća, javni dug, javne nabavke, makroekonomske i fiskalne politike i državne pomoći, u skladu sa Ustavom i važećim zakonima. MFRT ima agencije za upravljanje prihodima gde je i Carina Kosova deo ovih agencija. Posluje u bliskoj saradnji sa Ministarstvom Finansija, Rada i Transfera. Ova saradnja je strukturisana na nekoliko glavnih načina:

1. Sakupljanje Prihoda:

Carina Kosova sakuplja poreze i carinske doprinose od uvoza i izvoza robe. Ovi prihodi su važan deo državnog budžeta i izveštavaju se Ministarstvu Finansija, Rada i Transfera.

2. Sprovođenje Fiskalnih Politika:

Carina je odgovorna za sprovođenje fiskalnih politika koje se određuju od Ministarstva Finansija, Rada i Transfera. Ovo obuhvata sakupljanje PDV-a i akcize od robe koja ulazi na Kosovo.

33 Pravilnik (Qrk) - Br. 07/2020 o Izmeni i Dopuni Pravilnika Br. 06/2020 o Oblastima Administrativne Odgovornosti Kancelarije Premijera i Ministarstava.

3.Saradnja u Zakonodavstvu:

Carina radi zajedno sa Ministarstvom kako bi sačinila i poboljšala carinsko zakonodavstvo i politiku trgovine. Ovo obezbeđuje sklad sa međunarodnim standardima i zaštiti ekonomske Kosova.

4. Kontrola i praćenje:

Carina Kosova i Ministarstvo Finansija, Rada i Transfera sarađuju kako bi osigurali tačno praćenje i kontrolu komercijalnih i finansijskih tokova. Ovo uključuje borbu protiv krijumčarenja i utaje poreza.

5. Tehnologija i Obuka:

Postoji kontinuirana saradnja u oblasti informacionih tehnologija i obuke kadrova u cilju poboljšanja efikasnosti carinskog i finansijskog poslovanja.

6. Pregled i Izveštavanje:

Carina Kosova periodično razmatra i izveštava o svojim prihodima i aktivnostima Ministarstvu Finansija, Rada i Transfera, obezbeđujući transparentnost i odgovornost u upravljanju javnim fondovima.

Ove tačke pokazuju blisku i neophodnu vezu između Carine Kosova i Ministarstva Finansija, Rada i Transfera, koje ima za cilj da optimizuje fiskalnu i ekonomsku administraciju zemlje.

1.1.2. Carina Kosova

Carina Kosova je osnovana u avgustu 1999. godine od strane stuba EU, kako bi se obezbedila pravična i jednoobrazna primena carinskih pravila i drugih odredbi koje se primenjuju na robu koja je predmet carinskog nadzora. Carinska služba UNMIK-a je 12. decembra 2008. transformisana u Carinu Kosova. Carinski Zakonik,

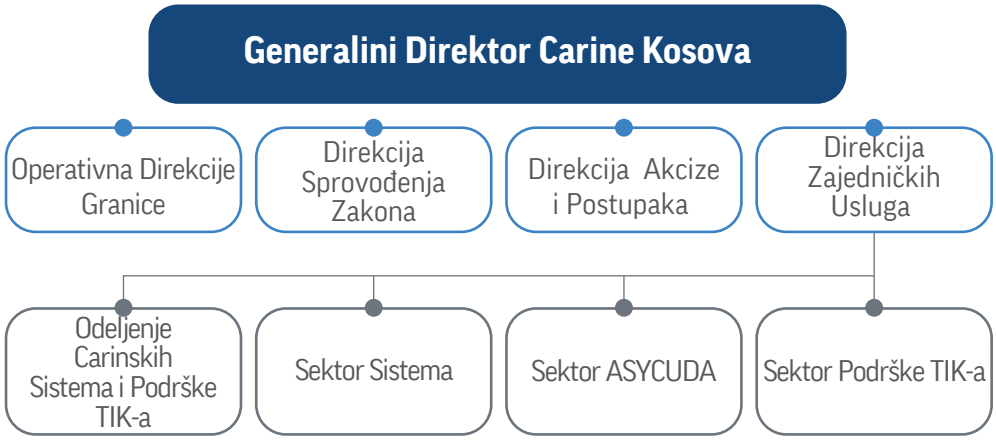
usvojen 11. novembra 2008.[34] od strane Skupštine Kosova, koji je omogućio ovu tranziciju, izmenjen je i dopunjen kasnije 2012. godine. Predmetni carinski zakonik je u potpunosti u skladu sa pravnim standardima Evropske Unije i, između ostalog, ima za cilj ekonomski razvoj Republike Kosovo. Pored carinskih obaveza koje dolaze od Carine, na granici se plaćaju PDV i akcize. Pored naplate prihoda, Carina Kosova štiti društvo od krijumčarenja droge i druge zabranjene robe sa štetnim posledicama privrednog kriminala, kao i utaje prihoda. Carina Kosova je razvijena na osnovu standarda EU i u potpunosti se finansira iz Konsolidovanog budžeta Kosova. Takođe ga podržava EU preko viših profesionalnih carinskih menadžera, kao izvršni organ koji je pozajmljen od Carinske službe EU. Carina takođe ima koristi od tehničke podrške Carine EU i Kancelarije za Fiskalnu Pomoć (KFP), koja je pomogla u razvoju osnova zakonodavstva, organizacije, strukture, obuke i razvoja osoblja. Carina Kosova se smatra jednom od institucija sa visokim organizacionim vrednostima i od svog osnivanja je bila glavni doprinositelj u pogledu prikupljanja prihoda i zaštite svojih građana od zabranjene i ograničene robe. Prihodi prikupljeni od strane Carine doprinose oko 60% ukupnih prihoda prikupljenih za budžet Republike Kosovo.[35]

