REPUBLIKA E SHQIPËRISË

KONTROLLI I LARTË I SHTETIT

AUDITIMET E TEKNOLOGJISË SË INFORMACIONIT

2014-2018

Tiranë, 2018

Seria: botime KLSH 13/2018/97

AUDITIMI I TEKNOLOGJISË SË INFORMACIONIT
2014-2018

Tiranë 2018

Titulli:

Auditimi i Teknologjisë së Informacionit

2014-2018

Përgatitur nga:

Dr. Bujar Leskaj

Kozma Kondakçiu

Redaktore:
Elsona Papadhima

Grafika:
Kozma Kondakçiu

Seria: botime KLSH 13/2018/97

ISBN: 978-9928-159-77-9

© Mundësohet përdorimi i këtij materiali kundrejt citimit të burimit:
“Departamenti i Auditimit të Teknologjisë së Informacionit, Kontrolli i Lartë i Shtetit”.

Shtypur në Shtypshkronjën ”Botime Morava”

Tiranë 2018

Lënda	Faqe
Hyrje	4
Auditime të Teknologjisë së Informacionit	10
Viti 2014	11
Fillimet e Auditimeve të Teknologjisë së Informacionit	11
Viti 2015	12
Auditim i Teknologjisë së Informacionit në AKBPM.	13
Auditim i Teknologjisë së Informacionit në APP.	22
Viti 2016	27
Auditim i Teknologjisë së Informacionit në MF.	28
Auditim i Teknologjisë së Informacionit në FSDKSH.	40
Viti 2017	66
Auditim i Teknologjisë së Informacionit në DPTTV.	67
Auditim i Teknologjisë së Informacionit në INSTAT.	79
Auditim i Teknologjisë së Informacionit në UK, Tiranë.	87
Auditim i Teknologjisë së Informacionit në ISSH.	99
VITI 2018	117
Auditim i Teknologjisë së Informacionit në AKSHI.	118
Auditim i Teknologjisë së Informacionit në DPGJC.	132
Auditim i Teknologjisë së Informacionit në DAP.	149
Auditim i Teknologjisë së Informacionit në QKB.	157
Auditim i Teknologjisë së Informacionit në Bashkinë Elbasan.	171
Auditim i Teknologjisë së Informacionit në APP.	179
Anekse	193
Metodologjia e Auditimit të Teknologjisë së Informacionit në KLSH	194
Lista e Auditimeve të Teknologjisë së Informacionit për vitet 2014-2018	195
Fjalori i shkurtimeve	196

Hyrje

Ky botim paraqet një dritare njohurish në duar të audituesve të T.I. dhe jo vetëm, të cilët duan të njihen me rrugëtimin e një sfide tashmë të fituar: atë të ngritjes dhe zhvillimit të Auditimit të T.I., një nga dhjetë risitë e paraqitura në Projekt-Ide-në e datës 14 dhjetor 2011, prezantuar pranë Komisionit për Ekonominë dhe Financat të Kuvendit të Shqipërisë, ku si kandidat i nominuar nga Presidenti i Republikës për detyrën e Kryetarit të Kontrollit të Lartë të Shtetit, parashtrova se: ***"Intensifikimi i përdorimit të metodave bashkëkohore të teknologjisë së informacionit do të jetë një nga instrumentet bazë të rritjes së performancës së punës së KLSH-së dhe do të lehtësojë kontrollet e kryqëzuara të transaksioneve financiare"****.*

Kjo risi u përfshi në planet strategjike të zhvillimit me objektiv Zhvillimin e Auditimit të T.I., ku KLSH guxoi të ndryshojë mënyrën e auditimit, duke futur përdorimin e Teknologjisë së Informacionit në të.

Auditimi i Teknologjisë së Informacionit(IT) si një nga llojet më të reja e të vështira të auditimit, përbën pa dyshim sot sfidën institucioneve të auditimit jo vetëm të rajonit tonë, por edhe institucioneve me të zhvilluara të auditimit, anëtare të INTOSAI-t.

Njëlloj si gjashtë vite më parë në tetor 2012 themeluam Departamentin e Auditimit të Performancës si një risi absolute në aktivitetin e KLSH, dy vite më vonë, në tetor 2014 ngritëm Drejtorinë e Auditimit të T.I., nisur nga një mungesë përvoje dhe njohurish në këtë lloj auditimi, por duke caktuar drejtues një audites dhe inxhinier me përvojë, si z, Kozma Kondakçiu, të cilin e falenderoj për punën e kryer. Kishim për orientim, krahas Projekt-Idesë, edhe Strategjinë e Zhvillimit te institucionit 2013 -2017, ku përvijuam drejtimet tona për zhvillimin e auditimeve të këtij lloji, si një nga objektivat strategjikë kryesorë, duke përcaktuar edhe partnerët dhe mbështetësit kryesorë të procesit.

Gjatë viteve 2012-2018, kemi hedhur hapa të konsiderueshëm drejt zhvillimit të plotë të auditimit të T.I., nëpërmjet:

1) *rekrutimit të punonjësve të rinj;*
2) *kryerjes së ndryshimeve të nevojshme ligjore dhe organizative,*
3) *zgjerimit të infrastrukturës fizike për auditimet e T.I.;*
4) *zhvillimit të kapaciteteve audituese;*
5) *pajisjes me metodologjinë e duhur si dhe trajnimin dhe çertifikimin e audituesve IT të KLSH nga organizatat ndërkombëtare.*

Të mbështetur fillimisht, që në vitin 2012 e në vijim nga SIGMA me trajnime në fushën e auditimit te T.I.-së dhe më pas, të përfshirë në Programin e Trajnimit të Institutit për Zhvillim të INTOSAI-t(IDI) për audituesit e T.I.së, filluam përpjekjet e para për të përgatitur stafin që në të ardhmen do të bëhej pjesë e këtyre auditimeve. Krahas këtyre

institucioneve, një numër të konsiderueshëm trajnimesh realizuam me ekspertë të Dhomës Kombëtare të Auditimit të Polonisë (NIK), SAI-t të Zvicrës dhe Kroacisë.

Këto zhvillime krijuan kushtet në ndërtimin dhe më pas rritjen e kapaciteteve audituese për teknologjinë e informacionit, duke pajisur audituesit e përzgjedhur me njohuritë dhe aftësitë e nevojshme për të qenë të aftë të kryejnë të tilla auditime. I konsideruar edhe nga audituesit profesionistë si një nga auditimet më komplekse, realizimi i auditimeve të T.I. ishte një nga sfidat me të cilat filluam të përballeshim që në tremujorin e fundit të 2014-ës. Nevoja për staf të kualifikuar, të pajisur me njohuri profesionale të T.I. dhe njëkohësisht me dëshirën për zhvillim dhe mësim u përball me vështirësitë për të rekrutuar stafin e duhur dhe të përshtatshëm që do të mundësonte suksesin në të ardhmen. Për këtë qëllim, trajnuam stafin e Drejtorisë në drejtime të ndryshme, sikurse Programi IDEA, përdorimi i teknikave CAAT në auditim, menaxhimi i riskut të T.I. dhe auditimi i sistemeve të T.I.. I rëndësisë së veçantë ishte trajnimi për çertifikimin e audituesve të T.I. nga IDI online. Hapi kryesor ishte ndërmarrja e misionit të vetëvlerësimit të Sistemeve të T.I. në KLSH, me moderimin e SAI-t Zviceran, i cili shërbeu si pikë referimi për të vlerësuar nivelin e maturitetit të stafit tonë dhe përcaktimin e objektivave të zhvillimit për të ardhmen. Krahas trajnimeve, i kushtuam shumë rëndësi dhe vëmendje përgatitjes së dokumenteve metodologjikë në fushën e auditimit të TI-së, të cilat janë ende në zhvillim.

Gjatë vitit 2015, realizuam për herë të parë dy auditime të sistemeve T.I:

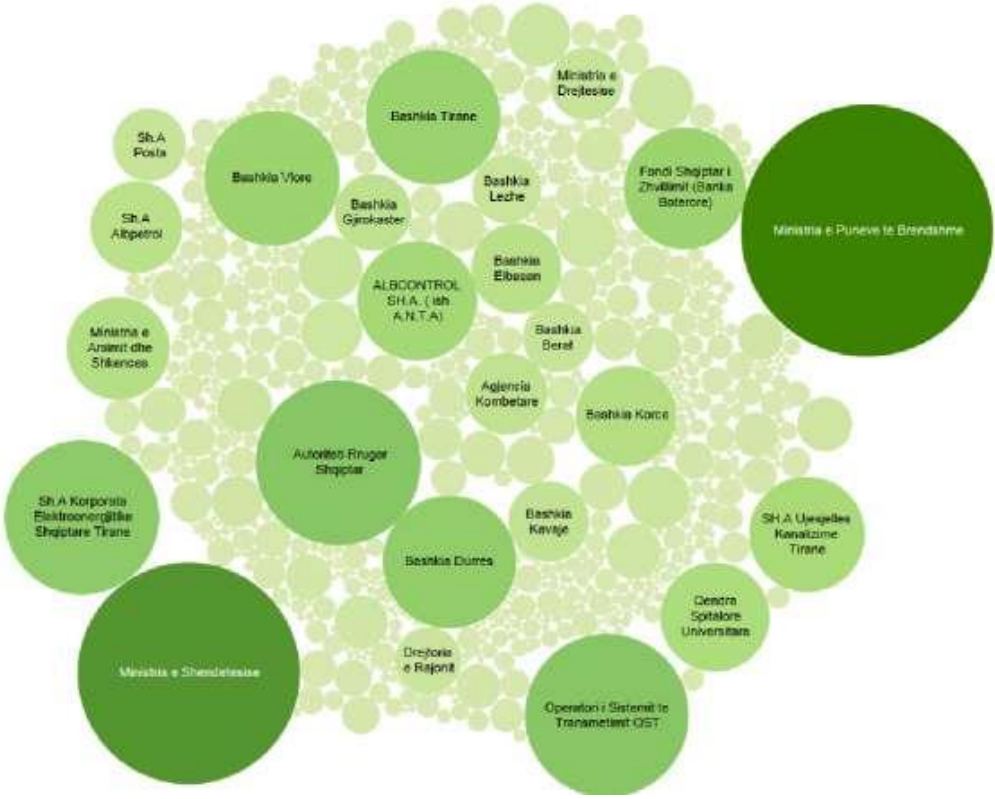
1. Auditimin e teknologjisë se informacionit në Agjencinë e Barnave dhe Paisjeve Mjekësore;
2. Auditimin e teknologjisë së informacionit në Agjencinë e Prokurimeve Publike

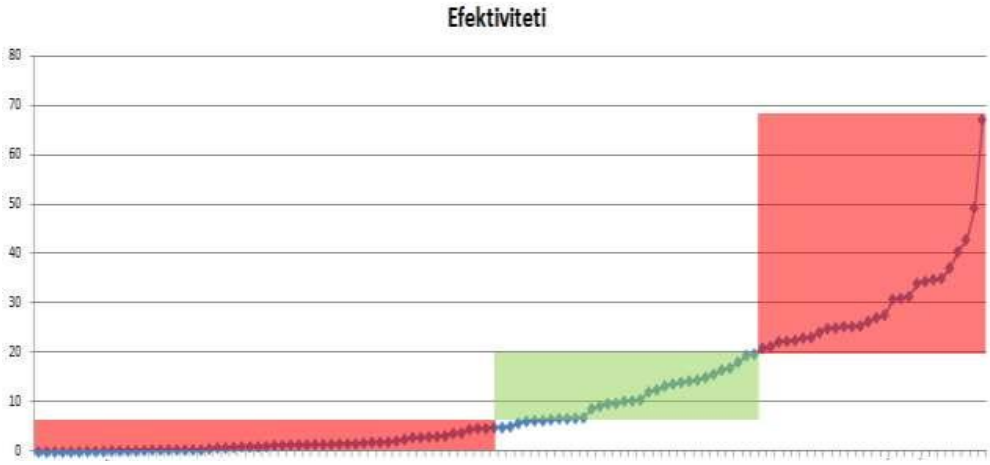
Krahas këtyre, institucioni kreu disa auditime me përdorimin e teknikave CAAT dhe vizualizimit të informacionit Auditimi i kryer në Agjencinë e Barnave dhe Paisjeve Mjekësore ishte një auditim pilot i mbështetur nga Inisiativa për Zhvillim e INTOSAI-t (IDI) i kryer pas trajnimit online njëvjeçar.

Përdorimi i teknikave vizualisuese në auditim është sot një realitet i diktuar jo vetëm nga sasia e madhe e informacionit që po rrethon gjithmonë e më shumë ambientin e auditimit por edhe për vlerat e shtuara që ai i ofron atij.

Teknikat për ***Analizimin Interaktiv të të dhënave*** *kanë përfshirë çdo fushë të jetës dhe pa dyshim edhe atë të auditimit. KLSH në zbatim të rekomandimeve të Simpoziumit për Teknologjinë e Informacionit mbajtur në Mars 2014 me rastin e 300 vjetorit të themelimit të Gjykatës së Auditimit të Gjermanisë si dhe Kongresit të IX-të të EUROSAI të mbajtur në Qershor 2014, në Hagë, për zbatimin e Teknikave Inovative në Auditim nëpërmjet vizualizimit të tyre po investon në zhvillimin e* ***burimeve njerëzore*** *dhe Mjeteve Analizuese dhe Vizualizuese. Gjatë vitit 2015 për herë të parë në KLSH u përdor në*

*auditim A**nalizë Interaktive e** riskut. Këto metoda u përdoren në identifikimin e zonave me risk në prokurimet publike dhe do të shtrihen në fusha të tjera të auditimit.*





Përdorimi i këtyre metodave na ka shërbyer në analizat e riskut që kryejmë në planifikimin e auditimeve, si dhe në zbulimin e zonave ku interesat publike kërkojnë përmirësime ligjore për përdorimin me efektivitet, efiçience dhe ekonomicitet të fondeve publike dhe burimeve njerëzore.

***

Në drejtim të zhvillimit të Auditimit të T.I., kemi shfrytëzuar mundësitë e brendshme dhe ato të ofruara nga partnerët ndërkombëtarë, ku veçojmë suportin e dhënë për trajnimin e 3 audituesve tanë nga Inisiativa për Zhvillim e INTOSAI-t (IDI), shkëmbimet dhe e trajnimet me grupet e punës së IT të EUROSAI-t dhe INTOSAI-t (ITWG dhe WGITA), bashkëpunimi me Zyrën e Auditimit të Zvicrës, konkretizuar me kryerjen e vetëvlerësimit të IT në vitin 2015 dhe atë të vetëvlerësimit të Auditimit TI në vitin 2016, trajnimet e kryera në qendrat e specializuara të auditimit IT gjatë vitit 2017 në Indi dhe Pakistan si dhe mbështetjen e dhënë nga specialistët e SAI-ve të Polonisë, Portugalisë e Estonisë nëpërmjet projektit të Binjakëzimit IPA (AL 13 IB FI 01) për trajnimin e stafit të drejtorisë së T.I. të KLSH, apo ekspertë vendas si informaticieni i njohur z. Endri Meksi.

Po ashtu, theksojmë ndihmesën në krijimin e bazës së të dhënave për subjektet e auditimit IT (ICTS Database), krijimin dhe trajnimin e linjës së parë të suportit me njohuri mbi auditimin IT dhe zhvillimit të ***Manualit Aktiv të Auditimit të Teknologjisë së Informacionit.***

Ky manual elektronik, me vlera të padiskutueshme në analizimin e riskut, planifikimin e auditimit si dhe përdorimit të eksperiencës së auditimeve të mëparshme, përbën ***një risi jo vetëm për KLSH por edhe për komunitetin botëror të auditimit.*** *Ky produkt i cili lindi, u testua në një auditim pilot, u përmirësua edhe me kontributin modest të audituesve të Teknologjisë së Informacionit të KLSH dhe është prezantuar në disa evente të grupeve të punës së IT së EUROSAI-t dhe INTOSAI-t, si frut i projektit të binjakëzimit IPA 2013 me specialistët polakë dhe kroatë.*

Ai është pranuar dhe po implementohet si një inovacion në fushën e auditimit nga komuniteti ndërkombëtar i Auditimit të T.I..

***

Ky botim vjen pas publikimit në kolanën "Botime KLSH" të Kornizës COBIT®4.1"Objektivat e Kontrollit të Teknologjisë së Informacionit" në gjuhën Shqipe (Control Objectives for Information and related Technolog) dhe Manualit të Auditimit të Teknologjisë së Informacionit.

Sot Auditimi i Teknologjisë së Informacionit në KLSH përdor Manualin Aktiv të Auditimit të Teknologjisë së Informacionit një risi kjo e komunitetit Auditues të Teknologjisë së Informacionit të INTOSAI-t, sidhe zhvillohet elektronikisht (krahas

auditimeve të tjera) në Sistemin e Menaxhimit të Proceseve të Auditimit dhe atyre ndihmëse në institucion SIMMPA (Rev-Zone).

Në qasjen tonë në zhvillimin e auditimit të T.I. na ka ndihmuar dhe orientuar drejt edhe eksperienca e Zyrës Supreme të Auditimit të Çekisë, Presidenti i së cilës dhe njëkohësisht Zv-President i EUROSAI-t, Inxh. Miloslav Kala ka kontribuar me një leksion dhënë audituesve shqiptarë në gusht 2017, ku theksoi rëndësinë e jashtëzakonshme për SAI-t të përdorimit dhe përpunimit të informacionit dixhital në dispozicion të agjencive qeveritare, si dhe solli raste të shumta nga eksperienca e auditimit të të dhënave të përqëndruara (Big Data) të SAI-t çek në projektet dhe shërbimet qeveritare

Këtë vit arritëm të ngrinim nivelin nga Drejtori në Departament të mirëfilltë të auditimit të T.I.. Në bazë të Strategjisë së Zhvillimit të KLSH 2018-2023, në të ardhmen, prioritet për auditimet e Teknologjisë së Informacionit do të jetë zhvillimi i kapaciteteve të auditimit IT nëpërmjet:

i) Konsolidimit të Departamentit të Auditimit të IT.
ii) Rekrutimit të stafit auditues me aftësi profesionale në IT
iii) Zhvillimit dhe rritjes së kapaciteteve audituese me njohuri në teknologjinë e informacionit në çdo departament auditimi,
iv) Plotësimit dhe zgjerimit të manualit interaktiv të auditimit IT.

Me konsolidimin e Departamentit të Auditimit të T.I., një strukturë që garanton rritjen e ritmit të zhvillimit të auditimeve të T.I. si në numër dhe në cilësi, duke zbatuar eksperiencën e fituar nga bashkëpunimi dhe trajnimet me ekspertët e SAI-ve partnerë të vendeve të zhvilluara të Evropës, si Polonia, Kroacia, etj., si dhe nga projektet e BE-së dhe të donatorëve të tjerë si USAID, si KLSH kemi krijuar kushtet për thellimin e një procesi që ka si qëllim kryesor rritjen e kapaciteteve audituese të stafit të KLSH, nëpërmjet përftimit të njohurive të reja për audituesit dhe aftësimit të tyre për t'iu përshtatur kërkesave të profesionit në kryerjen e Auditimeve të Sistemeve të Teknologjisë së Informacionit.

Në sajë të politikave institucionale të ndjekura që nga viti 2012 e në vazhdim, Auditimi i Teknologjisë së Informacionit ka fituar kartën e qytetarisë (Mandatin për të kryer auditimin e sistemeve të T.I. përshkruar në ISSAI 1-Deklarata e Limës, si dhe nenet 3 dhe 14 të ligjit 154 "Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit" datë 27.11.2014).

Rezultatet e punës së kryer për vitet 2014-2018, të paraqitura në këtë botim, e rreshtojnë KLSH në krah te simotrave në EUROSAI në këtë fushë të vështirë të auditimit, me arritje domethënëse të vlerësuara e të pakontestuara nga subjektet e audituar, si dhe nga partnerët tanë ndërkombëtarë.

Eksperienca e fituar në auditimet e kryera, e përshkruar në këtë libër, paraqitet shumë e dobishme për të vendosur piketat e një zhvillimi të qëndrueshëm të auditimit të T.I., në përputhje me misionin e institucionit për t'i shërbyer qytetarit dhe Kuvendit në garantimin e përdorimit me efektivitet, efiçiencë dhe ekonomicitet të parasë publike dhe në thellimin e luftës kundër korrupsionit dhe mashtrimit financiar, në përputhje të plotë me standardet ISSAI, duke zbatuar edhe në këtë fushë audituese moton "Experienta Mutua Omnibus Prodest" (Nga eksperienca e përbashkët, përfitojnë të gjithë) të INTOSAI-t.

Së fundi, drejtuesit dhe audituesve të Drejtorisë së Auditimit të T.I. të KLSH, të laureua në specialitete si informatikë, informatikë e aplikuar dhe informatikë ekonomike:

Kozma Kondakçiu, Armanda Begaj, Benard Haka, Elira Cukalla, Aldo Kita, Elisa Metaj, Meald Habazaj, Bledi Dervishi, Elsona Papadhima, Marsel Tufa dhe Rodjan Alimerkaj ju uroj suksese në punën e vështirë dhe sfiduese të auditimit të T.I., por me shumë vlerë të shtuar për auditimin e jashtëm publik të Shqipërisë!

Bujar Leskaj

AUDITIME TË TEKNOLOGJISË SË INFORMACIONIT

AUDITIMI I TEKNOLOGJISË SË INFORMACIONIT VITI 2014

Fillimet e Auditimeve të Teknologjisë së Informacionit

Drejtoria e Auditimit të Teknologjisë së Informacionit u krijua mbështetur në Urdhrin e Kryetarit të KLSH-së datë 15.10.2014, në pëbërje të Departamentit të Auditimit të Buxhetit Qendror, Administratës së Lartë Publike, Menaxhimit Financiar dhe Auditimit të Brendshëm me objektiv kryesor konsolidimin e njohurive dhe krijimin e një tradite në këtë fushë të re dhe të vështirë të Auditimit.

Gjatë vitit 2014 u krye procesi i rekrutimit të stafit të ri në një proces i cili rezultoi i vështirë pasi konkurrentet që paraqiteshin nuk plotësonin kriteret e kërkuara. Për këtë arsye procedurat e rekrutimit u përsëriten disa herë, pa ndryshuar kriteret e përzgjedhjes deri në zgjedhjen e stafit të drejtorisë.
Për vështirësi në procesit e rekrutimit ishim të përgatitur, pasi eksperienca e SAI homologe na tregonte se është e vështirë tërheqja e specialistëve të fushës së TI në sektorin publik, si dhe mbajtja e tyre nga SAI pas trajnimeve e certifikimeve përkatëse.
Puna me stafin e ri nisi njëkohësisht në disa drejtime kryesore si:

1. Trajnime.

– Në shtator të vitit 2013 stafi i TI dhe auditues të buxhetit morrën pjesë në trajnimin "Auditimi Teknologjisë së Informacionit në Sistemin e Thesarit në Shqipëri" nga projekti " SIGMA mbështetje për KLSH" Tiranë.

Gjatë vitit 2014 stafi i drejtorisë ka kryer trajnime të ndryshme, ku veçojmë trajnimet e muajit gusht 2014 mbi programin IDEA, Auditimi TI dhe përdorimin e teknikave CAAT në auditim. Në trajnimet e organizuara në bashkëpunim me SAI-et homologe u zhvilluan trajnimet:

- Vetëvlerësimi i TI dhe auditimit TI, Bernë të Zvicrës, janar 2014;
- "Auditimin e Sistemeve të Informacionit TI", në Gjykatën Turke të Llogarive, prill 2014;
- Certifikimin në TI Audit të 3 audituesve nga IDI (e- learning qershorit-korrik 2014);
- Procesi i vetëvlerësimit të TI me moderim nga SAI i Zvicrës, tetor 2014;
- Simpoziumi Evropian për Teknologjinë e Informacionit dhe 300 vjet Gjykatë e Auditimit të Gjermanisë. Potsdam, dt. 15.03.2014;
- "Roli i auditimit të brendshëm në menaxhimin e riskut, mashtrimit dhe riskun në TI" në Qendrën e Ekselencës në Financë (CEF), Slloveni, tetor 2014;
- "Planifikimi i Auditimit TI", organizuar nga IDI, Poloni, dhjetor 2014.

2. Hartimin, përkthimin dhe hartimit të:

a. Rregullores se drejtorisë;
b. Manualeve
c. Praktikave dhe Standardeve ndërkombëtare të TI dhe INTOSA-it në fushën e TI;
d. Ligjeve, VKM, udhëzimeve në fushën e TI.

3. Pjesëmarrjen në procesin e auditimit dhe proceseve ndihmëse në institucion.

1. Audituesit e drejtorisë u angazhuar në 10 auditime në përbërje të grupeve të punës të departamenteve të tjera. Në vitin 2014 filloi si pjesë trajnimit nga IDI Auditimi Pilot mbi Vlerësimin e Sistemeve të Teknologjisë së Informacionit në Agjencinë e Kontrollit të Barnave dhe Pajisjeve Mjekësore (AKBPM) me asistencën e ekspertëve: Shefali Andaleeb (IDI), Pawel Banas (Poland), Madhav Singh Panvvar (USA), Tameika Avagaye Fleming (Anguilla), Annette Mvvangi (Kenya) dhe Neelesh Kumar (India).

AUDITIMET E TEKNOLOGJISË SË INFORMACIONIT VITI 2015

Në vitin 2015 Drejtoria e Auditimit TI në përbërje të Departamentit të Auditimit të Buxhetit Qendror, Administratës së Lartë Publike, Menaxhimit financiar dhe Auditimit të Brendshëm, e sapo krijuar kishte në përbërje 5 anëtarë nga të cilët 4 audites.

Treguesit për vitin 2015

Treguesi	Njësia	Llogaritja	Vlera
Fuqia maksimale Audituese e drejtorisë	ditënjerëz	22 x 11x 5	1210
Auditime të parashikuara gjithsej	numër		2
Për çdo auditim mesatarisht	ditënjerëz	1210/2	605

Për konsolidimin e drejtorisë u zhvillua një proces intensiv trajnimi mbi Auditimin e Teknologjisë së Informacionit me qëllim kryesor rritjen e kapaciteteve audituese ku krahas trajnimeve të brendshme u mor pjesë në shumë trajnime dhe konferenca jashtë vendit të tilla si:

– Në Zyrën Federale të Auditimit të Zvicrës u mbajt takimi i grupit të punës mbi Vetëvlerësimin e Teknologjisë së Informacionit (ITSA) dhe Vetëvlerësimit të Auditimit të Teknologjisë së Informacionit (ITASA), mars 2015;

– Trajnimi “Prezantimi me Auditimin e TI”, në Gjykatën Europiane të Audituesve, mars 2015;

Vlen për tu përmendur që një zhvillim tjetër i rëndësishëm në KLSH, për Drejtorinë e Auditimit të Teknologjisë së Informacionit ishte edhe botimi i manualeve dhe standardeve, të cilat ndihmojnë dhe lehtësojnë punën e audituesve në përmbushjen me sukses të misionit të audituesit. Në kolonën e botimeve të KLSH për vitin 2015 u botuan:

- Manuali i Auditimit të Teknologjisë së Informacionit si dhe
- Objektivat e Kontrollit për Teknologjinë e Informacionit” (COBIT), për tu ardhur në ndihmë jo vetëm stafit të KLSH-së por dhe atyre të Auditimit të Brendshëm, si dhe atyre që duan të bëhen Auditues të Teknologjisë së Informacionit.

Auditimet TI

Auditimet e Teknologjisë së Informacionit të planifikuara e zhvilluara gjatë këtij viti:

1. Auditimi i Teknologjisë së Informacionit, në Agjencinë e Kontrollit të Barnave dhe Pajisjeve Mjekësore (AKBPM) "Mbi Vlerësimin e Sistemeve të Teknologjisë së Informacionit (auditim pilot nga IDI).

2. Auditimi i Teknologjisë së Informacionit, të Ushtruar në Agjencinë e Prokurimit Publik.

Rezultatet e auditimeve

Auditime të Planifikuara për vitin 2015	Subjekte të Audituara të Realizuara	Rekomandime Gjithsej	Rekomandime të Pranuara
2	AKBPM	7	-
	APP	10	19

AUDITIMI I USHTRUAR NË AGJENCINË E KONTROLLIT TË BARNAVE DHE PAJISJEVE MJEKËSORE (AKBPM) "MBI VLERËSIMIN E SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT" (AUDITIM PILOT NGA IDI).

Titulli: "Auditimi i Teknologjisë së Informacionit"

Subjekti: "**Agjencinë e Kontrollit të Barnave dhe Pajisjeve Mjekësore (AKBPM)"**

Përgatitur: 20.06.2015

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 1039/3, datë 19.01.2015.

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Armanda Bega anëtar
3. Lolita Baholli, anëtar
4. Yrjada Jahja, anëtar

Periudha e Auditimit: 01.01.2014 – 31.12.2014
Afati i auditimit: 20.01.2015 - 25.04.2015

Ky auditim është produkt i pjesëmarrjes së Grupit të Auditimit në programin e IDI-t (Iniciativa për zhvillim e INTOSAI-t) për zhvillimin e Auditimit TI në Institucionet Supreme të Auditimit, dhe mbështetet në Manualin e Auditimit të TI dhe ISSAI 5310 "Metodologjia e Rishikimit të Sigurisë së Sistemeve të Informacionit".

Raporti Përfundimtar i Auditimit të ushtruar në Agjencinë e Kontrollit të Barnave dhe Pajisjeve Mjekësore (AKBPM), me objekt "Vlerësimin e Sistemeve të Teknologjisë së Informacionit, për periudhën për periudhën 01.01.2014 - 31.12.2014, si dhe masat për përmirësimin e gjendjes, janë miratuar me Vendim të Kryetarit të KLSH-së Nr. 82, datë 20.06.2015. Bazuar në nenet 15, 25, 30 dhe 32 të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit", për përmirësimin e gjendjes, me shkresën nr. 1039/25, datë 20.06.2015, Raporti Përfundimtar i Auditimit dhe rekomandimet përkatëse i janë dërguar znj. Ornela Ymeraj, Drejtor i Agjencisë së Kontrollit të Barnave dhe Pajisjeve Mjekësore.

Në përfundim të auditimit për gjetjet e konstatuara u lanë rekomandimet përkatëse.

Më hollësisht:

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	Gjatë auditimit u konstatua se ka planifikime të dobëta strategjike, mungesë e planeve të shkruara mbi implementimin e teknologjisë në agjenci, implementimi i shërbimit për faqen web, nuk është dokumentuar si duhet nga agjencia edhe nga operatori. Nga auditimi i faqes së internetit regjistruar me domain-in *akbpm.gov.al* kryer sipas procedurave të urdhrit të prokurimit nr. 18. dt 12.09.2014 konstatohet se ka probleme në Aksesimin e faqes dhe probleme me lidhje të shkëputura. Këto problematika, kanë ardhur si pasojë e mungesës së planifikimit strategjik në drejtim të fushës së teknologjisë së informacionit. Si pasojë e kësaj, konstatohet edhe mosplanifikimi i vazhdueshmërisë së këtij shërbimi, duke e lënë faqen e internetit në kushtet e mosfunksionimit total	Referuar rëndësisë dhe kostove për prokurimet e kryera në fushën e teknologjisë së informacionit, rekomandojmë që AKBPM të marrë masa për hartimin e planit strategjik TI, të zbatojë në përputhje me të implementimin e investimeve në fushën e TI, si dhe të specifikojë procedura të monitorimit, për të shmangur risqet e lidhura me vazhdueshmërinë së infrastrukturës teknologjike.
2.	a. Nga auditimi i qeverisjes së teknologjisë së informacionit u konstatua se:	Institucioni të marrë masa për implementimin e ligjit të Menaxhimit

	b. Nuk ekziston një strukturë qeverisëse, strategjike, e cila do të kompletonte praktikat menaxhuese aktuale dhe do të ndihmonte në arritjen e objektivave të veprimtarisë së subjektit, c. Nuk janë marrë masa për ngritjen e Grupit të Menaxhimit Strategjik, i cili në bazë të Ligjit të Menaxhimit Financiar dhe Kontrollit, do të kishte në përbërje të tij, një specialist të fushës së teknologjisë së informacionit në institucion, i cili do të ishte pjesë e vendimmarrjes qoftë e institucionit, qoftë edhe e aspekteve që lidhen me TI. Mungesa e një Strategjie të teknologjisë së informacionit në AKBPM, sjell një risk të lartë për asetet që ajo posedon, për informacionin që përpunon, për të dhënat që ruhen në të, për të cilat nuk garantohet vazhdueshmëria në rast të ndodhjes së aktiviteteve me karakter negativ. Përshkrimet e punës nuk i nënshtrohen verifikimeve apo rishikimeve periodike të kryera nga eprorët e linjës, si dhe nuk është bërë vlerësimi vjetor i punës për çdo punonjës. Prania e strukturës së TI, larg vendimmarrjes si dhe e pa plotësuar me personel lë hapësira për risk të paidentifikuar, të pamatur, pasojat e të cilit nuk mund të evidentohen. Gjithashtu u konstatua se, për ruajtjen dhe zhvillimin e kompetencave profesionale të punonjësve gjatë vitit 2014, në agjenci nuk janë organizuar trajnime për rritjen e kapaciteteve profesionale të punonjësve në fushën e TI, në kundërshtim kjo me Manualin për	Financiar dhe Kontrollit në drejtim të misionit të fushës së teknologjisë së informacionit dhe ndërlidhjes së kësaj fushe me objektivat e veprimtarisë së AKBPM-së; identifikimit të risqeve; parashikimit të veprimeve të përshtatshme të kontrollit sistemet e TI; hartimit të gjurmëve të auditimit; hartimit të planeve të trajnimit për rritjen e kapaciteteve profesionale në fushën e TI, identifikimit të "Listës së proceseve të punës"; vendosja e një strukture TI në institucion e shoqëruar nga përshkrimet e punës si dhe ndarjet e detyrave si dhe ngritja e Grupit të Menaxhimit Strategjik, në përbërje të të cilit të jetë një specialist i TI, në përputhje me Ligjin për menaxhimin Financiar dhe Kontrollin. Zbatimi i Ligjit të Menaxhimit Financiar dhe Kontrollit në fushën e teknologjisë së informacionit, sjell më pranë vendimmarrjes sektorin e TI-së.

	Menaxhimin Financiar dhe Kontrollin, Kap. II, pika 2.5.1. Në aktet e auditimit nuk vërehen elemente të auditimit të Teknologjisë së Informacionit. Misioni i auditimit vëren se nuk janë hartuar gjurmët e auditimit të detajuara për procedurat kryesore, bazuar në gjurmët standarde të emetuara nga Ministria e Financave. Nuk janë identifikuar me emërtimin ”Lista e proceseve të punës”, nuk ka miratim dhe arkivim të kësaj gjurme, veprime këto në mospërmbushje të kërkesave të nenit 16, pika 2 dhe 3 të ligjit nr. 10296 datë 8.7.2010 “Për menaxhimin financiar dhe kontrollin” dhe të detyrimeve të kapitullit III të “Manualit për Menaxhimin Financiar dhe Kontrollin”, miratuar nga Ministri i Financave me Urdhrin nr. 54, datë 15.07.2010. Menaxherët e njësisë nuk zotërojnë informacion të mjaftueshëm për qëllimet dhe rëndësinë e menaxhimit financiar dhe të kontrollit, nuk është respektuar nga të gjithë hallkat e njësisë dhe se, institucioni nuk ka kryer trajnime për kuptimin dhe zbatimin e ligjit. Njësia nuk ka hartuar një procedurë për mbledhjen dhe dokumentimin e gabimeve dhe analizën e tyre. Nuk ekziston një protokoll i brendshëm për korrespondencat midis strukturave lart-poshtë e paralel, apo raportimet e kryera në nivelin e lartë të strukturave. Mos kryerja e këtyre veprimeve përbëjnë risk në këtë institucion pasi nuk lihen gjurmë për auditimin e veprimtarisë të nëpunësve të këtij Institucioni	

3	Nga auditimi në agjenci, u konstatua mungesë e praktikave dokumentare lidhur me sistemin e regjistrimit dhe ruajtjes së të dhënave të barnave, mungesë e marrëveshjeve ose kontratave të lidhura për përfitimin e këtij aplikacioni. Gjithashtu, u konstatua se kompjuterat që kryejnë regjistrimin e të drejta administratori në sistemin operativ. Nisur nga kjo, punonjësit me akses të pakontrolluar në kompjuter, mund të shkarkojnë programe të ndryshme nga interneti, duke dëmtuar së pari memorien e kompjuterit (duke e zënë hapësirën me regjistrat për programet e shkarkuara), më tej duke zënë kohën dhe fuqinë e procesorit të kompjuterit, si dhe së fundmi duke i dhënë mundësinë programeve me ndikim negativ (malware) të depërtojnë në kompjuter, dhe të modifikojnë ose të shkatërrojnë të dhënat e ruajtura aty, si dhe në rastin më të keq duke ndërhyrë në disponibilitetin dhe integritetin e të dhënave të ruajtura në program. Në agjenci nuk ka ndarje formale detyrash dhe përgjegjësish lidhur me sistemin e regjistrimit, duke lënë hapësirë procedurale për mbingarkesë funksionesh dhe kryerje detyrash të pacaktuara	-AKBPM të marrë masa për dokumentimin e programeve kompjuterik që shërbejnë për zhvillimin e proceseve të ndryshme të punës së institucionit; - Specifikimi i personave përgjegjës për përdorimin e programit, monitorimin e tij, specifikimi i të drejtave të përdoruesve të programit si dhe të sistemit operativ në kompjuterat ku është instaluar program aplikativ.
4	Nga auditimi i inputeve dhe outputeve të programit aplikativ mbi regjistrimin e barnave, u konstatua se: Agjencia nuk ka të hartuara politika për personat e autorizuar për të hyrë në program, kohëzgjatjen e aksesimit të programit, politika për anulimin e llogarive në program. Ekzistojnë ende 2 llogari të	Të merren masa për hartimin e politikave dhe procedurave standarde për specifikimin e kritereve për të gjitha inputet dhe outputet që gjenerohen nga programet të cilat funksionojnë aktualisht dhe në të ardhmen në AKBPM; llojin e të dhënave që futen në program; të merren masa të përcaktohen

	hapura për dy ish-punonjës të agjencisë, të cilët kanë kohë që kanë shkëputur marrëdhëniet e punës me agjencinë. Për këtë program, agjencia nuk disponon një përshkrim formal të të dhënave që regjistrohen dhe të të dhënave që përpunohen, nuk ekzistojnë mekanizma të kontrollit të inputeve që hyjnë në program, mungojnë kontrolle të evidentimit të rekordeve të duplikuara. Përsa i përket output-eve që gjenerohen nga ky aplikacion, ato përmbajnë dokumente administrative në funksion të institucionit, të tilla si autorizime importi, autorizim zhdoganimi, autorizim përdorimi të barnave. Ky proces i gjenerimit të output-IT, së pari nis me nxjerrjen e dokumenteve, të cilat më tej ekstraktohen me memorie të jashtme, dhe printohen në tjetër vendndodhje, kjo për shkak të mungesës së lidhjes midis terminaleve ku ruhet programi, dhe printerëve. Ky veprim lë hapësirë për tjetërsimin e informacionit të gjeneruar nga programi. Duhet theksuar se agjencia nuk përmban politika ose procedura të shkruara se cilat janë output- et e gjeneruara nga programi, dhe se cilët janë personat përgjegjës për marrjen dhe posedimin e këtyre dokumenteve. Mungesa e politikave dhe procedurave të shkruara lidhur me programin, sjell edhe mungesën e verifikimit të vlefshmërisë së raporteve të gjeneruara (dokumenteve zyrtare), duke dhënë mundësinë e gjenerimit të autorizimeve me të dhëna	personat përgjegjës për futjen e të dhënave, marrjen në dorëzim të output-eve, si dhe të hartohen procedura të shkruara për trajtimin e problemeve dhe pengesave të hasura gjatë futjes së të dhënave ose gjenerimit të outputit.

	jo të sakta. Nga auditimi i output-eve të programit, u konstatua se agjencia nuk disponon politika të shkruara të trajtimit të dokumenteve jo të sakta, duke mos lënë hapësirë për auditimin dhe kontrollin e këtyre output-eve, për të verifikuar eficencën dhe efektivitetin e gjenerimit të autorizimeve	
5	Nga auditimi i sigurisë logjike, u konstatua se agjencia nuk disponon procedura rishikimi të sigurisë së aplikacionit, logfilet regjistrohen në Server, dhe këto logfile nuk janë hapur asnjëherë, sepse nuk ka qenë e nevojshme; nuk janë hasur asnjëherë shkelje të sigurisë, konstatim i cili nuk mund të verifikohet, pasi agjencia nuk mban procesverbale të rregullta, mujore ose periudhe tjetër, me anë të të cilave do të konkludohej mbi statistikat dhe eficencën e sigurisë. Gjithashtu, agjencia nuk disponon plane të trajtimit të katastrofave, duke rritur në këtë mënyrë riskun e humbjes ose tjetërsimit të të dhënave të ruajtura në program; nuk posedon marrëveshje në nivel shërbimi (SLA), ose kontrata të ndryshme lidhur me aplikimin, backup-i i të dhënave kryhet ne mungesë të planeve dhe procedurave të shkruara. Ambienti në të cilin mbahet ky aplikim nuk plotëson standardet e përcaktuara nga AKSHI për ndërtimin e dhomës se serverëve (ambientet janë magazina pa nivele sigurie, pa ventilim e sinjalistikën e përcaktuar së bashku me barna e	Institucioni të marrë masa për nxjerrjen e rregullores së sigurisë TI, të kryejë monitorimin e sigurisë dhe trajtimit të incidenteve dhe problemeve të konstatuara në aplikimin e barnave, të evidentojë procesin për zgjidhjen e problemeve të ngjashme në të ardhmen.

	materiale të tjera pa lidhje funksionale me shërbimet e TI). Gjithsesi, mbajtja e të dhënave brenda institucionit, mbart riskun e humbjes së disponibilitetit dhe integritetit të të dhënave, në rast të ndodhjes së katastrofave ose shkatërrimeve të qëllimshme dhe jo të qëllimshme (aq më tepër që agjencia nuk ka një plan sigurie të shkruar të ndërtesës). Agjencia nuk ofron trajnime ose programe ndërgjegjësimi për mbrojtjen e të dhënave si dhe reagimin në rast të katastrofave të mundshme, duke rritur riskun e mosdijes së veprimeve për tu kryer nga punonjësit. Testime të integritetit dhe të disponibilitetit të të dhënave janë kryer në mënyrë vullnetare, por nuk janë dokumentuar. U konstatua mungesa e manualeve të përdorimit, të ndihmës online, të një qendre helpdesk-u. Nevojat për ndihmë, ose për rregullime të konfigurimeve të sistemit, bazohen në raste emergjente, të cilat nuk dokumentohen dhe nuk rishikohen. E drejta për kryerjen e veprimeve të mësipërme, në funksion të ndihmës, është e specialistit të TI	
6	Nga auditimi i informacioneve rezultoi se Agjencia nuk ka Strategji të TI dhe nuk kuptohet sa duhet roli kritik i Sigurisë së Informacionit; nuk ka plan të sigurisë së TI, regjistër risqesh dhe nuk kryhet menaxhimi i riskut; agjencia nuk analizon rastet e incidenteve të sigurisë dhe ka shkallen e ulet të kuptimit e menaxhimit sigurisë ne institucion; kuk ka rregulla të brendshme, referuar	Institucioni të marrë masa për krijimin e strukturës së përshtatshme teknologjike dhe logjike në mënyrë që të garantohet integriteti, konfidencialiteti, plotësia dhe saktësia e të dhënave. Për këtë: ▪ Përmirësimi i Rregullores së Brendshme të AKBPM, duke shtuar edhe elementë për garantimin e sigurisë së Informacionit si dhe infrastrukturës

	sigurisë së sistemeve të informacionit Gjithashtu, mungesa në staf dhe mungesa e strukturës TI si njësi më vete paraqet risk potencial në kryrjen e detyrave të sigurisë; nuk ka gjurmë të analizimit të sigurisë në raportet, analizat apo auditimet e brendshme; nuk ka politika formale dhe të shkruara të sigurisë së informacionit dhe komunikimin, përdoruesit e rrjetit kompjuterik kanë të drejta të pa kufizuara dhe nuk përdoret menaxhimi i përqendruar i të drejtave. Përdorimi i postës private ne sistemit të agjencisë për qëllime pune; Rregullorja Brendshme ekzistuese është e vitit 2006, nuk ka analiza e raporte të incidenteve nga ndërhyrje nga jashtë e nga brenda, rrjeti kompjuterik është i organizuar pa infrastrukturën e konfigurimin e nevojshëm për të mundësuar monitorimin nuk mjete për monitorimin dhe analizimin e rrjetit; nuk kryhet analizim e raportim të bllokimeve sulmeve nga brenda e jashtë. Kontrolli i statistikave të bllokimeve dhe sulmeve. Pajisjet e rrjetit shtrihet në ambiente që nuk kanë lidhje me funksionin e pajisjeve të vendosura aty; konstatojmë se AKBPM nuk ka zbatuar standardet e AKSHIT në ndërtimin e rrjetit kompjuterik dhomës së Serverëve dhe komunikimit i cili shtrihet në godinë në ambiente të pa përshtatshme e pa sigurinë e duhur në drejtim të sigurisë për të përmbushur objektivat e AKBPM; nuk ekzistojnë mjete dhe kontrolle mjedisorë (ndaluesi i zjarrit, alarmet, sistemet e energjisë.	teknologjike. ▪ Plotësimi i strukturës se TI me personelin e përcaktuar ne organike. ▪ Shtimi i funksioneve në përshkrimet e punës së personelit të TI, referuar sigurisë së informacionit ▪ Marrja e masave për njohjen dhe zbatimin e standardeve dhe specifikimeve teknike të Agjencisë Kombëtare të Shërbimit Informativ.