Carina Kosova u strukturi unutrašnje uredbe ima pet direktorata kao u nastavku:

- Generalni Direktor ;
- Direkcija Operative i Granice;
- Direkcija Sprovođenja Zakona;
- Direkcija Akciza i Postupaka ; kao i
- Direkcija Zajedničkih Usluga. U okviru Direkcije za Zajedničke Usluge uključeno je Odeljenje za carinske sisteme TIK podrške koje obuhvata sledeće sektore:
  - Odeljenje Sistema;
  - Odeljenje ASYCUDA; kao i
  - Odeljenje Podrške TIK

34 Kodeks Br. 03 L-109 Carine i Akcize na Kosovu.
35 Strateški Plan CK-a 2019-2023.

Figura 8. Organizacija direkcija, odeljenja i sektora obuhvaćenih u delokrug



Operativno-graničnom upravom (OGU) rukovodi direktor Uprave sa carinskim statusom, koji odgovara direktno GD. Ova direkcija, u okviru utvrđenih nadležnosti, koordinira i prati rad sa područnim odeljenjima i drugim upravama Carine. Nadležno je za planiranje, strategiju, donošenje odluka, koordinaciju i kontrolu sprovođenja strategija, kao i preduzima aktivnosti na sprovođenju carinskog zakonodavstva, čija je primena u nadležnosti OGK-a. Koordinira aktivnosti sa nacionalnim strukturama za sprovođenje zakona, kao i sa carinskim organima trećih zemalja u okviru važećih sporazuma. Odgovoran je za implementaciju i dalji razvoj sistema i povezanih procedura, carinskih procedura, nacionalnih strategija u saradnji i koordinaciji sa određenim direkcijama i odeljenjima, za prikupljanje zakonskih prihoda i podršku olakšavanju legalne trgovine.

Direkcija za Sprovođenje Zakona (DSZ) odgovara Generalnom Direktoru. U okviru operativnih strategija i planova Carine Kosova i u skladu sa vladavinom prava, DSZ je odgovorna za sprovođenje zakona čija je primena u nadležnosti Carine, obezbeđujući koordinaciju sa drugim odeljenjima, posebno regionalnim. Odgovorno je za implementaciju i razvoj nacionalnog sistema upravljanja rizicima zasnovanog na analizi rizika i obaveštajnim podacima i u punoj koordinaciji sa regionalnim jedinicama. Vodi računa i nadzire sprovođenje zakona i postupaka u vezi sa zaštitom Prava Intelektualne Svojine (PIS). Koordinira aktivnosti sa drugim nacionalnim agencijama za sprovođenje zakona, kao i carinskim organima trećih zemalja u okviru važećih sporazuma.