7	Nga auditimi i sistemit back-up, planit të vazhdueshmërisë në rast katastrofe dhe shërbimet e kontraktuara, u konstatua se Back up nuk përfshin të gjitha pajisjet, të dhënat dhe programet aplikativë kritikë; siguria dhe kushtet e këtyre ambienteve ku ruhet Back up nuk plotësojnë kushtet e përshtatshme të përcaktuara në Agjencinë Kombëtare të Shërbimit Informativ; auditimi nuk gjeti dokumentacion mbi testime të procedurave back up; agjencia nuk ka plane te rimëkëmbjes nga katastrofat; sistemi i furnizimit me energji i rrjetit kompjuterik i pa ndarë nga pajisjet e tjera të godinës komprometon dhe nuk garanton vazhdimësinë e punës në AKBPM. Gjithashtu u konstatua se vendi i ruajtjes së backup së bashku me mallra e pajisje të tjera pa siguri fizike dhe rruajtje nga zjarri; auditimi e cilëson me risk me nivel te lartë mbajtjen në sheet-e Excel të llogarive e kontabilitetit të institucionit e mos përdorimi programit financiar të kontabilitetit; agjencia nuk te përcaktuar ne SLA për mirëmbajtjen e faqes se internetit dhe postes elektronike procedurat e backup te tyre, nuk u gjeten procedura te kryerjes se tyre dhe testimeve përkatëse	Për garantimin e vazhdueshmërisë së infrastrukturës teknologjike e cila të përmbushë kërkesat e veprimtarisë së AKBPM-së, të merren masa për hartimin e planeve të backup-it dhe të rimëkëmbjes nga katastrofat. Gjithashtu procedurat e implementimit të këtyre planeve të përfshijnë pozicionimin e të dhënave të ruajtura në vendndodhje të sigurta, dhe larg institucionit.

Në përfundim të vlerësimit të Raportit të Auditimit të TI në AKBPM nga IDI-n (Iniciativa për zhvillim e INTOSAI-t, gusht 2015) rekomandimet dhe ky raport ju vunë në dispozicion Ministrisë të Shëndetësisë dhe Komisionit të Shëndetësisë në Kuvendin e Shqipërisë.

AUDITIMI I TEKNOLOGJISË SË INFORMACIONIT, TË USHTRUAR NË AGJENCINË E PROKURIMIT PUBLIK.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "Agjencinë e Prokurimit Publik"

Përgatitur: 15 Nëntor 2015

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 427/2, datë 08/05/2015, të ndryshuar me programin nr. 427/4, datë 20.07.2015 për periudhën 01.01.2014 deri më 30.03.2015.

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Yrjada Jahja, anëtar
3. Marenglen Sinani, anëtar
4. Elisa Metaj

Auditimi ka filluar më datë 01.05.2015
Auditimi ka përfunduar më datë 30.09.2015

Objektivi kryesor në këtë auditimi ishte sigurimi nëse TI në APP mbështet nevojat pa kompromentuar sigurinë, privatësinë, koston dhe elemente të tjera kritike. Dhënia e opinionit për: politikat e sigurisë, dhe masat që ky institucion ka implementuar kundrejt risqeve, ekzistencën e planeve të vazhdueshmërisë të sistemit të prokurimit publik dhe input-outputet e sistemit.
Drejtimet kryesore në këtë auditim ishin, Vlerësimi i ambientit, Verifikim i shkallës së sigurisë, Testime mbi input/output, Kontrolli i BCP, DRP, Kontrolli i të drejtave të përdoruesve dhe Vlerësimi i prokurimeve në fushën e TI.

Gjatë auditimit është pasur në konsideratë auditimi i çështjeve, që kanë të bëjnë me respektimin e akteve ligjore dhe nënligjore si dhe praktikat më të mira në fushën e teknologjisë së informacionit me qëllim garantimin e integritetit, konfidencialitetit dhe disponibilitetit të informacionit.

Gjatë kryerjes së auditimit, grupi ka hasur vështirësi në vënien në dispozicion të informacionit, për të cilën janë ndjekur edhe procedurat përkatëse.

ÇFARË KEMI AUDITUAR

Kontrolli i Lartë i Shtetit (KLSH) mbështetur në nenet 3 dhe 14 të ligjit 154 "Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit" datë 27.11.2014, auditoi Agjencinë e Prokurimit Publik (APP) duke i kushtuar vëmendjen e posaçme çështjeve që lidhen me Vlerësimin e ambientit në të cilin zhvillohet sistemi, vlerësimin e sigurisë së informacionit, vlerësimin e planeve të vazhdueshmërisë së veprimtarisë, verifikimin e inputeve dhe outputeve të gjeneruara nga sistemi dhe prokurimet kryera nga APP në fushën e TI.

Agjencia e Prokurimit Publik, është institucion në varësi të Kryeministrit, që financohet nga Buxheti i Shtetit. Aktiviteti i saj bazohet në Ligjin Nr. 9643/2006 "Për Prokurimin Publik", i ndryshuar, Ligjin Nr. 125/2013 "Për koncesionet dhe partneritetin publik privat" dhe Ligjin Nr. 9874/2008 "Për ankandin publik", i ndryshuar.

Sistemi i Prokurimit Elektronik është ndërtuar në vitin 2008 në kuadër të projektit Millennium Challenge Corporation Threshold nga Chemonics International.

Në nëntor 2012 sistemi është zgjeruar duke përfshirë edhe prokurimet me vlerë të vogël. Baza e të dhënave aktive të Sistemit të Prokurimit Elektronik (SPE) është rreth 561GB. Gjatë vitit 2014, autoritetet kontraktuese publikuan 4,152 njoftime për tendera me vlerë deri 507 milionë USD dhe lidhen rreth 3,449 kontrata prokurimi me vlerë 395 milionë USD për pune, mallra dhe shërbime. Sistemit është audituar nga palë të treta në vitet 2008 nga "X" dhe 2010 nga kompania "Y".
Ndër detyrat e APP janë përgatitja e projekt-propozimeve për rregullat e prokurimit publik, ankandeve publike dhe atyre në fushën e koncesioneve/partneriteteve publike private; hartimi i dokumentave standarte të tenderit dhe nxjerrja e udhëzimeve të nevojshme në ndihmë të autoriteteve që ndërmarrin këto procedura; verifikimin i zbatimit të procedurave të prokurimit publik, procedurave të koncesionit dhe ankandit publik pas fazës së nënshkrimit të kontratës dhe në rast shkeljesh të dispozitave ligjore dhe nënligjore, vendosjen e gjobave ose propozimin e marrjes së masave administrative; monitorimi i mbarëvajtjes së sistemit të prokurimit publik, hartimi dhe nxjerrja e buletinit të njoftimeve publike, etj.

Opinionet dhe konkluzionet tona të nxjerra gjatë kryerjes së auditimit i kemi diskutuar në zbatim të Standardeve Kombëtare dhe Ndërkombëtare të Auditimit, janë mbajtur aktet përkatëse të auditimit, janë shqyrtuar observacionet për aktet e mbajtura duke reflektuar në këtë raport si dhe kemi propozuar rekomandimet përkatëse.

Këto dhe të gjitha rekomandimet e tjera të bëra nga KLSH morën një feedback pozitiv nga subjekti për pranimin e të gjitha rekomandimeve dhe realizimin e tyre brenda afatit.

Më hollësisht:

OPINIONI I AUDITIMIT:

Teknologjia e Informacionit në Agjencinë e Prokurimit Publik nuk është në përputhje të plotë me kërkesat ligjore dhe nënligjore. Masat organizative të lidhura me sigurinë e informacionit nuk janë të mjaftueshme dhe trajtuar në mënyrë të përshtatshme, gjë që mund të çojë në shkeljet e sigurisë, keqtrajtimi i aseteve të informacionit, cënim i integritetit të të dhënave të prokurimit, risk në qasje të paautorizuar në të dhënat.

Masat e marra nga APP për sigurimin e Planit e Vazhdueshmërisë së Biznesit (BCP) dhe Planit të Rimëkëmbjes nga Katastrofat (DRP) janë të pa mjaftueshme.

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	Gjatë auditimit u konstatua se, masat e marra nga APP për sigurimin e Planin e Vazhdueshmërisë së Biznesit (BCP) dhe Planin e Rimëkëmbjes nga Katastrofat (DRP) janë të pa mjaftueshme. APP nuk zbaton Politikat e Menaxhimit të Ndryshimeve dhe nuk garanton vazhdimësinë e punës për prokurimin elektronik me pasojë ndërprerjen e shërbimit, humbjen e informacionit dhe besueshmërisë në kundërshtim me VKM nr. 710, dt. 21.08.2013, "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit" pika 1 a, b, c ç, d, dh, e, pika 3 dhe pika 4, Planin e Sigurisë së APP-së Prot.3076 Datë 25.02.2009 pika 9.2	APP të marrë masa administrative dhe organizative për krijimin, testimin dhe rishikimin periodik të Politikave dhe Planeve të Vazhdueshmërisë së Biznesit dhe Rimëkëmbjes nga Katastrofat (BCP dhe DRP).
2.	Gjatë auditimit u konstatua se në strukturën organizative dhe në detyrat funksionale të stafit të Agjencisë nuk është i rregulluar funksioni që garanton sigurinë e sistemit dhe mbrojtjen e informacionit e të integritetit të të dhënave që disponohen, kjo në kundërshtim me Planin e Sigurisë së Agjencisë, të datës 25.02.2009, Kapitulli 3, pika 3.1, duke krijuar hapësira për qasje të paautorizuar në të dhënat.	Nga ana e APP të marren masat për të plotësuar dhe rregulluar funksionin e "Oficerit të Sigurisë", plotësim që gjykojmë se do të sjellë eliminimin e risqeve të mundshme operacionale nga mungesa e një funksioni që garanton integritetin e të dhënave dhe mban përgjegjësi për çdo cënim të sigurisë së të dhënave të disponueshme duke garantuar edhe zbatimin e Planit të Sigurisë së Agjencisë.
3	Gjatë auditimit u konstatua se nga APP nuk ka politika të mjaftueshme të zhvillimit të Burimeve Njerëzore. Gjykojmë se një faktor i rëndësishëm në mirëfunksionimin e prokurimeve elektronike është profesionalizmi dhe trajnimi i vijueshëm i punonjësve sidomos atyre që garantojnë sigurinë në fushën e teknologjisë së informacionit,	APP të marrë masa për hartimin e politikave të trajnimit të Burimet Njerëzore në fushën e teknologjisë së informacionit, të vendosi standarde për trajnime të vijueshme të stafit, duke përcaktuar një numër të caktuar ditësh trajnimi për çdo funksion kryesor të lidhur me realizimin me sukses të objektivave institucional.

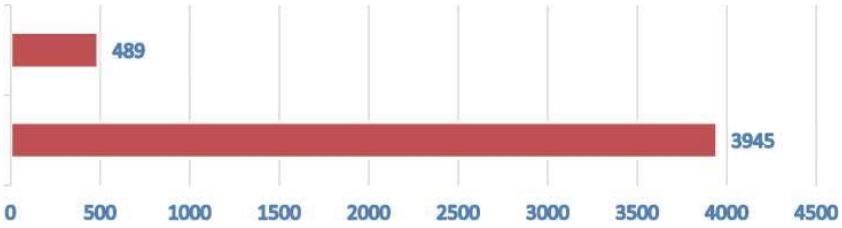
4	Gjatë auditimit u konstatua se, Politikat mbi gjurmët (log-et) e Sistemit të prokurimit nuk zbatohen. Me risk në qasje të paautorizuar në të dhënat, kërcënim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence, në kundërshtim me "e-Procurement Security Policy and procedures Manual" Kapitulli 6 "Audit Trail" pika 6.2 "Checking the log files"	APP të marrë masa për Analizimin e gjurmëve (Log-ve), dhe dokumentimi i këtij procesi, ruajtjen e një kopje të veçantë për tu përdorur në rastet e auditimit si dhe ankimimeve.
5	Gjatë auditimit u konstatua se, mbajtja dhe sinkronizimi manual i kohës (orës) të Sistemit të prokurimit nuk garanton transparencën e nevojshme për procedurat e prokurimit. APP nuk zbaton Politikat e menaxhimit të ndryshimeve. në kundërshtim me "Rregullore për Ofrimin e Shërbimeve të Përqendruara Elektronike në Administratën Publike", pika 1.4.4	APP të marrë masa për Sinkronizimi automatik të orës së sistemit të prokurimit elektronik me serverin e orës së AKSHI-t.
6	Gjatë auditimit u konstatua se në APP nuk ekziston një procedure zyrtare e raportimit, menaxhimit ndaj incidenteve, në kundërshtim me Planin e Sigurisë Kap 5.5 "Përgjigja të incidenteve",	APP të marrë masa për Hartimin e procedurave për evidentimin, raportimin, menaxhimin dhe përgjigjes ndaj incidenteve
7	Gjatë auditimit u konstatua se, masat e ndërmarra për Sigurinë Fizike dhe Mjedisore të sistemit të Prokurimit Publik nga APP janë të pamjaftueshme, në kundërshtim me Rregulloren e AKSH-it mbi "Ndërtimin e Dhomës së Serverave"	APP të marrë masa për ndërtimin e dhomës së serverave në përputhje me rregulloren e AKSH-it.
8	Gjatë auditimit u konstatua se, masat e ndërmarra në drejtim Backup-it janë të pamjaftueshme dhe nuk japin siguri në mbështetjen e BCP dhe DRP, në kundërshtim kjo me VKM nr. 710, dt. 21.08.2013 dhe me Planin e Sigurisë Nr	APP të marrë masa administrative dhe organizative për kryerjen e Backup-it në përputhje me kërkesat e VKM nr. 710, dt. 21.08.2013 dhe me Planin e Sigurisë Nr Prot.3076 Datë 25.02.2009.

	Prot.3076 Datë 25.02.2009 pika 7.4 “Backup i të Dhënave”	
9	Gjatë auditimit u konstatua se, nuk ka vlerësim të raporteve të monitorimit dhe përpilim të raporteve për përmirësimin e infrastrukturës, pa përjashtuar edhe sugjerimet në adresë të infrastrukturës, nuk ka raporte dhe sugjerime për diagnostifikimet e problemeve, nuk mbahen dokumentacione përkatës (Aktkolaudimi, procesverbal), për shërbimet që realizohen sipas kontratës, në kundërshtim me kontratën e shërbimit nr.01, datë 22.09.2014	Nëpunësi autorizues, referuar Udhëzimit nr.30 dt.27.12.2011 “Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik”, kreu III, pika 42, duhet të nxjerri urdhrin përkatës për ngritjen e komisionit për marrjen në dorëzim të shërbimeve
10	Gjatë auditimit u konstatua se, APP nuk siguron mbështetjen e mjaftueshme për Autoritetet Kontraktore dhe Operatorët ekonomikë,	Marrjen e masave administrative dhe organizative për sigurimin e mbështetjes me gjithë kanalet e komunikimit për Autoritetet Kontraktore dhe Operatorët Ekonomikë, Publikimi i orarit të kryerjes se këtij shërbimi.

AUDITIMET E TEKNOLOGJISË SË INFORMACIONIT VITI 2016

Drejtoria e Auditimit të Teknologjisë së Informacionit edhe për vitin 2016 ka qenë pjesë e Departamentit të Auditimit të Buxhetit Qendror, Administratës së Lartë Publike, Menaxhimit Financiar dhe Auditimit të Brendshëm me përbërje 5 anëtarë nga të cilët 4 Auditues.

Në aktivitetin e saj Drejtoria e Auditimit të TI u mbështet në planin strategjik të zhvillimit për vitet 2013-2017 me objektiv konsolidimin e njohurive dhe krijimin e një tradite në këtë fushe të re dhe të vështirë të mbështetur në objektivin 4 të planin strategjik të zhvillimit i cili përcakton si prioritet të KLSH zhvillimin dhe konsolidimin e auditimeve të Teknologjisë së Informacionit dhe përdorimi i Tl në auditim, sidhe objektivit 2.8 i cili përcakton si mjet për realizimin e objektivit 4 zhvillimin e trajnimeve në këtë fushë.



Për vitin 2016 nga burime të brendshme dhe të jashtme me objektiv rritjen e njohurive të stafit auditues me njohuri kompjuterike për përdorimin e tyre në auditim, u zhvilluan 489 ditë/njerëz trajnime ku u trajtuan temat:

- Auditimi i Teknologjisë së Informacionit / Manuali i Auditimit Tl-së;
- Programet Word, Excel;
- Teknikat CAATs në Auditim;
- Programi IDEA;
- Programi Financa 5;
- Metodat Vizualizuese në auditim.
- Raporti i trajnimeve TI/trajnime të tjera

Gjatë vitit 2016 u planifikuan 3 auditime të teknologjisë së informacionit, nga të cilat u realizuan 2 auditime dhe auditimi i tretë në proces për tu përfunduar në vitin 2017.

1. Drejtoria e Përgjithshme e Thesarit dhe Drejtoria e Shërbimeve dhe Teknologjisë së Informacionit në Ministrinë e Financave.

2. Fondi i Sigurimit të Detyrueshëm të Kujdesit Shëndetësor.

Treguesi	Njësia	Llogaritja	Vlera
Fuqia maksimale Audituese e drejtorisë	ditënjerëz	22 x 11x 5	1210
Auditime të parashikuara gjithsej	numër		3
Për çdo auditim mesatarisht	ditënjerëz	1210/3	403

Ecuria e procesit

Nr	Auditimet TI	Gjetje/Rekomandime
1.	FSDKSH	21
2.	THESARI MINFIN	13

MBI AUDITIMIT E TEKNOLOGJISË SË INFORMACIONIT TË USHTRUAR NË DREJTORINË E PËRGJITHSHME TË THESARIT DHE DREJTORINË E SHËRBIMEVE DHE TEKNOLOGJISË SË INFORMACIONIT NË MINISTRINË E FINANCAVE.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "**Drejtoria e Përgjithshme e Thesarit dhe Drejtoria e Shërbimeve dhe Teknologjisë së Informacionit në Ministrinë e Financave"**

Përgatitur: 30 Nëntor 2016

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 821, datë 23.07.2016 i ndryshuar Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Benard Haka, anëtar
3. Endi Meksi, anëtar

Periudha e Auditimit: 01.01.2015 – 31.12.2015
Afati i auditimit: 02.09.2016 – 21.11.2016

Auditimi ka përfunduar dhe është evaduar, subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve

ÇFARË KEMI AUDITUAR

Ministria e Financave është person juridik, publik që ka si Mision arritjen e stabilitetit ekonomik nëpërmjet drejtimit me eficiencë, efektivitet dhe transparencë të financave publike.

Ministria e Financave e ushtron veprimtarinë nëpërmjet këtyre fushave të përgjegjësisë shtetërore:

1. Politikës makroekonomike dhe fiskale;
2. Administrimit të të ardhurave;
3. Administrimit të buxhetit të shtetit;
4. Menaxhimit të borxhit publik;
5. Administrimit financiar;
6. Menaxhimit financiar dhe kontrollit;
7. Menaxhimit të asistencës financiare të Bashkimit Evropian dhe menaxhimit të fondeve të Bashkimit Evropian;
8. Inspektimit financiar publik;
9. Bashkërendimit të përgjithshëm të auditimit të brendshëm.

"Sistemi informatik financiar i Qeverisë (SIFQ)" është sistemi financiar, nëpërmjet të cilit Qeveria e Republikës së Shqipërisë kryen të gjitha proceset e ekzekutimit dhe raportimit financiar të Buxhetit të Shtetit.
SIFQ është një sistem Modular ku Zyrat e Degëve të Thesarit, Ministria e Financave dhe Institucionet paraqesin të gjithë transaksionet buxhetore, për regjistrimin e tyre në Sistem.
Për realizimin e këtij procesi Përdoruesit e Sistemit Informatik Financiar të Qeverisë përdorin shtatë module : Modulin e Buxhetit, Modulin e Urdhrave të Blerjes, Moduli i të Pagueshmeve, Moduli i të Ardhurave, Moduli i Aktiveve Fikse dhe Modulin e Librit të Madh.

Grupi i auditimit mblodhi informacione dhe zhvilloi analiza për caktimin e zonave me risk të lartë mbështetur në to hartoi matricat e auditimit.

Kërkesat për informacion për fushat përkatëse u hartuan në përputhje me manualin e Auditimit të Teknologjisë së Informacionit. Plani i auditimit i dalë nga informacionet dhe

analizat paraprake kishte për objektiv vlerësimin e sistemeve TI, dhe aspekteve që lidhen me mirëmbajtjen, zhvillimin dhe sigurinë e tyre.

Fushat e auditimit

Auditimi i funksionimit të qeverisjes TI në DPTH dhe DSTI.
- Verifikim i strategjisë së TI dhe lidhja me objektivat e veprimtarisë së institucionit.
- Verifikim i politikave dhe procedurave TI.
- Verifikim i menaxhimit të burimeve njerëzore në strukturën TI.

Auditimi i aplikacionit Sistemi Informatik Financiar të Qeverisë (SIFQ) të implementuara në Ministrinë e Financave.
- Verifikim i shkallës së sigurisë së aplikacionit.
- Kontrolli i shkallës së aksesit të përdoruesve të jashtëm dhe të brendshëm në aplikacion.

Auditimi i Planit të Vazhdueshmërisë së Biznesit dhe të Rimëkëmbjes nga Katastrofat.
- Verifikim i dokumentimit të Planeve për Vazhdueshmërinë e Biznesit dhe Rimëkëmbjes. nga Katastrofa.
- Verifikim i identifikimit dhe menaxhimit të risqeve në TI.
- Kontrolli i shkallës së sigurisë.

Auditimi i projekteve e investimeve në teknologjinë e Informacionit.

- Vlerësim i procedurave të investimeve në fushën e TI.

I. PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Auditimi i Sistemeve të teknologjisë së Informacionit në Drejtorinë e Përgjithshme të Thesarit dhe Drejtorinë e Shërbimeve dhe Teknologjisë së Informacionit, është i një rëndësie të veçantë pasi këto struktura janë përgjegjëse për mbajtjen e Sistemit informatik financiar të Qeverisë (SIFQ)", nëpërmjet të cilit Qeveria e Republikës së Shqipërisë kryen të gjitha proceset e ekzekutimit dhe raportimit financiar të Buxhetit të Shtetit. Në përfundim të auditimit për 13 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit

Më hollësisht:

<u>OPINIONI I AUDITIMIT:</u>

Grupi i auditimit arrin në konkluzionin se Ministria e Financave megjithë përpjekjet e bëra nuk ka marrë masa të mjaftueshme rregullatore dhe organizative për garantimin e sistemeve të informacionit. Në gjykimin tonë, menaxhimi i elementëve kritikë në sistemet e informacionit, është i pa pamjaftueshëm dhe i pa përshtatshëm.

Investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht sigurimin e Vazhdueshmërisë së Biznesit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat.

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	Nga auditimi i qeverisjes së TI u konstatua se MF nuk ka strategji për Teknologjinë e Informacionit, duke mos pasqyruar qartë objektiva lidhur me infrastrukturën, burimet e nevojshme si dhe indikatorë për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së MF	Strukturat drejtuese të MF, duke marrë në konsideratë kohën, burimet e nevojshme të marrin masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit.
2.	Nga auditimi i politikave dhe procedurave TI në MF, u konstatua se Manuali TI i vitit 2015 është i pa miratuar. Drejtoria e Shërbimeve dhe Teknologjisë së Informacionit nuk disponon dokumentacion mbi: Regjistrat/loget e administratorit të rrjetit dhe rezultatet e analizave të logeve; Listën e informacionit të kategorizuar; Politikat dhe procedura referuar çështjeve të konfigurimit në fushën e operacioneve; Planin e sigurisë së ndërtesave ku shtrihet Sistemi Informatik Financiar i Qeverisë; Listën/matricën e aksesit; Listën e artikujve të cilësuar si prioritare për proceset emergjente; Procedurat për Planin e Vazhdueshmërisë së Biznesit dhe Rimëkëmbjes nga Katastrofat dhe procedurat e Testimit; Listën e testeve të kryera për vitin 2015 dhe rezultatet veprimet e ndërmarra. Mungesa e dokumentacioneve të mësipërme bën që institucioni të mos ketë të identifikuar risqet me efekt negativ në TI dhe veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura	Strukturat drejtuese në bashkëpunim me Drejtorinë e Shërbimeve dhe Teknologjisë së Informacionit të marrin masat për hartimin e dokumentacionit të nevojshëm për zbatimit të politikave e procedurave TI në MF. Institucioni të identifikoje risqet me efekt negativ në TI dhe veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura.

3	**1.** Nga auditimi mbi menaxhimin e burimeve njerëzore në DPTH për vitin 2015 rezulton se ka pasur luhatje të vazhdueshme në Burimet njerëzore, shoqëruar me vende vakante të strukturës në disa prej pozicioneve të rëndësishme në Drejtori, mbart riskun e përmbushjes së misionit dhe funksioneve kryesore si sigurimi dhe realizimin e shërbimeve operacionale, garantimi i parasë së gatshme për kryerjen e transaksioneve dhe pagesave. Nga auditimi konstatohet se DPTH pa marrë në konsideratë natyrën specifike nuk ka hartuar politika të veçanta për rekrutimin e stafit. Përpjekjet për zhvillimin e kapaciteteve të stafit nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit gjatë vitit 2015 kanë qenë të pa mjaftueshme. Nga auditimi i menaxhimit të burimeve njerëzore në DSTI për vitin 2015 rezulton se ka pasur luhatje të vazhdueshme në Burimet njerëzore me krijimin e vendeve vakant në disa prej pozicioneve të rëndësishme, zhvillimi i kapaciteteve të stafit nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit gjatë vitit 2015 kanë qenë të pa mjaftueshme. Ndarja e detyrave në nivel sektorial është e njëjtë duke treguar formalizëm në hartimin e tyre. Mos menaxhimi i burimeve njerëzore përbën një risk në plotësimin e misionit të DSTI për sigurimin dhe realizimin e shërbimeve TI për qeverisjen e përgjithshme	Ministria e Financave të marrë masa për menaxhimin e burimeve njerëzore duke plotësuar vendet vakante dhe hartojë politika për zhvillimin e tyre nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit.

4	Nga auditimi i marrëveshjeve të nivelit të shërbimit për vitin 2015 rezulton se në DSTI dhe DPTH nuk ka patur suport mirëmbajtje e zhvillimi për disa nga sistemet, MF nuk ka ndërmarrë asnjë masë ndaj këtij risku. Në regjistrin e risqeve është caktuar si masë për minimizimin e këtij risku, zhvillimi i trajnimeve mbi TI. Por pavarësisht se është caktuar kjo masë, Grupi i auditimit konstaton se DSTI dhe DPTH për vitin 2015 kanë dobësi të theksuara në identifikimin, planifikimin dhe zhvillimin e trajnimeve, duke rritur vështirësinë e mirëmbajtjes së sistemeve	Ministria e Financave të marrë masa për kryerjen e analizave kosto-përfitim për suportet e nevojshme të sistemeve të Teknologjisë së Informacionit. Të hartojë politika për sigurimin e suporteve të nevojshme si dhe të zhvillojë burimet e brendshme nëpërmjet trajnimeve në lidhje e sistemeve, sigurinë dhe teknologjinë e informacionit
5	Nga auditimi i aplikacionit "Sistemi Informatik Financiar të Qeverisë" (SIFQ) të implementuar në Ministrinë e Financave gjatë vitit 2015 rezulton se Drejtoria e Përgjithshme e Tatimeve (Institucion Varësie) ka filluar zbatimin në kushtet reale të punës të sistemit të ri informatik tatimor. Pjesë e këtij procesi është edhe integrimi i këtij sistemi me SIFQ. Gjatë vitit 2015 nga SIFQ është dërguar informacion ditor mbi transaksionet e arkëtimeve të ardhurave tatimore për tu pasqyruar në Sistemin Informatik Tatimor. Nga Drejtoria e Përgjithshme e Tatimeve, në drejtim të Drejtorisë së Thesarit, janë dërguar informacione të të dhënave të sistemit C@ST në formë të pjesshme, jo në afat dhe manualisht. Përpjekjet e Ministrisë së Financave si Institucion Qendror administrues i SIFQ për zgjidhjen e problematikave të	Ministria e Financave si Institucion administrues i SIFQ të marri masa për koordinimit të veprimeve mes palëve të interesuara dhe dhënëse të informacionit nëpërmjet implementimit të politikave dhe procedurave për menaxhimin e ndryshimeve në sistemet dhe aplikacionet kryesore të TI

	shfaqura nuk kanë gjetur bashkëpunimin e duhur nga ana e Drejtorisë së Përgjithshme të Tatimeve duke shkaktuar një impakt konstant negativ në procesin e rakordimit dhe raportimit të treguesve fiskale të Qeverisë për vitin 2015	
6	Nga auditimi i shkallës së sigurisë së aplikacionit konstaton se Sektori i Sigurisë së Sistemit të Informacionit të Drejtorisë së Shërbimeve dhe e Teknologjisë së Informacionit, nuk kryen procesin e monitorimit logimeve për ngjarjet e sigurisë së informacionit në sistemin SIFQ dhe infrastrukturën e tij (databaza Oracle dhe platforma Solaris UNIX), si edhe tek pajisjet e rrjetit (firewall, routers, switches etj). Pa loget dhe rishikimin periodik të logeve të sigurisë, aktivitetet e dyshimta që ndodhin në sistemin SIFQ ose në nivelin e rrjetit mund të kalojnë pa u vënë re	Të merren masa për kryerjen procesit te monitorimit log-ve për ngjarjet e sigurisë së informacionit në sistemin SIFQ dhe infrastrukturën e tij (databaza Oracle dhe platforma Solaris UNIX), si edhe tek pajisjet e rrjetit (firewall, routers, switches, etj).
7	Nga auditimi i shkallës së aksesit të përdoruesve të jashtëm dhe të brendshëm në aplikacion “Sistemit Informatik Financiar të Qeverisë (SIFQ), sigurisë së tij dhe rëndësinë e informacionit që rrjedh prej tij grupi i auditimit konstaton se nuk ka një plan për ndryshimin e fjalëkalimeve të përdorueseve me të drejta të plota. Mungesa e ndryshimit të kriterit ose standardeve të fjalëkalimeve, rrit riskun e zbulimit të fjalëkalimeve dhe vjedhjen e tyre nga individë të pa autorizuar, duke përfituar akses në sistemet e informacionit	Drejtoria e Shërbimeve dhe Teknologjisë së Informacionit (Sektori i Sigurisë së Sistemit të Informacionit) të përgatisë dhe paraqesë për miratim në Strukturat drejtuese një manual me politika të qarta mbi sigurinë e informacionit mbi ndryshimin e fjalëkalimeve të përdorueseve me të drejta të plota. Procesi i ndërimit të fjalëkalimeve të monitorohet në vazhdimësi.

8	Nga auditimi i **Planeve për Vazhdueshmërinë e Biznesit dhe Rimëkëmbjes nga Katastrofat** rezultoi se Ministria e Financave nuk ka të ndërtuar një strategji të rimëkëmbjes nga katastrofat si dhe nuk ka plane që përcaktojnë vazhdimësinë e proceseve në rastet e dështimit të qendrës së të dhënave primare (data center) që suportojnë sistemin SIFQ. Momentalisht Ministria e Financave nuk ka qendër të rimëkëmbjen nga katastrofat (DRC) për data centerin primar ku hostohen serverat e sistemit SIFQ dhe infrastrukturën e rrjetit. MF nuk disponon dokumentacione në lidhje me Planet e vazhdueshmërisë së punës (BCP) dhe rimëkëmbjes nga katastrofat (DRC), Procedurat e testimit dhe rezultatet e tyre sidhe veprimet e rekomandimet e ndërmarra. MF nuk ka listë të artikujve të vlerësuar prioritare për proceset emergjente	Të merren masa për ndërtimin dhe hartimin e Planeve të Vazhdimësisë së Biznesit Rimëkëmbjen nga Katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat. Gjithashtu, të merren masa për hartimin e planit të sigurisë së informacionit dhe implementimi e tij duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TI. Planifikimi dhe testimi i sistemeve TI të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen.
9	Nga auditimi u konstatua se Procedura e backup për Sistemet e Informacionit në MF nuk janë në përputhje me VKM nr. 710, dt. 21.08.2013 “Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit”, backup tek AKSHI kryhen manualisht vetëm në raste të veçanta. Nuk u gjetën procedura të testimit të backup. Në Drejtorinë e Përgjithshme të Thesarit mbahen në PC e përdoruesve pa backup parashikime, analiza dhe të dhëna të tjera të rëndësishme në Excel	Të merren masa për kryerjen dhe testimin periodik të backup-it për sistemet, pajisjet kompjuterike dhe të dhënat. Të merren masa për klasifikimin e të dhënave të rëndësishme që ndodhen jashtë sistemit, kalimin e tyre në server, mbulimin e tyre me backup.

	dhe Word. Ky informacion mbart vlerë të shtuar dhe humbja e modifikimi i tyre mbart riskun e gabimeve dhe humbja e të dhënave për menaxhimin e aktivitetit të cash-it	
10	Nga Auditimi i **menaxhimit të risqeve në TI** u konstatua se nuk ka marrë masa të mjaftueshme për identifikimin dhe minimizimin e risqeve për: a. Qendrën BCC si mekanizëm për vazhdimësinë dhe rikuperimin e Sistemit të Thesarit në raste sulmesh të jashtme apo fatkeqësish natyrore, b. Vendndodhja e "datacenterit" në godinën e vjetër të ministrisë dhe ndërprerja e shpeshtë e energjisë elektrike; c. Teknologjia e vjetërsuar e serverave ekzistues dhe ulja e performancës së tyre. d. Memoria fizike e serverave është e ulët për shkak se janë pajisje të vjetra dhe me parametra të ulët me një jetëgjatësi 7 vjet . e. Mos përshtatshmëria e sistemeve ekzistuese për shkak të vjetërsimit të tyre. f. Kompleksiteti dhe vështirësia e mirëmbajtjes së sistemeve të reja që implementohen; g. Dokumentim i papërshtatshëm i procedurave të TI dhe sistemeve ekzistuese dhe të reja; h. Drejtoria e Shërbimeve dhe e	MF të bëjë përditësimin dhe dokumentimin e regjistrit të risqeve TI dhe të marrë masa për hartimin dhe dokumentimin e një plani veprimi për minimizimin/ parandalimin e risqeve të identifikuara, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave nga Drejtoria TI.

	Teknologjisë së Informacionit nuk ka një plan se si menaxhohen risqet e lidhura me projektet e investuara ku të përcaktohej, lista e risqeve, detyrat dhe përgjegjësitë për menaxhimin e risqeve. Ministria e Financave nuk ka marrë masa për minimizimin përditësimi e regjistrit të risqeve	
11	Nga Auditimi u konstatua se në MF nuk ekziston një procedurë e dokumentuar e identifikimit, trajtimit dhe raportimit të incidenteve. Mungesa e një procedure të menaxhimit të incidenteve sjell paqartësi dhe mangësi në trajtimin e tyre, njohjen e nivelit të riskut që kërcënime të përcaktuara mbartin për MF-në, nivelit të impaktit në veprimtarinë e MF-së, dokumentimin dhe zgjidhjen e tyre, e cila redukton kohën e zgjidhjes, në rast përsëritje të të njëjtit incident, etj	MF të marrë masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve.
12	Nga Auditimi u konstatua se ambienti fizik i dhomës së rrjetit nuk është në përputhje me standarted e përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI	Të merren masa për ndërtimin e ambienteve të dhomës së serverave në bazë të VKM nr. 248, datë 27.04.2007 "Për krijimin e Agjencisë Kombëtare të Shoqërisë së Informacionit" dhe Rregulloren për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK dhe praktikat më të mira kombëtare dhe ndërkombëtare.
13	Nga auditimi i kërkesave dhe procesit të aprovimit të tyre si dhe hartimit të regjistrit të prokurimeve rezulton se analiza "kosto përfitim" për mbajtjen e shërbimeve nëpërmjet zhvillimit të	MF në cilësinë e Autoritetit Kontraktor, kryejë analizën "kosto përfitim" për përcaktimin e shërbimeve që do mbahen nga burimet e brendshme dhe atyre që do kalojnë me MNSH ("outsourcing").

	burimeve të brendshme apo kalimit të tyre me MNSH ("outsourcing") nuk është zhvilluar. Nga audidimi u konstatua se në mospërputhje me VKM nr.710, datë 21.8.2013 mbi "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit" për vitin 2015 Drejtoria e TI-së nuk ka patur suport për disa nga sistemet në MF duke i krijuar vështirësi në mirëmbajtjen e sistemeve. Në regjistrin e risqeve është caktuar si masë për minimizimin e këtij risku, zhvillimi i trajnimeve mbi TI. Por pavarësisht se është caktuar kjo masë për minimizimin e riskut, nuk janë zhvilluar trajnime. Nga maj 2014 deri më shtator 2015 nuk ka patur suport funksional. Shërbimi është kërkuar nga DPTH dhe është buxhetuar por procesi i tenderimit ka dështuar. Gjatë kësaj periudhe ka patur problematika serioze në sistem edhe për vetë faktin e gjendjes së rënduar të makinerive të sistemit (HW). Kontrata Nr. 4330/16 datë 30.09.2015 me objekt "Shërbim Suporti AMOFTS (Oracle)" me kompaninë ".. sh.p.k." ka paraqitur probleme në zbatimin e saj. Nga shtatori 2015 e në vazhdim SIFQ është pa suport funksional Nga auditimi i procedurës së prokurimit "Krijimi i Sistemit të Informatizuar të Menaxhimit të Dëmshpërblimeve të Ish të Përndjekurve Politikë" për krijimin e Sistemit të Informatizuar të Menaxhimit të Dëmshpërblimit të ish të Përndjekurve	Të kihet parasysh që në të ardhmen në hartimin dhe zbatimin e projekteve të teknologjisë së informacionit të kryejë azhornimin e nevojshëm të dokumentacionit të prokurimit në përputhje me ndryshimet ligjore në fuqi. MF të marri masa për rritjen e bashkëveprimit ndërinstitucional në përputhje me politikat dhe strategjitë për parashikimin dhe koordinimit e investimet në fushën e TI, si dhe kalimin online të shërbimit të Sistemit të Informatizuar të Menaxhimit të Dëmshpërblimeve të Ish të Përndjekurve Politikë. Marrjen e masave për shfrytëzim i gjithë kapaciteteve që ofrojnë investimet e kryera.

	Politik dhe MNSH për 4 (katër) vite rezultoi kontrata është hartuar në përputhje me udhëzimin 1119 datë17.3.2014, të Ministrit të Shtetit për Inovacionin dhe Administratën Publike pa marrë në konsideratë ndryshimin që i bën këtij Udhëzimi Nr. 4099, datë 3.11.2014 Pikës 5 të udhëzimit nr. 1159, "pika 5. "5.MNSH-ja për pajisjet hardware, aplikacionet, licencat ose kombinimet e tyre duhet të fillojë me njëherë nga momenti i marrjes në dorëzim nga porositësi të pajisjes hardware, të aplikacionit, licencës apo kombinimit të tyre. Garancia për pajisjet hardware është me kohë zgjatje minimale 1-vjeçare." Për rrjedhojë AK ka filluar mirëmbajtjen pasi ka përfunduar garancia e cila ka shërbyer edhe si suport. Konstatohet mosrakordim në kohë i MF me Agjencinë Kombëtare Shoqërisë së Informacionit për kalimin online të shërbimit. Konstatohet një bashkëpunim i pa mjaftueshëm midis Drejtorisë së Pagesave dhe Dëmshpërblimeve dhe Drejtorisë së Shërbimeve dhe Teknologjisë së Informacionit për shfrytëzim i gjithë kapaciteteve që ofron programi në drejtim të gjenerimit të raporteve dhe statistikave	

MBI AUDITIMIN E TEKNOLOGJISË SË INFORMACIONIT TË USHTRUAR NË FONDIN E SIGURIMIT TË DETYRUESHËM TË KUJDESIT SHËNDETËSOR.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "**Fondin e Sigurimit të Detyrueshëm të Kujdesit Shëndetësor"**

Përgatitur: 10 Tetor 2016

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 227/1, datë 08.03.2016.

Auditimi është kryer nga:

1. Elira Cukalla, përgjegjës grupi
2. Yrjada Jahja, anëtar
3. Benard Haka, anëtar

Periudha e Auditimit: 01.01.2015 – 31.12.2015
Afati i auditimit: 10.03.2016 - 10.06.2016

Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve

ÇFARË KEMI AUDITUAR

Fondi i Sigurimit të Detyrueshëm të Kujdesit Shëndetësor ushtron veprimtarinë e tij në bazë të ligjit nr. 10 383, datë 24.2.2011, "Për sigurimin e detyrueshëm të kujdesit shëndetësor në Republikën e Shqipërisë", i ndryshuar. Fondi organizohet dhe funksionon në bazë të statutit të Fondit, i cili miratohet nga Këshilli i Ministrave.
Vizioni i FSDKSH, me qëllim rritjen e aksesit dhe përmirësimit të cilësisë së shërbimit shëndetësor për popullatën, fokusohet në prirje të rëndësishme që lidhen me ndryshimet demografike dhe epidemiologjike; zhvillimet teknologjike, si dhe pritshmërisë në rritje të konsumatorit për akses në trajtimet mjekësore cilësore dhe bashkëkohore.
Qëllimet strategjike të FSDKSH përfshijnë:

- ofrimi i shërbimeve për popullatën të bëhet nëpërmjet paketave standarde të shërbimeve në të gjitha nivelet e sistemit shëndetësor;
- përmirësimi i vazhdueshëm i metodave të pagesës së ofruesve të shërbimeve shëndetësore për rritjen e eficiencës dhe cilësisë së shërbimeve shëndetësore;
- fuqizimi i sistemit të informacionit nëpërmjet ofrimit të shërbimeve online për dhënësit e shërbimeve, funksionimit të regjistrave elektronike për pacientët, me qëllim rritjen e eficiencës, transparencës dhe afrimit të shërbimeve sa më afër qytetarëve;
- ofrimi i shërbimeve shëndetësore për të gjithë popullatën në përputhje me politikat qeveritare.

Fushat e auditimit

- Strategjia e TI dhe lidhja me objektivat e veprimtarisë së institucionit, burimet njerëzore, politikat dhe procedurat e kësaj njësie,
- Verifikim i kontrolleve të aplikacioneve për vlefshmërinë e të dhënave input dhe output, Verifikim i shkallës së sigurisë,
- Analiza dhe vlerësimi i zbatimit të procedurave të prokurimit në fushën TI,

- Planet për Vazhdueshmërinë e Biznesit dhe Rimëkëmbjes nga Katastrofa,
- Kontroll i të drejtave të përdoruesve,
- Verifikim i identifikimit dhe menaxhimit të risqeve në TI,
- Vlerësim i hartimit të nevojave dhe kritereve të vendosura për mallra, shërbime,

II. PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Auditimi i Sistemeve të Teknologjisë së Informacionit në Fondin e Sigurimit të Detyrueshëm të Kujdesit Shëndetësor është i rëndësishëm pasi ky institucion është i vetmi person juridik, publik, autonom, i cili ofron dhe administron sigurimin e detyrueshëm të kujdesit shëndetësor në Republikën e Shqipërisë. Ky institucion menaxhon skemën e sigurimit të detyrueshëm të kujdesit shëndetësor, në përputhje me politikat kombëtare të kujdesit shëndetësor, të vendosura nga Ministria e Shëndetësisë.
Buxheti i FSDKSH miratohet si pjesë përbërëse e pandarë e Buxhetit vjetor të Shtetit.

Objektivi i auditimit: Përcaktimi nëse sistemet e Teknologjisë së Informacionit në Fondin e Sigurimit të Detyrueshëm të Kujdesit Shëndetsor, mbrojnë asetet e informacionit, ruajnë integritetin e të dhënave; sigurojnë disponueshmërinë dhe konfidencialitetitn e informacionit; mbështeten në kontrolle të duhura.

Opinionet dhe konkluzionet tona të nxjerra gjatë kryerjes së auditimit janë mbështetur në zbatim të akteve ligjore/nënligjore si dhe Standardet Kombëtare dhe Ndërkombëtare të Auditimit, për të cilat janë mbajtur aktet përkatëse të auditimit. Observacionet lidhur me aktet e auditimit gjenden të reflekëtuara në këtë Raport. Grupi i auditimit propozon dhe rekomandimet përkatëse lidhur me rezultatet e auditimit.

Në përfundim të auditimit për 22 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit

Më hollësisht:

<u>OPINIONI I AUDITIMIT:</u>

Fondi i Sigurimit të Detyrueshëm të Kujdesit Shëndetësor, si institucioni përgjegjës për mbarëvajtjen e skemës së sigurimeve shëndetësore nëpërmjet shërbimit parësor, spitalor dhe rimbursimit të barnave, nuk ka marrë masa të mjaftueshme rregullatore dhe organizative për garantimin e konfidencialitetit, integritetit dhe gatishmërisë së të dhënave në sistemet e informacionit që ai posedon. Grupi i auditimit arrin në konluzionin se, sistemet aktuale të informacionit, nuk janë të mjaftueshme dhe të përshtatshme për menaxhimin e plotë dhe të sigurtë të skemës së rimbursimit të barnave, për shkak të mosfunksionimit dhe koordinimit të strukturave dhe hallkave menaxhuese.

Mungesa e kontrolleve rregullatore dhe e kontrolleve të aplikacioneve në institucion ka sjellë mungesën e standardizimit të operacioneve të teknologjisë së informacionit, keqtrajtim të aseteve, mosmenaxhim të elementëve kritikë të sigurisë, si dhe risk për qasje të paautorizuar në të dhënat. Masat e marra për sigurimin e Planit të Vazhdueshmërisë së Biznesit dhe Planit të Rimëkëmbjes nga Katastrofat kanë qenë të pa efektshme.

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	Nga auditimi i qeverisjes së TI në FSDKSH, u konstatua se Plani aktual Strategjik "Për zhvillimin e Sistemeve të Informacionit në FSDKSH", i miratuar me Vendimin nr. 13, dt. 26.02.2014 të Këshillit Administrativ, është fokusuar tërësisht në sistemet e informacionit që operojnë në institucion, duke mos pasqyruar objektiva lidhur me infrastrukturën dhe arkitekturën TI, burimet e nevojshme për kryerjen e operacioneve TI si dhe përcaktimin e indikatorëve të performancës për matjen e objektivave. Nga mungesa e një Plani Strategjik gjithëpërfshirës, ekziston risku i mospërkthimit të objektivave të institucionit në qëllime dhe kërkesa TI dhe risku i keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së FSDKSH	Strukturat drejtuese në bashkëpunim me Drejtorinë e Informacionit dhe Analizës Statistikore si dhe me strukturat këshilluese mbi TI, të marrin masa të rishikojnë dhe plotësojnë Planin Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit në operacione TI, duke marrë në konsideratë kohën, burimet e nevojshme dhe rishikim vjetor të indikatorëve të performancës së ecurisë së objektivave.
2.	Nga auditimi u konstatua se Teknologjia e Informacionit në FSDKSH zhvillohet në kushtet e mungesës së bazës rregullatore. FSDKSH nuk ka marrë masa për hartimin e rregullave dhe procedurave të proceseve të teknologjisë se informacionit në përputhje me aktet ligjore dhe nënligjore, dhe praktikat më të mira, duke mos konsideruar elementë të tillë si: rregulla mbi veprimtarinë e TI në institucion; rregulla mbi menaxhimin e incidenteve; procedura dhe indikatorë të matjes së performancës për gabimet/ incidentet e ndodhura dhe masat reaguese ndaj tyre; struktura kontrolli për verifikimin e	FSDKSH të marrë masa për hartimin e një Rregulloreje të Përgjithshme mbi Teknologjinë e Informacionit në FSDKSH, në të cilën të identifikikohen të gjitha operacionet TI në institucion, afatet dhe burimet e nevojshme për çdo veprimtari. Hartimi i kësaj Rregulloreje të marrë në konsideratë vendosjen e kontrolleve të brendshme lidhur me menaxhimin e riskut,

	efektivitetit të ndryshimeve të kryera; procedura për ndryshimet emergjente si dhe dokumentimin e të gjithë procesit të ndryshimeve. Mungesa e bazës së brendshme rregullatore për funksionimin e strukturave të teknologjisë së informacionit sjell operimin mbi baza ngjarjeje dhe jo sipas procedurave të përcaktura, duke rritur riskun e ekspozimit të institucionit ndaj situatave ku reagimi është i paidentifikuar, burimet njerëzore dhe përgjegjësitë të paalokuara si dhe koha e përgjigjes e papërcaktuar	përputhshmërinë me procedurat dhe rregullat e brendshme aktuale të institucionit si dhe me legjislacionin e Teknologjisë, Informacionit dhe Kounikimit në Shqipëri.
3	Nga auditimi u konstatua se FSDKSH nuk menaxhon ndryshimet në sistemet TI pasi mungojnë procedura për inicimin, rishikimin dhe aprovimin e ndryshimeve, prioritarizimin e tyre, mungojnë struktura kontrolli dhe ndarje të detyrave dhe përgjegjësive për kryerjen e ndryshimeve (update, upgrade, etj.) dhe nuk kryhet verifikimi i efektivitetit të ndryshimeve të kryera, procesi i ndryshimeve nuk dokumentohet. Nga mosimplementimi i një procdedurë të standartizuar për kontrollin e të gjitha ndryshimeve ekziston risku i mosidentifikimit të nevojës dhe arsyes për ndryshime, i mosidentifikimit të riskut që mund të sjell çdo ndryshim, i mosalokimit të burimeve të nevojshme për zbatimin e ndryshimit, i keqpërcaktimit të përgjegjësive përkatëse, i mostestimit të ndryshimit, i mosintegrimit të ndryshimeve, i ndrsyhimeve të paautorizuara, i rezultateve të paplanifikuara, i shkallës së ulët të suksesit, i rasteve të shumta emergjente pas ndryshimeve, si dhe risku i vonesave në operacionet TI.	Drejtoria e Informacionit dhe Analizës Statistikore, të përfshijë në Rregulloren e Përgjithshme mbi Teknologjinë e Informacionit në FSDKSH, rregulla për menaxhimin e ndryshimeve në sistemet TI, procedura për dokumentimin, inicimin, rishikimin dhe aprovimin e ndryshimeve, prioritarizimin e tyre, ndarje të detyrave dhe përgjegjësive për kryerjen e ndryshimeve dhe përcaktimin e treguesve të matjes së efektivitetit të ndryshimeve të kryera.
4	Nga auditimi u konstatuan dobësi të strukturave të Auditimit të Brendshëm në FSDKSH në Auditimin e sistemeve të Teknologjisë së Informacionit, mungesë të kapacitete njerëzore	Drejtoria e Burimeve në bashkpunim me Drejtorinë e Auditit të Brendshëm të mari masa për ngritjen e

	dhe kualifikimeve me pasojë rritje të riskut të mosidentifikimit të parregullsive në sistemet TI.	kapaciteteve në nëpërmjet rekrutimeve dhe trajnimeve për zhvillimin e Auditimit të Teknologjisë të Informacionit në FSDKSH
5	Nga auditimi në FSDKSH u konstatuan dobësi në sigurinë e teknologjisë së informacionit e konkretisht në: hartimin të politikave të sigurisë së informacionit, ngritjen e strukturave të sigurisë së TI, identifikimin, vlerësimin e menaxhimin risqeve dhe sigurisë fizike të ambienteve ku zhvillohet kjo Teknologji Informacioni. Dobësitë e evidentuara në sigurinë e teknologjisë së informacionit në FSDKSH mbartin riskun e mosgarantimit të konfidencialitetit, integritetit dhe gatishmërisë së infrastrukturës TI dhe të dhënave në institucion duke sjellë si rezultat pamundësinë e arritjes së objektivave të përgjithshëm dhe duke ndikuar në besueshmërinë e të dhënave të FSDKSH.	Drejtoria e Informacionit dhe Analizës Statistikore, të hartojë politika të sigurisë së informacionit dhe të përfshijë në Rregulloren e Përgjithshme mbi Teknologjinë e Informacionit në FSDKSH, rregulla për sigurinë e teknologjisë së informacionit. Gjithashtu të përcaktohet në strukturën organizative një pozicion i veçantë për verifikimin dhe garantimin e sigurisë së teknologjisë së informacionit në institucion.
6	**1.** Investimet për të krijuar sisteme të sigurta TI, përbëjnë një kusht të domosdoshëm për zhvillim të qëndrueshëm të këtyre sistemeve.Nga auditimi në FSDKSH i investimeve në sistemet TI dhe mirëmbajtjes së tyre për vitin 2015, u konstatua se: – Dokumentimi i nevojave, për investime nga ana e FSDKSH bëhet në mungesë të një analize të mirëfilltë dhe pa përcaktuar prioritetet, të cilat do të shërbenin për të vlerësuar në mënyrë optimale kërkesat për investime në fushën e teknologjisë së informacionit, për vitin 2015. U konstatua se në regjistrin e parashikimeve të prokurimeve, nuk është parashikuar mirëmbajtja (SLA-*Service Level Agreement*) për tre tendera të cilët kanë përfunduar në fund të vitit 2014. – Mungon konsistenca në programim të	FSDKSH të kryejë mbledhjen, analizimin, prioritarizimin, dokumentimin dhe miratimin e nevojave për investime, për çdo procedurë prokurimi në fushën e teknologjisë së informacionit bazuar në aktet ligjore dhe nënligjore në fuqi. Në rastet e nevojës për ndryshim regjistri të parashikimeve, strukturat përgjegjëse të argumentojnë në mënyrë të dokumentuar shkaqet që sjellin ndryshimin e regjistrit.

	investimeve në fushën TI dhe nuk kanë objektiva të qarta. Kështu për periudhat Janar-Prill dhe Janar-Gusht rregjistri i parashikimeve ka ndryshuar dy here. Me anë të shkresës përcjellëse nr.1772 datë 20.05.2015 është dërguar pranë Agjencisë së prokurimit publik "*Relacion për realizimin e prokurimeve publike për periudhën Janar–Prill 2015*" dhe raportimi i dytë është bërë me anë të shkresës nr.3160 datë 18.09.2015 të dërguar pranë Agjencisë së prokurimit publik "*Relacion për realizimin e prokurimeve publike për periudhën Janar–Gusht 2015*" bashkëngjitur këtyre shkresave ishin dhe ndryshimet e bëra në regjistrat e parashikimeve për periudhën Janar - Prill dhe Janar - Gusht 2015. Gjithashtu nga auditimi i dokumentacionit u vërejt se për të dy rastet e ndryshimit të regjistrit të parashikimeve nuk ka asnjë argumentim ose arsyetim se pse kanë ndodhur këto ndryshime. Konstatimet flasin për mungesë vizioni dhe për një strategji e cila nuk është zbërthyer në elementë konkretë veprimi si për bazë materiale dhe kapacitete njerëzore.	
7	Nga auditimi i implementimittë procedurës së prokurimit "Licenca për pajisjet e rrjetit firewall dhe shërbim mirëmbajtje/suport për sistemin e rrjetit "WAN" të Fondit", u konstatua se: Kjo procedurë është hapur më datë 27.04.2015 si "Procedurë e hapur" me vlerë 16,633,392 lekë me tvsh dhe ka përfunduar me lidhjen e kontratës në datën 11.06.2015 me firmën fituese "... shpk me vlerë 13,605,240 lekë me TVSH. Nga auditimi u konstatua se për instalimin e licencave, përditësimin e firewall, router dhe për SLA mungonte një plan i detajuar se si do të implementohej dhe realizohej kontrata. Në mungesë të këtij plani nuk janë parashikuar planifikime për përshkrimin e punës ose shërbimit	FSDKSH të marrë masat e nevojshme procedurale administrative e ligjore për përcaktimin dhe arkëtimin e pagesës së kryer për shërbimin e mirëmbajtjes përpara fillimit të tij.

	që do të kryhet, fillimin e procesit të punës, afatin për sa do të realizohet secili proces dhe datën/periudhën se kur fillon mirëmbajtja (SLA) etj. Gjithashtu rezultoi se raporti i instalimit, ku me anë të screenshots (*pamje nga instalimi i licencave dhe përditësimi i firewall dhe router*) bëhet përshkrimi i produkteve të instaluara nga kontraktuesi, nuk është i firmosur nga asnjë palë dhe nuk është e saktësuar që shërbimet që janë kryer "*Kanë përfunduar me sukses*", pra mungonte *Akti i kolaudimit*. Mungonte, Certifikata për kalimin në ambientin real të punës dhe Certifikata e pranimit përfundimtare. Gjithëashtu u konstatua se përveç pagesës për shërbimin e instalimit të licencave dhe përditësimit të firewall dhe router është bërë edhe pagesa për shërbimin e mirëmbajtjes,(nganënshkrimi i kontratës deri në marrjen në dorëzim të shërbimit dhe licencave). Pagesa e kryer për shërbimin e mirëmbajtjes (SLA) për procedurën "Licenca për pajisjet e rrjetit firewall dhe shërbim mirëmbajtje/suport për sistemin e rrjetit "WAN" të Fondit" është bërë në të njëjtën periudhë që është kryer dhe konfigurimi i shërbimit dhe në të njëjtën datë është marrë në dorëzim edhe shërbimi i instalimit dhe SLA (periudha 11.06.2015-11.07.2015), në kundërshtim me Udhëzimin nr. 4099, datë 03.11.2014, pika 5 ku specifikohet se mirëmbajtja duhej të fillojë pas konfigurimit të shërbimit dhe jo gjatë implementimit, "MNSH-ja për pajisjet hardware, aplikacionet, licencat ose kombinimet e tyre, duhet të fillojnë nga momenti i marrjes në dorëzim nga porositësi të pajisjeve hardware, të aplikacionit, licencës apo kombinimet e tyre".	
8	Nga auditimi i implementimit të procedurës së prokurimit "Shërbim mirëmbajtje/suport për	FSDKSH, për të gjitha procedurat e prokurimit në

	sistemin e Blade Serverave" rezultoi se, kjo procedurë është hapur më datë 27.04.2015 me procedurë prokurimi "Kërkesë për propozim" me vlerë 9,576,000 lekë me tvsh. Kjo procedurë prokurimi ka përfunduar me lidhjen e kontratës në datën 21.05.2015 me firmën fituese ".. shpk me vlerë 9,573,600 lekë me TVSH. Të dhënat tregojnë se kontrata është lidhur me rreth 100% të vlerës së hedhur në prokurim. Nga auditimi u konstatua se shërbimi do të lëvrohej për një periudhë dyvjeçare. Për këtë shërbim janë mbajtur procesverbalet e marrjes në dorëzim të shërbimit mirëmbajtje/suport nga komisioni i marrjes në dorëzim. Nga raportet e mirëmbajtjes që kontraktuesi sillte për FSDKSH në lidhje me kontrollin javor të sistemit të blade serverave, rezultoi se: pajisja "Storage FAS2040A/ BasePack /24 x 600GB SAS me nr serie 200000473291 dhe 200000473306)" HDD (Hard Disk) shfaqej me një problem. Që prej muajit që është mbajtur procesverbali i parë nga grupi i marrjes në dorëzim të shërbimit (përkatësisht Procesverbali nr.1 datë 28.05.2015 – Procesverbali nr.39 datë 31.12.2015) ky problem ka qenë prezent dhe nga kompania nuk janë marrë masat e duhura për ta riparuar këtë defekt ose zëvendësimin e HDD me një të ri. Ky fakt nxjerr problematikën e ndjekjes formale të plotësimit të kontratës së mirëmbajtjes, pasi kontrata specifikon afatin 45 ditë në zgjidhjen e problemeve. Pra nga ana e kontraktuesit janë tejkaluar të gjithë kufijtë kohor të përcaktuar edhe në specifikimet teknike për zgjidhjen e këtij problemi. Një problematikë tjetër që ka rezultuar sipas raportit të ardhur nga kontraktuesi, është se blloku i ushqimit Blade Server është dëmtuar. Ky bllok ushqimi është tërhequr për riparim nga kontraktuesi dhe sipas raportit të mirëmbajtjes	teknologjinë e informacionit, të marrë masa për caktimin e strukturave monitoruese për zbatimin e kontratave duke dokumentuar procesin monitorues. Gjithashtu të merren masa që këto struktura të mbajnë/ përgatisin raporte të detajuara përmbledhës për korrektësinë dhe cilësinë e zbatimit të kontratave

	nr.19, datë 11.09.2015 riparimi i bllokut ka qenë i pamundur, kështu që kontraktuesi ka bërë porosinë për një bllok tjetër të ri. Nga auditimi rezultoi se deri në fund të vitit 2015 nuk është zëvendësuar akoma blloku i djegur, duke mos plotësuar kushtet kontraktuale dhe kushtet e përcaktuara në specifikimet teknike dhe kohën e zgjidhjes së problemit. Pra FSDKSH nuk ka marrë masa për ngritjen strukturave monitoruese për zbatimin e kontratave, duke mos nxjerrë shkresa ose urdhra të brendshëm për përcaktimin e një personi/ personave të ngarkuar për ndjekjen e realizimit të kontratës, ku si rezultat i saj nuk janë mbajtur / përgatitur raporte përmbledhës për korrektësinë dhe cilësinë e zbatimit të kontratave.	
9	Nga auditimi i implementimit të procedurës së prokurimit "*Blerje pajisje kompjuterike për implementimin e Sistemit Receta Elektronike*" zhvilluar më 24.04.2015 me procedurë prokurimi "*Kërkesë për propozim*" me vlerë 8.898.360 lekë me tvsh. Kjo procedurë prokurimi ka përfunduar me lidhjen e kontratës në datën 15.05.2015 me firmën fituese ".. shpk me vlerë 8,362,680 lekë me TVSH. Të dhënat tregojnë se kontrata është lidhur me rreth 94% të vlerës së hedhur në prokurim. Nga auditimi i dokumentacionit në lidhje me procedurën "*Blerje pajisje kompjuterike për implementimin e Sistemit Receta Elektronike*" rezultoi se blerja e këtyre pajisjeve ka ardhur si rezultat, i implementimit të sistemit të Recetës Elektronike për projektin pilot të rrethit të Durrësit. Me shkresën nr. 6991 prot. datë 23.12.2014 të Ministrisë së Shëndetësisë është dërguar Urdhri i Ministrit nr. 556, datë 22.12.2014 "*Për kalimin kapital të pajisjeve informatike të sistemit e-Receta*" nga Ministria e Shëndetësisë tek FSDKSH. Është mbajtur procesverbali i datës 26.12.2014 nga Komisioni për kalimin kapital të	FSDKSH në cilësinë e Autoritetit Kontraktor, të ketë parasysh në të ardhmen që: - në zbatimin e procedurave të prokurimit në teknologjinë e informacionit, të marrë masa ligjore për caktimin e strukturave monitoruese për zbatimin e kontratave duke dokumentuar procesin monitorues. - të marri masa për rritjen e bashkëveprimit ndërinstitucional në përputhje me politikat dhe strategjitë për parashikimin dhe koordinimit e investimet në fushën e TI.

	pajisjeve informatike të sistemit e-Receta të ngritur me urdhrin nr. 619, datë 26.12.2014 të Drejtorit të Përgjithshëm të FSDKSH. *Ky sistem është instaluar në platformën ekzistuese të FSDKSH-së dhe është aplikuar për të gjithë rrethin e Durrësit.* Ky sistem është një sistem i qendërzuar, *web-aplication* dhe ndodhet në FSDKSH. Nga auditimi i procedurës për blerjen e pajisjeve kompjuterike për implementimin e sistemit Receta Elektronike (e-receta në rrethin e Durrësit, projekt pilot) nga FSDKSH-ja rezultoi se: Mungonte Akt dorëzimi i mallit nga kontraktuesi tek Autoriteti Kontraktor. Shpërndarja, shërbimi i konfigurimit dhe instalimi i sasisë së pajisjeve kompjuterike pranë çdo Qendre Shëndetësore do të bëhej sipas një grafiku lëvrimi të përcaktuar në aneksin A të kontratës nr.4/13 prot, datë 15.05.2015, por mungonte një raport i detajuar se si do të instaloheshin paketat e programeve, particionizimi dhe implementime të tjera për çdo qendër shëndetësore. Në mungesë të këtij raporti nuk janë parashikuar planifikime për përshkrimin e punës ose shërbimit që do të kryhet. Nuk është mbajtur raporti i instalimit ku bëhet përshkimi i produkteve të instaluara nga kontraktuesi dheqë "*Kanë përfunduar me sukses*", pra mungonte *Akti i Kolaudimit*. Nuk janë dorëzuar Certifikatat e Instalimi mbi produktet e instaluara nga kontraktuesi. Mungonte Certifikata e kalimit në ambientin real të punës, si dhe Certifikata e Pranimi përfundimtar ku saktësohet se "*ka përfunduar implementimi dhe instalimi me sukses i mallrave dhe shërbimeve".* Sipas kushteve të kontratës nr. 4/13 prot, datë 15.05.2015, cilësohet se shpërndarja, shërbimi i konfigurimit dhe instalimit të sasisë së pajisjeve kompjuterike pranë çdo QSH *do të realizohej me*	

	mjetet dhe personelin e kontraktuesit sipas paketës së programeve dhe plan-shpërndarjes që do të jetë pjesë e kësaj kontrate. Nga auditimi rezultoi se shpërndarja, transporti i këtyre pajisjeve është bërë nga vetë Fondi drejt të gjitha qëndrave shëndetsore. Gjithashtu edhe shërbimi i konfigurimit dhe instalimit të pajisjeve kompjuterike pranë çdo Qendre Shëndetësore është kryer nga specialistët e drejtorisë së DIAS. Nga ana e Kontraktuesit nuk është sjellë asnjë dokumentacion justifikues, si raporte shërbimi, instalimi apo konfigurimi që është kryer nëpër qendrat shëndetësore të rajonit të Durrësit ku do të implementoheshin këto pajisje	
10	Nga auditimi në FSDKSH mbi "*Sistemin e auditit për sistemin financiar të Fondit*" dhe "*Sistemin për integrimin, konsolidimin, monitorimin e informacionit të sistemit të kujdesit shëndetësor dhe ndërtimi i indikatorëve dhe analizave*" u konstatua se: FSDKSH-ja nuk ka staf për suportin e këtyre sistemeve. Personat që u trajnuan dhe u certifikuan për këto sisteme kanë ndërprerë marrëdhëniet e punës me FSDKSH dhe për këto arsye këto sisteme nuk përdoren dhe mirëmbahen. Për këto sisteme, ka mbaruar dhe shërbimi i mirëmbajtjes dhe për vitet pasardhës këto sisteme kanë mbetur pa suport dhe të ekspozuar ndaj dështimeve të mundshme si ndërprerjen e shërbimit, humbjen e të dhënave etj. Nga ana e institucionit nuk është marrë asnjë masë për sigurimin e shërbimeve të Sistemeve: - Të auditit për sistemin financiar të Fondit. - Të integrimit, konsolidimit, monitorimit të informacionit të sistemit të kujdesit shëndetësor dhe ndërtimi i indikatorëve dhe analizave.	FSDKSH të kryejë evidentimin e proceseve kritike të teknologjisë së informacionit dhe burimet njerëzore të lidhura me to, të marrë masa organizative për garantimin e vazhdueshmërisë së punës për këto procese nëpërmjet rekrutimit dhe trajnimit të punonjësve.

11	Nga auditimi në FSDKSH mbi zbatimin e kontratës datë 09.09.2014 mbi shërbimin e mirëmbajtjes (Service level agreement) për sistemin *"Për administrimin, monitorimin dhe vlerësimin e shpenzimeve spitalore"rezultoi: Për vitin 2015 shërbimi i mirëmbajtjes për këtë sistem ka mbaruar dhe për vitet pasardhës ky sistem ka mbetur pa suport dhe i ekspozuar ndaj dështimeve të mundshme si ndërprerjen e shërbimit, humbjen e të dhënave etj*. Bazuar në nenin 9 të kontratës, kohëzgjatja e shërbimit SLA do të jetë një vit duke filluar nga data e hartimit të procesverbalit të marrjes në dorëzim të software-it, ndërkohë që sipas VKM nr.710, datë 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", kohëzgjatja e kësaj marrëveshjeje duhet të jetë jo më e shkurtër se 4 (katër) vjet". Raporti përmbledhës i bërë nga grupi i marrjes në dorëzim të produkteve është jo i plotë pasi duhet të kishte një përshkrim të punëve të kryera dhe jo vetëm konstatime të shprehura shkurt.	FSDKSH të kryejë analizimin, prioritarizimin dhe planifikimin e nevojave për sistemet e reja dhe ekzistuese të teknologjisë së Informacionit, për mbështetjen e tyre me Marrëveshje të Nivelit të Shërbimit, të hartojë dhe zbatojë Marrëveshje të Nivelit të Shërbimit sipas përcaktimeve ligjore në fuqi.
12	Nga auditimi i zbatimit të shërbimeve të mirëmbajtjes (*SLA-Service level agreement, Marrëveshje të Nivelit të Shërbimit*) për projektet e realizuara: - *Licenca për pajisjet e rrjetit firewall dhe shërbim mirëmbajtje/suport për sistemin e rrjetit "WAN" të Fondit;* - *Shërbim mirëmbajtje/suport për sistemin e Blade Serverave;* - *Për administrimin, monitorimin dhe vlerësimin e shpenzimeve spitalore;* - *Implementimin e sistemit të auditit për sistemin*	FSDKSH në cilësinë e Autoritetit Kontraktor të kryejë analizimin, prioritarizimin dhe planifikimin e nevojave për sistemet e reja dhe ekzistuese të teknologjisë së Informacionit, për mbështetjen e tyre me Marrëveshje të Nivelit të Shërbimit, të hartojë dhe zbatojë Marrëveshje të Nivelit të Shërbimit sipas përcaktimeve ligjore në fuqi.

financiar të Fondit dhe suport (SLA);

- *Blerje sistemi për integrimin, konsolidimin, monitorimin e informacionit të sistemit të kujdesit shëndetësor dhe ndërtimi i indikatorëve dhe analizave;*

- *Implementimi në DRC Durrës (Disaster Recovery Centre) i sistemit të indikatorëve, raporteve dhe analizave (BI), si dhe ndërtimin e e-Shërbimeve për shkëmbim informacioni ndërmjet FONDIT, DPT, DPD, AKBPM nëpërmjet platformës qeveritare të ndërveprimit (ESB).*

U konstatua se:

-Hartimi i MNSH-ve për projektet e realizuara në FSDKSH nuk janë hartuar në përputhje të plotë me aneksin 2, të Udhëzimit nr. 2, datë 02.09.2013 "*Për standardizimin e hartimit të termave të referencës për projektet TIK në Administratën Publike*" pjesa III pika 10 Aneksi 2. Sipas Udhëzimit të Ministrit të Shtetit për Inovacionin dhe Administratën Publike, nr. 1159, datë 17.03.2014 "*Për Hartimin e Marrëveshjeve të Nivelit të Shërbimit"*, i ndryshuar, MNSH-ja duhet të ishte si aneks më vete bashkëlidhur kontratës administrative. Sipas Aneksit 1 të këtij urdhri ndër të tjera duhet të ishin përcaktuar elementë të rëndësishëm për realizimin e procesit të mirëmbajtjes, si *drejtuesi i projektit, personin e kontaktit, përkufizimet e termave teknikë, përshkrimi i shërbimeve, të drejtat dhe detyrimet e institucionit dhe të ofruesit të shërbimit, menaxhimi i shërbimeve, disponueshmëria e shërbimit, kufizimet e mundshme, mirëmbajtja e sistemit, matja e cilësisë së shërbimit, kërkesat e shërbimit, raporti i shërbimit dhe vlerësimet periodike, menaxhimi i vazhdueshmërisë së shërbimit, trajtimi i informacionit konfidencial, njoftimi i palëve, penalitetet e mundshme,*

	dokumentacioni mbështetës, ndërprerja e MNSH-së, dhe të tjerë elementë të rëndësishëm që përcaktohen në aneksin 1. -Gjithashtu kohëzgjatja e këtyre MNSH-ve nuk janë hartuar në përputhje të plotëme VKM nr. 710, datë 21.08.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit*" pika 2, paragrafi a dhe Udhëzimin nr. 1159, datë 17.03.2014 i ndryshuar "*Për hartimin e marrëveshjes së nivelit të shërbimit*" pika 3. Pra për vitet pasardhëse këto sisteme mbeten pa suport dhe të ekspozuar ndaj dështimeve të mundshme si ndërprerja e shërbimit, humbjen e të dhënave etj	
13	Nga auditimi i dokumentacionit mbi procedurën "Implementimi në DRC Durrës (Disaster Recovery Centre) i sistemit të indikatorëve, raporteve dhe analizave (BI), si dhe ndërtimin e e-Shërbimeve për shkëmbim informacioni ndërmjet FONDIT, DPT, DPD, AKBPM nëpërmjet platformës qeveritare të ndërveprimit (ESB)" që kishte qëllim ngritjen e sistemit Disaster Recovery për rivendosjen e punës në rast fatkeqësie (Disaster Recovery, DRC), vazhdueshmërisë së punës dhe backup për bazat e të dhënave shtetërore të sistemit të indikatorëve të FSDKSH dhe ndërveprimi me DPT, DPD, AKBPM. Kjo procedurë prokurimi është hapur në sistemin elektronik më date 14.12.2015 me procedurë prokurimi "Procedurë e hapur" me vlerë 83,814,287 lekë me tvsh. Lidhur kontratë në datën 24.12.2015 me bashkimin e operatorëve ekonomik fitues ".. shpk dhe ".. shpk me vlerë 82,777,500 lekë me TVSH. Kontrata është fituar me rreth 99% të vlerës së hedhur në prokurim. Nga analiza dhe vlerësimi i zbatimit të kontratës	*Procedura e prokurimit me objekt "Shërbimi i intranetit dhe internetit për zyrat qendrore të Fondit, Drejtoritë Rajonale, Degët dhe Agjensitë e Fondit" është hapur në datë 10.08.2015 me procedurë prokurimi "Procedurë e hapur" me vlerë 44,006,400 lekë me tvsh. Kjo procedurë prokurimi është anulluar me argumentimin (shkresa nr. 212, datë 15.01.2015, drejtuar APP) e mungesës së konkurencës, pasi ofertat e paraqitura nga operatorët ekonomik nuk përputhet me kriteret e përcaktuara në dokumentet standarde të tenderit.*FSDKSH të marrë masa për vendosjen e lidhjes me fibër optike me DRC-në dhe të ribëhet testimi i

	nr.18/11 prot, datë 24.12.2015 u konstatua se: Janë dorëzuar Certifikata e instalimit mbi produktet e instaluara nga kontraktuesi me datë 29.12.2015 e nënshkruar nga të dyja palët, Certifikata për kalimin në ambientin real të punës me datë 29.12.2015 e nënshkruar nga të dyja palët, si dhe Certifikata e Pranimit përfundimtare me datë 29.12.2015 "ka përfunduar implementimi dhe instalimi me sukses i mallrave dhe shërbimeve", e nënshkruar nga të dyja palët. Nga auditimi rezultoi se funksionaliteti dhe testimi i DRC–Durrës nuk është testuar realisht nëse është funksional apo jo, sepse për të testuar këtë gjë duhet që "qendra e rimëkëmbjes nga katastrofat" të ketë ndërlidhje (lidhja me fibër optike) me FSDKSH, ky shërbim i fibrës mungon[1], gjë që do të thotë se i gjithë dokumentacioni i sipërcituar, për kalimin në ambientin real të punës dhe marrjen në dorëzim të produktit është i paplotë sepse kalimi i shërbimit është i pamundur të bëhet automatikisht. Sipas dokumentacionit dhe intervistave me stafin TI testimi është realizuar në ambientet e FSDKSH ku është krijuar një "klon" ose backup i DRC Durrës dhe testimi është kryer në ambientet e FSDKSH (dmth nga kati i dytë në katin e parë). Gjithashtu sipas fletë-daljes nga magazina me nr.765, datë 29.12.2015 e nënshkruar nga specialistët e drejtorisë së DIAS, të gjitha produktet e këtij projekti janë bërë dalje nga magazina për në dhomën e serverëve në FSDKSH, por nuk ka asnjë urdhër që të jepte direktiva që këto produkte duhet të kalohen në DRC Durrës. Kjo formë testimi bie ndesh me VKM 710, datë 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit" pika 1, nënpikat (ç), (dh),	funksionalitetit të DRC-së Durrës sipas standardeve për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe rimëkëmbjes nga katastrofat. Gjithashtu, DRC Durrës të vihet në funksionalitet të plotë në përputhje me objektivat e përcaktuara në këtë projekt.