Direkciju za Akcize i Postupke (DAP) vodi direktor Uprave sa carinskim statusom, koji odgovara direktno GD. U okviru definisanih nadležnosti koordinira i prati aktivnosti DAP-a i podređenih struktura. Nadležna je za planiranje, strategiju, koordinaciju, donošenje odluka i kontrolu sprovođenja strategija, kao i aktivnosti na sprovođenju carinskog zakonodavstva, olakšavanju trgovine, unapređenju relevantnih carinskih procedura, čije sprovođenje je povereno nadležnost DAP-a. Koordinira aktivnosti sa drugim upravama, carinskim službama i drugim agencijama, kao i sa carinskim organima trećih zemalja u okviru važećih sporazuma. Odgovoran je za razvoj sistema i instituta u okviru direkcije i podršku u njihovoj pravilnoj primeni od strane drugih direkcija. Brine o sprovođenju carinskog zakonodavstva u pogledu procedura, akciza, pravila porekla, carinske klasifikacije robe i carine, carinske vrednosti, carinske laboratorije i nadzora duga.

Direkcija Zajedničkih Usluga (DZU) vodi direktor direkcije sa carinskim statusom, koji je direktno odgovoran generalnom direktoru (GD) u okviru definisanih ovlašćenja, i ima dužnosti i odgovornosti da koordinira i prati aktivnosti DZU i podređene strukture. Nadležno je za planiranje, strategiju, koordinaciju i kontrolu sprovođenja strategija, kao i preduzima aktivnosti i odluke za sprovođenje propisa, čija je primena u nadležnosti DZU. Odgovoran je za politiku budžeta carine i za računovodstvene i rashodne obaveze. Brine o razvoju politika i strategija ljudskih resursa i primeni relevantnog zakonodavstva. Priprema godišnji plan budžeta za Carinu i njene organizacione jedinice. Nadgleda i prati politiku nabavke i IT, uključujući inovacije u IT sistemima i ASYCUDA. DZU se sastoji od organizacionih jedinica, odeljenja i sektora pod rukovodstvom direktora DZU-a ili relevantnih odeljenja, u čijem sastavu je i Odeljenje za carinske sisteme i informacione tehnologije (OCS&TIK).

Odeljenje za Carinske Sisteme i informacione tehnologije - Ovo odeljenje vodi šef odeljenja sa carinskim statusom i odgovara direktno direktoru DZU. Ovo odeljenje je odgovorno za definisanje strategije i operativnih planova CK-a informaciono-komunikacionih tehnologija. Preduzima radnje i koordinira aktivnosti na implementaciji, razvoju i upravljanju IT sistemima, bezbednošću i infrastrukturom, kao i koordinira i podržava organizacione jedinice CK na centralnom i regionalnom nivou za korišćenje IT sistema, alata i resursa.

Sledeći sektori su deo ovog odeljenja:

- •Sistemski sektor;
- •ASYCUDA sektor;
- •Sektor IT podrške.

Sektorom za sisteme (SS) rukovodi rukovodilac sektora sa carinskim statusom, koji odgovara načelniku DSD-TIK. Dužnosti i odgovornosti ovog sektora su da doprinese implementaciji i razvoju strategije carinskih sistema i automatizaciji procedura.

Upravlja i administrira sisteme za sprovođenje zakona i slučajeve, VMware virtuelnu platformu i reviziju sistema, sistem upravljanja osobljem i druge sisteme koji se odnose na elektronsko podnošenje i carinske procedure. Odgovorno je za upravljanje i razvoj svih alata i aplikacija koje su neophodne za automatizaciju carinskih procedura. Vrši analizu za inovacije i razvoj CK-a tehnoloških sistema. Predlaže izmene i nova tehnička rešenja za poboljšanje funkcija carinskih sistema. Obezbeđuje tehničke specifikacije i dokumenta i rešenja neophodna za unapređenje funkcija kompjuterizovanih carinskih sistema i procedura i infrastrukture Carinskih sistema.

Sektorom ASYCUDA (SAW) rukovodi vođa sektora sa carinskim statusom, koji odgovara šefu DSD-TIK-a. Zadaci i odgovornosti ovog sektora su upravljanje i administracija razvoja sistema ASICUDA Vorld (AW), administracija i razvoj BI – Cognos platforme, Sistematske elektronske razmene podataka (SEED)[36] i drugih sistema vezanih za elektronsku prezentaciju i carinske procedure. Obezbeđuje redovno održavanje kompjuterizovanih carinskih sistema i održavanje različitih aplikacija i alata neophodnih za podršku radu kancelarija. Doprinosi implementaciji projekata među agencijske i regionalne saradnje kao što je SEED itd. Odgovorno je za obavljanje usluga instalacije baze podataka za Carinske Sisteme i testiranje u vezi sa novim verzijama operativnog sistema, održavanje i praćenje promena u zakonodavstvu i procedurama u cilju njihovog uvođenja u sistem. Na osnovu

36 Sistemska razmena elektronskih podataka.

relevantnih ovlašćenja i izveštaja dobijenih od organizacionih jedinica vrši neophodna poboljšanja sistema.