	(e) dhe me mënyrat e përshtatshme dhe praktikat më të mira të zhvillimit të testimeve të DRC- ve, për arsye se ndërtimi i tyre vjen për arsye Sigurie. Aktualisht DRC Durrës nuk i përgjigjet funksionaliteteve duke mos arritur të përmbushë objektivat për të cilat është investuar. Në qoftëse në momente të caktuara do të ndodhnin evente me pasoja negative në FSDKSH (mosfunksionim, rreziqe natyrore, katastrofa), funksionaliteti i shërbimeve do të ndërpritej. Me shkresën nr. 1210, datë 24.12.2015 në kuadër të zbatimit të kontratës nr. 18/11 datë 24.12.2015 në datat 24, 26, 27, 28 dhe 29 dhjetor 2015 janë zhvilluar trajnime mbi krijimin, editimin dhe zhvillimin e raporteve dhe indikatorëve dhe analizave në këtë sistem (BI), si një prej zërave të kontratës dhe me datë 29.12.2015 është lëshuar certifikata e trajnimit, bashkëngjitur, janë edhe listëprezenca e pjesëmarrësve dhe temat e seancave të trajnimit për pesë ditë të firmosura nga drejtori i DIAS dhe kontraktuesi.	
14	Nga auditimi i masave të marra nga FSDKSH për ndërtimin dhe mirëmbajtjen e dhomave të serverave në Drejtorinë Qendrore dhe në Qendrën DRC në Durrës, u konstatua se në të dyja këto ambiente mungonin elementë që garantojnë siguri të plotë të pajisjeve dhe të dhënave që ruhen në to. Kështu, FSDKSH, për vetë të dhënat që posedon dhe gjeneron, nuk ka treguar angazhim në përmbushjen e rregullave të përcaktuara nga AKSHI, në Rregulloren "Për ndërtimin e Dhomës së Serverave", në elementë të tillë si: pozicionimi fizik i dhomës së serverave, ndarje të pajisjeve që duhet të ruhen në këto dhoma dhe pajisjeve të papërshtatshme dhe të tepërta për këto ambiente, vendosjen e sistemeve të parandalimit të zjarrit, sistemeve ftohës, sistemeve elektrike dhe sistemeve të alarmit, dobësi në aksesin fizik në	FSDKSH të marrë masa të dokumentuara për përmirësimin e kushteve në dhomat e serverave të ndodhura në Drejtorinë Qendrore dhe në DRC, duke analizuar dobësitë, krijuar një plan veprimi bazuar në Rregulloren e AKSHI-t "Për ndërtimin e Dhomës së Serverave", dhe duke vijuar me zbatimin, për të rritur maksimalisht sigurinë fizike dhe logjike të këtyre ambienteve në drejtim të uljes së riskut të aksesit të paautorizuar, ruajtjen vetëm të

	dhomë, si dhe dobësi në hartimin e rregullave dhe procedurave të brendshme për aksesin fizik.	pajisjeve të përcaktuara në këto ambiente, si dhe përforcimin e sistemeve ftohës, sistemeve elektrike dhe sistemeve të alarmit.
15	Mbi verifikimin e dokumentimit të Planeve për Vazhdueshmërinë e Biznesit dhe Rimëkëmbjes nga Katastrofat, u konstatua se në kundërshtim me VKM nr. 710 datë 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", FSDKSH, si institucion që posedon disa sisteme informacioni, që ruajnë, përpunojnë dhe gjenerojnë të dhëna me rëndësi për realizimin e skemës së sigurimit shëndetësor: - Nuk ka identifikuar sistemet ose pjesët e tyre të cilat janë kritike për ofrimin e shërbimit 24 orë në 7 ditë të javës, dhe nuk ka plane të dokumentuara për menaxhimin e riskut, teknikat e menaxhimit dhe të performancës së tij. Po, ashtu institucioni nuk ka kryer auditime të brendshme me qëllim garantimin e mirëfunksionimit të këtyre teknikave për menaxhimin e riskut (ose në mungesë të teknikave, identifikim të riskut); - Nuk ka hartuar planin e politikave të vazhdueshmërisë së biznesit si dhe një plan për ruajtjen e informacionit, dokumenta këto që të përmbanin politikat dhe objektivat që sigurojnë vazhdueshmërinë e punës së sistemeve. Po ashtu deficenca konstatohen edhe në hartimin dhe dokumentimin e planit të rimëkëmbjes nga katastrofa, i cili do të përmbante masa dhe proceduratë mirëdokumentuara për rivendosjen në funksionim të sistemit në rastet e emergjencave. Në këto procedura duhet të ishin përcaktuar koha e rivendosjes në funksionim, disponueshmërinë e	FSDKSH, të marrë masa të parashikojë dhe të realizojë investime për krijimin e Planit të Vazhdueshmërisë së Biznesit dhe sistemit të ruajtjes së informacionit (Backup) me qëllim mundësimin e ofrimit të shërbimit pa ndërprerje dhe parandalimin e humbjes ose të shkatërrimit aksidental të të dhënave, duke konsideruar të gjitha pjesët e identifikuara si kritike për vazhdueshmërinë e punës, plane mbi proceset për menaxhimin e riskut, kohën e rivendosjes në funksionim të sistemeve, dhe burimet e nevojshme njerëzore për kryerjen e procedurave, në përputhje me aktet ligjore dhe nënligjore në fuqi.

	burimeve njerëzore, mënyra e informimit dhe personat përgjegjës të cilët do të njekin këto procedura; - Nuk ka të specifikuar/ dokumentuar kohën maksimale në të cilën shërbimet dhe sistemet nuk mund të jenë funksionale; - Nuk ka identifikuar të dhënat parësore dhe të dhëna të tjera, me rëndësi për funksionimin e sistemeve të teknologjisë së informacionit; - Nuk ka identifikuar pajisjet hardware dhe varësinë që sistemi, të dhënat dhe shërbimet kanë ndaj tyre. Nuk janë planifikuar masa që në rast dështimi të një/ disa pajisjeve të mos ndikohet në funksionimin e sistemeve dhe shërbimeve të ofruara. Munesa e Planeve të Vazhdueshmërisë së Biznesit dhe të Rimëkëmbjes nga Katastrofa në FSDKSH ekspozon institucionin së bashku me asetet, burimet njerëzore dhe palët e interesit ndaj riskut të ndodhjes së ngjarjeve me pasoja negative për të cilat nuk janë të identifikuara masat reaguese.	
16	Nga auditimi në FSDKSH u konstatua se niveli i kapaciteteve TI në disa Drejtori rajonale të FSDKSH është i ulët duke sjellë si rezultat kryerjen e detyrave të këtij funksioni nga punonjës të tjerë të cilët nuk kanë kualifikimet e duhura (Drejtorinë Rajonale Berat, Drejtorinë Rajonale Dibër, Drejtorinë Rajonale Gjirokastër, Drejtorinë Rajonale Shkodër, Degën Tropojë dhe Degën Sarandë). U konstatua se në Rregulloren e Funksionimit të Drejtorive Rajonale, pozicioni i punës Specialist Informaticien, si Diplomë Kualifikuese përcakton Informatikë/ Inxhinieri Elektronike, ndërkohë që në rast se nuk plotësohet ky kusht, atëherë ka kritere zëvendësuese: Arsim i lartë, eksperiencë mbi 10 vjet në Drejtorinë	FSDKSH të marrë masa për kryerjen e ndryshimeve në Rregulloren e Brendshme duke përcaktuar në mënyrë specifike kriteret që duhen për pozicionin Specialist Informaticen në Drejtoritë Rajonale, duke rritur nivelin e kapaciteteve me rezultat punësimin e personave të përshtatshëm për realizimin e detyrave të menaxhimit të teknologjisë së informacionit, e cila për sistemin e sigurimit shëndetësor ka rëndësi të

	Rajonale, dhe certifikatë kualifikimi të kësaj fushe (informatikë). Niveli i ulët i kapaciteteve lidhur me njohuritë, kualifikimet, dhe eksperiencën TI në të gjithë rrjetin e strukturës së FSDKSH mbart riskun e eficencës së dobët dhe mosefektivitet në kryerjen e detyrave që lidhen me teknologjinë e informcionit në këtë institucion.	madhe. Po ashtu të merren masa për plotësimin e pozicioneve të Specialistit të TI në Drejtoritë Rajonale.
17	Nga auditimi në FSDKSH u konstatua se për aplikacionet e implementuara dhe në funksion në FSDKSH, mungojnë kontrolle automatike në këto aplikacione për refuzimin e të dhënave jo të vlefshme, si dhe kontrolle të kombinuara të proceseve që realizohen nga secili aplikacion për menaxhimin e barnave me rimbursim. Nuk janë ngritur kontrolle të përshtatshme periodike për vlefshmërinë dhe korrigjimin e të dhënave në funksion të saktësisë së informacionit të regjistruar për bazat e të dhënave në aplikacionet Depo, Recetat me Rimbursim, e-Farmacia. Nga auditimi i Aplikacioneve dhe ambientit ku ato zhvillohen rezulton se informacioni i tyre nuk është i sigurt kundrejt keqpërdorimeve. Mungojnë kontrolle të veçanta të ndërtuara me skripte që gjenerojnë të dhëna nga baza e të dhënave për ato raste kur kontrolle automatike programet apo aplikacionet nuk kanë, dhe ndërtimi i raporteve mund të jetë i pamundur. Drejtoria DIAS nuk dokumenton modifikime në funksion të të paturit të dhëna të sakta nga ana faktike në bazën e të dhënave edhe kur kjo ka qenë e nevojshme.	Të ndërtohen dhe të dokumentohen skripte dhe procedura për nxjerrjen e informacioneve që nuk gjenerohen nëpërmjet raporteve aktuale të çdo sistemi apo nga kombinimi i tyre. Korrigjimet në të dhëna duhet të bëhen sa herë është e nevojshme, shoqëruar me dokumentacion/ procedura të ndërtuara për sigurimin e të dhënave të sakta. Të merren masa për ndërtimin e kontrolleve të përshtatshme lidhur me programet/ aplikacionet për parandalimin/ regjistrimin/ korrigjimin e të dhënave jo të sakta apo jo të plota, importimin e të dhënave në qendër dhe ushtrimin e kontrolleve mbi saktësinë e informacionit të importuar përpara se të zhvillohen kërkesa të tjera për raportime.
18	Nga auditimi i kontrolleve të aplikacioneve për vlefshmërinë e të dhënave input dhe output, u konstatua se: ***a.*** **Në programin DEPO,** i cili shërben për	FSDKSH, të marrë masa që të identifikojë origjinën dhe sistemimin e të gjitha problematikave lidhur me parregullsitë e konstatuara në

	regjistrimin e inventarëve, faturat hyrëse dhe faturat dalëse që deklarojnë Depot Importuese/Distributore të cilat kanë kontratë me FSDKSH, *konstatohet se janë deklaruar më shumë shitje se sa hyrje të barnave të rimbursueshme, si nga depot, ashtu dhe nga rrjeti i hapur farmaceutik,* ***gjithsej në shumën 1,627,500 mijë lekë.*** *Konkretisht nga auditimi i të dhënave të regjistruara në këtë program evidenton problematikat:* • 5 Depo Farmaceutike rezultojnë të kenë mbyllur vitin 2015 (Dhjetor 2015) me gjendje *negative për 14 barna të rimbursueshme* ***në shumën 1,086,307 mijë lekë,*** *çka do të thotë që referuar të dhënave të sistemit janë deklaruar shitje të barnave drejt rrjetit të hapur farmaceutik më shumë se sa deklarimi në hyrje i tyre (bashkëlidhur Aneksi nr.1).* • Nga përpunimi i të dhënave është konstatuar, se në 10 raste në bilancin shitje, konsum, gjendje të barnave të rimbursuara, rezulton një diferencë, *ku vlera e rimbursuar është më e madhe se vlera e barnave të shitura nga Depot dhe rrjeti Farmaceutik me* ***541,192 mijë lekë*** *(bashkëlidhur Aneksi nr.2).* • Në 16 raste janë regjistruar shitje me minus, të cilat rezultojnë të jenë kthime të *barnave nga Qendrat Spitalore në drejtim të Depove Farmaceutike brenda datës së skadencës në shumën* ***7,731 mijë lekë****, për barna si Ketosteril, Mircera syringe, Renvela, Zelboraf, etj (bashkëlidhur Aneksi nr.3), me argumentimin e nevojës për barna të tjera.* • Regjistrohen fatura shitje kur sasia e barnave në faturë është më e madhe se gjendja e tyre;	bazën e të dhënave, për të tre sistemet të cilët mbajnë të dhëna për rimbursimin e barnave. FSDKSH, të marrë masa për saktësimin e deklarimeve me më shumë shitje se sa hyrje e barnave të rimbursueshme, si nga depot, ashtu dhe nga rrjeti i hapur farmaceutik, gjithsej në shumën 1,627,500 mijë lekë dhe nxjerrja e përgjegjësive dhe rikthimi në buxhetin e tij të vlerave, në rast se konstatohen përfitime të padrejta. Strukturat drejtuese të FSDKSH të sigurojnë marrëdhënie bashkëpunimi në mënyrë sistematike me institucionet të cilat mbajnë të dhëna të rëndësishme lidhur me barnat e rimbursueshme dhe pacientët si: Agjencia e Kontrollit të Barnave dhe pajisjeve Mjekësore (AKBPM), Qendra Kombëtare e Regjistrimit (QKR), Drejtoria e Përgjithshme e Gjendjes Civile (DPGJC), Urdhri i Farmacistëve të Shqipërisë (UFSH), për të ngritur kontrolle periodike në lidhje me monitorimin e të dhënave të Subjekteve, Pacientëve dhe Barnave. Të ndërtohen dhe të

	• Nuk regjistrohen të dhëna për barnat që shkojnë tek subjektet që nuk kanë kontratë me FSDKSH për Depo apo Farmaci; • Nuk ekzistojnë kontrolle për sasinë e barit të cilën subjekti blen dhe sasinë po për të njëjtin bar që i njëjti subjekt kthen, ku kthimi i tij regjistrohet si Shitje me minus (-); • Nuk rezulton të jetë bërë ndonjëherë gjatë vitit 2015 automatikisht apo manualisht kryqëzimi i të dhënave për hyrjet e barnave që Depot deklarojnë, me të njëjtin informacion që ka Agjencia e Kontrollit të Barnave dhe Pajisjeve Mjekësore (AKBPM). • Përditësimi i listës së Farmacive dhe Depove që gjenden në program bëhet vetëm dy herë në vit, një herë në lidhje të kontratës në fillim të vitit dhe herën tjetër me hyrjen në fuqi të listës së barnave, duke mos i update-uar në kohë këto subjekte për kontratat e reja, duke krijuar kushtet për regjistrime jo të sakta në këto raste. • Nuk rezulton të ketë ndonjë krahasim të subjekteve farmaceutikë regjistruar në sistemet Depo, Recetat Offline, E-farmacia me të dhënat për këto subjekte nga Qëndra Kombëtare e Regjistrimit(QKR). • Nga DIAS nuk rezultojnë gjurmë auditimi mbi këtë sistem në zbatim të Rregullores nr. 4, "*Për mbrojtjen, ruajtjen, sigurinë dhe administrimin e te dhënave personale dhe të bazave të të dhënave në Fond*", neni 4, në të cilën thuhet se: *"... mund të bëhet përditësimi e kryerja e çdo veprimi për të siguruar që të dhënat e pasakta e të parregullta të fshihen apo të ndryshohen..."*. **b. Sistemi i recetave te rimbursueshme,** i cili shërben për regjistrimin (hedhjen) e të dhënave të recetës fizike të rimbursimit dhe nxirren statistika	ekzekutohen kontrolle në mënyrë periodike, për të gjitha dobësitë e sistemeve përmendur më sipër, për të monitoruar, cdo rast për cdo të dhënë të regjistruar si të pasaktë/të paplotë.

	për sasinë e barnave të konsumuara, vlerat e rimbursimit për çdo bar sipas mjekut dhe subjekteve farmaceutike. *Nga auditimi mbi këtë program u konstatua se:* – Në këtë program lejohet regjistrimi i recetave që dalin jashtë kufijve të listës së rimbursimit në sasi dhe në kohë, për ato barna për të cilat ekziston një kufizim. – Në këtë program regjistrohen receta me rimbursim të ekzekutuara nga farmaci të cilave ju ka mbaruar kontrata. – Në këtë program për mjekët që punojnë në dy QSH, hapen dy kode të ndryshme nga njëri tjetri, gjë e cila jo vetëm nuk e bën mjekun unik në identifikimin e tij me recetat e rimbursimit, por rrit mundësinë e gabimit nga ana e regjistruesve të këtyre recetave**.** – Për 754 barna (nga 1030 barna në total në listën e rimbursimit miratuar në Prill të vitit 2015), kufizimi në sasi është 999 (pra pacienti mund të marrë një bar në sasinë 999) dhe për 337 prej këtyre ka një kufizim "*Sipas protokollit të Fondit*", që në fakt nuk ekziston sepse asnjë program/sistem nuk mund ta kuptojë shprehjen si kufizim. Saktësia e recetave të lëshuara që përmbajnë barna të cilat kufizohen në sasi "*Sipas protokollit të Fondit*" si dhe mjekët që kanë dhënë këtë mjekim, nuk mund të kontrollohen/monitorohen nëpërmjet sistemit në rrugë elektronike. – Ky program lejon të regjistrohen receta me rimbursim për pacientë që nuk gjenden të regjistruar në tabelën e pacientëve. – Ky program lejon të regjistrohen receta me rimbursim për diagnoza që nuk gjenden të	

	regjistruara në tabelën e diagnozave. – Ky program lejon të regjistrohen receta me rimbursim të lëshuara nga mjek që nuk rezultojnë aktiv. – Në këtë program nuk ekziston ndonjë opsion kontrolli mbi sasinë e barnave që kërkon një recetë me rimbursim të ekzekutohet, sepse nuk ruhen të dhëna mbi Hyrjet dhe Inventarët e Rrjetit farmaceutik, përfshirë këtu dhe farmacitë spitalore. Këto të dhëna nuk kontrollohen me ato të deklaruara nga vetë rrjeti farmaceutik (hyrjet, Inventarët, gjendja), për të siguruar jo vetëm një informacion të saktë në të dy programet, por edhe identifikim të ngjarjeve që kanë nevojë për sistemim veprimi, apo ushtrim kontrolli mbi aktivitetin e tyre. *Auditimi mbi të dhënat në këtë program evidenton problematikat në vijimësi:* – Në 264 raste të evidentuara, janë regjistruar receta për farmaci të cilave ju ka mbaruar kontrata. – Në 115049 raste të evidentuara me vlerën 654,796,437 lekë, janë regjistruar receta të përfituara nga pacientë që nuk rezultojnë të regjistruar në tabelën e pacientëve (bashkëlidhur Aneksi 5) – Në 1078 raste të evidentuara, recetat janë regjistruar në sistem për mjekë të cilët rezultojnë jo aktiv. – Në 1598 raste janë regjistruar barna të dhëna mbi kufizimin e përcaktuar në listën e barnave. – Në 18614 raste të recetave janë ekzekutuar me vlerë shtesë 104,563,845 lekë, ku 30% e kësaj vlere është ekzekutuar vetëm tek subjekti farmaceutik “x”, dhe 11.5% e kësaj shume është	

lëshuar vetëm nga një mjek.

– Në 60 raste të evidentuara të recetave me rimbursim diagnoza nuk gjendet në tabelën e diagnozave.

Nga auditimi u konstatua se, **Drejtoria DIAS** në bashkëpunim me drejtori të tjera si atë të

Cmimeve dhe Rimbursimit të Barnave, **Kontrollit Parësor Farmaceutik**, nuk kanë ushtruar kontrollet e nevojshme mbi bazën e të dhënave dhe marrjen e masave në rastin e shkeljeve të rregullave në fuqi për menaxhimin e rimbursimit.

c. Sistemi i e-farmacisë, shërben për vetdeklarimin e recetave me rimbursim, hyrjet, inventarët dhe kthimet e barnave të rrjetit farmaceutik që kanë kontratë me Fondin. Ky program funksionon Online i tipit Web Based, i lokalizuar në Zyrat qëndrore të FSDKSH-së me bazën e të dhënave në Oracle dhe platforma në Apex.

Auditimi mbi të dhënat në këtë program evidenton problematikat e mëposhtme:

– Lista e barnave regjistrohet pa kufizimet për çdo bar, për të cilin ekziston një kufizim, çfarë do të thotë se përdoruesi (Farmacia) nuk është i kufizuar nga sasia apo koha e përdorimit të barit që ndodhet në një recete rimbursimi.

– Përdoruesit mund të regjistrojnë të dhëna edhe në rastet kur kontrata e subjektit me FSDKSH, ka mbaruar, çfarë tregon një mungesë kontrolli midis përdoruesit dhe kontratës së subjektit për të cilin ky përdorues ekziston.

– Nuk ekzistojnë kontrolle për sasinë të cilën subjekti farmaceutik kthen dhe asaj që ka blerë nga i njëjti furnitor. Kontrolle automatike nuk

	ekzistojnë edhe në lidhje më furnitorin, në mënyrë që të parandalohet procesi i hyrjes së barnave në një sasi të caktuar nga një furnitor dhe kthimi i tij dhe sasisë tek një tjetër. Kthimi i mallit në këtë program regjistrohet si hyrje me minus (-). – Nuk shkarkohen nga subjektet farmaceutike barnat e listës së rimbursimit që shiten pa rimbursim, duke mos dhënë një pamje reale të gjendjes në sistem të këtyre barnave për një subjekt farmaceutik të caktuar. – Ky program nuk ka ndërveprim të të dhënave me sistemin DEPO, për të marrë shitjet e tyre të cilat automatikisht duhet të jenë hyrje për farmacinë, madje për vitin 2015 nuk rezulton të jetë bërë as manualisht ky kryqëzim të dhënash. – Farmacitë spitalore nuk ekzistojnë të regjistruara si "*Farmaci*", por vetëm farmacia e QSUT, çfarë do të thotë se shitjet apo kthimet që deklarojnë depot farmaceutike në programin Depo, në drejtim të këtyre farmacive, nuk mund të monitorohen nëpërmjet sistemit. – Nuk ekziston ndonjë kontroll në regjistrimin e furnitorit për administratorin, drejtuesin teknik, niptin etj. – Nuk rezulton të ketë ndonjë krahasim të subjekteve farmaceutikë regjistruar në programin e- FARMACI me të dhënat për subjekte nga Qendra Kombëtare e Regjistrimit (QKR). Gjithashtu nuk rezulton të ketë ndonjë kryqëzim të dhënash për të dhënat e drejtuesve teknik me UFSH (Urdhrin e Farmacistëve të Shqipërisë). Nuk rezultojnë të ketë ndonjë krahasim edhe me statusin e pacientëve me DPGJC. – Regjistrohen shitje të barnave nëpërmjet recetave të rimbursueshme edhe kur nuk ka	

	gjendje, duke e çuar gjendjen e tyre me minus. *Nga auditimi mbi të dhënat në sistem u konstatua se:* – Nisur nga fakti që jo çdo recetë e deklaruar nga rrjeti farmaceutik në programin e-farmacia është detyrim për t'u regjistruar e më tej rimbursuar, janë konstatuar diferenca ndërmjet recetave me rimbursim të vetdeklaruara në programin e-farmacia dhe recetave fizike të regjistruara në sistemin e recetave. – Në program janë evidentuar raste të recetave që nuk kanë mjekë me statusin "Pranuar", në total 80123 rekorde. – Në program janë evidentuar raste të hyrjeve të farmacive nga furnitor që ju ka mbaruar kontrata me FSDKSH, me statusin "Pranuar", në total 321042 rekorde. – Në program janë evidentuar raste të faturave hyrëse me minus (pra kthime) dhe statusin "Pranuar" të farmacive nga furnitor që ju ka mbaruar kontrata me FSDKSH, në total 1253 rekorde. – Edhe në këtë sistem nuk ka asnjë gjurmë të sistemimit të veprimeve të regjistruara gabim, duke mbartur ngjarjet njëra pas tjetrës. – Në kontratën e lidhur ndërmjet DRSKSH dhe rrjetit farmaceutik, kërkohet që hyrja të deklarohet për një afat më të gjatë se shitja, dhe konkretisht për vitin 2015, hyrja ka qenë detyrim të deklarohet për 7 ditë ndërsa dalja për 2 ditë, cfarë sjell një mosbarazim të gjendjes elektronike të barnave për një subjekt të caktuar, me inventarin e tyre. – Gjithashtu, në sistem nuk regjistrohen Recetat që përmbajnë barna të listës së rimbusueshme, të cilat rrjeti farmaceutik i ka shitur pa rimbursim,	

	çfarë tregon se gjendja elektronike e barnave me rimbursim, për një subjekt të caktuar nuk mund të jetë sa gjendja fizike e tyre. – Mungesa e të dhënave të regjistruara në programin e-farmacia për subjektet Spitalore si dhe subjekte që nuk kanë kontratë me FSDKSH (hyrjet/daljet/kthimet në drejtim të farmacive dhe depove si dhe anasjelltas), bëjnë që procesi i monitorimit për qarkullimin e barnave me rimbursim për këto subjekte të mos mbyllet vetëm në rrugë elektronike. Si rezultat i kësaj analizë, *grupi i auditimit konstaton se gjendja elektronike e barnave në rrjetoin e lirë farmaceutik, nuk është aspak e besueshme.*	

AUDITIMET E TEKNOLOGJISË SË INFORMACIONIT 2017

Drejtoria e Auditimit të Teknologjisë së Informacionit për vitin 2017 ka qenë pjesë e Departamentit të Auditimit të Departamenti i Auditimit të Teknologjisë së Informacionit dhe Investimeve të Huaja me përbërje 5 anëtarë nga të cilët 4 Auditues.

Ndër rezultatet e arritura nga kjo drejtori gjatë vitin 2017 veçojmë:

- Zhvillimi i një Auditimi Tl pilot me asistencë të IPA-s.
- Përdorimi i manualit activ të auditimit në auditim.
- Nisja e krijimit të bazës së të dhënave për subjektet e auditimit TI(ICTS Database).
- Krijimi i linjës së parë të suportit me njohuri mbi auditimin TI dhe trajnimi i tyre.

Si rezultat i përdorimit të analizës së riskut në planifikimin e auditimit nëpërmjet manualit aktiv të auditimit TI u arrit një rritje e treguesve gjatë vitit 2017 si më poshtë.

Treguesi	Njësia	Vlera
Fuqia maksimale Audituese e drejtorisë	Ditë/njerëz	1210
Auditime të planifikuara	numër	4
Për çdo auditim mesatarisht	Ditë/njerëz	302

Subjekte e planifikuara për auditim

1. Drejtoria e Përgjithshme të Taksave dhe Tarifave Vendore (Auditim Pilot IPA).
2. Instituti i Statistikave.
3. Drejtoria e Ujësjellës Kanalizimeve, Tiranë.

4. Instituti i Sigurimeve Shoqërore.

MBI AUDITIMIN E USHTRUAR NË DREJTORINË E PËRGJITHSHME TË TAKSAVE DHE TARIFAVE VENDORE (AUDITIM PILOT IPA).

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "**Drejtorinë e Përgjithshme të Taksave dhe Tarifave Vendore"**

Përgatitur: 1.12.2017

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 619/1 prot, datë 26.09.2017.

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Meald Habazaj, anëtar
3. Elira Cukalla, anëtar
4. Bledi Dervishi anëtar

Periudha e Auditimit: 01.01.2016. 31.12.2017

Afati i auditimit: 30.05.2017 - 17.11.2017
Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve

ÇFARË KEMI AUDITUAR

Kontrolli i Lartë i Shtetit në zbatim të planit të auditimit nr. 5/5 datë 30.05.2017 dhe të programit të auditimit nr.619/1, datë 26.09.2017 ushtroi një auditim të sistemeve të teknologjisë së informacionit në Drejtorinë e Përgjithshme të Taksave dhe Tarifave Vendore
Ky auditim në kuadër të binjakëzimit IPA, AL 13 IB FI 01 u zgjodh si "Auditim pilot të TI-së në një sistem tipik të TI-së së administratës shtetërore" dhe u asistua nga ekspertet e TI-së :z. Banaś Pawel i SAI-t të Polonisë, z. Carlos Cardoso i Gjykatës së Llogarive të Portugalisë dhe z. Alo Lääne i SAI-t të Estonisë.

Drejtoria e Përgjithshme e Taksave dhe Tarifave Vendore (DPTTV) është institucion buxhetor, që e zhvillon aktivitetin e saj në territorin e qytetit të Tiranës. Kjo drejtori është në varësi administrative nga Drejtoria e Përgjithshme Ekonomike pranë Bashkisë Tiranë.

Struktura organizative, emërtimet dhe numri i personelit të Drejtorisë miratohet nga Këshilli Bashkiak, sipas përcaktimeve të legjislacionit në fuqi.

Vizioni i Drejtorisë së Përgjithshme të Taksave dhe Tarifave Vendore është të ofrojë një sistem të ndershëm të administrimit të taksave vendore, të arritshëm dhe që t'ju përgjigjet taksapaguesve.

Qëllimet strategjike të DPTTV përfshijnë:

- ofrimin e shërbimeve me cilësi dhe në kohë për taksapaguesit, nëpërmjet menaxhimit të sistemeve të regjistrimit,
- dhënien e informacionit, shpjegimit, llogaritjes së detyrimit/ve;
- përshpejtim dhe lehtësim të procedurave për pagesat e taksave vendore për të gjitha subjektet taksapaguese që ushtrojnë aktivitetin e tyre në qytetin e Tiranës.

Aktiviteti i Drejtorisë së Përgjithshme të Taksave dhe Tarifave Vendore është i përqendruar në dy drejtime:

a. Mbledhja e taksave dhe tarifave vendore;

b. Administrimi dhe mirëmenaxhimi i tregjeve publike.

Për realizimin e objektivave DPTTV, ka implementuar një infrastrukturë TI për ofrimin e shërbimeve të planifikuara për të gjithë taksapaguesit, qytetarët.

Për mirëmbajtjen e sistemit DPTTV ka ngritur një strukturë të Teknologjisë së Informacionit në nivel sektori me emërtim "Sektori i TI dhe Statistikës" i cili është pjesë përbërëse e Drejtorisë së Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe mbështet aktivitetin e saj kryesor në zbatimin e Vendimit të Këshillit Bashkiak Nr. 59, datë 30.12.2015, i ndryshuar, mbi "Sistemin e Taksave dhe Tarifave Vendore në Qytetin e Tiranës".

Fushat e auditimit

1. Auditimi i funksionimit të Qeverisjes TIK

1.1 *Verifikimi i Strategjisë, politikave dhe procedurave në TIK*

1.2 *Vlerësimi i burimeve njerëzore në strukturën TIK*

2. Auditimi i Sigurisë së Informacionit

2.1 *Identifikimi dhe menaxhimi i risqeve në TIK*

2.2 *Siguria e të dhënave dhe vazhdimësia e biznesit*

2.3 *Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet*

3. Auditimi i sistemit Informatik të Taksave dhe Tarifave Vendore

3.1 *Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output*

***3.2** Kontrolli i shkallës së sigurisë të aplikacioneve, përdoruesve të jashtëm dhe të brendshëm.*

PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Auditimi i Teknologjisë së Informacionit në Drejtorinë e Përgjithshme e Taksave dhe Tarifave Vendore paraqet një rëndësi të vçantë pasi nëpërmjet tij kryhet mbledhja e Taksave e Tarifave vendore të kryeqytetit, dhe krijohen facilitetet jo vetëm taksapaguesve të saj por edhe duke qenë mjeti për mbledhjen e të ardhurave të buxhetit të Bashkisë së Tiranës.
Në përfundim të auditimit për 23 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit

Më hollësisht:

<u>OPINIONI I AUDITIMIT:</u>

Grupi i auditimit duke pasur parasysh rolin e teknologjisë se informacionit në përmbushjen e misionit të Drejtorisë së Përgjithshme të Taksave dhe Tarifave Vendore në mbledhjen e të ardhurave tatimore dhe tarifore përmes procedurave të thjeshtuara dhe me kosto minimale, për të siguruar aplikimin e politikave fiskale të Bashkisë së Tiranës ndaj qytetareve. Për sa më sipër, mbështetur në Standardet Kombëtare dhe Ndërkombëtare të Auditimit, si më poshtë:ISSAI 1 Neni 22, Ligjin e KLSH Nr.154/2014 Neni 3 dhe 14, Manualin e Auditimit të Teknologjisë së Informacionit (WGITA), COBIT 4.1, ISSAI 5300.6, 8 dhe 12.2, 16.19, 21.1, 23,

ISSAI 100.36,48, ISSAI 5310, pas shqyrtimit të të dhënave dhe dokumentacionit TI të vënë në dispozicion nga DPTTV, arriti në konkluzionin se:

Zhvillimi i Teknologjisë së Informacionit në mungesë të një Strategjie në DPTTV ka sjellë mos pasqyrimin qartë të objektivave të institucionit lidhur me infrastrukturën TI dhe burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen e saj.

Mungesa e Planit Strategjik mbart riskun e keq adresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së DPTTV nga Teknologjia e Informacionit

Me gjithë përpjekjet e bëra, DPTTV nuk ka marrë masa të mjaftueshme rregullator dhe organizative për garantimin e sistemeve të informacionit.

Në gjykimin tonë, menaxhimi i elementëve kritikë në sistemet e informacionit, është i pa pamjaftueshëm dhe i papërshtatshëm, Investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht sigurimin e Vazhdueshmërisë së Biznesit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	DPTTV nuk ka një Plan Strategjik të shkruar e miratuar për Teknologjinë e Informacionit duke mos bërë planifikime strategjike mbi sigurinë institucionale dhe infrastrukturën TI si dhe duke mos pasqyruar qartë objektivat lidhur me burimet dhe instrumentet e nevojshme për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së DPTTV.	Strukturat drejtuese të DPTTV, duke marrë në konsideratë kohën, burimet e nevojshme si dhe rëndësinë e të dhënave që institucioni posedon dhe përpunon, të marrin masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit.
2.	Manuali i sistemit informatik për Menaxhimin e Taksave Vendore në DPTTV është i pa updatuar me ndryshimet që ka pësuar sistemi ndër vite (*ri programim i moduleve, shtimi i tyre etj*).	Strukturat drejtuese të DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës të marrin masa për updatimin e manualit për Sistemin Informatik për Menaxhimin e Taksave Vendore, ku të përfshihen të gjitha operacionet TI
3	*Rregullorja e Brendshme, lidhur me strukturën TI në DPTTV*, nuk është në përputhje me rekomandimet e AKSHIT, rregullorja nuk përmban elementët e nevojshëm për të siguruar funksionim e përshtatshëm të strukturës TI në institucion	DPTTV në bashkëpunim me Bashkinë Tiranë dhe strukturat këshilluese mbi TI, të hartojë, dhe miratojë në Këshillin Bashkiak, *Rregulloren e Funksionimit të Drejtorisë së Përgjithshme të Taksave dhe Tarifave Vendore*. Hartimi i kësaj Rregulloreje të marrë në konsideratë vendosjen e kontrolleve të brendshme lidhur me menaxhimin e riskut, përputhshmërinë me procedurat dhe rregullat e brendshme aktuale të drejtorisë si dhe me legjislacionin e

		Teknologjisë së Informacionit dhe Komunikimit në Shqipëri
4	*Rregulla lidhur me trajtimin e incidenteve*. Situata në DPTTV, për periudhën nën auditim, menaxhohet mbi bazë ngjarjesh (*d.m.th. për raste të veçanta është dhënë zgjidhje praktike, jo e paracaktuar*), d.m.th. ndihma, mbështetja teknike dhe logjike për operacionet TI që ndihmojnë mbarëvajtjen e strukturave të institucionit, kryhet nëpërmjet shkëmbimeve verbale dhe nëpërmjet emaileve, në mungesë të procedurave të shkruara. Në këtë mënyrë, institucioni nuk ka të dokumentuar një plan masash për trajtimin e gabimeve dhe incidenteve që kanë ndodhur ose mund të ndodhin në infrastrukturën TI. *Rregulla për menaxhimin e ndryshimeve*. U konstatua se DPTTV nuk ka të implementuar një procedurë të standardizuar për kontrollin e ndryshimeve në infrastrukturë dhe në sistemet e TI në institucion. Pra DPTTV nuk ka: • procedura për inicimin, rishikimin dhe aprovimin e ndryshimeve, prioritarizimin e tyre; • struktura kontrolli për verifikimin e efektivitetit të ndryshimeve të kryera; • procedura për ndryshimet emergjente si dhe dokumentimin e të gjithë procesit të ndryshimeve.	Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës të marrin masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve. Të marren masa për menaxhimin e ndryshimeve dhe dokumentimin e të gjithë procesit të ndryshimeve. Institucioni të identifikojë risqet me efekt negativ në TI dhe veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura.
5	Nisur nga objektivat e DPTTV, nga	Strukturat drejtuese të DPTTV, duke

	shtrirja e teknologjisë së informacionit në institucion si dhe nga rëndësia e të dhënave që ruhen dhe përpunohen nga Sektori i TI dhe Statistikës për mbledhjen e taksave në Bashkinë Tiranë me anë të sistemit informatik për Menaxhimin e Taksave Vendore, grupi i auditimi gjykon që struktura e Sektorit të TI-së dhe Statistikës në nivel sektori sjell uljen e ndikimit të TI-së në qeverisjen e DPTTV dhe zbehjen e ndikimit të varësinë direkt nga Drejtori i Përgjithshëm.	marrë në konsideratë kohën, burimet e nevojshme të marrin masa për ngritjen në nivel të strukturës së TI nga nivel sektori në nivel Drejtorie
6	**1.** Me qëllim që të sigurohet parashikimi, programimi dhe implementimi i suksesshëm i veprimtarive trajnuese është e nevojshme që procesi të mbështetet në një identifikim dhe analizë të nevojave për trajnim të stafit. Në këtë kuadër, për vitin 2016 nuk është zhvilluar asnjë ditë trajnimi për specialistët e Sektorit TI dhe Statistikës. • *DPTTV nuk ka kërkesa dhe analiza të nevojave për trajnim të stafit të Sektorit të TI dhe Statistikës;* *DPTTV nuk ka plan dhe nuk ka zhvilluar trajnime për sistemet, sigurinë dhe teknologjinë e informacioni për stafin e Sektorit të TI dhe Statistikës gjatë vitit 2016.*	Strukturat drejtuese të DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës të marrin masa për identifikimin e nevojave për trajnimin e stafit TI dhe të çdo përdoruesi të sistemeve TI si dhe të hartojë e miratojë plane dhe politika për zhvillimin e trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit.
7	Nga auditimi se si DPTTV identifikon dhe menaxhon risqet në teknologjinë e informacionit, u konstatua se DPTTV nuk disponon një regjistër risku për teknologjinë e informacionit në	Strukturat drejtuese të DPTTV në bashkëpunim me Drejtorinë e Auditit të Brendshëm, Drejtorinë e Burimeve Njerëzore dhe me Sektorin e TI dhe Statistikës të marrë masa për hartimin e

	mospërputhje me ligjin nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar, Udhëzimi nr. 30, datë 27.12.2011 "Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik".	një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve. Të marren masa për menaxhimin e ndryshimeve dhe dokumentimin e të gjithë procesit të ndryshimeve, si dhe monitorimin periodik për zbatimin e masave të marra nga sektori përgjegjës
8	Nga Auditimi u konstatua se ambienti fizik i dhomës së rrjetit nuk është në përputhje me standardet e përcaktuara në Rregulloren për Ndërtimin e Dhomës së Serverëve (Versioni 1.0, datë 02.12.2008) miratuar nga AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit) *Pika 4.3. Parandalimi i zjarrit. Pika 4.5. Sistemi Elektrik. Pika 4.6. Sistemi i Alarmit.*	Të merren masa për ndërtimin e ambienteve të dhomave të serverave në bazë të VKM nr. 248, datë 27.04.2007 "Për krijimin e Agjencisë Kombëtare të Shoqërisë së Informacionit" dhe Rregulloren për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK dhe praktikat më të mira kombëtare dhe ndërkombëtare
9	Për testimin e performacës së faqes së internetit të DPTTV *http://www.dpttv.gov.al* u bënë disa teste të thyerjes së sigurisë dhe mangësive nga ku rezultoi se: Skaneri zbuloi më shumë se një dobësi të tipit të riskut të lartë. Një përdoruesi me qëllim të keq mund të shfrytëzojë këto dobësi dhe të komprometojë bazën e të dhënave ose të fshij faqen e internetit.	Të merren masa për pajisjen e faqes së Webit të DPTTV me Çertefikatë Sigurie, pasi kur instalohet në web, aktivizon hapjen dhe protokollin https dhe kryen lidhje të sigurta ndërmjet shfletuesit (browserit) dhe faqes së Webit
10	DPTTV nuk ka Plan të miratuar emergjence dhe politika të miratuara për vazhdimësinë e biznesit, vlerësim/analizë risku për sigurinë e të dhënave, identifikimin e të dhënave kritike si dhe kërcënimet e mundshme,	Strukturat drejtuese të DPTTV me sektorin TI, të hartojnë dhe miratojnë me përparësi një plan emergjence si dhe politika të analizuara, për të garantuar vazhdimësinë e ofrimit të shërbimeve ku në përbërje të gjejnë zgjidhje të gjithë

	për çdo proces kritik të aktivitetit të DPPTV.	elementët përmendur më sipër, për të qenë të përgatitur nga kërcënime te mundshme të ndërprerjes së shërbimit të ofruar.
11	DPTTV nuk disponon dokumentim/ implementim të politikave mbi sigurinë e informacionit duke patur parasysh: objektivat, qëllimin, konfidencialitetin e të dhënave, parimet dhe standardet, përcaktim të përgjegjësive të përgjithshme dhe specifike, backup-it, trajnim dhe edukim mbi sigurinë, monitorim dhe raportim të elementëve të implementuar të sigurisë.	Strukturat drejtuese të DPTTV me sektorin TI, të hartojnë dhe implementojnë me përparësi politika mbi sigurinë e të dhënave që disponon.
12	Nga auditimi u konstatua një mungesë ambienti i veçantë për testime përpara kalimit të ndryshimeve në sistemin Live të sistemit të tatim taksave Tiranë, e cila komprometon sigurinë e sistemit, të të dhënave si dhe vazhdimësinë e ofrimit të shërbimeve.	Strukturat drejtuese të DPTTV me Sektorin TI, të marrë masa për një riorganizim të hapësirave fizike dhe logjike në pajisjet server lidhur me shërbimet që ofron aktualisht, me qëllim: – Krijimin e Active Directory dhe Domain Controller për një identifikim të qendërzuar të sigurt, kontrollin dhe menaxhimin e shërbimeve në përputhje me standardet – Përfitimin e një performance më të mirë të aplikacionit – Garantimin e vazhdimësisë së shërbimeve të ofruara – Krijim hapësire për një kopje të sistemit në funksion të testimeve apo trajnimeve të ndryshme sipas rastit.
13	Nga auditimi i trigera-ve që popullojnë tabelën e auditimit, rezultoi se: **a** Ndryshimet në të dhëna,	Të analizohen të gjitha mundësitë, për të siguruar gjurmën e auditimit lidhur me të dhënat më të rëndësishme që DPTTV

	pasqyrohen në trajtën e komenteve, çka e bën të vështirë ndjekjen e gjurmës së auditimit, apo nxjerrjen e raporteve dhe evidentimin e saktë të rasteve të ndërhyrjeve në sistem për ato rekorde që ruhen. **b.** Mungojnë fusha të tjera të rëndësishme si: Hyrje në sistem (login); Viti i detyrimit; Afati i likuidimit të Taksës; Numri i këstit; Emërtimi i Taksës; Vlera e vjetër (old value) dhe vlera e re (new value); Dalje nga sistemi (logout) **c.** Mungon gjurma e auditimit për veprime si: modifikimin, heqjen dhe dhënien e të drejtave një përdoruesi si dhe veprime të tjera që lidhen me aktivitetet e përdoruesve**.**	disponon, atë të tatim-taksapaguesve të rrethit të Tiranës, duke rritur sigurinë e duke garantuar kështu zbulimin në rast tjetërsimi të informacionit nga përdorues të brendshëm apo të jashtëm
14	Nga auditimi i parametrizimit të bazës së të dhënave lidhur me sigurinë, rezulton se afërsisht 90 konfigurime të identifikuara i përkasin një niveli risku të lartë, për të cilat DPTTV nuk disponon asnjë informacion lidhur me to apo të ketë marra masat e nevojshme për adresimin e këtyre çështjeve.	Të merren masat e nevojshme, për një adresim të saktë të konfigurimeve me risk të lartë, dokumentimi e ndjekja deri në zgjidhjen më të mirë, të parametrizimit.
15	**2.** Nga auditimi mbi rolet dhe të drejtat e përdoruesve u konstatuan: • 325 funksionalitete të krijuara në role të ndryshme rezultojnë të pa lidhur tek të paktën një përdorues. • Disa funksione rezultojnë të regjistruara në më shumë se një rekord dhe identifikimi i roleve nuk realizohet me anë të një kodi unik, duke mundësuar	DPTTV të kërkojë zgjidhjen e këtyre problematikave nga ana e subjektit që ka ndërtuar këtë aplikacion të cilët janë edhe të kontraktuar për mirëmbajtjen e tij, si detyrim kontraktual i mirëmbajtjes nëse është e mundur.

	përsëritjen e funksionaliteteve tek një përdorues. • Sistemi lejon lidhjen e të njëjtit përdorues me të njëjtin rol-përdorimi në më shumë se një herë, pasi kontrolli lidhur me këtë çështje mungon. Mirëmbajtësit e aplikacionit punojnë me përdoruesin "*Administrator*" i njëjti përdorues që disponon dhe përgjegjësi i sektorit, duke krijuar kështu mangësi në identifikim të veprimeve që realizon kontraktori me veprimet operacionale që kryen përgjegjësi i sektorit. • Passwordi i përdoruesve në sistemin e tatim taksave vendore kërkohet në mënyrë të kushtëzuar të përbëhet nga 6 karaktere, por nuk ka asnjë specifikim lidhur me llojin e karaktereve (alfa, numerike) si dhe afatin e përcaktuar mbi vlefshmërinë dhe ndryshimin e tij. Ky kushtëzim e klasifikon paswordin në të dobët çka rrit mundësinë e humbjes apo thyerjes së tij. • Arkivimi elektronik i të dhënave të sistem taksave nuk kryhet, duke ulur në këtë mënyrë performancën e sistemit, duke patur parasysh që në këtë sistem ndodhen rekorde që prej vitit 2003.	
16	Nga auditimi, rezultojnë 139,086 persona të lidhur me një subjekt/pronë, por nga auditimi mbi të dhënat e regjistruara lidhur me saktësinë e regjistrimit, rezulton se: • 60,442 persona rezultojnë me NID null	DPTTV, të realizojë kontrolle periodike me DPGJC, për të siguruar një informacion të saktë të të dhënave të taksapaguesve Tiranë.