Sektor za podršku informacionoj tehnologiji – Sektorom za Podršku Informacionim Tehnologijama (SPIT) rukovodi rukovodilac sektora sa carinskim statusom, koji odgovara šefu DSD-TIK. Odgovoran je za razvoj bezbednosti sistema, mrežne infrastrukture, počev od internih korisnika mreže, zaštitnog zida, bezbednosnih sertifikata i PKI (Public Kei Infrastructure), implementacije kontinuiteta poslovanja za infrastrukturu, sisteme i IT bezbednost. Organizuje, prati, upravlja i ocenjuje performanse IT resursa, aktivnosti i infrastrukture. Razvija, administrira, održava i nadgleda sprovođenje politika, procedura i planova koji se odnose na administraciju bezbednosnih sistema, infrastrukture, serverskih sistema, baza podataka, aplikacija i pristupa korisnika sistemu. Definiše i sprovodi plan oporavka (plan oporavka od katastrofe), za: mrežnu infrastrukturu, serverske sisteme, baze podataka, aplikacije i bezbednost sistema. Garantuje ispravan rad serverskih sistema i uređaja kao što su: Kontroler Domena, Fajl Server za skladištenje podataka, Firevall, Backup i drugi IT sistemi; kao i sistemi za nadzor kamera, u zavisnosti od potreba organizacije, da garantuju pravilno ažuriranje i rad baza podataka i aplikacija koje se odnose na finansije, ljudske resurse, logistiku, nabavku i druge aplikacije, za koje je odgovoran IT – ovde garantuje neophodnu tehničku podršku za sve kancelarije CK, za instalacije, održavanje, korišćenje opreme i mreže.

Delokrug i pitanja revizije

Delokrug ove revizije biće Carina Kosova i relevantna odeljenja za IT upravljanje, sistem ASYCUDA i carinske procese.

Direkcija za Zajedničke Usluge - Odeljenje za Carinske Sisteme i TIK podršku sa sektorima: Sektor sistema; Sektor ASYCUDA i Sektor podrške TIK.

Direkcija za Granične Operacije sa carinskim odeljenjima i sektorima uključujući kopnenu graničnu tačku, vazdušnu graničnu tačku i morski granični punkt.

Uprava za sprovođenje zakona – Sektor za Rizik i Praćenje (SRP).

Direkcija za Akcize i Postupke (DAP) – Odeljenje za Akcize, Tarifu, Poreklo i Postupke (OATPP) sa sektorima: Sektor Porekla, Sektor za Tarife, Sektor za Procedure i Ovlašćenja (SPO), Sektor za Akcize i Sektor za Dugove.

Fokus revizije biće bezbednost informacija i kontrole unosa i obrade aplikacija za sisteme informacionih tehnologija koji se koriste za carinske procese sa fokusom na sistem ASICUDA Vorld. Revizija će obuhvatiti period od 2022. do 2024. godine.

Revizijska pitanja

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

1. Da li Carina Kosova sprovodi politiku ugovaranja?
2. Da li je Carina Kosova identifikovala i adresirala bezbednosne zahteve u razvijenim ugovornim procedurama?
3. Da li Carina Kosova ima i sprovodi politiku bezbednosti informacija?
4. Da li Carina Kosova ima jasnu IT bezbednosnu strukturu?
5. Da li su zaposleni svesni svojih dužnosti i odgovornosti u vezi sa bezbednosnim dužnostima i odgovornostima i da li im se nudi obuka o bezbednosti informacija?

6. Da li je proces za obezbeđivanje i ukidanje kontrole pristupa zaposlenima i ugovaračima efikasan i bezbedan?
7. Da li u organizaciji postoji efikasna politika kontinuiteta poslovanja?
8. Da li ovlašćeno osoblje unosi tačne podatke u bazu podataka i u aplikaciju?
9. Da li aplikacija obezbeđuje integritet podataka, validnost i pouzdanost tokom ciklusa obrade transakcije?

Kriterijumi revizije[37]

Korišćeni kriterijumi revizije iz Aktivnog Priručnika Revizije IT-je.[38]

Međunarodni Standardi bezbednosti[39], kao i dokumentacija Carine Kosova: Sporazum o razvoju i održavanju sistema [40] i usvojen dokument za ocenu rizika.[41]

Da bi se ocenila identifikacija potreba i adresiranje zahteva bezbednosti informacije u ugovorenim projektima u Carini Kosova postavljeni su sledeći kriterijumi:

- Organizacija mora da sprovodi organizacione politike o ugovaranju.[42]

  Carina Kosova mora da sprovede potpisani sporazum koji uključuje sledeći član: U početnim fazama projekta, pripremne aktivnosti koje će biti preduzete, uključujući napore da se obezbedi da svest i mobilizacija dođu do žena u različitim zainteresovanim grupama (carina, trgovci). U skladu sa svojom posvećenošću promovisanju rodne ravnopravnosti/podizanju

37 Za više informacija konsultujte ISSAI 300, Criteria, p.7
38 Priručnik Revizije Informacione Tehnologije je proizvod radnih grupa informacione tehnologije EUROSAI-t (WGITA) kao i Inicijative za razvoj INTOSAI-t (IDI) za određivanje pravila standarda Revizije Informacione Tehnologije .- nadalje Priručnik revizije Informacione Tehnologije.
39 Sistem upravljanja bezbednosti informacija ISO/IEC 27000/01.
40 Sporazum između Vlade Republike Kosova i Specijalizovane Agencije Ujedinjenih Nacija – UNCTAD o Projektu softver Carine , ratifikovan u Skupštini Republike Kosova.
41 Identifikacija rizika za Carinu Kosova 2023.
42 Priručnik Revizije Informacione Tehnologije – Ugovaranje.

svesti, UNCTAD snažno podstiče učešće ženskog osoblja u projektima i aktivnostima obuke i drugim događajima.[43]

- Ugovarač mora da istakne bezbednosne zahteve organizacije na odgovarajući način.[44]

  Ugovor sa spoljnim stranama koji uključuje pristup, obradu, komunikaciju ili upravljanje informacijama ili strukturom obrade informacija organizacije, ili uvođenje proizvoda ili usluga u sistem za obradu informacija, u skladu je sa svim odgovarajućim bezbednosnim zahtevima..[45]

Da bi se procenilo da Carina Kosova ima mehanizme za bezbednost informacija i kontinuitet poslovanja, ustanovljeni su sledeći kriterijumi:

- Carina Kosova mora da dokumentuje, odobri i saopšti odgovarajuće politike i procedure za usmeravanje poslovanja i IT operacija kako bi ostvarila svoj mandat. Politike bezbednosti informacija treba da pokriju sve operativne rizike i da budu u stanju da razumno zaštite sva kritična informaciona sredstva od gubitka, oštećenja i zloupotrebe. (Ref. ISO 27000: Sistem upravljanja bezbednošću informacija i druge primenljive interne politike, procedure ili pravila).[46]
- Carina Kosova treba da ima jasne IT dužnosti i odgovornosti u vezi sa politikom bezbednosti informacija, bez sukoba odgovornosti ili neusaglašenosti u aktivnostima bezbednosti informacija (poziva se na ISO 27000).[47]

  Aktivnosti u oblasti bezbednosti informacija treba da koordiniraju predstavnici iz različitih delova organizacije, sa odgovarajućim ulogama i odgovornostima. Proces autorizacije menadžmenta za postojeće i nove informacione sisteme mora biti definisan i implementiran. Zahtevi

43 Dodatak 2 Sporazum između Carine Kosova i Konferencije Ujedinjenih Nacija o Trgovini i Razvoju (UNCTAD), Mart 2023.
44 Priručnik Revizije Informacione Tehnologije – Ugovaranje, Bezbednost
45 ISO 27001 – Politike Bezbednosti Informacije.
46 Priručnik Revizije Informacione Tehnologije – Informacija i Kibernetička Bezbednost, Politika Bezbednosti informacije.
47 Priručnik Revizije Informacione Tehnologije – Informacije i Kibernetičke Bezbednosti, Strukture bezbednosti IT-je.

poverljivosti ili ugovori o ne otkrivanju podataka koji odražavaju potrebe organizacije za zaštitu informacija treba da budu identifikovani i redovno pregledani. Rizici za informacije i objekte za obradu informacija organizacije iz poslovnih procesa koji uključuju eksterne strane moraju biti identifikovani i primenjene odgovarajuće kontrole pre nego što se pristup dozvoli. Informacioni sistemi moraju biti konfigurisani i operativni kako bi se osiguralo da se revizijski tragovi generišu za sve podatke o transakcijama. Izveštaji o događajima moraju biti tačni za sve aktivnosti koje obavljaju korisnici sistema. Pristup evidenciji revizorskog traga treba da bude ograničen i kontrolisan, a integritet podataka revizorskog traga treba da bude osiguran protiv modifikacija.[48]

- Carina Kosova mora da obezbedi da svi zaposleni (uključujući ugovarače ili korisnike osetljivih podataka) budu kvalifikovani za održavanje podataka, korišćenje resursa, razumeju dužnosti i odgovornosti. Od regrutovanja do prestanka radnog odnosa, osoblje mora da održava Bezbednost Informacija. Po prestanku ugovora o radu prestaje im pristup.