	• 43,694 persona rezultojnë me NID jo në formatin e duhur • 34,949 persona rezultojnë me NID sipas formatit LNNNNNNNNL (ku L- Letter dhe N- Number) nga të cilët në Drejtorinë e Përgjithshme të Gjendjes Civile, të saktë rezultojnë 24,375 persona ose 17% e gjithë taksa paguesve Tiranë.	
17	Nga analizimi i bazës së të dhënave të Sistemit "Manaxhimi i Taksave Vendore për periudhën 01.01.2016 deri me 31.12.2016 me teknikat CAAT rezultuan parregullsi në fusha të ndryshme të bazës së të dhënave që tregojnë për: **a.** mungesën e kontrolleve të sistemit në input-in e të dhënave. **b.** probleme të sigurisë së sistemit. **c.** formatime jo te rregullta te fushave	Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës duke vlerësuar burimet të marrin masa për formatimin e fushave të bazës së të dhënave sipas qëllimit për të cilën janë dizenjuar si dhe vendosjes se "Regular Expression" për kontrolle për inputin e informacionit në këto fusha.
18	Baza e të dhënave të Sistemit "Manaxhimi i Taksave Vendore nuk është e regjistruar si bazë të dhënash shtetërore në ARK në kundërshtim me ligjin nr. 10325, datë 23.09.2010 "Për bazat e të dhënave shtetërore" dhe VKM Nr. 945, datë 2.11.2012 Regjistrimi i bazës së të dhënave është i nevojshëm për standardizimin dhe sigurimin e saj.	Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës të marrin masa për plotësimin e kërkesave ligjore dhe regjistrimin e bazës së të dhënave si bazë të dhënash shtetërore
19	Nga auditimi i ndërfaqes web të Sistemit "Manaxhimi i Taksave Vendore vërehet se kjo bazë të dhënash nuk ka module të komunikimit përmes web-serviceve me: a. bazën e të dhënave të ZVRPP për	Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës të marrin masa për Akses përmes web-

	identifikimin i të gjitha pasuritë e paluajtshme që ndodhen në territorin e Bashkisë Tiranë me impakt uljen e saktësisë e të dhënave të pronave në sistem. b. bazën e të dhënave të QKB për identifikimin i të gjitha subjekteve që ndodhen në territorin e Bashkisë Tiranë.	serviceve dhe një ndërfaqeje te re te sistemit aktual për: a. Komunikim përmes web-serviceve dhe ndërfaqeje te re te sistemit aktual për "Shkëmbimin e informacionit për pronat nga ZVRPP" b. Krijimi i një moduli te ri, i cili përmes web-serviceve te mundësojë shkëmbimin e informacionit nga QKB.
20	Nga auditimi i komunikimit të njoftimeve e të dhënave tek portali e-Albania konstatohet se krahas info mbi pagesat për subjektet, i cili transferohet aktualisht te portali e-albania, nuk publikohen edhe njoftime të tjera mbi të dhënat aktuale apo ndryshimet e subjektit, duke mos pasur një qasje e plotë e në kohë reale të subjektit me të dhënat e tij të drejtorisë së taksave dhe tarifave vendore.	Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës të marrin masa për të pasur një qasje të plotë e në kohë reale të komunikimin të njoftimeve e të dhënave të subjektit në portalin e- Albania
21	Nga auditimi i kontrolleve në hedhjen e të dhënave dhe logimit në sistem, konstatohet se Log-et, të cilat gjenerohen nga sistemi i taksave nuk analizohen përmes një ndërfaqeje aplikative, e cila të mundësojë një shfletim në kohe reale të tyre. Në këtë mënyrë specialistet TI nuk kanë akses në mënyrë të shpejtë për të bërë kërkime si: tentativat e dështuara për log-in, nr e login nga një PC etj.	Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës duke vlerësuar burimet të marrin masa për implementimin e një programi aplikativ për leximin e log-eve.
22	Nga auditimi i programit vërehen pasaktësi në adresat si dhe të dhënat e tjera të subjekteve te cilat ndikojnë direkt në procesin e identifikimit dhe	Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e TI dhe Statistikës dhe

	grumbullimit të informacionit, përcaktimin e parametrave të subjekteve prej të cilave pritet të gjenerohen detyrimet.	strukturat e DPTTV në teren duke vlerësuar burimet të marrin masa për plotësimin e informacioneve mbi subjektet.

AUDITIMI I TEKNOLOGJISË SË INFORMACIONIT USHTRUAR NË INSTITUTIN E STATISTIKAVE.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "**Instituti i Statistikave"**

Përgatitur: 25 dhjetor 2017

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 866/1, datë 10.10.2017.

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Armanda Begaj, anëtar

Periudha e Auditimit: 01.01.2016 – 31.12.2016
Afati i auditimit: 08.09.2017 - 31.10.2017

Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve.

ÇFARË KEMI AUDITUAR

Instituti i Statistikave (INSTAT) është institucioni kryesor prodhues i statistikave zyrtare dhe koordinatori i sistemit kombëtar statistikor, i cili ka për detyrë të ofrojë të dhëna të besueshme dhe të krahasueshme, përdoruesve për vendimmarrje dhe kërkime, të përshtatë metodologjitë dhe shtojë listën e treguesve statistikor. Në zbatim të Ligjit nr.9180, datë 05.02.2004 "Për statistikat zyrtare", ky sistem përbëhet nga një numër institucionesh të ngarkuar për prodhimin e statistikave zyrtare dhe institucione të tjera, publike ose jo, të cilët nxjerrin statistika të fushave të ndryshme për monitorimin apo zbatimin e politikave të veta zhvilluese.

Veprimtaria e INSTAT rregullohet me Ligjin Nr.9180, datë 5.2.2004 "Për Statistikat Zyrtare", ndryshuar me Ligjin nr. 21/2012 "Për një ndryshim në Ligjin nr. 9180, datë 5.2.2004 "Për statistikat zyrtare""; dhe me Ligjin nr. 7/2013 "Për disa ndryshime dhe shtesa në Ligjin nr. 9180, datë 5.2.2004 "Për statistikat zyrtare", i ndryshuar".

Misioni i INSTAT

Misioni i INSTAT-it është të prodhojë statistika asnjanëse, transparente dhe të përditësuara, të cilat ndihmojnë në gjykimin e përdoruesve mbi proceset e zhvillimit e transformimit në fushat ekonomiko sociale brenda vendit.

Në shumicën e rasteve të dhënat statistikore janë rezultat i vrojtimeve statistikore. Një vrojtim statistikor përfshin të gjitha aktivitetet e mbledhjes, përpunimit dhe shpërndarjes së të dhënave statistikore. Përmes viteve praktika e organizatave statistikore ka krijuar lloje të ndryshme të vrojtimeve statistikore. Metoda e mbledhjes së të dhënave input krijon dallime midis llojeve të ndryshme të burimeve statistikore:

- Censuset: Të dhënat mblidhen për të gjitha njësitë e popullsisë së synuar.
- Vrojtimet: Të dhënat mblidhen për një kampion rastësisht të zgjedhur të njësive të popullatës së synuar.
- Burimet administrative: Të dhënat që fillimisht janë mbledhur për ndonjë qëllim tjetër dhe përdoren nga INSTAT për nxjerrjen e treguesve statistikorë.

Në varësi të metodës së mbledhjes së të dhënave, ndërtohet edhe aplikacioni i kapjes së të dhënave si edhe procesi në vazhdim për prodhimin e statistikave zyrtare.

Lista e aplikacioneve për vrojtimet e ndryshme jepet tek “Surveys.xlsx”, ku paraqiten vrojtimet sipas mënyrës së mbledhjes së të dhënave, si edhe platformat ku janë ndërtuar aplikacionet e kapjes së të dhënave.

Për çdo produkt statistikor, statisticienët prodhojnë statistika duke u mbështetur në platforma të ndryshme si: SAS, SPSS, MS Access, MS Excel, etj. Kopjet finale të tyre ruhen në Sql Server. Dokumentimi i tyre duhet të bëhet në një platformë të quajtur “Metaplus”, nga e cila janë gjeneruar materialet e vendosura tek folder “Metaplus Raporte”. Këto raporte përmbajnë informacion mbi strukturë e të dhënave të bazave të dokumentuara. Aktualisht INSTAT është në proces dokumentimi dhe është përfunduar dokumentimi i 20 bazave (2 regjistra, 9 burime administrative, 5 vrojtime dhe 4 bazat e Censusit të Popullsisë dhe Banesave 2011).

INSTAT në kuadër të IPA 2013 është duke punuar për ndërtimin e një Sistemi të Integruar të Teknologjisë së Informacionit (SI), mbështetur në një databazë me të dhëna të strukturuara në formë metadatash, bazuar në modelin e proceseve të GSBPM (Generic Statistical Business Processes Model). Çdo modul i SI përfaqëson një fazë të ciklit të sistemit të prodhimit statistikor. Sistemi po ndërtohet ndërtuar në .net me databazë SQL server.

Fushat e auditimit

Auditimi i funksionimit të Qeverisjes TI

a. Verifikimi i Strategjisë, politikave dhe procedurave në TI;

b. Vlerësimi i burimeve njerëzore në strukturën TI.

Auditimi i Sigurisë së Informacionit

a. Identifikimi dhe menaxhimi i risqeve në TI;
b. Siguria e të dhënave dhe vazhdimësia e biznesit.

Të ndryshme të dala gjatë auditimit

III. PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Auditimi i Sistemeve të Teknologjisë së Informacionit në Instituti i Statistikave (INSTAT) u përzgjodh pasi ky institucion është prodhuesi kryesor i statistikave zyrtare dhe koordinatori i sistemit kombëtar statistikor, që ka për detyrë të ofrojë të dhëna të besueshme dhe të krahasueshme, përdoruesve për vendimmarrje dhe kërkime, Në përfundim të auditimit për 7 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit.

Më hollësisht:

<u>OPINIONI I AUDITIMIT:</u>

Grupi i auditimit duke pasur parasysh rolin e teknologjisë se informacionit në përmbushjen e misionit të INSTAT-it në prodhimin e statistikave asnjanëse, transparente dhe të përditësuara, si dhe rëndësinë e tyre në proceset e zhvillimit e transformimit të fushave ekonomiko sociale mbështetur në Standardet Kombëtare dhe Ndërkombëtare të Auditimit, si më poshtë:ISSAI 1 Neni 22, Ligjin e KLSH Nr.154/2014 Neni 3 dhe 14, Manualin e Auditimit të Teknologjisë së Informacionit (WGITA), COBIT 4.1, ISSAI 5300.6, 8 dhe 12.2, 16.19, 21.1, 23, ISSAI 100.36,48, ISSAI 5310, pas shqyrtimit të të dhënave dhe dokumentacionit TI të vënë në dispozicion nga INSTAT, arriti në konkluzionin se:

Zhvillimi i Teknologjisë se Informacionit në mungesë të një Strategjie në INSTAT ka sjellë mos pasqyrimin qartë të objektivave të institucionit lidhur me infrastrukturën TI dhe burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen e saj.

Mungesa e Planit Strategjik mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së INSTAT nga Teknologjia e Informacionit

Me gjithë përpjekjet e bëra, INSTAT nuk ka marrë masa të mjaftueshme rregullatore dhe organizative për garantimin e sistemeve të informacionit.

Në gjykimin tonë, menaxhimi i elementëve kritikë në sistemet e informacionit, është i pa pamjaftueshëm dhe i papërshtatshëm, Investimet në sistemet e informacionit nuk kanë

zgjidhur përfundimisht sigurimin e Vazhdueshmërisë së Biznesit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat.

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	Nga auditimi i Strategjisë, politikave dhe procedurave në TI) rezultoi se INSTAT nuk ka Strategji të veçantë për Teknologjinë e Informacionit, mungesa e të cilës ka sjellë mos pasqyrimin e qartë të objektivave TI lidhur me infrastrukturën, burimet e nevojshme, si dhe instrumenteve të nevojshëm për realizimin e objektivave. Mungesa e Planit Strategjik të TI, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së INSTAT	Drejtoria e Teknologjisë së Informacionit dhe strukturat drejtuese të INSTAT-it të adresojnë qartë objektivat në fushën e Teknologjisë së Informacionit dhe duke marrë në konsideratë kohën, burimet e nevojshme të marrin masa për hartimin e miratimin e Planit Strategjik të Teknologjisë së Informacionit.
2.	Drejtoria e Teknologjisë së Informacionit në aktivitetin e saj për vitin 2016 ka vepruar me bazë rregullatore për Teknologjinë e Informacionit të pa miratuar nga strukturat drejtuese.	Strukturat drejtuese të INSTAT-i të marrë masa në të ardhmen që për standardet, politikat dhe rregulloret e reja dhe ndryshimet e tyre të aprovohen nga organet përkatëse përpara përdorimit. Drejtoria e Teknologjisë së Informacionit duhet të marri masa për menaxhimin e ndryshimit nëpërmjet komunikimit, trajnimit e testimit në të gjitha nivelet e organizatës në intervale sistematike kohore të ndryshimeve në rregulloret dhe procedurat korresponduese.
3	Grupi i auditimit konstaton dhe vlerëson kryerjen nga INSTAT-ti i një auditimi të brendshëm për TI gjatë vitit 2016, por shikon se plani i veprimit për zbatimin e të metave të konstatuara është formal si	Strukturat drejtuese të INSTAT, duke marrë në konsideratë kohën dhe burimet e nevojshme, të marrin masa për hartimin e politikave dhe planeve të menaxhimit të riskut, si dhe të përcaktojë

	rezultat i mungesës së vlerësimit real të impaktit që mbartin risqet e të metat e konstatuara. Përpjekjet për vlerësimin dhe menaxhimin e risqeve janë të pa mjaftueshme.	burimet e mjaftueshme për të menaxhuar risqet.
4	Nga auditimi i burimeve njerëzore në strukturën e TI u konstatua se ka një strukturë të plotë, me ndarje detyrash e përshkime pune, e cila ka zhvilluar dhe ka marre trajnime sipas një plani të miratuar gjatë vitit 2016, por krahas kësaj grupi i auditimit konstaton se INSTAT-i gjatë vitit 2016 ka pasur: a. Lëvizje të shpeshta të burimeve njerëzore në Drejtorinë e Teknologjisë së Informacionit. Mungesa në organikën e Drejtorisë së TI në pozicionet kritike gjatë vitit 2016	INSTAT të marrë masa për plotësimin e burimeve njerëzore në Drejtorinë e Teknologjisë së Informacionit duke plotësuar vendet vakante si dhe hartimit të politikave për menaxhimin e ndryshimeve të tyre për pozicionet kritike
5	Nga auditimi i procedurave të dhënies, ndryshimit apo heqjes së aksesit të përdoruesve të jashtëm dhe të brendshëm në infrastrukturën e TI të INSTAT-it, konstatohet se për vitin 2016 ka pasur një sasi të konsiderueshme shtimi heqje apo ndryshimi të përdoruesve në sistemet TI. Grupi i auditimit konstaton se kryerja pa formular i hapjes, mbylljes dhe ndryshimit të përdoruesve nuk siguron menaxhimin e sigurtë të procesit dhe krijon precedent që përdorues që kanë ndryshuar statusin të kenë të drejtë aksesi në sistemet e INSTATIT-t	Drejtoria e Teknologjisë së Informacionit INSTATIT të hartojnë, miratojnë e zbatojnë rregulla për hapjen dhe mbylljen e përdoruesve në sistemet e teknologjisë së informacionit, gjurmët e procesit procesit të dokumentohen
6	Nga auditimi u konstatua se INSTAT-ti në mospërputhje me VKM nr. 710, dt. 21.08.2013 “Për krijimin dhe	INSTAT, të marrë masa të për të: a. ndërtuar një strategji të rimëkëmbjes

	funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", si dhe praktikave më të mira të fushës nuk ka: a. strategji të rimëkëmbjes nga katastrofat; b. plane që përcaktojnë vazhdimësinë e proceseve, në rastet e dështimit të qendrës së të dhënave që suportojnë sistemet; c. listë të testeve të BACKUP të kryera për vitin 2016. d. listë të artikujve të vlerësuar prioritare për proceset emergjente	nga katastrofat; b. kryerjen e vlerësimin e aseteve të Teknologjisë së Informacionit dhe hartimin e listës të artikujve prioritare për proceset emergjente; c. të parashikojë dhe të realizojë investime me qëllim mundësimin e ofrimit të shërbimit pa ndërprerje dhe parandalimin e humbjes ose të shkatërrimit aksidental të të dhënave; d. të hartojë Planin e Vazhdueshmërisë së Biznesit; e. Të marri masa për krijim e ambienteve të testimit të BACKUP dhe kryeje testimet dhe dokumentimin e procesit.
7	**1.** Masat e ndërmarra për Sigurinë Fizike dhe Mjedisore të janë të pamjaftueshme, në kundërshtim me Rregulloren e AKSH-it mbi "Ndërtimin e Dhomës së Serverave", si dhe rregullores së dhomës së serverave, të miratuar nga vetë INSTAT-i. Më specifikisht: a. Mbajtja e temperaturës së ambientit në 17 gradë celcius nuk është në përputhje me Rregulloren e AKSH-it, pika 4.4/b, në të cilën ndër të tjera specifikohet "sistemi ftohës i dhomës ....duhet të vendosen në 22 gradë celcius"; b. Tipi i kondicionerëve të përdorur dhe vendosja e tyre nuk siguron mbajtjen e parametrave optimale dhe nuk favorizon	INSTAT për të rritur sigurinë fizike dhe logjike të dhomës se serverave në drejtim të uljes së riskut të aksesit të paautorizuar,vendosjes vetëm të pajisjeve të përcaktuara në këto ambiente, ngritjes se sistemeve të përshtatshme kondicionimi, ndarjes së sistemeve elektrike, vendosjes së sistemeve të mbrojtjes e sinjalizimit të marrë masa të dokumentuara për përmirësimin e kushteve në dhomat e serverave, duke analizuar dobësitë të hartohet një plan veprimi bazuar në specifikimet e rregullores së AKSHI-t "për ndërtimin e dhomës së serverave".

	qarkullimin natyral të ajrit; c. Konsiderojmë me risk mbajtjen e sistemit të kondicionimit të qendërzuar në dhomën e serverave pavarësish mos përdorimit; d. Nga verifikimi i mureve të dhomës së serverave u konstatua se nuk ishin të pajisur me skermo kundër emetimeve të valëve elektromagnetike (Kafazi Faraday), në kundërshtim kjo me pikën 4.1/c të Rregullores së AKSHI-t; e. Prania e dritares nuk plotëson kushtet e përcaktuara sipas Rregullores së AKSH-it mbi Ndërtimin e Dhomës së Serverave pika 4.1/e dhe cënon sigurinë fizike të dhomës; f. Ambienti nuk ishte i pajisur me sensorë për detektimin e lëvizjeve në kundërshtim me Rregullore e AKSH-it pika 4.6/b, në të cilën specifikohet "Hyrja në dhomë duhet të jetë e siguruar me anë të një sistemit elektronik dhe natyrisht duhet të ketë sistem alarmi në rast thyerje të saj"; g. Në dhomën e serverave u identifikuan objekte që nuk kishin lidhje me funksionin e saj, të tilla si: h. Panel i energjisë elektrike i godinës i cili cënon sigurinë e ambientit. i. Pajisje të vjetra jashtë funksionit të cilat ruheshin për efekt të mungesës së magazinimit. j. Ekzistenca e objekteve që nuk kanë lidhje të drejtpërdrejtë me funksionimin e dhomës së serverave, të hapësirë për	

	ngarkesë të panevojshme të ambientit dhe rrit riskun e cënimit të sigurisë fizike. k. Në këtë ambient, u konstatua një situatë kaotike e kabllimit, e cila vështirëson dhe rrit në mënyrë të panevojshme kohën e riparimit në rast defekti. l. Nuk ka kamera sigurie e cila do mundësonte indentitikimin e personave të cilët aksesojnë dhomën e serverëve; m. Hyrja në dhomën e servera nuk bëhet nëpërmjet akses kontrollit dhe regjistri i përdorur për regjistrimin e hyrjeve nuk plotëson rregullat si: vendosjen e numrit te faqes dhe vendosjen e vulës së institucionit në faqe (miratimin); Sistemet nuk janë të mbrojtura nga dëme që mund të shkaktohen nga zjarri	

MBI AUDITIMIN E TEKNOLOGJISË SË INFORMACIONIT TË USHTRUAR NË DREJTORINË E UJËSJELLËS KANALIZIMEVE, TIRANË.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "Drejtoria e Ujësjellës Kanalizimeve, Tiranë"

Përgatitur: 10 Shtator 2017

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 479/1, datë 05.06.2017.

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Meald Habazaj, anëtar
3. Elira Cukalla, anëtar

Periudha e Auditimit: 01.01.2016 – 31.12.2016
Afati i auditimit: 30.05.2017 - 21.07.2017

ÇFARË KEMI AUDITUAR

Ujësjellës Kanalizimeve Tiranë është një Shoqëri Aksionere e organizuar në bazë të vendimit të gjykatës së Rrethit Gjyqësor Tiranë nr. 24875, datë 28.12.2000, në përputhje me ligjin nr. 9901, datë 14.04.2008 ”Për tregtarët dhe Shoqëritë Tregtare”.

Aktivitet kryesor i UKT

-Shërbimin e furnizimit me ujë të pijshëm i konsumatorëve dhe shitja e tij
-Mirëmbajtjen e sistemeve të furnizimit me ujë të pijshëm
-Prodhimin dhe/ose blerja e ujit për plotësimin e kërkesave të konsumatorëve
-Shërbimi i grumbullimit, largimit dhe trajtimit të ujërave të ndotura dhe shitja e tij
-Mirëmbajtja e sistemeve të ujërave të ndotura si dhe të impianteve të pastrimit të tyre

UKT ka për objektiv rritjen e cilësisë së shërbimit, përmirësimi i infrastrukturës së rrjetit të shpërndarjes, furnizimin me ujë i qytetit të Tiranës 24 orë në ditë dhe sigurimi i cilësisë sipas standardit shtetëror 3604:

Menaxhimi i lartë

Organet drejtuese të UKT sipas shkallës hierarkike të drejtimit janë: Asambleja e Aksionerëve; Këshilli Mbikëqyrës dhe Drejtori i Përgjithshëm.

Fushat e auditimit

Auditimi i funksionimit të Qeverisjes TIK

a. Verifikimi i Strategjisë, politikave dhe procedurave në TIK
b. Vlerësimi i burimeve njerëzore në strukturën TIK

Auditimi i projekteve e investimeve në teknologjinë e informacionit

a. Identifikimi, hartimi i nevojave dhe kritereve të vendosura për mallra dhe shërbime në TIK
b. Procedurat e investimeve në fushën e TIK

Auditimi i Operacioneve në TIK

a. Vlerësimi i menaxhimit të shërbimit, kapacitetit të sistemeve
b. Menaxhimi dhe dokumentimi i problemeve, incidenteve dhe ndryshimeve.

Auditimi i Sigurisë së Informacionit

c. Identifikimi dhe menaxhimi i risqeve në TIK
d. Siguria e të dhënave dhe vazhdimësia e biznesit

Auditimi i sistemit të faturimit AL Billing

Të ndryshme të dala gjatë auditimit

PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Auditimi i Sistemeve të Teknologjisë së Informacionit në UKT rrjedh nga rëndësia që ka kjo SHA për sigurimin e Shërbimin e furnizimit me ujë të pijshëm të qytetit të Tiranës e konkretisht:

-Mirëmbajtjen e sistemeve të furnizimit me ujë të pijshëm
-Prodhimin dhe/ose blerja e ujit për plotësimin e kërkesave të konsumatorëve
-Shërbimi i grumbullimit, largimit dhe trajtimit të ujërave të ndotura dhe shitja e tij
-Mirëmbajtja e sistemeve të ujërave të ndotura si dhe të impianteve të pastrimit të tyre

Në përfundim të auditimit për 15 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit

Më hollësisht:

OPINIONI I AUDITIMIT:

Grupi i auditimit arrin në konkluzionin se mungesa e Strategjisë së Teknologjisë së Informacionit në Drejtorinë e Ujësjellës Kanalizime, Tiranë ka sjellë mos pasqyrimin qartë të objektivave te Sh.a lidhur me infrastrukturën TI dhe burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen e saj.

Mungesa e Planit Strategjik mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së UKT nga Teknologjia e Informacionit.

Teknologjia e Informacionit duhet të shtrihet në gjithë proceset e aktivitetit të Ujësjellës Kanalizime Tiranë

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	Nga auditimi i Strategjisë, politikave dhe procedurave në TIK) rezultoi se: • UKT nuk ka Strategji për Teknologjinë e Informacionit, mungesa e të cilës sjell mos pasqyrimin e qartë të objektiva lidhur me infrastrukturën, burimet e nevojshme si dhe indikatorëve për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së UKT • Struktura e TI në nivel sektori sjell uljen e ndikimit të TI në qeverisjen e UKT	Strukturat drejtuese të UKT, duke marrë në konsideratë kohën, burimet e nevojshme të marrin masa për: a. Hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e Shoqërisë. b. Ngritjen në nivel të strukturës së TI nga nivel sektori në nivel Drejtorie.

	sh.a dhe zbehjen e ndikimit të varësinë direkte nga Drejtori i Përgjithshëm. • Mungesa e këshilltarit të Drejtorit të Përgjithshëm me profili teknologji informacioni ka ndikuar në vendimmarrjen e qeverisjes TI. Struktura e Auditit të Brendshëm e cila siguron pavarësinë e punës nëpërmjet varësisë direkt nga Këshilli Mbikëqyrës nuk ka në përbërje të saj auditues me profil teknologji informacioni	
2.	Nga auditimi i bazës rregullatore të sektorit TI u konstatua se UKT nuk ka rregullore të veçantë për Teknologjinë e Informacionit.	UKT të marrë masa për hartimin e një Rregulloreje të Përgjithshme mbi Teknologjinë e Informacionit, në të cilën të përfshihen të gjitha operacionet TI, afatet dhe burimet e nevojshme. Hartimi i kësaj Rregulloreje të marrë në konsideratë vendosjen e kontrolleve të brendshme lidhur me menaxhimin e riskut, përputhshmërinë me procedurat dhe rregullat e brendshme aktuale të shoqërisë si dhe me legjislacionin e Teknologjisë së Informacionit dhe Komunikimit në Shqipëri.
3	Nga auditimi i Burimeve njerëzore në strukturën TI të UKT u konstatua se ka mangësi për pozicionin e Specialistit për Menaxhimin e Rrjetit/ Serverave në strukturën e Sektorit të Teknologjisë së Informacionit (STI). Pozicioni i Specialistit për Menaxhimin e Rrjetit/ Serverave është një pozicion i rëndësishëm dhe mungesa e tij mbart risk të lartë	Strukturat drejtuese të UKT në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Sektorin TIK të marrin masa për plotësimin e strukturës së Sektorit të Teknologjisë së informacionit.

4	Nga auditimi u konstatua se UKT dhe STI nuk ka një analizë të nevojave për trajnim të stafit të STI. Nuk ka plan për trajnime dhe për vitin 2016 stafi i STI nuk ka kryer asnjë ditë trajnim për sistemet, sigurinë dhe teknologjinë e informacionit.	Strukturat drejtuese të UKT në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Sektorin TIK të marrin masa për identifikimin e nevojave për trajnim të stafit TI dhe çdo përdoruesi të sistemeve TI për sistemet, sigurinë dhe teknologjinë e informacionit. Te hartoje e miratoje planet trajnimit si dhe zhvillojë ato
5	Nga auditimi se si UKT identifikon, harton nevojat dhe vendos kritere për marrjen e vendimeve për mallra dhe shërbime në TIK u konstatua një mos angazhim dhe mungesë të njohjes e analizës nga ana e sektorit TIK, mbi atë çfarë kërkohet në planifikimin e projekteve të teknologjisë së informacionit, për një optimizim sa më të mirë të investimeve në TIK.	Strukturat drejtuese të UKT në bashkëpunim me Sektorin TIK dhe të gjitha drejtoritë, bazuar në praktikat më të mira për zhvillimin e sistemeve të teknologjisë së informacionit apo përmirësimin e tyre, ti kushtojnë rëndësi identifikimit të nevojave dhe kërkesave, analizimit, prioritarizimit, aprovimit, si dhe zhvillimin e një analize kosto/përfitim, midis zgjidhjeve të mundshme për të arritur të zgjidhja më optimale për çdo investim në teknologjinë e informacionit, duke përfshirë pajisjet periferike (*si printer fotokopje*) dhe licencat.
6	Nga auditimi i procedurave të prokurimit zhvilluar për projektet e teknologjisë së informacionit për: 1. *Krijimi i një mjedisi të ri dhomë serverash për drejtorinë e Ujësjellës Kanalizime Tiranë sh.a,* 2. *Blerje pajisje monitorimi, licenca, software financiar dhe faturimi (SMI) sistem menaxhimi informacioni për UKT sh.a,*	Strukturat drejtuese të UKT në bashkëpunim me Drejtorinë e Auditit të Brendshëm si dhe me Drejtorinë e Shërbimeve Mbështetëse, të marrin masat e nevojshme për: a. Ngritjen e grupit të punës në hartimin e specifikimeve teknike dhe grupin e ndjekjes së kontratës, për procedurat TIK, në përputhje me VKM nr. 914, datë 29.12.2014, për "*Miratimin e rregullave të prokurimit*

	3. *Infrastrukturë TI Server, pajisje Data Center për UKT sh.a, U konstatuan të njëjtat mangësi, si më poshtë:* a. Në asnjë rast nuk rezulton i dokumentuar urdhër titullari, për ngritjen e grupit të punës, për hartimin e specifikimeve teknike, si dhe ngritjen e grupit për ndjekjen e kontratës dhe hartimin e raportit përmbledhës për realizimin e saj, në kundërshtim me VKM nr. 914, datë 29.12.2014 për "*Miratimin e rregullave të prokurimit publik*". b. Në të gjitha rastet e procedurave të audituara u konstatua një shmangie nga përgjegjësitë e përgjegjësit të sektorit TIK, pasi shprehet në mënyrë konstante për specifikimet teknike që ka hartuar dhe dokumentuar: "*Nga zyra TI është ngritur një komision për hartimin e specifikimeve teknike sipas njohurive të gjithsecilit duke menduar që nuk janë më të mirat jemi gjithmonë të hapur*". c. Përllogaritja e fondit limit ka ardhur si rezultat i studimit të tregut tek operatorët ekonomikë vetëm nëpërmjet tabelës për zërat e punimeve që përmban çdo projekt, por jo me të gjitha specifikimet e secilit prej tyre (Mosnjohja e operatorëve me të gjitha specifikimet teknike, tregon për fond limit të përllogaritur larg realitetit). d. Kriteret e vendosura nga NjP mbi kapacitetin teknik si pjesë e kritereve të veçanta të kualifikimit, nuk janë bërë në përputhje me volumin e punimeve apo rëndësinë e tyre. Mungesa e specialistit të fushës në NjP, kompromenton kriteret e vendosura në lidhje me kapacitetin teknik	*publik*". b. Marrjen e asistencës së nevojshme nga institucione apo specialistë të fushës së teknologjisë, në hartimin e specifikimeve teknike për projektet TIK, në mungesë të kapaciteteve të vet shoqërisë, në funksion të zgjidhjes më të mirë me kosto me të pranueshme. c. Studimi i tregut, për përllogaritjen e fondit limit të realizohet duke i njohur operatorët ekonomikë me të gjithë përmbajtjen e specifikimeve teknike, si domosdoshmëri në marrjen e një oferte sa më afër realitetit. d. Njësia e prokurimit, të ketë në përbërjen e saj specialistë të fushës për hartimin e kritereve të veçanta për investimet e reja dhe atyre që do të përmirësonin aktivitetin e UKT nëpërmjet teknologjisë. e. Dokumentimin e shërbimit përfundimtar si një të tërë, i përftuar nga çdo projekt i ri apo përmirësim i atij ekzistues, lidhur me teknologjinë e informacionit. Auditimin e procedurave të prokurimit TIK si dhe auditimin e proceseve të automatizuara, në përputhje me ligjin nr.10296, datë 8.7.2010 "*Për menaxhimin financiar dhe kontrollin*" dhe udhëzimin nr.30 datë 27.12.2011 "*Për menaxhimin e aktiveve në njësitë e sektorit publik*".

	në të gjitha procedurat, duke sjellë në këtë mënyrë një kufizim në pjesëmarrje. e. Përfundimi i implementimit të çdo projekti shoqërohet me kolaudime të pjesshme, por akt-kolaudimi i shërbimit të përfituar si një i tërë nuk rezulton të jetë kryer në asnjërën prej tyre. Asnjë procedurë prokurimi TIK zhvilluar në vitin 2016, nuk është audituar nga Drejtoria e Auditit të Brendshëm të UKT-së, për shkak të mungesës së kapaciteteve në burime njerëzore në këtë drejtori.	
7	7. Nga auditimi i procedurave zhvilluar në funksion të sistemit Al-Billing, rezulton se: a. Procedurat me objekt "*Shërbim mirëmbajtje dhe zhvillim të mëtejshëm të sistemit të faturimit "Al-Billing*" dhe "*Shërbimi dhe konfigurimi i kasave dhe sistemit të faturimit për UKT sha*", janë realizuar jashtë parashikimit, pasi nuk rezultojnë si zëra të planifikuar për vitin 2016. b. Marrja në dorëzim e shërbimeve të reja dhe mirëmbajtjes, në zbatim të kontratës së lidhur për "*Shërbim mirëmbajtje dhe zhvillim të mëtejshëm të sistemit të faturimit "Al- Billing"*, nuk dokumentohet asnjë detaj lidhur me shërbimin kërkuar i cili mund të jetë i ri apo përmirësuar/përshtatur, duke mos lënë asnjë gjurmë, nëse kompania e kontraktuar i ka përmbushur specifikimet teknike lidhur me kërkesat për mirëmbajtjen dhe mirë funksionimin e sistemit. Në kontratën e shërbimit nënshkruar midis	a. Të merren masat për projektet që do të gjejnë zbatim në të ardhmen për planifikimin e saktë të nevojave që institucioni ka mbi mirëmbajtjet, apo përmirësimet bazuar në kapacitetet njerëzore që disponon për të siguruar mbarëvajtjen e shërbimeve që UKT ofron nëpërmjet teknologjisë. b. Të merren masa në të ardhmen për dokumentimin me detaje të shërbimit të kërkuar, duke përfshirë afatin brenda të cilit shërbimi i kërkuar është realizuar, punonjësi që ka paraqitur kërkesën, përfshirjen e tij në testimet e zhvilluara për marrjen në dorëzim si dhe pajisjet apo softet të cilat janë prekur për realizimin e tij. c. Të merren masa për hartimin e marrëveshjeve nivel shërbimi (SLA) që UKT do të nënshkruajë në vijim, për të drejtat dhe detyrimet që i takojnë palëve në përputhje të plotë me DST dhe specifikimet teknike, duke parandaluar në këtë mënyrë çdo

	palëve, UKT dhe X”, *për mirëmbajtje dhe zhvillim të mëtejshëm të sistemit të faturimit Al- Billing*, nuk ka në asnjë nen i cili të përcaktojë detyrimin e realizimit të objektit të kontratës në përputhje me dokumentat standarde të tenderit pjesë integrale e saj. Kjo mangësi ka sjellë që në procedurën e zhvilluar 2 muaj më vonë, për “*Shërbimi dhe konfigurimi i kasave dhe sistemit të faturimit për UKT sha”,* ku fitues është i njëjti bashkim operatorësh, të ekzistojë zëri *“zhvillimin e sistemit të faturimit që pagesa të kalojë në mënyrë automatike në sistem dhe kasë për të gjitha arkat”*, pagesa e këtij zhvillimi është në një vlerë shumë më të madhe se sa mirëmbajtja vjetore e Al-Billing	hapësirë për kosto të paparashikuara. Nisur nga sa me lart njësia e Auditit të Brendshëm në UKT të planifikojë një mision auditimi mbi e kontratën e shërbimit nënshkruar midis palëve, UKT dhe y”, *për mirëmbajtje dhe zhvillim të mëtejshëm të sistemit të faturimit Al-Billing.*
8	Nga auditimi se si UKT menaxhon shërbimet, kapacitetin e sistemeve rezultoi se procedurat e raportimit nuk dokumentohen. Në këtë mënyrë, nuk ka një strukturë kontrolli të mirëfilltë për auditimin e teknologjisë së informacionit të UKT, duke rritur riskun e mos identifikimit të parregullsive që mund të ndodhin në sisteme. Përfshirja e auditimit të teknologjisë së informacionit në Drejtorinë e Auditimit të Brendshëm, do të siguronte nivel më të lartë të integritetit të të dhënave që sistemet përmbajnë, duke evidentuar dobësitë e deri tek parregullsitë që mund të ndikojnë në vendimmarrje	Strukturat Drejtuese në UKT në bashkëpunim me Sektori i Teknologjisë së Informacionit të marrin masa për raportimin e aktivitetit të tyre të përditshëm dhe për ruajtjen (dokumentimin) e këtyre procedurave. Strukturat Drejtuese në UKT në bashkëpunim me Drejtoria e Auditimit të Brendshëm të marrin masa për përfshirjen e Sektorit i Teknologjisë së Informacionit në procesin e auditimit.
9	Nga auditimi se si UKT **Menaxhon dhe dokumenton problemet, incidentet dhe ndryshimet** rezultoi se situata në UKT në mungesë të procedurave të shkruara, për periudhën nën auditim, menaxhohet mbi	Strukturat Drejtuese në UKT në bashkëpunim me Sektorin e Teknologjisë së informacionit të marrë masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin,

	bazë ngjarjesh, d.m.th jepet suport, mbështetje teknike dhe logjike për operacionet TI që ndihmojnë mbarëvajtjen e strukturave të institucionit, procedurat kryhen nëpërmjet shkëmbimeve verbale dhe nëpërmjet email- eve. Në këtë mënyrë, institucioni nuk ka politika të ruajtjes së dokumenteve dhe ***nuk ka të dokumentuar një plan masash për trajtimin e gabimeve dhe incidenteve*** që mund të ndodhin në infrastrukturën TI	dokumentimin dhe monitorimin e incidenteve. Gjithashtu të marren masa për menaxhimin e ndryshimeve dhe dokumentimin e të gjithë procesit të ndryshimeve.
10	Nga auditimi u konstatua se faqia e Web të UKT ka këto mangësi: -Në kuadrin e transparencës UKT duhet të afishojë në faqen e saj web Organigramën e institucionit, ku të përfshihen, strukturat e të gjithë UKT, me adresat e sakta, numrat e kontaktit dhe orarin e ofrimit të shërbimeve ndaj publikut; -Kategoria vende pune nuk gjendet në faqen web të UKT, duke mos krijuar asnjë mundësi intervistimi për njerëz të cilët kanë interes dhe duan të kontribuojnë në UKT; Tek menuja "Kontakte" nuk ka të afishuar për publikun oraret e pritjes së publikut në degët e UKT-së.	Strukturat drejtuese në UKT në bashkëpunim me Sektorin e Teknologjisë së Informacionit, të marrin masa për përmirësimin dhe përditësimin e faqes web për të rritur ndihmesën ndaj qytetarëve në lidhje me problematikat e përditshme.
11	Nga auditimi se si UKT Identifikon dhe menaxhon risqet në teknologjinë e informacionit, u konstatua se UKT nuk disponon një regjistër risku për teknologjinë e informacionit në mospërputhje me ligjin nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar, Udhëzimi nr. 30, datë 27.12.2011 "*Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik*". Nga strukturat drejtuese të shoqërisë nuk është	Strukturat drejtuese të UKT në bashkëpunim me Drejtorinë e Auditit të Brendshëm, të marrin masat e nevojshme për hartimin dhe dokumentimin e një plan-veprimi, në përputhje me ligjin nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar, Udhëzimin nr. 30, datë 27.12.2011 "*Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik*", për

	iniciuar asnjë proces për identifikimi i risqeve të lidhura me aktivitetet/funksionet e UKT të ofruara nëpërmjet aplikacioneve si dhe menaxhimi i tyre. UKT nuk disponon asnjë mekanizëm për vlerësimin e proceseve të kompjuterizuara dhe sigurisë së të dhënave në funksion të ofrimit të shërbimeve dhe vazhdimësisë së aktivitetit, lidhur me gjenerimin, sistemimin e faturës, arkëtimin e saj si dhe shërbimeve online, si elementë shumë të rëndësishëm të analizës së riskut	shmangien, adresimin, transferimin apo pranimin e risqeve të identifikuara, si dhe monitorimin periodik për zbatimin e masave të marra nga sektori përgjegjës.
12	Nga auditimi i Planeve për Vazhdueshmërinë e Biznesit dhe Rimëkëmbjes nga Katastrofat në UKT rezultoi se: a) UKT nuk ka të ndërtuar një strategji të rimëkëmbjes nga katastrofat si dhe nuk ka plane që përcaktojnë vazhdimësinë e proceseve në rastet e dështimit. UKT nuk disponon dokumentacione në lidhje me Planet e vazhdueshmërisë së punës (BCP) dhe rimëkëmbjes nga katastrofat (DRC), Procedurat e testimit dhe rezultatet e tyre sidhe veprimet e rekomandimet e ndërmarra. UKT nuk ka listë të artikujve të vlerësuar prioritare për proceset emergjente b) Mbajtja e Rrjetit network i UKT ndodhet në dhomën e vjetër të serverave janë jashtë çdo standardi përbën risk për funksionimin sistemit TI të UKT. Institucioni nuk ka politika në lidhje me aksesin në rast emergjence në qendrën e të dhënave.	Të merren masa për ndërtimin dhe hartimin e Planeve të Vazhdimësisë së Biznesit Rimëkëmbjen nga Katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat. Gjithashtu, të merren masa për hartimin e planit të sigurisë së informacionit dhe implementimi e tij duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TI. Planifikimi dhe testimi i sistemeve TI të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen.

13	Nga Auditimi i bazës të dhënave të **sistemit të faturimit AL Billing** për vitin 2016 rezulton se: a) UKT nëpërmjet aplikacionit Billing ka gjeneruar 2 670 281 fatura (transaksione) me numrave seriale të pa certifikuar nga Autoriteti Tatimor, në kundërshtim me ligjet tatimore. Në këto fatura është aplikuar edhe mbajtja e taksave të tjera të cilat UKT mbledh. b) UKT nuk ka bërë kërkesën pranë Drejtorisë se Tatimpaguesve te Mëdhenj për miratimin dhe tërheqjen e diapazonit të numrave seriale. Drejtorisë se Tatimpaguesve të Mëdhenj e cila është venë në dijeni për miratimin e kësaj fature kompjuterike tatimore me shkresën nr 6613/1 date 07.03.2016 nuk rezulton të ketë kryer asnjë kontroll për të detyruar UKT të zbatojë ligjet tatimore	UKT të marri masa të menjëhershme për bërjen e kërkesës pranë Drejtorisë së Tatimpaguesve të Mëdhenj për miratimin e diapazonit të numrave seriale, gjenerimit të faturave tatimore kompjuterike të shitjes nga UKT vetëm me numrat e miratuar nga organet tatimore.
14	Auditimi i Sigurisë së të dhënave të *programit të faturimit Billing u* konstatua se: a) UKT nuk ka rregulla të shkruara për procedurat e mbylljes së përdoruesve të sistemit. Nuk kryhet njoftimi nga departamentet përkatëse si dhe nga burimet njerëzore i sektorit TI për mbylljen e përdoruesve që kanë ndërprerë marrëdhëniet e punës,". b) Lënia aktivë e përdoruesve të sistemit pasi kanë ndërprerë marrëdhëniet e punës (faturistë, arkëtare TI e specialiste të departamentit të shitjes etj) përbën shkelje të sigurisë në Aplikacionit të	UKT dhe STI të hartojnë, miratojë e zbatojë rregulla për hapjen dhe mbylljen e përdoruesve në sistemet e teknologjisë së informacionit sidhe për vendosjes dhe nderimin e fjalëkalimeve të përdoruesve. Të mos përfshijnë sektorin e TI në procese operacionale (sistemime te dhënash). Sektori i TI në UKT të kryejë analizimin e logeve të sistemit për identifikimin e incidenteve dhe ndërhyrjeve në sistemet e teknologjisë së informacionit.

	faturimit duke e bërë atë të pa sigurte ndaj ndërhyrjeve. c) Siguria e sistemeve të informacionit në UKT është në risk në saj të mungesës së rregullave të shkruara për ndërrimin e fjalëkalimeve. d) Përfshirja e Sektori i TI në procese operacionale (sistemime te dhënash) në sistem krahas detyrave për mirëmbajtjen e zhvillimin e sistemit përbën konflikt në ndarjen e përgjegjësive dhe përbën risk për UKT. Mos ruajtja dhe analizimi nga ana e sektorit te TI në UKT i logeve të sistemit për vitin 2016 (për mungesë hapësirash) mbartin riskun që ndërhyrjet në sistemet e teknologjisë së informacionit të mos identifikohen	
15	**8.** Nga auditimi se si menaxhimi i Lartë në UKT drejton, vlerëson, përdor dhe monitoron efektivisht përdorimin e teknologjinë e Informacionit, me qëllim përmbushjen e misionit të shoqërisë konstatohet se: a. Investimet TI të kryera nga UKT kanë lënë jashtë vëmendjes investimet në TI për automatizimin e impianteve të prodhimit, trajtimit dhe pompimit të ujit. Nuk ka kërkesa nga Departamenti i prodhim shpërndarjes e Departamenti Inxhinerik për futjen e automatizimeve dhe përdorimin e teknologjisë së informacionit. b. Serveri i aplikacionit për komandimin e monitorimin e procesit të përpunimit të ujit në impiantin e Bovillës ishte jashtë	a. UKT për të përmbushur misionit e shoqërisë të hartojë një plan strategjik duke shfrytëzuar burimet e brendshme si dhe eksperiencat e burime të jashtme, me qëllim automatizimin dhe përdorimin e teknologjisë së informacionit në gjithë proceset e UKT. Krijimi i një qendre dispeçeri moderne dhe informatizimi i të dhënave të saj duhet të shikohet si një mjet për rritjen e 3E-ve të Shoqërisë. b. Këshilli Mbikëqyrës i UKT të analizojë rekomandimet e lëna në Raportin Përfundimtar të Auditimit të Teknologjisë së Informacionit dhe të marri masat përkatëse për përmirësimin e gjendjes.

	funksionit dhe zëvendësuar me 2 pc. Aplikacioni i kontrollit të impiantit ruhej pa backup. Sistemi mund të komandohej manualisht vetëm 4 ore në rast avarie të aplikacionit të mësipërm. Ambienti ku ndodhej pc ishte pa ventilim efikas dhe pa sisteme alternative energjie, ruajtja e impiantit kryhet nga rroje private pa sisteme sinjalizimi dhe kamera sigurie. c. Komunikimi i impiant depo stacione pompimi kryhet me celular. d. Nuk ka automatizim për matjen e niveleve të ujit në depo. e. Mos përdorimi i sistemeve inteligjente në depo sjell zbatimin e grafikun e miratuar për furnizimin e Tiranës me ujë 3 herë në ditë pavarësisht nga kërkesat e gjendja në sistem. f. Depot ndodhen të rrethuara nga zona urbane, ruhen nga rroje private për vetëm 2 turne pa sisteme sinjalizimi dhe kamera sigurie. g. Nuk përdoren Automatizim e sisteme inteligjente për trajtim, komandim, sinjalizim, matjen e parametrave kryesorë të transmetimit, akumulimit dhe shpërndarjes së ujit, siç janë matja e presioneve, matja e prurjeve dhe niveleve të ujit në sistem. Dispeçeria e UKT në shërbimin e saj 24 orësh nuk përdor sisteme të teknologjisë së informacionit si për marrjen e informacioneve nga burimet e prodhimit, linjat e transmetimit, depot dhe rrjetin shpërndarës, regjistrimin e informacioneve dhe veprimeve të kryera. Dokumentimi i	

	veprimtarisë së dispeçerisë manualisht nuk jep mundësinë e përdorimit të informacionit për analiza.	

MBI AUDITIMIN E TEKNOLOGJISË SË INFORMACIONIT TË USHTRUAR NË INSTITUTIN E SIGURIMEVE SHOQËRORE.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "**Institutin e Sigurimeve Shoqërore"**

Përgatitur: 12 Qershor 2017

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 1222/1, datë 26.01.2017.

Auditimi është kryer nga:

1. Kozma Kondakciu, përgjegjës grupi.

2. Benard Haka, anëtar.

3. Elira Cukalla, anëtar

3. Endri Meksi, anëtar (Ekspert i jashtëm).

Periudha e Auditimit: 01.01.2016 – 31.12.2016

Afati i auditimit: 23.01.2017 - 28.04.2017

Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve.

ÇFARË KEMI AUDITUAR

Instituti i Sigurimeve Shoqërore (ISSH), është institucion publik i pavarur, organizimi dhe funksionimi i të cilit rregullohet me ligjin nr. 7703, datë 11.05.1993 "Për sigurimet shoqërore në Republikën e Shqipërisë", i ndryshuar. Instituti i Sigurimeve Shoqërore drejtohet nga:

- Këshilli Administrativ;
- Drejtori i Përgjithshëm.

Misioni i Institutit të Sigurimeve Shoqërore (ISSH) është administrimi i sigurimeve shoqërore në përgjithësi dhe i politikave të pensioneve në veçanti, vendosja e personave të siguruar dhe përmirësimi i shërbimit ndaj tyre në qendër të veprimtarisë së këtij institucioni, mbulimi i popullsisë me elemente të sigurimeve shoqërore në çdo vend dhe

kohë kur lind kjo e drejtë, rritja e numrit të kontribuesve dhe grumbullimi i të ardhurave nga kontributet e fermerëve dhe të siguruarit vullnetar, përmirësimi i efiçiencës në menaxhimin e fondeve të sigurimeve shoqërore, i fondeve përkohësisht të lira dhe fondit rezervë.

Misioni i sistemit të sigurimeve shoqërore është mbulimi i të gjithë popullsisë me elementë të sigurimeve shoqërore dhe akordimi i përfitimeve për pension, paaftësi të përkohshme në punë, barrëlindje, aksidente në punë dhe sëmundje profesionale e përfitime suplementare në momentin e lindjes të së drejtës dhe nevojës për to.

Vizioni i sistemit të sigurimeve shoqërore është fokusuar në përmirësimin e skemave aktuale nëpërmjet reformimit të shtyllës publike të pensioneve e forcimit të një lidhjeje më të drejtpërdrejtë midis kontributeve të paguara dhe përfitimeve të ardhshme, futjes graduale të skemave të përfitimeve suplementare të menaxhuara nga subjekte jopublike, krijimit të llogarive personale të çdo kontribuesi dhe përfituesi, arritjen e transparencës maksimale, duke krijuar akses personal tek klientët.

Menaxhimi i lartë

Këshilli Administrativ i Institutit të Sigurimeve Shoqërore është organi më i lartë ekzekutiv.

Ai përbëhet nga 12 anëtarë dhe mbështetur në VKM nr. 263, datë 07.05.2014 "Për caktimin e funksioneve të përfaqësuesve të institucioneve shtetërore në përbërje të Këshillit Administrativ të Institutit të Sigurimeve Shoqërore", janë përcaktuar përfaqësuesit, si më poshtë:

- Ministria e Mirëqenies Sociale dhe Rinisë – Ministër;
- Ministria e Financave - Zv/Ministër;
- Ministria e Zhvillimit Ekonomik, Turizmit, Tregtisë dhe Sipërmarrjes – Drejtor Drejtorie;
- Ministria e Shëndetësisë - Drejtor i Përgjithshëm i Fondit të Sigurimit të Detyrueshëm të Kujdesit Shëndetësor;
- Ministria e Drejtësisë – Drejtor Drejtorie;
- Instituti i Statistikave – Drejtor i Përgjithshëm;

Me VKM nr. 262, datë 07.05.2014 "Për përzgjedhjen e organizatave të punëdhënësve dhe të sindikatave më të përfaqësuara në Këshillin Administrativ të Institutit të Sigurimeve Shoqërore", janë përcaktuar 6 përfaqësues nga këto organizata.

Fushat e auditimit

Auditimi i funksionimit të Qeverisjes TIK

Verifikimi i Strategjisë, politikave dhe procedurave në TIK

Vlerësimi i burimeve njerëzore në strukturën TIK

Auditimi i projekteve e investimeve në teknologjinë e informacionit

Identifikimi, hartimi i nevojave dhe kritereve të vendosura për mallra dhe shërbime në TIK
Procedurat e investimeve në fushën e TIK

Auditimi i Operacioneve në TIK

Vlerësimi i menaxhimit të shërbimit, kapacitetit të sistemeve
Menaxhimi dhe dokumentimi i problemeve, incidenteve dhe ndryshimeve.

Auditimi i Sigurisë së Informacionit

Identifikimi dhe menaxhimi i risqeve në TIK
Siguria e të dhënave dhe vazhdimësia e biznesit
Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet

Auditimi i sistemeve DMAIS, PCAMS, CMIS

Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output
Kontrolli i shkallës së sigurisë të aplikacioneve, përdoruesve të jashtëm dhe të brendshëm

Të ndryshme të dala gjatë auditimit

IV. PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Auditimi i Sistemeve të Teknologjisë së Informacionit në ISSH është i rëndësishëm pasi ISSH është Institucioni që administron sigurimet shoqërore në përgjithësi dhe harton i politikat e pensioneve në veçanti.
Në përfundim të auditimit për 21 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit

Më hollësisht:

<u>OPINIONI I AUDITIMIT:</u>

Grupi i Auditimit konstaton se Instituti i Sigurimeve Shoqërore po zhvillon Teknologjinë e Informacionit duke shfrytëzuar burimet e vëna në dispozicion duke dhënë një kontribut në administrimin e sigurimeve shoqërore në përgjithësi dhe në zbatimin e politikave të pensioneve në veçanti.

Në saj të përdorimit të TI është përmirësuar mbulimi i popullsisë me elemente të sigurimeve shoqërore, është rritur numri i kontribuesve dhe grumbullimi i të ardhurave nga kontributet, TI ka ndikuar në përmirësimin e efiçiencës dhe transparencës në menaxhimin e fondeve të sigurimeve shoqërore.

Zbatimi i rekomandimeve të këtij raporti si dhe mbështetja e zhvillimit të TI në ISSH nga strukturat qeveritare do të rris stabilitetin dhe sigurinë e skemës së pensioneve.

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	Nga auditimi u konstatua se ISSH nuk ka Strategji të veçantë për Teknologjinë e Informacionit, duke mos pasqyruar qartë objektivat lidhur me infrastrukturën, burimet e nevojshme si dhe instrumentave te nevojshëm për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së ISSH. DBI funksionon me një rregullore për teknologjinë e Informacionit të pa updatuar e pa miratuar.	Strukturat drejtuese të ISSH, duke marrë në konsideratë kohën, burimet e nevojshme të marrin masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit. DBI të kryejë updatimin dhe miratimin e rregullores së teknologjisë së Informacionit
2.	Nga auditimi i burimeve njerëzore në strukturën e TIK u konstatua se ato janë të qëndrueshme dhe të plota sipas strukturës organike të Drejtorisë Burimeve të Informacionit por krahas kësaj grupi i auditimit konstaton se ISSH: **a.** Ka mungesa në personel të kualifikuar në pozicionet kritike të DBI. **b.** Nuk zhvillon analizimin e nevojave për trajnim të stafit të DBI. **c.** Nuk ka plan për trajnime për vitin 2016, stafi i DBI nuk ka kryer asnjë ditë trajnim për sistemet, sigurinë dhe teknologjinë e informacionit.	ISSH të marrë masa për menaxhimin e burimeve njerëzore të DBI duke plotësuar nevojat për trajnime të stafit të DBI dhe të hartojë plane dhe politika për zhvillimin e trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit.
3	Nga auditimi i *Menaxhimit të Incidenteve dhe Problemeve* në ISSH dhe DBI u konstatua se nuk janë hartuar rregulla mbi menaxhimin e incidenteve	Strukturat Drejtuese në ISSH në bashkëpunim me Drejtorinë e Burimeve të Informacionit të marrë masa për hartimin e një plani veprimi për

	dhe institucioni nuk ka të dokumentuar një plan masash për trajtimin e gabimeve dhe incidenteve që mund të ndodhin në infrastrukturën TI. Mungesa e këtij plani masash bën që institucioni të mos ketë të identifikuar risqet me efekt negativ në TI dhe në proceset e punës, të mos ketë të përcaktuara veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura në drejtorinë qendrore dhe ato rajonale mbi bazë ngjarjeje. Si hallkë monitoruese, nuk ekzistojnë procedura dhe indikatorë të matjes së performancës për gabimet/ incidentet e ndodhura dhe masat reaguese ndaj tyre për të verifikuar efektivitetin e punës së kryer. *Menaxhimi i ndryshimit.* Nga auditimi u konstatua se nuk ekzistojnë procedura për inicjimin, rishikimin dhe aprovimin e ndryshimeve, prioritarizimin e tyre, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve (update, upgrade, etj.), struktura kontrolli për verifikimin e efektivitetit të ndryshimeve të kryera, procedura për ndryshimet emergjente si dhe dokumentimin e të gjithë procesit të ndryshimeve.	identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve. Gjithashtu të marren masa për menaxhimin e ndryshimeve dhe dokumentimin e të gjithë procesit të ndryshimeve.
4	Në faqen Web nuk është e afishuar procedura paraprake që personat në prag pensioni duhet të ndjekin për plotësimin e dokumentacionit për përfitimin e pensionit të pleqërisë, ky informacion do të lehtësonte procedurat e ndjekura nga qytetarët dhe administrata e ISSH. Nuk ka të afishuar procedurat se si një qytetar mund ta transferojë pensionin nga një qytet në tjetrin , ku duhet ta bëjë	Strukturat drejtuese në ISSH në bashkëpunim me strukturat përgjegjëse për mbarëvajtjen e faqes web, të marrin masa për përmirësimin dhe përditësimin e faqes web (informacione, ligje, rregullore, akte, etj) për të rritur ndihmesën ndaj qytetarëve në lidhje me problematikat e përditshme, duke reflektuar mangësitë e dala nga auditimi dhe duke shtuar elementë inovativ në faqen web për ta bërë atë sa më

	kërkesën , cilat janë procedurat që duhet të ndiqen. Në kuadrin e transparencës ISSH duhet të afishojë në faqen e saj web Organigramën e institucionit, ku të përfshihen, strukturat e të gjithë Drejtorive Rajonale të ISSH, me adresat e sakta, numrat e kontaktit dhe orarin e ofrimit të shërbimeve ndaj publikut. Nuk janë të afishuara procedurat dhe shkallët administrative, që duhet të ndjekë një qytetar në rastet kur ka kontestime dhe mos dakordësi me përllogaritjen e pensioneve. Tabelat e moshës së daljes në pension pleqërie dhe tabela e pagave referuese të para vitit 1994 të afishuara në faqen web janë të paqarta për publikun. Nuk ka rregullore për faqen e webit si dhe mungon shërbimi i intranetit. Kategoria vende pune nuk gjendet në faqen web të ISSH, duke mos krijuar asnjë mundësi intervistimi për njerëz të cilët kanë interes dhe duan të kontribuojnë në ISSH; Lista e kompensimeve nuk është e plotë në faqe, aty gjenden vetëm 2 lloje kompensimesh; Tek menuja “Kontakte” nuk ka të afishuar për publikun oraret e pritjes së publikut në Drejtoritë Rajonale të Sigurimeve Shoqërore. Kontaktet për marrjen e informacionit të afishuar në faqen ëeb nuk janë funksional; Mungon shërbimi i intranetit.	interaktive dhe ndihmëse për qytetarët. Të publikohen në faqen web informacion mbi procedurat paraprake që personat në prag pensioni duhet të ndjekin për plotësimin e dokumentacionit për përfitimin e pensionit të pleqërisë.

	Gjithashtu nga auditimi në praktikë i faqes web të ISSH u konstatua se: - Nuk është realizuar updatimi i faqes web në versionin anglisht edhe pse nga ISSH- ja për këtë specifikë është investuar; - Nuk ka raporte të dokumentuara për monitorimin dhe rregullimin e problemeve; - Faqja nuk ka përshtatshmëri me të gjithë llojet e browserave (shfletuesave), - Nuk ka dokumentacion të administruar nëse janë bëre modifikime të përmbajtjes të faqes web.	
5	Nga auditimi u konstatua se për vitin 2016 nuk është kryer përditësimi (*update*) i regjistrit të riskut për Drejtorinë e Burimeve të Informacionit në mospërputhje me: nenet 19-21 të ligjit nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar, Udhëzimi nr. 30, datë 27.12.2011 "*Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik*", Udhëzimin nr. 21, datë 25.10.2016 "*Për nëpunësit zbatues të të gjitha niveleve*", UMF nr. 16, datë 20.07.2016 "*Për përgjegjësitë dhe detyrat e koordinatorit të menaxhimit financiar dhe kontrollit dhe koordinatorit të riskut në njësitë publike*", si dhe Rregulloren TI të ISSH-së pika 4.4 "*Analiza e riskut dhe ndryshimit të dokumenteve*". Gjithashtu u konstatua: **d.** Nuk ka kryer vlerësime të risqeve dhe	Strukturat drejtuese në ISSH në bashkëpunim me Drejtorinë e Burimeve të Informacionit të bëjnë përditësimin dhe dokumentimin e regjistrit të risqeve TI dhe të marrin masa për hartimin dhe dokumentimin e një plani veprimi për minimizimin/ parandalimin e risqeve të identifikuara, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave nga DBI.

	nuk ka identifikuar dhe prioritarizuar të dhënat kritike, programet aplikativë, operacionet dhe burimet si edhe ndikimi i këtyre vlerësimeve në institucion, dhe nuk ka plan për menaxhimin e riskut nga DBI. **e.** Nuk ka një mekanizëm efektiv dhe të mirë dokumentuar të vlerësimit të riskut të sigurisë së informacionit. Për sa i përket vlerësimit të riskut dhe sigurisë së informacionit DBI, duke mos mbuluar të gjitha risqet e brendshme dhe të jashtme, duke përfshirë dhe politikat e sigurisë së informacionit.	
6	Nga auditimi u konstatua se ISSH-ja nuk ka të ndërtuar një strategji të rimëkëmbjes nga katastrofat si dhe nuk ka plane që përcaktojnë vazhdimësinë e proceseve në rastet e dështimit të qendrës së të dhënave primare që suportojnë sistemet PCAMS, CMIS dhe DMAIS. Instituti i Sigurimeve Shoqërore nuk ka qendër të rimëkëmbjes nga katastrofat (DRC) për data centerin primar ku hostohen serverat e sistemeve PCAMS, CMIS dhe DMAIS dhe infrastrukturën e rrjetit. Backup-et e sistemeve PCAMS, CMIS dhe DMAIS janë të ruajtura në Tape library, të cilat pasi mbushen ruhen në të njëjtën godinë me sistemet PCAMS, CMIS dhe DMAIS në mospërputhje me VKM nr. 710, dt. 21.08.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit*",	Strukturat drejtuese në ISSH në bashkëpunim me Drejtorinë e Burimeve të Informacionit të marrin masa për ndërtimin dhe hartimin e Planeve të Vazhdimësisë së Biznesit duke përfshirë planet për backup dhe rimëkëmbjen nga katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat. Gjithashtu, të merren masa për hartimin e planit të sigurisë së informacionit dhe implementimin e tij duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TI. Planifikimi dhe testimi i sistemeve TI të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen

	mbartur riskun e humbjes së informacionit në raste avarish apo katastrofash. ISSH nuk disponon dokumentacione në lidhje me: a. Planet e vazhdueshmërisë së punës (BCP) dhe rimëkëmbjes nga katastrofat (DRC); b. Procedurat e testimit; c. Nuk ka listë të testeve të kryera për vitin 2016 dhe rezultatet me veprimet e ndërmarra ose rekomandimet për to; d. Planet e sigurisë; Listë të artikujve të vlerësuar prioritare për proceset emergjente.	
7	Nga auditimi u konstatua se Rregullorja e Teknologjisë së Informacionit "*Mbi parimet dhe rregullat e përgjithshme të sigurisë së informacionit*" (version i vitit 2016) është e pa miratuar, Drejtoria e Burimeve të Informacionit ka mbështetur aktivitetin e saj në këtë rregullore, e cila nuk përmban elementë për të siguruar funksionim të përshtatshëm të strukturave TI në institucion.	ISSH në bashkëpunim me Drejtorinë e Burimeve të Informacionit dhe me strukturat këshilluese mbi TI, të hartojë një *Rregullore të Përgjithshme mbi Teknologjinë e Informacionit për Drejtorinë Qendrore dhe ato Rajonale*, rregullore e cila të përfshijë identifikimin, vlerësimin, analizën dhe menaxhimin e riskut të TI në institucion duke hartuar plane veprimi për incidentet e mundshme si dhe për menaxhimin e ndryshimeve. Krahas Rregullores së Përgjithshme të TI, ISSH duhet ti kushtojë një rëndësi të veçantë planifikimit strategjik të teknologjisë së informacionit, duke patur në konsideratë rëndësinë e të dhënave që institucioni posedon dhe përpunon. Po ashtu, të përcaktohet në strukturën organizacionale, një funksion i veçantë

		për verifikimin dhe garantimin e sigurisë së teknologjisë së informacionit në institucion.
8	Kopjet (backup) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Për testimin e këtyre kopjeve janë marrë si efektive rastet kur nga ISSH- ja është kërkuar informacion nga Prokuroria për çështje sensitive nën hetim nga ky Institucion (*Prokuroria e Rrethit Gjyqësor Durrës*). Në këto raste nga ISSH-ja është dashur të provojë backupet e saj për periudhat e kërkuara (*kthim i backup- it të muajit prill 2015*). Këto backup-e janë testuar dhe kanë rezultuar efektive. - Procedurat e rikrijimit (restore) të të dhënave nuk testohen për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar. Këto procedura duhet të testohen rregullisht, sistematikisht dhe vazhdimisht.	Drejtoria e Burimeve të Informacionit të marri masa për kryerjen dhe testimin periodik të backup-it për sistemet, pajisjet kompjuterike dhe të dhënat. Të kryejë klasifikimin e të dhënave të rëndësishme që ndodhen jashtë sistemit, kalimin e tyre në server, si dhe mbulimin e tyre me backup.
9	Nga auditimi u konstatua se kërkesat për zhvillimin e procedurave të prokurimit të zhvilluara në vitin 2016, kanë ardhur si domosdoshmëri për minimizimin e problematikave të mundshme në sistemin DMAIS, sigurimin e vazhdueshmërisë së shërbimeve PCAMS, FMS siguruar nëpërmjet storage-t të ri dhe migrimit të tij.. Nga auditimi u konstatua një mungesë angazhimi dhe bashkpunimi nga të githë punonjësit përdorues të sistemeve në lidhje me përmirësimin apo zhvillimin e	ISSH të përfshijë në përshkrimet e punës për specialistët TI të drejtorive rajonale, raportimin i problematikave të konstatuara nga përdoruesit e sistemit. DBI të ndërtojë modele mbi grumbullimin, analizimin dhe raportimin e problematikave. si dhe të kryejë ndjekjen e zgjidhjes së tyre.

	mëtejshëm të tij. Në asnjë rast nuk është raportuar në Drejtorinë e Burimeve të Informacionit, ndonjë problem i konstatuar me sistemin.	
10	Nga auditimi u konstatua se mungojnë raporte kontrolli mbi të dhënat të cilat konsiderohen të detyrueshme, raporte statistikore të përhershme apo të përkohshme në shërbim të përdoruesve dhe struturave të ISSH për analiza dhe kontrolle të ndryshme sipas përgjegjësive të dhëna me rregullore.	ISSH të kryejë hartimin dhe miratimin e raporteve në të tre aplikacionet CMIS, DMAIS dhe PCAMS, në funksion të analizave dhe detyrave që realizojnë sektorë dhe drejtori e degë rajonale në ISSH.
11	Nga auditimi u konstatua se importimi i bazës së të dhënave të DPT në ISSH i informacionit mbi derdhjen e kontributeve të 896,191 punonjësve nga punëmarrësit për vitet 2013-2016, NID-i për 31,938 punëmarrës nuk është në formatin e duhur për identifikin e shtetësisë, pasi kjo e dhënë nuk ka qenë pjesë e protokollit të komunikimit dhe as marrëveshjes ISSH-DPT. Mos identifikimi i shtetësisë nga ISSH sjell vështirësi në lidhjen e marrëveshjeve të bashkëpunimit me institucione homologe, për njohjen respektive të periudhave të kontributive	ISSH të hartojë kërkesat e specifikuara për informacionin që futet në bazën e të dhënave si rezultat i shkëmbimeve me bazën e të dhënave të DPT, në marrëveshjen e re mbi protokollin e komunikimit ndërmjet ISSH dhe DPT të përfshijë fushën e shtetësisë si element i rëndësishëm në lidhjen e marrëveshjeve të bashkëpunimit me institucione homologe, për njohjen respektive të periudhave të kontributive.
12	Nga auditimi u konstatua se të dhënat (NID, emër, mbiemër) e punonjësve të importuar nga DPT, me ato të regjistrit të gjendjes civile u identifikuan disa problematika lidhur me informacionin e importuar nga DPT: - Janë identifikuar 669 punonjës të cilët nuk gjenden në regjistrin e DPGJC. Këta punonjës nuk gjenden as në	Nga ana e ISSH të ndiqen të gjithë hapat e nevojshëm, për saktësimin dhe ndjekjen deri në zgjidhje të pasaktësive mbi të dhënat e importuara në vite. Njoftimin e punëmarrësve nëpërmjet kanaleve të komunikimit sipas problematikave që ata kanë.

	regjistrin e personave që kanë ndërruar jetë. *Bashkëlidhur Aneksi 2* - Janë identifikuar 26,314 raste kur **emri ose mbiemri** i punonjësit të deklaruar nuk është i njëjtë me atë të DPGJC për të njëjtin NID. - Janë identifikuar **80 raste kur të dhënat për emrin dhe mbiemrin janë të ndryshëm**, çfarë do të thotë se këta persona janë të ndryshëm. *Bashkëlidhur Aneksi 3* - Nga kontrolli i të dhënave për NID-et e "sakta në format" me regjistrin e personave që kanë ndërruar jetë të DPGJC, rezulton se DPT i dërgon ISSH informacion për 4,028 persona të cilët kanë ndërruar jetë prej kohësh. *Bashkëlidhur Aneksi 4* - Të dhënat mujore dhe progresive për kontributet e papaguara në afat, në mënyrë të përmbledhur dhe për çdo tatimpagues, nuk dërgohen në sistemin CMIS të ISSH nëpërmjet protokollit të komunikimit, në të njëjtën mënyrë komunikimi, për të siguruar integritetin e tyre dhe njëkohësisht respektimin e afateve. *Pasaktësi janë konstatuar edhe në të dhënat e importuara gjatë viteve lidhur me:* - Përllogaritjen e kontributeve shoqërore për punëmarrësin - Përllogaritjen e kontributeve shoqërore për punëdhënësin - Përllogaritjen e kontributeve për	

	pagat që janë mbi pagën maksimale dhe nën pagën minimale duke patur parasysh që pagesat nën pagën minimale janë kryer edhe kur punëmarrësi ka 22 ditë pune ose më shumë. Deklarime të pasakta në lidhje më numrin e ditëve të punës (ditët e punës janë më shumë se 31 ditë).	
13	Nga auditimi i kontrollit automatik mbi listpagesat, të implementuar në shërbim të ISSH, rezultojnë pasaktësi. Në këto kontrolle janë përfshirë dhe kontributi shëndetsor, një element jo i domosdoshëm për ISSH, kur jashtë kontrollit kanë mbetur element të rendësishëm të listë pagesës si p.sh. numri i ditëve të punës, përllogaritjet e kontributeve brenda pagës minimale dhe maksimale si dhe jashtë kufijve minimalë dhe maksimalë**.**	ISSH të sistemojë procedurat e kontrollit automatik të listpagesave për të dhënat e importuara nga DPT. Të shtohen fusha kontrolli të tjera mbi të dhënat e listpagesave si: ditët e punës duke i kategorizuar sipas kodit të punës, formati i NID-it si dhe elemente të tjerë të nevojshëm për kontroll. Të ndërtohen raporte periodike mbi të dhënat e identifikohen me pasaktësi në: NID, ditë pune, përllogaritje kontributi shoqëror mbi maximumin dhe nën minimumin, përllogaritje gabim të kontributit shoqëror edhe për pagat midis min-max.
14	Nga auditimi me zgjedhje mbi të dhënat e përdoruesve në sistemin DMAIS në muajt Janar, Mars dhe Qershor 2016, rezulton se numri i përdoruesve aktiv në system për çdo muaj është shumë më i vogël se Operator të deklaruar në DPT nga DAQ, me detyrë "Operator Kompjuteri" kategori e cila përfshin operatorët hedhës H1 dhe H2. Procesi i dixhitalizimit për vitet pas 1994 nuk ka nevojë për dy operatorë hedhës (H1 dhe H2), për arsye se të dhënat janë të lexueshme dhe të padëmtuara.	ISSH të marrë masa për përshpejtimin e procesit të dixhitalizmit për vitet përpara 1994, duke e përfshirë në kontratën e çdo punonjësi normativën për hedhjen e të dhënave të pozicionit "Operator". ISSH të marrë masa për ndryshimin e manualit të përdorimit të systemit DMAIS për bashkimin e pozicioneve hedhës H1 dhe H2 në një të vetëm.
15	Nga auditimi mbi të dhënat *input* të	ISSH të sistemojë dosjet e lidhura që

	sistemit PCAMS, u konstatuan mungesa në të dhëna parësore lidhur me: kërkesat për caktim pensioni (numrin dhe datën); kërkesat për rishqyrtim pensioni (numrin, datën dhe arsyen); kërkesat për transferim pensioni (numrin, datën); si të dhëna parësore, datë fillim pensioni duke patur parasysh që asnjë dosje pensioni nuk mund të lidhet pa plotësuar këto të dhëna	kanë këto mangësi. Pas përfundimit të këtij procesi të bëhet i detyrueshëm (mandator) plotësimi i tyre për të mos lejuar dosje me mangësi në të dhëna të rëndësishme. Të kryhen validime mbi fusha të caktuara, për të lehtësuar përdorimin dhe parandalimin e gabimeve llogjike.
16	Nga auditimi i informatizimit të raporteve mjekësore në modulin PASH, pjesë e sistemit PCAMS, rezulton se nuk ka filluar në vitin 2013 i cili konsiderohet si fillimi i procesit të informatizimit, por në vitin 2016.	ISSH krahas vazhdimit të punës për hedhjen e të dhënave të reja, të fillojë regjistrimin në system e të dhënave dhe raporteve mjekësore në modulin PASH nga viti 2013 deri në vitin 2016.
17	Nga auditimi i të drejtave në sistemet e ISSH, për punonjës të Drejtorisë së Burimit të Informacionit rezulton se, nuk janë në përputhje me përshkrimin e punës dhe detyrat që ka ky pozicion përcaktuar në rregulloren e TI.	Drejtoria e Burimeve të Informacionit të sistemojë të drejtat e punonjësve në Drejtorisë së Burimit të Informacionit për të gjitha sistemet PCAMS, CMIS, DMAIS, të pajisen me përdorues me të drejta të kufizuar për të përmbushur detyrat që ju janë caktuar me rregullore.
18	Nga auditimi i përdoruesve dhe përgjegjësive që kanë në DMAIS, janë konstatuar disa problematika me impakt në sigurinë e të dhënave, detajuar si më poshtë: - Në sistem rezultojnë përdorues që kanë akses në më shumë se një rol dhe në shumë raste role në konflikt që do të thotë se punonjësit që regjistron të dhënat mbi vjetërsinë si H1 ka të drejta në system të kontrollojë si H2 apo edhe ti certifikojë këto të dhëna si H3.	Administratorët e sistemit të sistemojnë përdoruesit në DMAIS, duke populluar për cdo rast të dhëna mbi datën e fillimit dhe të drejtat e tyre në system. Të aktivizohet statusi i përdoruesit.

	- Në sistem rezultojnë përdorues me status aktiv edhe punonjësit të cilët kanë ndërprerë marrëdhëniet e punës. - Krijimi për herë të parë i përdoruesve administrohet nga ISSH, ndërsa dhënia e aksesit në rolin e krijuar në system, administrohet nga DAQ. Kjo marrëveshje nuk rezulton e dokumentuar, duke krijuar një konfuzion në menaxhimin e përdoruesve dhe duke lejuar përdoruesit të kenë të drejta që janë në konflikt veprimi. - Data e fillimit (Start Date) për përdoruesit mungon në të gjitha rastet. - Nuk ka përdorues me të drejta administrative të kufizuara për të kryer mirëmbajtjet në system si: krijim roli apo përdoruesi, mbyllje roli apo përdoruesi, por përdoruesit krijohen më roli Administrator dhe të drejtat jepen me një tjetër rol. - Statusi i përdoruesit është i pa kategorizuar dhe jo funksional. Aktualisht të gjithë përdoruesit rezultojnë aktiv në system edhe në rastet kur kanë ndërprerë marrdhëniet e punës. - Data e mbarimit të përgjegjësisë që i është caktuar një përdoruesi, mungon në të gjithë përdoruesit edhe nëse punonjësi mund të ketë ndryshuar pozicionin e detyrimisht edhe profilin në sistem. Në system rezultojnë si përdorues aktive edhe përdoruesit që janë përdorur për testimet e implementimit të sistemit si dhe përdorues të krijuar me të dhëna jo	

	të plota për emrin.	
19	Nga auditimi i kritereve të vendosura për parametrizimin e fjalëkalim-it të përdoruesit në aplikacionet CMIS, DMAIS dhe PCAMS rezulton se fjalëkalimi kategorizohet në "i dobët", për arsye se mungojnë elementet si: mospërsëritja e të njëjtit fjalëkalim për të paktën 3 herë, gjatësi fjalëkalimi në 6 karaktere e pa kategorizuar në numra dhe shkronja apo karaktere speciale si dhe numri logimeve të dështuara (failure login).	Drejtoria e Burimeve të Informacionit të ndjekë hapat e nevojshëm për përmirësimin e kritereve të vendosura për fjalëkalimin duke marrë në konsideratë këta elementë: mospërsëritja e të njëjtit fjalëkalim për të paktën 3 herë, gjatësi fjalëkalimi në 6 karaktere të kategorizuar në numra dhe shkronja si dhe bllokimi i përdoruesit në rast se arrin maksimalisht 5 numri i logimeve të dështuara (failure login).
20	Nga auditimi i regjistrit të prokurimeve për vitit 2016 konstatohet se ISSH ka kërkuar ndryshimin e Regjistrit të prokurimeve për shtesë për fonde për blerje storage dhe migrimi i sistemeve PCAMS & FMS me fond 24,485,000 leke pa tvsh me shkresën nr. 6936 datë 29.08.2016 dhe për shtesë për fonde për mirëmbajtja dhe suporti i shërbimeve të arkivit qendror të sigurimeve shoqërore me fond 71,700,000 lekë pa tvsh me shkresën nr. 7350 date 16.09.2016. Grupi i auditimit konstaton se ndryshimi i regjistrit të prokurimeve në tremujorin e katërt ka detyruar Autoritetin kontraktor të veprojë në minimumin e afateve ligjore për realizimin e procedurave të prokurimit.	Me qëllim rritjen e efiçencën dhe efikasitetin dhe sigurimin e mirëpërdorim të fondeve publike në projektet e teknologjisë së informacionit të ketë parasysh në të ardhmen lënien e hapësirave kohore të nevojshme në hartimin, planifikimin, prokurimin dhe implementimin e tyre.
21	Nga auditimi i procedurave të prokurimit rezulton se Instituti i Sigurimeve Shoqërore për periudhën nën auditim ka aktive të lidhura dy kontrata të Marrëveshjes së Nivelit të Shërbimit.	ISSH në cilësinë e Autoritetit Kontraktor, kryejë analizën "kosto përfitim" për përcaktimin e shërbimeve që do mbahen nga burimet e brendshme dhe atyre që do kalojnë me MNSH

	a. Kontrata nr. 2860/7, datë 29.10.2014, me objekt "*Marrëveshje Shërbimi për Sistemet Informatike të PCAMS për Llogaritjen dhe Caktimin e Pensioneve, FMS për Menaxhimin Financiar, CMIS për Menaxhimin e Deklarimit Online të Kontributeve, Rrjeti informatik dhe pajisje të caktuara të dhomës së Serverave, Pajisje TI për ISSH dhe komunikimin ISSH –Arkiva*". Kjo kontratë është e lidhur për një periudhë 4 vjeçare, me fitues bashkimin e operatorëve ekonomik " " dhe " ". Vlera e kontratës është 163,920,000 lekë pa tvsh, ose 196,704,000 lekë me tvsh, dhe faturimet do të bëhen mbi bazë mujore (vlerë mujore shërbimi) 3,415,000 lekë pa tvsh ose 4,098,000 lekë me tvsh në muaj. **b.** Kontrata nr. 7467/5, datë 02.12.2016, me objekt "*Mirëmbajtje dhe suporti i shërbimeve të Arkivit Qendror të Sigurimeve Shoqërore*". Kjo kontratë është e lidhur për një periudhë 24 muaj (2 vjet) duke filluar nga data e nënshkrimit të kontratës, me fitues operatorin ekonomik " ". Vlera e kontratës është 67,750,000 lekë pa tvsh ose 81,300,000 lekë me tvsh dhe faturimet do të bëhen mbi bazë mujore (vlerë mujore shërbimi). **Nga auditimi rezultoi se hartimi i këtyre kontratave të shërbimit (*MNSH- marrëveshje e nivelit të shërbimit*) nuk janë hartuar në përputhje me aneksin 2, të Udhëzimit nr. 2, datë 02.09.2013 "*Për*	("outsourcing"). Të ketë parasysh në të ardhmen që në hartimin dhe zbatimin e projekteve të teknologjisë së informacionit të kryejë azhornimin e nevojshëm të dokumentacionit të prokurimit në përputhje me ndryshimet ligjore në fuqi.

	***standardizimin e hartimit të termave të referencës për projektet TIK në Administratën Publike*"** **pjesa III pika 10 Aneksi 2.** Sipas Udhëzimit të Ministrit të Shtetit për Inovacionin dhe Administratën Publike nr. 1159, datë 17.03.2014 "*Për Hartimin e Marrëveshjeve të Nivelit të Shërbimit"*, i ndryshuar, MNSH-ja duhet të ishte si aneks më vete bashkëlidhur kontratës administrative. Sipas Aneksit 1 të këtij slaudhëzimi duhet të ishin përcaktuar elementë të rëndësishëm për realizimin e shërbimit të mirëmbajtjes, si *drejtuesi i projektit, personin e kontaktit, përkufizimet e termave teknikë, përshkrimi i shërbimeve, të drejtat dhe detyrimet e institucionit dhe të ofruesit të shërbimit, menaxhimi i shërbimeve, disponueshmëria e shërbimit, kufizimet e mundshme, mirëmbajtja e sistemit/ve, matja e cilësisë së shërbimit, kërkesat e shërbimit, menaxhimi i vazhdueshmërisë së shërbimit, trajtimi i informacionit konfidencial, njoftimi i palëve, penalitetet e mundshme, dokumentacioni mbështetës, ndërprerja e MNSH-së,* dhe të tjerë elementë të rëndësishëm që përcaktohen në këtë aneks.	