  I nudi vam se periodična obuka za osvežavanje. Obuka, koja pruža odgovarajuće veštine i znanja zaposlenima čija je uloga u organizaciji značajna za informacionu bezbednost i kibernetiku..[49]

- Politika pristupa Carine Kosova mora da obezbedi osnovu za kontrolu mešanja u informacije. Funkcija bezbednosti informacija prati efektivnost kontrole operacija upravljanja korisničkim nalogom na vreme i izveštava o efikasnosti i efektivnosti operacije.[50]

  Dodela i korišćenje privilegija u okruženju informacionog sistema mora biti ograničeno i kontrolisano, odnosno privilegije se dodeljuju na osnovu potrebe za korišćenjem, privilegije se dodeljuju tek nakon formalnog procesa autorizacije.[51]

48 ISO 27001 – Struktura Bezbednosti IT-je.
49 Priručnik Revizije Informacione Tehnologije- Informacija i Kibernetička Bezbednost, Bezbednost IT -ja Ljudskih Resursa.
50 Priručnik Revizije Informacione Tehnologije– Informacija i Kibernetička Bezbednost, Kontrola Pristupa.
51 ISO 27001 – Kontrola Pristupa.

- Carina Kosova mora da pokrije sve kritične oblasti organizacije u grupi. Zahteve za dužnosti i odgovornosti i uslove za članove grupe.[52]

  Testovi plana kontinuiteta poslovanja treba da osiguraju da su svi članovi tima za oporavak i drugo relevantno osoblje svesni planova i svoje odgovornosti za kontinuitet poslovanja i bezbednost informacija i da znaju svoju ulogu kada se plan pozove.[53]

Da bi se procenilo da u informacionom sistemu ASYCUDA World postoje mehanizmi kontrole aplikacija koji omogućavaju siguran, logičan i pouzdan pristup informacionom sistemu, utvrđeni su sledeći kriterijumi::

- Pravila validacije moraju biti dobro dizajnirana, dokumentovana i implementirana u interakciji ulaznih podataka; različite metode unosa podataka treba dokumentovati; nevažeći podaci moraju biti pravilno odbačeni od strane aplikacije; kriterijumi validnosti se ažuriraju na odgovarajući i ovlašćen način; sveobuhvatne kontrole kao što su pravila registracije i autorizacije treba da budu na mestu u slučaju mogućnosti suštinskih kontrola pristupa; postoje odgovarajuće kontrole i dokumentacija za unose aplikacija. [54]

  Trebalo bi da postoje dokumentarne i fizičke provere robe koja izlazi u crvenom kanalu (ekipe za posmatranje), kao i kontrola dokumentacije u žutom kanalu. Dokumentarna kontrola na osnovu analize rizika za supstance koje izlaze u zelenom i plavom kanalu. Ostale kontrole naknadne dokumentacije iz Sektora za Post Dokumentacionu Kontrolu.

  Trgovačke marke moraju biti identifikovani tokom faze carinjenja u DUD odeljku 31 DUD-a, tako da nakon registracije trgovačke marke, AW sistem upozorava da li se radi o zaštićenoj trgovačkoj marki..[55]

52 Priručnik Revizije Informacione Tehnologije – PVB – PRF – Struktura Funkcije Kontinuiteta Poslovanja.
53 ISO 27001 – Struktura funkcionisanja kontinuiteta poslovanja.
54 Priručnik Revizije Informacione Tehnologije – Kontrola Aplikacije, kontrole ulaza.
55 Carina Kosova – Identifikacija Rizika Carine Kosova 2023.