AUDITIMET E TEKNOLOGJISË SË INFORMACIONIT VITI 2018

Në zbatim të strategjisë së zhvillimit duke shikuar arritjet dhe prespektivën e këtij auditimi gjatë vitit 2018, Drejtoria e Auditimit të Teknologjisë së Informacionit kalon si drejtori e Auditimit të Teknologjisë së Informacionit nën varesi direkte nga Drejtori i Përgjithshëm dhe në nëntor 2018 kalon në shkallën më të lartë të organizimit të një strukture audituese, në atë të ate të Departamentit të Auditimit të Teknologjisë së Informacionit.

Struktura
Audituesë.....6
Kryeauditues 1
Drejtor.....1

Numri i Auditime të parashikuara për vitin 2018.....6 auditime

Treguesi	Njësia	Llogaritja	Vlera
Fuqia maksimale Audituese	ditënjerëz	22 x 11x 8	1936
Auditime të parashikuara gjithsej	numër		6
Për çdo auditim mesatarisht	ditënjerëz	1936/6	323

Subjekte e audituara

1. Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI).
2. Ministria e punëve të Brendshme Drejtoria e Përgjithshme e Gjendjes Civile.
3. Departamenti i Administratës Publike (Dap).
4. Qendra Kombëtare e Biznesit (QKB).
5. Bashkia Elbasan.
6. Agjencia e Prokurimit Publik(APP).

Ecuria e procesit të auditimeve TI për vitin 2018

Janë zbuluar 120 gjetje dhe janë rekomanduar masat respektive për përmiresimin e gjendjes.

Mesatarisht për çdo auditim janë zbuluar 20 gjetje.

Për herë të parë drejtoria është ndare në dy grupe auditimi.

Pjestarë të drejtorisë kanë marë pjesë në 5 auditime (pjesë e grupeve të departamenteve të tjera, krahas detyrave të tjera të ngarkuara).

1. AGJENCIA KOMBËTARE E SHOQËRISË SË INFORMACIONIT (AKSHI).

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "**Agjencia Kombëtare e Shoqërisë së Informacionit"**

Përgatitur: 10 Maj 2018

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 160/1, datë 01/03/2018.

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Meald Habazaj, anëtar
3. Aldo Kita, anëtar

Periudha e Auditimit: 01.01.2017 – 01.12.2017
Afati i auditimit: 07.02.2018 – 30.04.2018

Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve.

ÇFARË KEMI AUDITUAR

AKSHI është Institucion publik në fushën e teknologjisë së informacionit dhe komunikimit (TIK) e cila ofron shërbime të përqendruara nëpërmjet TIK për qeverisjen elektronike, për administratën shtetërore, qytetarët, bizneset. Administron portalin qeveritar **e-Albania**, është autoritet rregullator-koordinues/përgjegjës i bazave të të dhënave shtetërore, garanton një nivel të lartë të sigurisë kibernetike, ofron shërbimin e nënshkrimit elektronik dhe vulës dixhitale etj.

Grupi i auditimit mblodhi informacione dhe zhvilloi analiza për caktimin e zonave me risk të lartë dhe mbështetur në to hartoi matricat e auditimit.

Kërkesat për informacion për fushat përkatëse u hartuan në përputhje me manualin e Auditimit të Teknologjisë së Informacionit. Plani i auditimit i dalë nga informacionet dhe analizat paraprake kishte për objektiv vlerësimin e sistemeve TI, dhe aspekteve që lidhen me mirëmbajtjen, zhvillimin dhe sigurinë e tyre.

Fushat e auditimit

Auditimi i funksionimit të Qeverisjes TIK

a. Verifikimi i Strategjisë, politikave dhe procedurave TIK

b. Vlerësimi i burimeve njerëzore në strukturat TIK

Auditimi i projekteve e investimeve të teknologjisë së informacionit

a. Identifikimi, hartimi i nevojave dhe kritereve të vendosura për mallra dhe shërbime në TIK

b. Auditimi i projekteve të investimeve në teknologjinë e informacionit për platformën e-Albania

Auditimi i Operacioneve në TIK e-Albania

a. Vlerësimi i menaxhimit të platformës e-Albania

b. Menaxhimi dhe dokumentimi i problemeve, incidenteve dhe ndryshimeve.

Auditimi i Sigurisë së Informacionit

a. Identifikimi dhe menaxhimi i risqeve në TIK

b. Siguria e vazhdimësisë së punës dhe masat e marra.

Të ndryshme të dala gjatë auditimit

a Trajtimi i informacioneve në AKSHI

V. PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Auditimi i Sistemeve të teknologjisë së Informacionit në Agjencinë Kombëtare të Shoqërisë se Informacionit me fokus portalin e-Albania është i rëndësishëm pasi ai është portali i vetëm qeveritar ku shërbimet publike që gjenden në zyrat dhe sportelet fizike të institucioneve ofrohen në mënyrë elektronike falë Platformës Qeveritare të Ndërveprimit që ndërlidh sistemet e institucioneve me njeri-tjetrin.

Në përfundim të auditimit për 16 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit.

Më hollësisht:

OPINIONI I AUDITIMIT:

Grupi i auditimit mbështetur në Standartet ndërkombëtare të Auditimit përkatësisht në ISSAI 100, ISSAI 5300, ISSAI 5310 si dhe nenet 3 dhe 14 të ligjit 154 "Për Organizimin dhe Funksionimin e KLSH " datë 27.11.2014 *konstaton se portali qeveritar e-Albania me gjithë përpjekjet dhe arritjet e AKSHI-t për ngritjen e një Platforme Qeveritare të Ndërveprimit që ndërlidh sistemet e institucioneve dhe ofrimin e shërbimeve publike të zyrave dhe sportelet fizike të institucioneve në mënyrë elektronike, mbart problematikat e investimeve në sistemet e Teknologjisë së Informacionit të institucioneve pa një Strategji në përgjithësi me objektiv ndërveprimi në veçanti. Mbështetja e strategjisë së AKSHI-t vetëm në Strategjinë Ndërsektoriale 2015-2020, Indikatorët dhe Planin e veprimit i strategjisë 2015-2020, mbart riskun e keq adresimit të burimeve të nevojshme. Me gjithë përpjekjet e bëra, AKSHI nuk ka marrë masa të mjaftueshme rregullatore dhe organizative për menaxhimin e ndryshimit. Në gjykimin tonë, menaxhimi i elementëve kritikë në sistemet e informacionit, është i pa pamjaftueshëm,*

Investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht sigurimin e Vazhdueshmërisë së Biznesit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat.

Nr.	**Gjetje nga auditimi**	**Rekomandimi**
1.	AKSHI nuk ka strategji të veçantë zhvillimi, plan-veprimin të strategjisë dhe indikatorët e matjes së perfomancës së strategjisë të veçantë. Në planin e veprimit e zbatimit të strategjisë 7% të veprimeve i takojnë AKSHI-t pjesa prej 93.% i takon institucioneve të tjera të përfshira në Axhenda Dixhitale të Shqipërisë 2015-2020. Në 120 indikatorët e përcaktuar për matjen e strategjisë, 77 indikatorë (64%) janë klasifikuar si të pa matshëm. Ndryshimet në qeverisje dhe shkrirja e Ministrisë të Shtetit për Inovacionin dhe Administratën Publike MIAP me VKM Nr. 504. Dt. 13/09/2017 dhe ndryshimi i statusit të AKSHI-t me VKM Nr. 673, Datë 22.11.2017 nuk janë reflektuar në Strategjinë ndërsektoriale 2015-2020, Indikatorët dhe Planin e Veprimit të Strategjisë 2015-2020.	Strukturat drejtuese të AKSH, duke marrë në konsideratë kohën, burimet e nevojshme si dhe rëndësinë e të dhënave që institucioni posedon dhe përpunon, të marrin masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit.
2.	Rregullorja e brendshme “Mbi detyrat dhe funksionimin e AKSHIT” e miratuar me Nr. Prot 691/1 Dt. 27/04/2015 nuk është në përputhje me organizimin, strukturën dhe funksionalitetin e AKSHI-t sipas statuti të ri që ky institucion ka marrë.	AKSHI në të ardhmen për menaxhimin e ndryshimit organizativ e ligjor që prekin funksionalitetet kryesore të tij të marrë masa për menaxhimin e këtyre ndryshimeve duke rishikuar aktet rregullative, dhe siguruar që këto ndryshime të jenë regjistruar, vlerësuar, autorizuar, prioritarizuar, planifikuar, testuar, implementuar, dokumentuar dhe rishikuar në përputhje me procedurat e dokumentuar dhe të aprovuara të menaxhimit të ndryshimit.

3.	Burimet njerëzore në Agjencinë Kombëtare të Shoqërisë së Informacionit për periudhën Janar – Dhjetor të vitit 2017 kanë rezultuar me mungesa të theksuara, me 30% më pak se struktura plan e miratuar. Situata e burimeve njerëzore për strukturat e shtuara në periudhën Tetor – Dhjetor 2017 paraqitet edhe më e rënduar Grupi i auditimit konstaton se mungesa e burimeve njerëzore në Drejtoria e Vazhdimësisë së Punës BCC,Back-up dhe DRC, Drejtoria e Sigurisë e-Gov, Drejtoria e Infrastrukturës e-Gov, Drejtoria e Sistemeve e-Gov, Drejtoria e Bazave të të Dhënave Shtetërore, Drejtoria e Kërkimit dhe e Zhvillimit, mbart riskun e performancës së dobët të personelit ekzistues si rezultat e mbingarkesës me pasojë mosarritjen e objektivave dhe mosplotësimin e kërkesave për dhënien e shërbimeve.	Strukturat drejtuese të AKSHI-t të marrin masa për plotësimin e strukturës dhe të kryejnë vlerësimet e herë pas hershme të burimeve njerëzore TI të nevojshme dhe mjaftueshme për arritjen objektivave, si dhe të marrin masa për plotësimin e strukturës TI sipas planit të miratuar.
4.	Grupi i auditimit duke marrë parasysh ndryshimin e statusit dhe të strukturës së institucionit me VKM Nr. 673, datë 22.11.2017 si dhe specifikën e Institucionit, ku përdoret një teknologji e niveleve të larta, Vlerëson se shkalla e mbulimit me auditim të brendshëm nga Institucioni nga i cili mbulohet me auditim është i pa specializuar për kryerjen e auditimit të Teknologjisë së Informacionit.	AKSHI duke marrë parasysh ndryshimin e statusit dhe të strukturës së institucionit me VKM Nr. 673, datë 22.11.2017 si dhe specifikën dhe teknologjinë e përdorur të kryej vlerësimin, propozimet e nevojshme për mbulimin me auditim të brendshëm ku të përfshihet dhe auditimi i Teknologjisë së Informacionit.
5.	AKSHI gjatë vitit 2017 nuk ka zhvilluar analizimin e nevojave të burimeve njerëzore të tij për trajnime si dhe nuk e ka konkluduar këtë analizë (në përputhje	Strukturat drejtuese të AKSHI-t të kryejnë analizimin e nevojave për trajnime të burimeve njerëzore në fushën e Teknologjisë së Informacionit në

	me burimet njerëzore dhe financiare) në miratimin e një plani trajnimesh. Zhvillimi i paplanifikuar i trajnimeve ka sjellë mos mbulimin me trajnim të stafit si dhe shpërndarjen sporadike të trajnimeve gjatë vitit, gjë e cila mbart risqet e produktivitetit të ulët, menaxhimit jo efektiv, rritje të shanseve për mosarritje të objektivave, si dhe mos shfrytëzim në mënyrë efektive të kohës dhe burimeve.	përputhje me burimet njerëzore dhe financiare (të brendshme dhe të jashtme) të hartojnë e zbatojnë trajnimin e tyre sipas një plani të miratuar e dinamik në përputhje me ndryshimet teknologjike të fushës.
6.	Grupi i auditimit konstaton se ndryshimet strukturore të miratuara të AKSHI-t, nuk janë paraprirë me ndryshime në bazën rregullatore për funksionimin e strukturës së institucionit.	Strukturat drejtuese të AKSHI-t, në të ardhmen të menaxhojnë ndryshimet, duke i paraprirë zbatimit me hartimin e bazave rregullatore për funksionimin e funksionaliteteve të reja të strukturave të institucionit. Në çdo rast procesi duhet të kalojë në procese pilote si dhe nënshtrimin e testimeve të nevojshme.
7.	Në procedurat e prokurimit për vitin 2017 vërehet mungesa e hartimeve specifike të kritereve të veçanta. Nuk ka një argument të hollësishëm mbi vendosjen e këtyre kritereve, duke pasur parasysh edhe rëndësinë, natyrën dhe vëllimin e kontratës. Në Standardet TIK për vitin 2017, Specifikimet Teknike nuk janë përcaktuar kushtet e veçanta të karakterit teknik (Licenca, Trajnime, Kapacitete, etj), të cilat duhet t'i plotësojë Operatori Ekonomik në kundërshtim me VKM Nr. 703, Datë 29.10.2014 "Për Agjencinë Kombëtare të Shoqërisë së Informacionit" pika 3.c në të cilën citohet se *"AKSHI ka për detyrë dhe përgjegjësi të përcaktoj standardet e*	AKSHI në të ardhmen të marre masa për shmangien e praktikave të tilla me qëllim hartimin e Standardeve TIK, Specifikimet Teknike të rekomandojë kushtet e veçanta të karakterit teknik (Licenca, Trajnime, Kapacitete, etj), të cilat duhet t'i plotësojë Operatori Ekonomik, bazuar në standardet ndërkombëtare dhe evropiane, të adoptuara, që do të ndiqen nga administrata shtetërore.

	TIK-ut, bazuar në standardet ndërkombëtare dhe evropiane, të adoptuara, që do të ndiqen nga administrata shtetërore".	
8.	Nga auditimi i procedurave të marrjes në dorëzim të shërbimeve në përputhje me MNSH e lidhura për platformën e-Albania rezulton se grupet e marrjes në dorëzim nuk mbajnë raporte të marrjes në dorëzim të punimeve të kryera nga OE në kundërshtim me VKM Nr. 914, datë 29.12.2014, Neni 77, Pika 3 mbikëqyrja e kontratës. Nga auditimi i Amendamentit me Nr. 1876, me objekt shtyrjen me 3 muaj (dt. 14/08/2017) i implementimit të kontratës Nr. Prot. 2571 datë 14.12.2015 për "Shtimi i 209 shërbimeve të reja elektronike për 18 institucione" ka mangësi pasi në të nuk janë paraqitur dhe cilësuar arsyet që kanë pasur palët për shtyrjen e kontratës.	AKSHI në të ardhmen për të shmangur mangësi në praktikat e zbatimit të kontratave duhet të marrë masa që gjatë zbatimit të kontratave të MNSH të lidhura me OE për përfitimin e shërbimeve të mirëmbajtjes së platformës e-Albania (dhe jo vetëm), duhet të ushtrojë kujdesin e duhur në përputhje me legjislacionin në fuqi për monitorimin e zbatimit të kontratave duke matur, vlerësuar e dokumentuar procesin
9.	Nga auditimi rezultoi se mungesat në strukturën e Drejtorisë së Sigurisë e-Gov me 10 punonjës në organike dhe me dy sektorë, me vartësi direkt nga Drejtori i Përgjithshëm përkatësisht në Sektorin e Sigurisë së Informacionit (me 5 punonjës në organike nga të cilët 2 vende vakante) dhe Sektorin e Infrastrukturës dhe çelësave publikë (me 5 punonjës në organike nga të cilët 2 vende vakante), përbëjnë risk në sigurinë e Gov e me gjerë. U konstatua se regjistri i risqeve i miratuar për vitin 2017 është në mospërputhje me kërkesat e Ligjit Nr.	AKSHI të marrë masa me qëllim përmbushjen e misionit të tij duke marrë parasysh dhe funksionalitetet e reja të përcaktuara nga VKM Nr. 673, Datë 22.11.2017, me një proces dinamik dhe gjithë përfshirës të strukturave kryesore të kryej identifikimin dhe vlerësimin e risqeve, dhe në varësi të burimeve të hartojë masat dhe politikat e nevojshme, reale për minimizimin e tyre.

	10296, Datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar, Udhëzimi Nr. 30, Datë 27.12.2011 "Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik" . Grupi i auditimit konstaton se ai është një proces i nisur, por i pa finalizuar pasi nga 86 risqe të klasifikuar 48 % te tyre nuk është përcaktuar asnjë masë veprimi, nuk janë përcaktuar saktë objektivat dhe nuk janë përfshire drejtuesit kryesorë në procesin e menaxhimit të riskut Me konkretisht: **a. Drejtoria e Vazhdueshmërisë së Punës BCC, Backup & DRC** Nuk kanë të identifikuar si risk mungesën e DRC dhe nuk ka masa për minimizimin e këtij risku Risqet e identifikuara përgjithësisht janë risqe të mbartura nga institucionet e tjera dhe jo risqet e AKSHI-t Nuk identifikohet si risk mungesat në personel **b. Për Drejtorinë e Bazave të të Dhënave Shtetërore** Nuk ka veprime të përcaktuara për adresimin e boshllëqeve për: Mungesa e stafit dhe kapaciteteve të duhura në burimeve njerëzore, përbën vonesë në regjistrimin e bazave të të dhënave shtetërore. Mosbashkëpunimi i institucioneve. Vonesa në regjistrimin e bazave të të dhënave me impakt në ndërveprimin e tyre.	

	Ndryshimet ligjore të ndodhura ndikojnë në procesin e regjistrimit të bazave të të dhënave shtetërore. **c. Drejtorinë e Portalit Qeveritar e-Albania** Nuk ka veprime të përcaktuara për adresimin e boshllëqeve për: Vonesat në plotësimin e informacionit nga personat përgjegjës të institucioneve të administratës publike për shtimin e shërbimeve në portalin qeveritar e-Albania. Mungesë pjesëmarrje e aktorëve përkatës në takime. Vonesa në dorëzime nga operatori ekonomik. Mungesa e trajnimeve për përdorimin e backend-it të portalit. **d. Sektori i financës, Burimet njerëzore.** Nuk ka veprime të përcaktuara për minimizimin e riskut të identifikuar për : Mospërputhja e kërkesave të përcaktuar për pozicionin e punës me rezultatet e konkursit apo intervistës së zhvilluar. Mungesa e stafit dhe kapaciteteve të duhura në burimeve njerëzore, përbën vonesë në zgjidhjen e problemeve.	
10.	Nga auditimi u konstatua se prej vitit 2013, AKSHI ka investuar për zhvillimin e vazhdueshëm të Portalit e-Albania, dhe rritjen e numrit të shërbimeve elektronike të ofruara për qytetarët dhe bizneset, por kryerja e	AKSHI në të ardhmen t'i kushtojë një vëmendje të veçantë efektivitetit të përdorimit të fondeve publike duke mbështetur ato në kohë me bazën e duhur rregullatore në përputhje me të drejtat e e reja të përcaktuara në VKM.

	investimeve për krijimin e shërbimeve elektronike dhe ngritjen e protalit, nuk është sinkronizuar në kohë me nxjerrjen e bazës ligjore për vulën elektronike nga strukturat që kishin të drejtën për të nisur propozimet legjislative (VKM nr.495, datë 13.9.2017). Veprim i cili ka sjellë mos efiktivitet në përdorim të portalit për muajt janar – shtator 2017.	Nr. 673, Datë 22.11.2017.
11.	Grupi i auditimit konstaton se suporti ndaj përdoruesve të platformës është i ulët me impakt të drejtpërdrejtë në uljen e numrit të përdorueshmërisë së platformës nga qytetarët, strukturat për auditimin e këtij procesi i cili konsiderohet si një proces tepër sensitiv dhe i domosdoshëm janë të mjaftueshme dhe më konkretisht: a. Suporti me telefon/chat nuk është funksional dhe koha e kthimit të përgjigjes për suport me formën e aplikimit është relativisht e gjatë, nuk ka ofrimin e shërbimit për përdorues me aftësi të veçanta (probleme shikimi) platforma ofron mundësinë e vendosjes së kontrollit të sigurisë (Captcha) me tinguj zanorë por këto tinguj nuk janë në gjuhën Shqip, gjë e cila sjell vështirësi ne përdorim nga qytetarët në mospërputhje edhe me Ligjin nr. 93/2014 ”Për Përfshirjen dhe Aksesueshmërinë e Personave me Aftësi të Kufizuara”. Shkalla e ulët e përdorimit të e-Albania nga grup moshat 35-65 + tregon se këto mosha të nga grup moshat 35-65 + tregon se këto mosha të cilat përbejnë 51.3 % të popullsisë megjithëse kanë nevoja më të	Drejtoria e platformës e-Albania me qëllim rritjen e përdorimit të platformës të analizojë në mënyrë periodike shkaqet e mos marrjes së shërbimit si dhe të kryejë rivendosjen e suporteve në gjuhën shqipe me telefon/chat me mbulim 24/7. Në ofrimin e suportit të kihet parasysh kuadri ligjor në lidhje me kërkesat e kategorive me aftësi të veçanta.

	mëdha për këto shërbime hasin vështirësi në përdorim të shërbimeve online. b. Shkalla e ulët e rikthimit të përdoruesve tregon se duhet bërë akoma më shumë punë për analizimin e shkaqeve për të cilat përdoruesit nuk kanë arritur dot të marrin shërbimin e nevojshëm. Mungesa e asistencës në kohë reale bën që grup moshat të cilat kanë nevojë më të madhe për thjeshtëzim në ndërveprim me e-Albania me qëllim të përfitimit të shërbimeve, nuk kanë përdorueshmëri të lartë të platformës për shkak se nuk arrijnë të kryejnë përdorimin e shërbimeve në platformë. c. Shkalla e ulët e përdorimit të portalit nga përdorues jashtë Shqipërisë për vende me emigracion të lartë të shqiptarve si Italia, Greqia etj nuk janë në listën e përdoruesve më të mëdhenj të sistemit lidhet me faktin e mungesës së asistencës online si dhe shtrirjen e kësaj asistence 24/7 dhe mos marrjen parasysh se shumë nga bashkatdhetarët tanë jetojnë në zona orare të ndryshme nga ajo e Shqipërisë. Grupi i auditimit konstaton se në platformën e-Albania nuk janë eliminuar plotësisht bug-et dhe ofruar facilitet e nevojshme: d. Procesi i resetimit të fjalëkalimit nuk është i konsoliduar plotësisht. Është konstatuar se në raste të veprimeve jo të sakta të përdoruesve që kërkojnë të resetojnë fjalëkalimin ka problematika	

	që e pengojnë këtë proces. Duke pasur parasysh se niveli i aftësive ndërvepruese të qytetarëve me platformën e-albania është i llojeve të ndryshme, është tepër e domosdoshme që procesi i resetimit të fjalëkalimit të jetë një proces i konsoliduar dhe pa probleme teknike, pavarësisht veprimeve të sakta ose të pasakta që mund të kryejnë përdoruesit e platformës. Problematikat që mund të shfaqen në këtë proces kanë impakt të drejtpërdrejtë në uljen e numrit të përdoruesve që kërkojnë të marrin shërbime nga platforma e-albania. e. Grupi i auditimit konstaton se në shërbimin "Kërkesë për transferim dosje përfitimi (pensioni)" në platformen e-albania kur përdoruesi ka hapur këtë e-shërbim, nuk ka mundësi të bëjë kërkim për shërbime të tjera. Në momentin që përdoruesi klikon butonin "search" pasi shkruan një shërbim tjetër që dëshiron të kërkojë i shfaqet "error" kthimi back të browser-it, përdoruesit i rishfaqet "error". f. Disa fusha si 'e-mail, emër, mbiemër, NID duhet të merren automatikisht nga profile i përdoruesit në rastet kur përdoruesi është i loguar në platform. Aktualisht një përdorues mund të vendosi çfarëdo vlere në fushat e kërkuara dhe të dërgojë një kërkesë për suport.	
12.	Grupi i auditimit konstaton se loget e përgjigjeve të kërkesave dhe ankesave fshihen automatikisht 30 ditë pasi ka	AKSHI të marri masa për analizimin e konfigurimeve dhe kapaciteteve ekzistuese ruajtjes se logeve, dhe të

	ndodhur veprimi. Nuk ka gjurmë të analizimit të procesit të ndihmës dhe suportit për përdoruesit e e-Albania në kundërshtim me Rregulloren e Sigurisë së AKSHI-t miratuar me Nr.Prot. 2420 dt.29/08/2016 ; Kreu VI Administrimi i Sistemeve të Informacionit, Neni 21 Mbajtja e Logeve i cili përcakton: "Do të mbahen dhe do të ruhen loget (shënimet e shkurtuara) për të gjithë aksesimet në sistemet e AKSHI-t, për të gjithë përdoruesit e brendshëm dhe të jashtëm, si dhe me Ligjin Nr. 10 273, datë 29.4.2010 Neni 18 "Ruajtja e dokumentit elektronik".	hartojë dhe miratojë në përputhje me legjislacionin e "ruajtjes së dokumentit elektronik", kohën e ruajtjes, procedurat e analizimit dhe fshirjes së logeve.
13.	Grupi i auditimit konstaton se Platforma E-Albania, publikon informacione dhe shërbime nga burime të cilat kanë data baza të pa certifikuara (nga AKSHI) duke mos siguruar ndërveprimin e duhur për ruajtjen e të dhënave personale. Grupi i auditimit konstaton se politikat e privatësisë janë thyer dhe të dhënat personale janë të ekspozuara, me konkretisht: Gjenerimi i faturës të UKT-së në platformën e-Albania pa bërë lidhjen me numrin NID me 'KODI I KLIENTIT', mundëson leximin e informacioneve të faturimeve që nuk i përkasin personit të loguar në platformë. Nga auditimi konstatohet se pavarësisht se Regjistri i Drejtorisë së Përgjithshme të Shërbimeve të Transportit Rrugor është bazë të dhënash e regjistruar, si rezultat i problematikave në ndërveprimin e kësaj baze të dhënash me	AKSHI me grupe të përbashkëta me institucionet që ofrojnë shërbime në platformën e-Albania të marrë masa për analizimin e bazave të të dhënave të platformës dhe të kryejë ndërhyrjet e nevojshme për plotësimin e kritereve të domosdoshme për ndërveprim duke respektuar përcaktimet e Ligjit Nr. 9887 datë 10.03.2008 (ndryshuar) "Për Mbrojtjen e të Dhënave Personale". Për shërbimet apo elementë të tyre të cilat nuk plotësojnë kriteret e nevojshme ligjore të merren masa e pezullimit të shërbimit deri sa të sigurohet plotësimet e nevojshme.

	regjistrin e gjendjes civile (identifikimi i mbështetur në NID) identifikimi i përdoruesit që kërkon shërbimin jo gjithmonë është i saktë.	
14.	AKSHI nuk po zhvillon teknologji të cilat do ti përgjigjen fluksit në rritje të të dhënave (big data) mbështetur në të ashtuquajturin "programim logjik" i cili mbështetet në logjikën e vetë zhvilluesve të softuerëve për përzgjedhjen, grupimin e ndërlidhjen e informacioneve. Grupi i auditimit konstaton se AKSHI nuk ka bërë përpjekje të mjaftueshme për të: g. Reduktuar pasigurinë që ka të bëjë me përpunimin dhe përdorimin e të dhënave masive (Big Data), dhe ofrimi i një platformë të plotë dhe efektive të dhënash për vendimmarrësit. h. Ulur marzhin e gabimeve në analizën e të dhënave masive (Big Data) duke udhëzuar përdoruesit për rrugën e duhur janë të pa mjaftueshme. i. Përdorimin e Big Data-t për të ndihmuar vendimmarrësit të marrin vendimet e duhura bazuar në të dhëna dhe analiza të menaxhimit të cilësisë (Managing Total Quality/MTQ). Grupi i auditimit konstaton se funksionalitetet e gjenerimit të statistikave në Drejtorinë Juridike nuk përbën oportunitet për zhvillimin e statistikave në përgjithësi dhe data analitics në veçanti.	AKSHI të marrë masa në zbatim të praktikave me të mira të fushës analizimin e situatës me objektiv ndryshimet e nevojshme strukturore dhe planifikimin e burimeve të nevojshme për përdorimin e statistikave dhe big data me prioritet zhvillimin e Teknologjive të cilat do ti përgjigjen fluksit në rritje të të dhënave (big data) mbështetur në programe logjike.
15.	Grupi i auditimit konstaton se AKSHI	AKSHI duke marrë parasysh edhe

	nuk ka Disaster Recovery Plan (DRP) dhe Disaster Recovery Center (DRC), mungesa e të cilave mbart riskun e humbjes së të dhënave të cilat ruhen dhe përpunohen në Data Center e AKSHI-t me një impakt të madh, të një rëndësie mbarë kombëtare.	shtimin e funksionaliteteve të marri masat e nevojshme për hartimin e një Disaster Recovery Plan (DRP) si dhe duke kryer vlerësimin e impaktit mbarë kombëtar të humbjes së informacionit nga mungesa e DRC të paraqesë projekte konkrete pranë instancave përkatëse për financimin e një Disaster Recovery Center (DRC).
16.	Grupi i auditimit konstaton se portali e Albania nga data e krijimit 28 nëntor 2012 deri me datë 21.09.2017 ka funksionuar pa një rregullore të miratuar. Kjo rregullore nuk ka politika në hapjen dhe mbylljen e userave, për punonjësit e Administratës Publike dhe Institucioneve Publike dhe Jo publike, të cilët kanë akses në shërbimet e e-Albania. Gjithashtu në sistem ndodhen usera të pa identifikuar me emër, mbiemër me impakt në përdorimin e pakontrolluar të të dhënave personale të mbrojtura me ligj. Procesi i dërgimit të emailit nuk kërkon verifikimin e vërtetësisë së adresës së e-maileve si dhe nuk ka info shtesë për vendndodhjen e dërguesit të këtij emaili që kërkon suport ose ndihmë si dhe mosha e tij.	Me qëllim mbrojtjen e të dhënave personale AKSHI të marrë masa për ndërhyrjet e nevojshme ne rregulloren e portalit për plotësimin e politikave në hapjen dhe mbylljen e userave, për punonjësit e Administratës Publike dhe Institucioneve Publike dhe Jo publike, të cilët kanë akses në shërbimet e e-Albania.

2. MINISTRIA E PUNËVE TË BRENDSHME, DREJTORIA E PËRGJITHSHME E GJENDJES CIVILE.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: Drejtoria e Përgjithshme e Gjendjes Civile

Përgatitur:

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 152/1 datë 02.03.2018

Auditimi është kryer nga:

- Elira Cukalla, përgjegjës grupi
- Benard Haka, anëtar
- Bledi Dervishaj, anëtar

Periudha e Auditimit: 01.01.2016 – 01.12.2017
Afati i auditimit: 05.03.2018 – 27.04.2018

Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve.

ÇFARË KEMI AUDITUAR

Fushat e auditimit

1 Auditimi i projekteve e investimeve në teknologjinë e informacionit / Marrëveshjet e Nivelit të Shërbimit (MNSH)
2 Auditimi i Operacioneve në TIK / Vlerësimi mbi menaxhimin e shërbimeve dhe dokumentimi i problemeve, incidenteve,ndryshimeve
3 Auditimi i Sigurisë së Informacionit / Identifikimi dhe menaxhimi i risqeve në TI / Siguria e të dhënave dhe vazhdimësia e biznesit
4 Auditimi i Sistemit Informatik të Gjendjes Civile / Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output dhe shkalla e sigurisë së përdoruesve.

PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Tërësia e të dhënave personale të shtetasve shqiptarë, shtetasve të huaj, si dhe të personave pa shtetësi, që janë me banim të përkohshëm apo të përhershëm në Republikën e Shqipërisë, të cilat regjistrohen dhe mbahen në Regjistrin Kombëtar të Gjendjes Civile dhe që vërtetojnë lindjen, ekzistencën, individualitetin, lidhjet ose marrëdhëniet ndërmjet tyre, përbëjnë elementë të Gjendjes Civile.

Në përfundim të auditimit për 21 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit

Më hollësisht:

OPINIONI I AUDITIMIT:

Drejtoria e Përgjithshme e Gjendjes Civile, si institucioni përgjegjës për tërësinë e të dhënave personale të shtetasve shqiptarë, shtetasve të huaj, si dhe të personave pa shtetësi, që janë me banim të përkohshëm apo të përhershëm në Republikën e Shqipërisë, të cilët regjistrohen dhe mbahen në Regjistrin Kombëtar të Gjendjes Civile, nuk ka marrë masa të mjaftueshme rregullatore dhe organizative, për garantimin e

shërbimeve, konfidencialitetit, integritetit dhe gatishmërisë së të dhënave në sistemet e informacionit që posedon. Mungesa e Strategjisë lidhur me sistemet e Teknologjisë së Informacionit dhe burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen tyre, janë mjet për realizimin e objektivave të DPGJC-së. Mungesa e rregulloreve dhe ushtrimit të vazhdueshëm të kontrolleve në aplikacion ka sjellë mosmenaxhim të elementëve kritikë të sigurisë, si dhe ka rritur riskun për qasje të paautorizuar në të dhënat.

Nr.	Gjetje nga auditimi	Rekomandimi
1	Nga auditimi i procedurës së prokurimit me objekt "*Mirëmbajtja dhe zhvillimi i mëtejshëm i Regjistrit Kombëtar të Gjendjes Civile*", u konstatua se: - Nuk ka argumente në lidhje me vendosjen e kërkesave dhe kritereve për kualifikimin, veprim në kundërshtim me nenin 61 pika 2 të VKM nr. 914, datë 29.12.2014 "Për miratimin e rregullave të prokurimit publik", i ndryshuar, nenin 46, pika 3, dhe nenin 23, pika 1 të ligjit nr. 9643, datë 20.11.2006 "Për prokurimin publik", i ndryshuar. - Në shkresën me nr. 33/4 prot, datë 27.09.2017 të Drejtorit të Përgjithshëm të Gjendjes Civile, është kërkuar ndryshimi i kritereve për kualifikim, për të cilën nuk rezulton asnjë relacion në lidhje me arsyetimin apo argumentimin e këtyre ndryshimeve nga specialistët e fushës si dhe nuk ka asnjë kërkesë apo ankesë të operatorëve ekonomik.	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile në vazhdimësi të merren masa për argumentimin e kritereve për kualifikim dhe ndryshimeve të mundshme të tyre duke rritur kështu nivelin e transparencës në përputhje me parimet e zhvillimit të procedurave të prokurimit publik.
2	Nga auditimi i procedurës së prokurimit me objekt "*Mirëmbajtja dhe zhvillimi i mëtejshëm i Regjistrit Kombëtar të Gjendjes Civile*", u konstatua se përcaktimi i fondi limit është realizuar	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile, krahas testimit të tregut të merret në konsideratë edhe kontratat e ngjashme për përllogaritjen e fondit limit, për të qenë sa më afër saktësisë së

	me metodën e çmimit të tregut duke marrë tre oferta. Kjo metodë konsiderohet si e papërshtatshme, pasi bëhet fjalë për një program specifik të krijuar nga kompania "X". Ky veprim është në kundërshtim me VKM nr. 914, datë 29.12.2014 "*Për miratimin e rregullave të prokurimit publik*", i ndryshuar, neni 9 "*Llogaritja e vlerës së kontratës*".	këtij fondi.
3	Aktualisht sistemi i Regjistrit Kombëtar të Gjendjes Civile është pa mirëmbajtje, duke vënë në rrezik vazhdueshmërinë e punës së këtij institucioni si dhe ofrimit të shërbimit online ndaj qytetarëve. (*Gjatë periudhës së auditimit në terren janë evidentuar 5 raste të ndërprerjes së shërbimit të sistemit të Gjendjes Civile*). Grupi i auditimit vlerëson se kjo situatë ka ardhur si pasojë e ngjarjeve të mëposhtme: -Përgatitja me vonesë e specifikimeve teknike nga grupi i punës i ngritur me urdhrin nr. 689, datë 24.05.2017 të Sekretarit të Përgjithshëm të Ministrisë së Brendshme. Relacioni i përgatitur nga ky grup është me datë 15.09.2017, pra rreth 4 muaj më pas. Theksojmë se kjo është një procedurë e cila nuk zhvillohet për herë të parë dhe për përfitim kohor mund të përdoreshin për referencë specifikimet e kontratës së kaluar. -Vonesa e dhënies së vendimit nga ana e Komisionit të Prokurimit Publik në kundërshtim me ligjin nr. 9643, datë 20.11.2006 "Për prokurimin publik", i ndryshuar, Kreu VII "Procedurat e	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të analizohet situata e krijuar duke përcaktuar shkaqet, pasojat dhe përgjegjësitë individuale dhe institucionale, për mungesën e mirëmbajtjes të sistemit "*Regjistrit Kombëtar të Gjendjes Civile*", i cili është në shërbim të qytetarëve të Republikës së Shqipërisë. Gjithashtu, DPGJC të marrë masat e nevojshme për garantimin e ofrimit të shërbimeve online në vazhdimësi.

	rishikimit administrativ", Neni 63 "Të drejtat e personit të interesuar", pika 9. Sa më sipër, afati maksimal ligjor për kthimin e përgjigjes nga ana e Komisionit të Prokurimit Publik ishte data 03.02.2018, pra KPP ka shkelur afatin maksimal të shqyrtimit të ankesës me 2 muaj e 13 ditë.	
4	Nga auditimi i procedurës së mirëmbajtjes, kontratë shërbimi nr. 64/7 datë 31.12.2014 "*Mirëmbajtja dhe Zhvillimi i mëtejshëm i sistemit të RKGJC*" u konstatua se: - Nuk ka asnjë dokumentacion shkresor që të përcaktojë personat që do të jenë për nivelin e parë dhe të dytë të suportit, në kundërshtim me pikën 7.8 "*Mbështetja operacionale TI*" e MNSH të specifikimeve teknike. - Nga auditimi u konstatua se raportet (ditore/javore) nuk janë gjeneruar dhe nuk kanë qenë pjesë e dokumentacionit shoqërues mujor për marrjen në dorëzim të MNSH, në kundërshtim me pikën 7.8.3 "*Dorëzimi dhe Miratimi i Raporteve*" dhe pikën 7.11 të MNSH-s "*Kontraktori duhet të shkruajë një raport të përditshëm deri në orën 09:00 të ditës vijuese".* - Nga auditimi u konstatua se stafi i DPGJC ka zhvilluar trajnimin për pjesën e parë pas nënshkrimit të kontratës, ndërsa trajnimet në përfundim të kontratës nuk janë zhvilluar, në kundërshtim me pikën 7.8.6 të specifikimeve teknike të MNSH-së. Trajnimet e stafit të DPGJC referuar	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të merren masa, për vendosjen e treguesve të matshëm për monitorimin dhe ndjekjen e kontratave për kontratat që i përkasin të ardhmes. Saktësimi i treguesve për matjen e efektivitetit dhe disponueshmërisë së shërbimit për të cilat këto kontrata realizohen do të lehtesojë dhe përllogaritjen e penaliteteve në rastet e nevojshme.

	pikës 7.8.6 të specifikimeve teknike duhej të realizoheshin përgjatë gjashtëmujorit të parë pas nënshkrimit të kontratës dhe gjashtëmujorit të fundit në përfundim të kontratës. - Nga dokumentacioni i administruar u konstatua se nuk ka asnjë plan të detajuar për marrjen në dorëzim të gjithë elementëve të shërbimit të mirëmbajtjes, në kundërshtim me pikën 7.9.6 të specifikimeve të MNSH-s, nga ku Kontraktori ka për detyrim të ndihmojë DPGJC-në në hartimin e një plani të detajuar të marrjes në dorëzim nga ana e DPGJC, të gjithë elementëve të këtij shërbimi në tremujorin e fundit të kontratës.	
5	Nga auditimi i procedurës së mirëmbajtjes, kontratë shërbimi nr. 64/7 datë 31.12.2014 "*Mirëmbajtja dhe Zhvillimi i mëtejshëm i sistemit të RKGJC*" u konstatua se nga ana e kontraktuesit janë zhvilluar 3 module të reja (Importimin e dokumenteve të letërnjoftimit në sistemin e RKGJC, Reflektimin e adresave nga sistemi i ndërfaqes RKA, Shërbimet Web me palët e treta) me kërkesë të bazuar në kushtet e kontratës, të cilat rezultuan se nuk janë kaluar në LIVE në kundërshtim me pikën 7.9.4 të MNSH-së "*Zhvillime të mëtejshme, ndërfaqe të reja për aplikacione të tjera, funksionalitete të reja*".	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile në kuadër të respektimit të marrëdhënieve kontraktuale me ofruesin e shërbimit të mirëmbajtjes duhet të marrë masa për kalimin në Live të funksionaliteteve të kërkuara që kanë mbetur në mjedisin test, për mos u përballur me kosto shtesë për të njëjtën nevojë në zhvillim me ofruesin e shërbimeve në vijim.
6	Nga auditimi i kontratës shtesë shërbimi nr. 730/10 datë 17.07.2017 me objekt "*Mirëmbajtja dhe Zhvillimi i Mëtejshëm*	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile, në të ardhmen të marrë masa që hartimi i kontratave të kryhet në

	i Regjistrit Kombëtar të Gjendjes Civile" shtesë kontrate për mirëmbajtjen e site-t sekondar të lokalizuar tek AKSHI u konstatua se specifikimet teknike të shtesës së kontratës së shërbimit nr. 730/10 datë 17.07.2017 me objekt "*Mirëmbajtja dhe Zhvillimi i Mëtejshëm i Regjistrit Kombëtar të Gjendjes Civile"*, janë identike me kontratën fillestare të procedurës së mirëmbajtjes. Këto specifikime nuk janë përgatitur në përpjesëtim me objektin e prokuruar duke mos u ndalur në zërat e nevojshëm, por duke vendosur specifikimet bruto të kontratës së mëparshme. Grupi i auditimit e vlerëson se përpilimi i kontratës shtesë nuk reflekton saktësisht objektin për të cilin kërkohet shërbim.	mënyrë specifike për çdo rast, në përputhje me nevojat reale të shërbimit të prokuruar, e për pasojë realizimi i këtij shërbimi të jetë sa më objektiv.
7	Mirëmbajtja për dy sistemet: "*Ndërtimi i një sistemi funksional online të adresave dhe përditësimi i të dhënave të tij*" dhe "*Ndërtimi i ndërfaqes së komunikimit ndërmjet RKGJC dhe RKA*". Nga auditimi i specifikimeve teknike, të MNSH si pjesë e kontratave për projektet "*Ndërtimi i një sistemi funksional online të adresave dhe përditësimi i të dhënave të tij*" dhe "*Ndërtimi i ndërfaqes së komunikimit ndërmjet RKGJC dhe RKA*", u konstatua se kërkesat për mirëmbajtjen nuk janë hartuar në përputhje me Udhëzimin nr. 1159 datë 17.03.2014 "*Për Hartimin e Marrëveshjeve të Nivelit të Shërbimit*", duke lënë jashtë saj detaje të rëndësishme si: - Pika 4 Përkufizimet e termave teknik	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të marrë masat për kontratat që do të ketë në të ardhmen, në mënyrë që të përfshijë të gjithë elementët që përshkruhen në udhëzimet lidhur me mirëmbajtjen, si standard detyrues.