- • Aplikacija mora ispravno identifikovati greške u transakcijama. Integritet podataka se mora čuvati čak i tokom povremenih prekida u obradi transakcija. Trebalo bi da postoji adekvatan mehanizam za rukovanje greškama u obradi, pregledu i pojašnjenju datoteka na čekanju.[56]

  Službenici iz relevantnog sektora moraju kontinuirano da ažuriraju procenu rizika, primaju informacije i obrađuju ih u sistemu ASYCUDA World, koji se zatim mogu pročitati u obliku kriterijuma tokom faze ispitivanja, kao i svaki korisnik AW, da na osnovu ovih kriterijumi (nivoi rizika) subjekti se ponovo kanališu iz samog AW sistema u Žuti, Plavi, Zeleni i Crveni kanal.[57]

Metodologija revizije

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

Da bi se procenila identifikacija potreba i adresiranje zahteva za bezbednost informacija u projektima ugovorenim sa Carinom Kosova, biće sprovedeno sledeće:

- Pregled ugovornih politika i dokumenata kako bi se osiguralo da su odobrene i sprovedene.
- Pregled dokumenata kako bi se procenilo da je organizacija identifikovala rizike i da je svesna njih.
- Pregled dokumenta kako bi se procenilo da li je organizacija identifikovala bezbednosne zahteve i unela ih u ugovor ili SLA.
- Verifikacija da li organizacija ima sigurnost u odnosu na bezbednosne mehanizme koje je uspostavio provajder usluga.

56 Priručnik Revizije Informacione Tehnologije– Kontrola aplikacije, Kontrola obrade.
57 Carina Kosova – Identifikacija Rizika za Carinu Kosova 2023.

Da bi se procenilo da Carina Kosova ima mehanizme za bezbednost informacija i kontinuitet poslovanja, biće sprovedeno sledeće:

- Provere dokumenata kako bi se potvrdilo da IT strategija na adekvatan način rešava kritičnu ulogu bezbednosti informacija. Takođe, pogledajte upotrebu matrice upravljanja IT i matrice IT strategije. Provera da li IT bezbednosni plan identifikuje: dužnosti i odgovornosti, zahteve osoblja, svest o bezbednosti i obuku, implementaciju praksi, potrebu za ulaganjem u potrebne bezbednosne resurse. Pregledajte i analizirajte dijagram kako biste potvrdili da se odnosi na organizacioni apetit za rizik u vezi sa bezbednošću informacija i da ovaj dijagram jasno uključuje svrhu i ciljeve funkcije upravljanja bezbednošću.
- Utvrđivanje da li su odgovornosti za IT bezbednost dobro definisane. Provera da li postoji proces za određivanje prioriteta predloženih bezbednosnih inicijativa, uključujući potrebne nivoe politika, standarda i procedura.
- Provera da li su uloge koje su kritične za bezbednost informacija jasno definisane i dokumentovane. Zaposleni i treća lica kojima su dodeljene takve uloge moraju znati svoje odgovornosti u pogledu zaštite informacionih sredstava organizacije. Pregledajte za ispravnu identifikaciju kritičnih uloga za koje su potrebne kontrole verifikacije bezbednosti. Kontrola za odgovarajuću podelu dužnosti između upravljanja IT bezbednošću i operacija. Kontrola da li je politika raspoređivanja, transfera i rotacije IT osoblja, kao i otpuštanja zaposlenih jasna kako bi se smanjila zavisnost od pojedinca. Provera koji su mehanizmi prenosa znanja ispoštovani.
- Kontrolne procedure za utvrđivanje koliko često se proverava pristup korisnika i privilegije. Kontrola kako se privilegije dodeljene korisnicima potvrđuju.

  Intervju sa mostrom korisnika i provera uputstva da biste proverili kako su korisnici obavešteni o svojim odgovornostima u zaštiti osetljivih informacija ili imovine, ako im je dat odgovarajući pristup.

- Pregled dokumenata/intervju sa odgovornim osobljem za procenu svih kritičnih oblasti organizacije koje treba da budu zastupljene u grupi za kontinuitet poslovanja.

  Pregled dokumenata za procenu vlasništva i odgovornosti za kontinuitet poslovanja odgovornosti u višem rukovodstvu. Na primer, ako je menadžment

identifikovao nivo i hitnost oporavka i ako se to odražava u politikama. Pregled dokumenata kako bi se procenilo da su sva kritična odeljenja odredila članove tima za oporavak od katastrofe zajedno sa dobro definisanim dužnostima. Intervju sa određenim brojem osoblja u grupi za kontinuitet poslovanja/ili ekvivalentu, kako biste procenili da li su svesni svoje uloge u kontinuitetu poslovanja za svaku kritičnu poslovnu jedinicu/odeljenje.

Da bi se procenilo da u informacionom sistemu ASYCUDA World postoje mehanizmi kontrole aplikacija koji omogućavaju bezbedan logičan i pouzdan pristup informacionom sistemu treba se realizovati:

- Provera da li su pravila validacije dobro osmišljena i dokumentovana. Provera da li postoje provere validacije za ulazne podatke: posmatranje korisnika aplikacije u stvarnoj akciji, pokretanje aplikacije u test okruženju i testiranje različitih interakcija za ulazne podatke; analiza evidencije podataka uskladištenih u bazi podataka korišćenjem CAAT (IDEA). Dobiti funkcionalni opis za svaku klasu ulaznih informacija i dizajn za snimanje podataka o transakcijama. Provera funkcionalnosti i modela za prisustvo blagovremenih, kompletnih provera i poruka o greškama.

  Procena da li kriterijumi i parametri validacije na ulaznim podacima odgovaraju poslovnim pravilima i sprovođenje odbacivanja tipova podataka koji se ne uklapaju. Inspekcija rukovodilaca o periodičnoj kontroli kriterijuma i parametara validnosti ulaznih podataka, ako su potvrđeni i ovlašćeni na odgovarajući način. Sigurnost se mora održavati kroz pregled dokumentacije, analizu kodiranja i intervjua. Određivanje koje interakcije postoje sa aplikacijom. Ove interakcije moraju biti u obliku prenosa podataka u realnom vremenu ili periodičnog prenosa putem paketnih procesa. Pregled dijagrama toka procesa i sistemskog koda.

- Procena da li aplikacija sadrži ispravne provere valjanosti da bi se obezbedio integritet obrade. Inspekcija bilansa stanja i drugih dokumenata kako bi se potvrdilo da su ulazni brojevi u skladu sa izlaznim brojevima kako bi se osigurala obrada podataka. Izvođenje transakcija kroz proces radi verifikacije usaglašavanja efektivno određuje da li ukupni podaci odgovaraju prijavljenim vanbilansnim uslovima.

  Inspekcija revizorskih tragova i drugih dokumenata, planova, politika i procedura kako bi se potvrdilo da su mogućnosti sistema efikasno dizajnirane

da automatski održavaju integritet podataka. Provera funkcionalnog opisa i informacija o dizajnu za unos podataka o transakciji da bi se potvrdilo da se transakcije koje ne funkcionišu u rutinama validacije postavljene su u datotekama za odlaganje. Potvrda da su starije neuspele transakcije ispravno korigovane.

Relevantna dokumentacija

Uredbe

Uredba (Qrk) - Br. 06/2020 za Oblasti Administrativne Odgovornosti Kancelarije Premijera i Ministarstava

Ova uredba određuje oblasti administrativne odgovornosti Kancelarije Premijera i Ministarstava Vlade Republike Kosova.

Relevantna Dokumentacija

Kodeks Br.03 L-109 Carina i Akciza Kosova

Ovaj kodeks reguliše osnovne elemente sistema za carinsku zaštitu ekonomije Republike Kosovo i prava i obaveze svih učesnika, u sprovođenju carinskih zakona.

Strateški plan CK-a 2019-2023

Ovaj dokument definiše prioritete i strateške ciljeve, kao i aktivnosti koje Carina Kosova namerava da sledi za period 2019-2023. Ovom strategijom predviđeno je da se, uz što racionalnije korišćenje raspoloživih resursa, sprovode politike i razvijaju procedure vezane za međunarodni trgovinski lanac, promet vozila i putnika, kao i graničnu i unutrašnju carinsku kontrolu.

Dodatak II: Pismo potvrde

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

Njesia Org. Org. Jedin. Org. Unit	Shif.klasif. Klasif. Kod Class. Code	Nr. Prot. Br. Prot. Prot. No.	Nr. faqeve Br. Stranica No. Pages
06	47	2255	1

19.12.2024

01/1029/2024

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

Dogana e Kosovës – Carina Kosova – Kosovo Customs
Zyra e drejtorit të përgjithshëm
LISTË DISTRIBUIMI/ CIRKULARNO PISMO/ ROUTING SLIP

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit **'Sistemet e Informacionit në Doganën e Kosovës - ASYCUDA World'**, dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data: Prishtinë
19 Dhjetor 2024

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **Sistemet e Informacionit në Doganën e Kosovës - ASYCUDA World** (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.

DOGANA E KOSOVËS · CARINA KOSOVA · KOSOVO CUSTOMS

Agron Lluganiu
Drejtori i Përgjithshëm
Dogana e Kosovës

Prishtinë

19 Dhjetor 2024

Informacioni
Sistem Carine Kosova –
ASYCUDA World

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