	në dokument - Pika 5 Përshkrimi i shërbimeve me përgjegjësitë që ka secila palë - Pika 8 Menaxhimi i Shërbimeve, disponueshmëria, kufizimet e mundshme, vazhdueshmëria e punës duke qenë se janë ndërtuar 2 site (parësor dhe dytësor), si dhe matja e cilësisë së shërbimit.	
8	Nga Auditimi për sistemet "*Ndërtimi i një sistemi funksional online të adresave dhe përditësimi i të dhënave të tij*" - RKA dhe "*Ndërtimi i ndërfaqes së komunikimit ndërmjet RKGJC dhe RKA*" – Ndërfaqja rezultoi se: – Dy sistemet e mësipërme RKA dhe Ndërfaqja që janë në mirëmbajtje nuk janë në "LIVE" sepse nuk ka përfunduar popullimi plotësisht me të dhëna mbi adresat në përmbushje të qëllimit për të cilin janë ndërtuar. – Në marrëveshjen institucionale ndërmjet OSHEE dhe MPB nuk është përcaktuar një afat përfundimtar në lidhje me të dhënat, që OSHEE si institucion i ngarkuar për popullimin, duhet t'i dorëzojë DPGJC-së. – DPGJC nuk ka bërë asnjë përpjekje për një shtyrje të afatit të mirëmbajtjes (marrëveshje mirëkuptimi), deri në popullimin e plotë të informacionit pa të cilin këto sisteme nuk kanë kuptim.	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile në bashkëpunim me OSHEE të marrë masat për analizimin e shkaqeve që kanë shkaktuar vonesë në popullimin e të dhënave lidhur me adresat, duke nxjerrë edhe përgjegjësitë. Gjithashtu, të merren masat për kalimin sa më shpejt të sistemit të adresave në LIVE, nga i cili varet dhe sistemi i ndërfaqes së komunikimit, me qëllim realizimin e objektivit për secilën prej kontratave.
9	Nga auditimi mbi vazhdimësinë e Dixhitalizimit të regjistrave dhe akteve u konstatua se:	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të marrë masat e nevojshme për vazhdimin e

	– Fotografimi nuk vazhdon të kryhet dhe transkriptimi nga regjistrat në programin e arkivës realizohet sa herë që ka një kërkesë (rast pas rasti). – Të dhënat, për periudhën 1974-2010 plotësohen manualisht nga punonjësi i zyrës së gjendjes civile sipas kërkesës së çdo shtetasi, për efekt gjenerimi certifikate, por ruajtja e të dhënave nuk bëhet në sistem, për arsye se sistemi aktual i RKGJC nuk është zhvilluar, për ruajtjen e rekordeve me të dhëna të mëparshme, që i përkasin kësaj periudhe.	dixhitalizimit të arkivave duke trajtuar me përparësi fotografimin e regjistrave dhe akteve. Transkriptimi të kryhet me punonjësit e zyrave të gjendjes civile dhe ata të arkivës, në mënyrë që gabimi material të jetë sa më i vogël.
10	Nga auditimi u konstatua se DPGJC: - Nuk ka Rregullore të Teknologjisë së Informacionit ku të mbështesë aktivitetin e saj; - Nuk disponon rregullore/udhëzime operacionale që përcakton detyra periodike apo të vazhdueshme, hapat që duhet të ndiqen, si dhe personat përgjegjës lidhur me veprimet, që përdorues të ndryshëm kryejnë në sistem, sipas pozicionit të punës dhe të drejtave të çdo punonjësi/përdoruesi; - Nuk disponon procedura kontrolli apo rregullore, për menaxhimin dhe zhvillimin e ndryshimeve që implementohen në sistem me përfshirjen e autorizimit nga menaxhimi; rezultatet e testimeve, autorizim nga menaxhimi përpara kalimit të ndryshimeve në mjedisin live, rishikimi i menaxhimit të efekteve të çdo ndryshimi, mirëmbajtje e regjistrimeve të përshtatshme; procedura	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të merren masa për hartimin e një Rregulloreje të Përgjithshme mbi Teknologjinë e Informacionit, ku të përfshihen operacionet TI, afatet dhe burimet e nevojshme, kontrollet e brendshme, menaxhimi dhe miratimi i ndryshimeve, kryerja e analizave periodike lidhur me performancën e sistemit, përshkrimet e sakta të punës dhe trajnimet periodike për gjithë punonjësit klasifikuar sipas profilit dhe përgjegjësive përkatëse.

	e kthimit në një hap më përpara (rollback) në rast se diçka nuk shkon mirë si dhe procedurat për kryerjen e ndryshimeve emergjente. Shqyrtimi dhe marrja e masave lidhur me incidentet është bërë rast pas rasti nga specialistët TI. - Nuk disponon analizë të dokumentuar mbi performancën e sistemit në kohë reale apo periodike në funksion të përmirësimeve të tij. - Nuk ka të dokumentuar një procedurë, për përfshirjen e kërkesave të përdoruesve në kërkesat e MNSH. - Mungojnë trajnimet për rritjen profesionale të një stafi të brendshëm të kualifikuar specialistë TI, me qëllim rritjen e nivelit të suportit dhe zvogëlimin në kosto të mirëmbajtjeve. Nuk rezulton e dokumentuar ndarja e detyrave nga nivel drejtorie deri në nivel specialisti, në mënyrë që përmbushja e detyrave dhe përgjegjësia mbi punën e kryer të kenë tregues të matshëm.	
11	Nga auditimi i veprimeve operacionale mbi korrigjimet materiale që DPGJC kryen lidhur me të dhëna jo të sakta të regjistruara për shtetasit, konstatojmë se: - Kërkesat e shtetasve për korrigjime materiale vijnë si rezultat i hedhjes gabim të dhënave në regjistrin elektronik të gjendjes civile, në periudhën kur ka filluar dixhitalizimi për popullimin e regjistrit elektronik në vitin 2010. - DPGJC nuk disponon regjistër, me	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile si institucion qendror që menaxhon të dhënat personale, të veprojë për hartimin dhe miratimin e veprimeve unifikuese, rregulloreve, standardeve, në monitorimin dhe përmirësimin e sistemeve, materialeve trajnues dhe udhëzues për punonjësit dhe zyrave të gjendjes civile si dhe shtetasit Shqiptarë.

	detajet e nevojshme mbi vendimet e marra edhe pse ka një numër të konsiderueshëm vendimesh vetëm për vitin 2017 janë 3,700 vendime për korrigjime materiale, gjë që ka penguar vetë institucionin në analizimin dhe zgjidhjen e rasteve të ngjashme. - Nga auditimi i praktikës së ndjekur për korrigjimin material, konstatohet se duhet një kohë e gjatë, që kërkesa të pasqyrohet në sistem, pasi shërbimi postar dhe ditët e nevojshme për marrjen e një vendimi i cili nuk mund të jetë negativ në momentin që ka një dokumentacion justifikues, kërkon të paktën 20 ditë pune nga momenti i kërkesës deri në pasqyrimin e ndryshimit në sistem.	
12	Nga auditimi mbi gjenerimin e certifikatave nëpërmjet portalit e-albania rezultoi se mungon dokumentimi dhe udhëzimi lidhur me çfarë hapash do të ndjekin institucionet apo qytetarët Shqiptarë, që marrin të dhënat online kur portali e-albania, për shkaqe të njohura ose të panjohura nuk funksionon, ndërkohë që punonjësit e zyrës së gjendjes civile janë urdhëruar me urdhrin nr. 933, datë 27.09.2017 "*Për marrjen e masave për zbatimin e rregullave për përfitimin e certifikatave nëpërmjet shërbimit publik elektronik*", në të cilin kërkohet që zyrat e gjendjes civile të mos lëshojnë më certifikata personale dhe familjare për shtetasit, por ti informojnë ata mbi ofrimin e këtij shërbimi nëpërmjet portalit e-albania.	a. Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile në plotësim të urdhrit nr. 933, datë 27.09.2017 "*Për marrjen e masave për zbatimin e rregullave për përfitimin e certifikatave nëpërmjet shërbimit publik elektronik*", të marrë masat, duke udhëzuar punonjësit dhe shtetasit lidhur me veprimet që duhet të ndiqen kur sistemet (Portali, Regjistri apo çdo sistem i ndërmjetëm) nuk janë në funksion për arsye të ndryshme. b. Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile në bashkëpunim me AKSHI-n, të marrë masat e nevojshme për unifikimin e fushave që gjenden në dy dokumentat personal që gjenerohen nga portali e-albania.

	Gjithashtu, nga verifikime të certifikatës personale/familjare të gjeneruar nga e-albania u konstatuan mospërputhje lidhur me "*Gjendja civile*" dhe "Lidhja *me Kryefamiljarin*", në kundërshtim me nenin 13, të ligjit nr.134/2016 "Për disa shtesa dhe ndryshime në ligjin nr. 10129, në të cilin specifikohet emërtimi mbi gjendjen civile.	
13	Nga auditimi i identifikimit, dokumentimit dhe menaxhimit të incidenteve dhe problemeve në DPGJC u konstatua se nuk janë hartuar rregulla mbi menaxhimin e incidenteve, problemeve dhe institucioni nuk ka të dokumentuar një plan masash për trajtimin e problemeve dhe incidenteve që mund të ndodhin në infrastrukturën TI. Në mungesë të këtyre procedurave të shkruara, problemet dhe incidentet për periudhën nën auditim, menaxhoheshin mbi bazë ngjarjesh dhe nëpërmjet shkëmbimeve verbale dhe nëpërmjet email-eve. Si hallkë monitoruese, nuk ekzistojnë procedura dhe indikatorë të matjes së performancës për gabimet ose incidentet e ndodhura dhe masat reaguese ndaj tyre për të verifikuar efektivitetin e punës së kryer. Në këtë mënyrë, institucioni nuk ka politika të ruajtjes së dokumenteve dhe nuk ka të dokumentuar një plan masash për trajtimin e gabimeve dhe incidenteve që mund të ndodhin në infrastrukturën TI.	Strukturat Drejtuese dhe zbatuese në DPGJC të marrin masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve. Të merren masa për menaxhimin e ndryshimeve dhe dokumentimin e të gjithë procesit të ndryshimeve. Institucioni të identifikojë risqet me efekt negativ në TI dhe veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura.
14	Nga auditimi se si DPGJC Identifikon dhe menaxhon risqet në teknologjinë e	Strukturat drejtuese të DPGJC në bashkëpunim me Drejtorinë e Auditit të

	informacionit, u konstatua se DPGJC nuk disponon një regjistër risku për teknologjinë e informacionit në kundërshtim me ligjin nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar, Udhëzimi nr. 30, datë 27.12.2011 "*Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik*", i ndryshuar, Udhëzimin nr. 21, datë 25.10.2016 "*Për nëpunësit zbatues të të gjitha niveleve*", UMF nr. 16, datë 20.07.2016 "*Për përgjegjësitë dhe detyrat e koordinatorit të menaxhimit financiar dhe kontrollit dhe koordinatorit të riskut në njësitë publike*". Nga strukturat drejtuese të Drejtorisë nuk është iniciuar asnjë proces për identifikimi i risqeve të lidhura me projektet e investuara, ku të përcaktohej lista e risqeve, detyrat dhe përgjegjësitë për menaxhimin e risqeve, aktivitetet/funksionet e DPGJC të ofruara nëpërmjet aplikacioneve si dhe menaxhimi i tyre. DPGJC nuk disponon asnjë mekanizëm për vlerësimin e proceseve të kompjuterizuara dhe sigurisë së të dhënave në funksion të ofrimit të shërbimeve dhe vazhdimësisë së aktivitetit, si elementë shumë të rëndësishëm të analizës së riskut.	Brendshëm, të marrin masat e nevojshme për hartimin dhe dokumentimin e një plan-veprimi për identifikimin, raportimin, trajtimin dhe dokumentimin e risqeve, në përputhje me ligjin nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar, Udhëzimin nr. 30, datë 27.12.2011 "*Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik*", i ndryshuar, për shmangien, adresimin, transferimin apo pranimin e risqeve të identifikuara, si dhe monitorimin periodik për zbatimin e masave të marra nga sektori përgjegjës.
15	Nga auditimi u konstatua se DPGJC, si institucion përgjegjës për të dhënat e Regjistrit Kombëtar të Shtetasve Shqiptar, nuk rezulton të ketë asnjë kërkesë apo marrëveshje dypalëshe të	a. Strukturat drejtuese të DPGJC në bashkëpunim me MB dhe Komisionerin për Mbrojtjen e të Dhënave Personale, të marrin masa për përditësimin në mënyrë të vazhdueshme të Aneksit 1 të

	dokumentuar me institucionin/organin përkatës, për aksesin në të dhënat personale në kundërshtim me përmbledhësen e miratuar nga MB me Komisionerin për Mbrojtjen e të Dhënave Personale, aneksi 1 i udhëzimit nr. 95, datë 07.04.2014 "*Për përcaktimin e institucioneve dhe organeve që marrin të dhëna personale nga shërbimi i gjendjes civile, si dhe mënyrën, llojin dhe sasinë e informacionit që duhet të marrin*" dhe me nenin 3 të ligjit nr. 10129, datë 11.05.2009 "*Për Gjendjen Civile*" i ndryshuar.	Udhëzimit nr. 95, datë 07.04.2014 "*Për përcaktimin e institucioneve dhe organeve që marrin të dhëna personale nga shërbimi i gjendjes civile, si dhe mënyrën, llojin dhe sasinë e informacionit që duhet të marrin*". b. Drejtori i Drejtorisë së Përgjithshme i Gjendjes Civile, në vazhdimësi të autorizojë aksesin mbi të dhënat në përputhje me përmbledhësen e përditësuar dhe miratuar prej tij dhe Komisionerit për Mbrojtjen e të Dhënave Personale në përputhje me kërkesat e ligjit nr. 10129, datë 11.05.2009 "*Për Gjendjen Civile*" i ndryshuar dhe Udhëzimit nr. 95, datë 07.04.2014 "*Për përcaktimin e institucioneve dhe organeve që marrin të dhëna personale nga shërbimi i gjendjes civile, si dhe mënyrën, llojin dhe sasinë e informacionit që duhet të marrin*".
16	Nga auditimi u konstatua se DPGJC nuk ka të ndërtuar një strategji të rimëkëmbjes nga katastrofat si dhe nuk ka plane të shkruara që përcaktojnë vazhdimësinë e proceseve të punës. Mungesa e Strategjisë së Teknologjisë së Informacionit ka sjellë mos pasqyrimin qartë të objektivave të DPGJC lidhur me infrastrukturën TI dhe burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen. DPGJC, nuk rezulton të ketë dokumentim/implementim të politikave mbi sigurinë e informacionit duke patur parasysh disa elementë si: - Përkufizim dhe kategorizim të	Strukturat drejtuese në DPGJC, duke marrë në konsideratë kohën dhe burimet e nevojshme të marrin masa për: a. Hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektiva e Drejtorisë; b. Ndërtimin dhe hartimin e Planeve të Vazhdimësisë së Biznesit duke përfshirë planet për backup dhe rimëkëmbjen nga katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat. Gjithashtu, të merren masa për hartimin e planit të sigurisë së informacionit dhe implementimin e tij duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TI. Planifikimi dhe testimi i

	sigurisë së informacionit me objektivat, qëllimin, konfidencialitetin e të dhënave, parimet dhe standardet, të përcaktuara në ligjin nr. 10129, datë 11.05.2009 "*Për Gjendjen Civile*", i ndryshuar. - Përkufizim të përgjegjësive të përgjithshme dhe specifike për të gjitha aspektet e sigurisë së informacionit; - Të përdorimit të aseteve të informacionit dhe aksesit në informacion; - Procedurat e backup-it, trajnimit dhe edukimit mbi sigurinë; - Planet e vazhdueshmërisë së punës (BCP) dhe rimëkëmbjes nga katastrofat (DRC); - Dokumentim të ndikimit nga ndërprerjet në lidhje me: kohën, burimet dhe sistemet e tjera të lidhura me sistemin e RKGJC; - Planet e sigurisë.	sistemeve TI të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen.
17	DPGJC është përgjegjëse për të siguruar që të gjitha të dhënat e ruajtura në serverat e DPGJC, t'u bëhet backup (kopje) e rregullt në përputhje me procedurat e përcaktuara. Nga auditimi u konstatua se: - Ruajtja e backup në vende jashtë godinës së DPGJC-së (MB), në distancë realizohet tek AKSHI në Qendrën e Vazhdimësisë së Biznesit; - Kopjet (backup) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme;	DPGJC të marri masa për kryerjen dhe testimin periodik të backup-it për sistemet, pajisjet kompjuterike dhe të dhënat që disponon, për të siguruar vazhdimësinë e ofrimit të shërbimeve në rast ndërprerje.

	- Procedurat e rikthimit (restore) të të dhënave nuk testohen për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar.	
18	Nga auditimi i gurmëve të komunikimit me zyrat e gjendjes civile u konstatua se: - Nuk ka një procedurë standarde se si veprohet për komunikimin e përdoruesve të sistemit RGJKC me Drejtorinë e Përgjithshme të Gjendjes Civile në lidhje me problematikat e ndryshme që hasen gjatë punës. Gjithashtu këto komunikime, si dhe zgjidhjet e problemeve nuk ruhen, duke humbur kështu eksperiencë për zgjidhjen e problemeve të njëjta. - Nga ana e DPGJC-së nuk disponohet dokumentacion për kontrollin e konfigurimeve dhe rregullimet e aplikacioneve TI. Nga auditimi i dokumentacionit të vënë në dispozicion u konstatua: - Nuk ka një rregullore apo përcaktim të saktë për sa i përket llojit të profileve për përdoruesit. Rastet vlerësohen në vazhdimësi dhe në bazë të situatës, duke u konfirmuar më pas nga Drejtori i Gjendjes Civile. Kjo mënyrë e përcaktimit rast pas rasti të profilit të përdoruesit nuk jep garanci të arsyeshme, për mirëfunksionimin e hierarkisë së përdoruesve në sistemin e RKGJC-së.	c. Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të merren masa për hartimin e një procedure standarde për mënyrën e komunikimit me zyrat e Gjendjes Civile, si dhe të ruhen e të dokumentohen zgjidhjet për problemet e hasura, kontrollet e konfigurimeve dhe rregullimet e aplikacionit, veprim i cili do të mundësojë krijimin e një arkive me eksperiencat e mëparshme. d. Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të merren masa për standardizimin e llojit të profilit të user-ave, veprim i cili ndihmon në uljen e riskut të dhënies së gabuar të aksesit për përdoruesit si dhe garantimin e mirëfunksionimit të hierarkisë së përdoruesve në sistemin e RKGJC-së.
19	Nga auditimi u konstatua se nuk ka politika apo procedura për zbulimin dhe	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të merren masa për

	trajtimin e ndërhyrjeve, si dhe nuk ka kontrolle rutinë periodike. Në rast sinjalizimi, verifikohen loget nga Sektori i Zhvillimit në DPGJC në bashkëpunim me operatorin ekonomik mirëmbajtës së sistemit. Në lidhje me këtë, edhe pse ekziston një sektor kontrolli të procedurave i cili verifikon procedurat fizike dhe ato elektronike, niveli i trajtimit të ndërhyrjeve konsiderohet i pamjaftueshëm duke marrë në konsideratë rëndësinë kombëtare të sistemit të DPGJC.	hartimin e një procedure dhe caktimin e personave përgjegjës për zbulimin, trajtimin dhe monitorimin e vazhdueshëm të ndërhyrjeve. Sistemi i RKGJC-së është një sistem me rëndësi kombëtare si dhe konsiderohet si sistem me të dhëna sensitive për shoqërinë, e për pasojë kontrollet periodike janë të detyrueshme për ruajtjen e sistemit dhe të dhënave që mban.
20	DPGJC nuk ka caktuar Administrator sistemi për asnjërin prej tyre, veprim i cili rrezikon menaxhimin dhe vazhdimësinë e punës, kryesisht në rastet kur nuk ka mirëmbajtje nga kompanitë e specializuara të kontraktuara (aktualisht sistemi i RKGJC është pa mirëmbajtje) si dhe nuk ka një pikë reference në lidhje me trajtimin e problemeve të ndryshme që dalin gjatë punës.	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile të merren masa për emërimin apo kalimin e një punonjësi me detyrë Administrator i sistemit, duke shërbyer si pikë reference në lidhje me trajtimin e problemeve të ndryshme të dala gjatë punës, si dhe të mundësojë vazhdimësinë e sistemit në rastet e përkohshme kur të jemi në kushtet e mungesës së mirëmbajtjes së sistemit nga kompanitë e specializuara.
21	Nga auditimi i të dhënave të sistemit të RKGJC me 4,537,448 rekorde të sistemit “Regjistrit kombëtar të gjendjes civile” me teknikat CAAT rezultoi: Ekzistojnë 30,249 fusha të paplotësuara për “adresën”, 8 fusha të paplotësuara për “ID familjare”, 28,858 fusha të paplotësuara për “lidhja me kryefamiljarin”; Ekzistojnë 588 rekorde të përsëritura U konstatuan rekorde jashtë logjikës; 5,555 raste kombësia e të cilave është	Nga ana e Drejtorisë së Përgjithshme të Gjendjes Civile: a. Të analizohen rastet e konstatuara, duke dhënë zgjidhje të cilat të shërbejnë jo vetëm për rregullimet momentale të problematikave por gjithashtu për krijimin e një kontrolli paraprak të këtyre inputeve edhe në vazhdimësi. b. Të merren masa që në bashkëpunim me institucionet vendore dhe të tjera sipas nevojës, të kryejnë verifikimet e nevojshme për shtetasit mbi 100 vjec duke mos i ndërprerë automatikisht të

	shënuar XXX, XXA apo XXZ; Fusha "*radha në familje*" në 2,787 raste ka vlerë "0", dhe në mjaft raste ka numra që nuk përputhen minimalisht me numrin e anëtarëve në familje; u konstatuan 6 emra me përbërje "Xxx", nga të cilët 1 prej tyre ka edhe mbiemrin "*Xxx*", dhe 1 rast ka edhe emrin e të atit "Xxx". - Numri i personave me moshë mbi 100 vjeç rezultoi 8,674, nga të cilët 485 janë të bllokuar dhe nuk marrin shërbim, ndërsa 8,189 persona rezultojnë nga sistemi si marrës të shërbimit (mosha e personave të filtruar arrin deri në afërsisht 150 vjeç). Referuar të dhënave nga ISSH, janë në kushtet e përfitimit të pensionit rreth 603 persona. Bazuar në komunikimet verbale me përfaqësues të DPGJC, personat mbi 100 vjeç u hiqet e drejta për të votuar deri në momentin që vetëdeklarohen. Ky veprim është konsideruar diskriminues edhe nga raporte periodike të OSBE-ODIHR, për arsye se çdo shtetas i Republikës së Shqipërisë ka të drejtën e votës. - Në sistemin e DPGJC, mungojnë parametrizime të fushave të detyrueshme"*mandatory fields*", cfarë ndikon në numrin e konsiderueshëm të fushave të paplotësuara si dhe mangësi në "*logical conditions*", duke pranuar të dhëna shpesh herë jashtë logjikës së përdorimit të sistemit. - Kontrollet e inputit të të dhënave nga sistemi nuk japin siguri të arsyeshme për marrjen e të dhënave 100% të sakta.	drejtën e votimit në përputhje me parimet e mosdiskriminimit dhe të drejtave të barabarta para ligjit.

3. DEPARTAMENTI I ADMINISTRATËS PUBLIKE DAP.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: "**Departamenti i Administratës Publike"**

Përgatitur: 10 Shtator 2018

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 551/1, datë 12/06/2018.

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Meald Habazaj, anëtar
3. Aldo Kita, anëtar
4. Elsona Papadhima, anëtare

Periudha e Auditimit: 01.01.2017 – 31.12.2017
Afati i auditimit: 09.05.2018 – 16.07.2018

ÇFARË KEMI AUDITUAR

Fushat e auditimit

Auditimi i funksionimit të Qeverisjes TIK

Vlerësimi i burimeve njerëzore në strukturat TIK

Auditimi i projekteve e investimeve të teknologjisë së informacionit

a. Identifikimi, hartimi i nevojave dhe kritereve të vendosura për mallra dhe shërbime në TIK

b. Auditimi i Marrëveshjeve të Nivelit të Shërbimit (MNSH).

Auditimi i Sigurisë së Informacionit

a. Identifikimi dhe menaxhimi i risqeve në TIK

b. Verifikim i shkallës së sigurisë së aplikacioneve.

Zbatimi i rekomandimeve të auditimeve të mëparshme.

Të ndryshme të dala gjatë auditimit

Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve.

PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Departamenti i Administratës Publike është institucioni publik përgjegjës për: menaxhimin dhe implementimin e shërbimit civil në të gjitha institucionet e administratës qendrore; hartimin dhe implementimin e politikave në fushën e pagave dhe ndërtimit të institucioneve të administratës publike si dhe hartimin dhe zbatimin e politikave dhe programeve të përgjithshme të trajnimit të zbatueshme për administratën publike në tërësi.

Se fundmi DAP ka investuar për implementimin e një sistemi të teknologjisë së informacionit për menaxhimin e proceseve të dosjeve dhe jo vetëm, të punonjësve të administratës publike i quajtur HRMIS.

Duke pasur parasysh investimet e kryera nga DAP në informatizimin e të dhënave të administratës publike si dhe rolin e TI në menaxhimin e burimeve njerëzore u krye ky projekt Auditimi.

Në përfundim të auditimit për 11 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit

Më hollësisht:

OPINIONI I AUDITIMIT:

Baza ligjore për krijimin e Opinionit të Auditimit mbështetet në Standardet Kombëtare dhe Ndërkombëtare të Auditimit (ISSAI 1 Neni 22, Ligjin e KLSH Nr.154/2014 Neni 3 dhe 14, Manualin e Auditimit të Teknologjisë së Informacionit (WGITA), COBIT 4.1, ISSAI 5300.6, 8 dhe 12.2, 16.19, 21.1, 23, ISSAI 100.36,48, ISSAI 5310). Grupi i auditimit pas shqyrtimit të të dhënave dhe dokumentacionit të vënë në dispozicion nga DAP, arriti në Opinionin se:

DAP ka zhvilluar sisteme të Teknologjisë së Informacionit në funksion të përmbushjes së objektivave të institucionit duke shfrytëzuar burimet e vëna në dispozicion si dhe kryer thithjen e investimeve të konsiderueshme nga donatorët e huaj për zhvillimin dhe mirëmbajtjen e infrastrukturës TI. Megjithatë investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht problemet e sigurisë së informacionit, sigurimin e Vazhdueshmërisë së veprimtarisë së Institucionit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat.

Me gjithë përpjekjet e bëra, DAP duhet të vazhdojë të intensifikojë përpjekjet duke përdorur mjetet e kompetencat që i jep ligji për shtrirjen e sistemit HRMIS në gjithë institucionet Qendrore, të Pavarura dhe ato Lokale.

Shkalla e rritjes së ndërveprimit të sistemit HRMIS me sistemet e tjera ngelet një sfidë për gjithë institucionet e parashikuara të veprojnë me këtë sistem.

Nr.	Gjetje nga auditimi	Rekomandimi
1	**Nga verifikimi i dokumentacionit për zbatimin e rekomandimeve të auditimit të mëparshëm të dërguara në Departamentin e Administratës Publike nga KLSH me shkresën nr. prot. 69/17 datë 29.09.2017 në mënyrë të përmbledhur zbatimi i rekomandimeve paraqitet si më poshtë:** Për përmirësimin e mëtejshëm te rezultateve janë lënë 18 rekomandime, të përmbledhura në 6 grupe, të cilat janë pranuar plotësisht, janë zbatuar pjesërisht 2 dhe janë në proces zbatimi 4 rekomandime për të cilat janë lënë rekomandimet përkatëse.	
2	Nga auditimi u konstatua se për vitin 2017 për përdoruesit e sistemit janë kryer rreth 2 herë më shumë trajnime se ato të zhvilluara gjatë vitit 2016, trendi në rritje vazhdon edhe për trajnimet e kryera gjatë vitit 2018. Ndryshimet e strukturës së TI-së përgjatë vitit 2017 e në vazhdim, mbështetur në Urdhrit e KM nr. 178, datë. 10.10.2017 dhe VKM nr. 673, datë. 22.11.2017 mbartin riskun e mos kryerjes së funksionaliteteve të kësaj strukturë TI si rezultat i frekuencës së shpeshtë të ndryshimeve me impakt e mos përmbushjen e objektivave dhe plotësimit të misionit të DAP. Qenia e strukturave TI të përqendruara për vitin 2018 e në vijim (tek AKSHI) zgjidh problemet e mungesës në staf TI të vërejtura në DAP gjatë vitit 2017, por mbart risqet që vinë nga menaxhimi të tyre nga dy struktura (DAP dhe AKSHI).	DAP në cilësinë e autoritetit përfitues së shërbimeve të mirëmbajtjes dhe zhvillimit të sistemeve të Teknologjisë së Informacionit nga AKSHI-n të marrë masa institucionale dhe ndërinstitucionale për menaxhimin e ndryshimeve të burimeve njerëzore të lidhura me teknologjinë e informacionit nëpërmjet lidhjes dhe ndjekjes së marrëveshjeve dypalëshe.
3	Nga auditimi u konstatua se gjendja e infrastrukturës TIK në Departamentin e Administratës Publike nuk garanton funksionimin normal të sistemeve, ajo është e vjetruar dhe amortizuar, investimet e kryera në këtë fushë janë të pa pamjaftueshme, përpjekjet për identifikimin e nevojave duke bashkëpunuar edhe me institucione të specializuara të fushës (AKSHI) rezultojnë se nuk kanë arritur të zgjidhin problemet e financimit për garantimin e	DAP me qëllim përthithjen e investimeve nga buxheti i shtetit dhe nga donatorët në bashkëpunim me AKSHI-n të marri masa për kryerjen e vlerësimit të nevojave për investime në sistemet e informacionit që mbështesin veprimtarinë e institucionit, si dhe të hartojnë projekte për

	vazhdimësisë së punës.	ngritjen e një infrastrukture TIK që siguron Vazhdueshmërinë e veprimtarisë së Institucionit dhe Rimëkëmbjen nga Katastrofat.
4	Grupi i auditimi konstaton se përdoruesit e HRMIS (burimet njerëzore të Institucioneve publike) të cilët janë të lidhur në "mënyrë të sigurt" me aplikacionin nëpërmjet Web VPN nuk arrijnë të shikojnë raportet që gjeneron sistemi, me pasojë mos shfrytëzimin e këtyre raporteve në menaxhimin me efektivitet, efiçencë dhe ekonomicitet të burimeve njerëzore në plotësimin e misioneve dhe arritjen e objektivave të institucioneve përkatëse.	DAP me qëllim përdorimit me efektivitet, efiçencë dhe ekonomicitet të burimeve njerëzore nga institucionet që përdorin sistemin HRMIS në funksion të plotësimit të misioneve dhe arritjes së objektivave përkatëse të marri masa për sigurimin jo vetëm të lidhjeve të sigurta por edhe ofrimin e mundësive për shfrytëzimin e raporteve që gjenerohen nga ky sistem.
5	Nga analiza e përdorueseve aktiv dhe të bllokuar në sistem për vitin 2017, konstaton se drejtuesit e institucioneve nuk informojnë ose informojnë me vonesë mbi largimin nga detyra të burimeve njerëzore përdorues të HRMIS. Për vitin 2017, nga 302 përdorues të hapur në sistemin HRMIS, ndodhen në statusin të bllokuar 34 përdorues, mos mbyllja e tyre përbën cenim të sigurisë së sistemit dhe është në kundërshtim me Vendimin Nr. 117, datë 05.03.2014, "Mbi praktikat që duhet të ndjekin institucionet për informimin e DAP-it mbi largimin e përdoruesve të HRMIS".	DAP në cilësinë e autoritetit i cili menaxhon sistemin HRMIS në bashkëpunim me institucionet përdoruese të sistemit të marri masa për evidentimin dhe vënien para përgjegjësisë të çdo rasti të thyerjes se përcaktimeve të Vendimit Nr. 117, datë 05.03.2014, "Mbi praktikat që duhet të ndjekin institucionet për informimin e DAP-it mbi largimin e përdoruesve të HRMIS".
6	Përdoruesit e sistemi HRMIS përgjegjës për hedhjen e të dhënave janë punonjës në strukturat e burimeve njerëzore dhe të financës të Institucioneve përkatëse. Nga analizimi i bazës së	DAP në cilësinë e autoritetit i cili menaxhon sistemin HRMIS në bashkëpunim me institucionet përdoruese të

	të dhënave të sistemit HRMIS rezulton se ky sistem për vitin 2017 ka patur mesatarisht 643 përdorues. Nga analiza në vite e përdorueseve të sistemit rezulton një trend rritës i numrit të përdorueseve Grupi i auditimi konstaton se ky sistem aksesohet nga përdoruesit e institucioneve me një frekuencë të çrregullt dhe përdoruesit e tij përqendrojnë punën vetëm në muajt e fundit të vitit, duke rënduar sistemin në këtë periudhë me pasojë mos pasqyrimin në sistem të gjendjes reale të burimeve njerëzore.	sistemit të marri masa për evidentimin dhe vënien para përgjegjësisë të rasteve të mos plotësimit ritmik dhe në kohë reale të sistemit me informacion.
7	**Nga analizimi i bazës së të dhënave të sistemit HRMIS mbi shkallën e plotësimit të dosjeve të punonjësve për Institucionet Vendore për vitin 2017 rezulton se Institucionet Vendore paraqiten me një shkallë të ulët të përdorimit të sistemit HRMIS.** Grupi i auditimi konstaton se shkaqet e këtij mospërdorimi janë: a. Mos qenia e sistemeve të pushtetit lokal në gov.net. b. Shkalla e ulët e informatizimit në këto institucione. c. Përdorimi në disa raste i programeve të tjerë për menaxhimin e burimeve njerëzore. Më hollësisht situata në Institucionet e Qeverisjes Vendore paraqiten: - 24 Institucione rezultojnë me mospërdorim total të sistemit HRMIS - 21 Institucionet rezultojnë me përdorim më të ulët se mesatarja e përdorimit nga Institucionet e Qeverisjes Vendore të sistemin HRMIS	**b. DAP në cilësinë e autoritetit administrues për sistemin HRMIS në bashkëpunim me AKSHI-n dhe institucionet vendore përdoruese të sistemit të marri masa për:** a. Kapërcimin e pengesave të rrjedhura nga mos qenia e sistemeve të pushtetit lokal në gov.net. b. Analizimin e situatës dhe nxitja e investimeve për informatizimit në këto institucione. c. Rishikimin e kuadrit ligjor për mos lejimin e investimeve në programe të tjerë për menaxhimin e burimeve njerëzore.
8	**Institucionet e Administratës Qendrore dhe Institucionet e Pavarura**:	DAP në cilësinë e autoritetit i cili menaxhon sistemin

	- Nga analizimi i bazës së të dhënave të sistemit HRMIS mbi shkallën e plotësimit të dosjeve të punonjësve për Institucionet e Pavarura rezulton se gjatë vitit 2017 ka një përmirësim të ndjeshëm për plotësimin e dosjeve krahasuar me një vit më parë. Nga analizimi i bazës së të dhënave për këto institucione rezulton se ka një përdorim mesatar prej 73% të sistemit HRMIS, por 2 Institucione rezultojnë me mospërdorim total të sistemit HRMIS - Nga analizimi i bazës së të dhënave të sistemit HRMIS mbi shkallën e plotësimit të dosjeve të punonjësve për Institucionet e Administratës Qendrore rezulton se gjatë vitit 2017 ka një përmirësim të ndjeshëm nga këto institucione, për plotësimin e dosjeve, krahasuar me një vit më parë. Situata për 6 mujorin e parë të viti 2018 paraqitet pa ndryshime në krahasim me një vit më parë. Këto institucione përbejnë 755 përdorues me një shkallë mesatare përdorimi në Sistemit HRMIS prej 60 %. Grupi i auditimit konstaton se me gjithë arritjet, vërehen diferenca të theksuara të grupuara si vijon: - 271 (36%) Institucione të Administratës Qendrore rezultojnë me shkallë përdorimi 0%. - 13 (2%) Institucione të Administratës Qendrore rezultojnë me shkallë përdorimi nga 1% -8%. - 37 (5%) Institucione të Administratës Qendrore rezultojnë me shkallë përdorimi nga 11% - 59%, që është nën mesataren e përdorimit nga Institucionet e Administratës Qendrore - 434 (57%) Institucione të Administratës Qendrore rezultojnë me shkallë përdorimi nga 60% - 100%.	HRMIS në bashkëpunim me institucionet përdoruese të sistemit të marri masa për evidentimin e shkaqeve specifike, të cilat pengojnë zgjerimin e përdorimin e sistemit si dhe bashkëveprojnë veprimet me Ministrinë e Financave dhe Ekonomisë dhe AKSHI-n për ndërprerjen e investimeve paralele që këto institucione kryejnë për ngritjen dhe mirëmbajtjen e këtyre sistemeve të menaxhimit të Burimeve Njerëzore.

9	Grupi i auditimit konstaton DAP në përpjekje për të mbajtur dhe zhvilluar sistemin ka kryer edhe po kryen manualisht detyra të cilat janë përgjegjësi e punonjësve të burimeve njerëzore dhe financës së institucioneve të pushtetit qendror, vendor dhe të pavarura të cilët janë përdoruesit e sistemit (Hapja e një institucioni, hedhjen e Nipt, Kodi i njësisë qeveritare, Kodi i ministrisë se Linjës, Kodi i programit, Kodet e thesarit etj).	DAP në cilësinë e autoritetit i cili menaxhon sistemin HRMIS të hartojë një plan veprimi ku të identifikohen masat për ndërprerjen e kryerjes së detyrave të përdoruesve të sistemit nga punonjësit e DAP duke e koordinuar këtë veprim në intensifikimin e trajnimeve për rritjen e kapaciteteve njerëzore të përdoruesve të sistemit HRMIS.
10	Nga analiza e bazës së të dhënave të sistemit HRMIS u konstatua mospërputhje në datën për rastet e ristrukturimit e një institucioni ekzistues. Mos respektimi i afateve ligjore të hedhjes së strukturës nga autoriteti përgjegjës i miratimit të strukturës sjell impakt financiar në rekordet e lidhjes dhe shkëputjes së marrëdhënieve financiare të punonjësve.	DAP në cilësinë e autoritetit i cili menaxhon sistemin HRMIS në bashkëpunim me AKSHI-n, për rritjen e efektivitetit, efiçencës dhe ekonomicitit të burimeve njerëzore dhe plotësimin e misioneve dhe arritjen e objektivave të institucioneve publike të marri masa për rritjen e ndërveprimit me sistemet që kanë baza të dhënash shtetërore si dhe të kryej investimeve në sisteme inteligjente për analizimin e bazës së të dhënave për monitorimin e aktivitetit të përdoruesve.
11	Matja e performancës së aplikimeve(online) për vendet vakante. Nga analizimi i të dhënave të nxjerra nga programi i aplikimeve për vendet vakante të shërbimit civil për vitin 2017, rezulton se janë	DAP në cilësinë e autoritetit i cili menaxhon sistemin HRMIS të marri masat e nevojshme organizative duke kryer propozimet e nevojshme për ndryshime ligjore me

	zhvilluar: - 242 procedura konkurrimi për 481 pozicione të kategorisë ekzekutive, të ulët dhe të mesme drejtuese. - Gjatë vitit 2017 janë prodhuar mbi 3900 teza duke përdorur aplikacionin SPEEDWELL Software Question Bank për 240 procedura të ndryshme të shërbimit civil (mesatarisht *një teze provimi ka 30 pyetje me përgjigje ABCDE*). - Në testimet me shkrim janë paraqitur mbi 1500 kandidatë tezat e të cilëve janë skanuar duke përdorur skanerin SCANTRON iNsight 4 ES me barkode dhe për të cilët është bërë vlerësimi elektronik përmes përdorimit të aplikacionit SPEEDWELL Software Multi Quest. Grupi i auditimit konstaton se DAP ka zbatuar kornizën ligjore (*Vendimin e KM nr. 108, datë 26.2.2014 "Për planin vjetor të pranimit në shërbimin civil" si dhe nga ligji 152/2013 "Për nëpunësin civil", Neni 18 "Plani vjetor i pranimit në shërbimin civil"..... Këshilli i Ministrave, jo më vonë se fundi i muajit shkurt, miraton planin vjetor të pranimit në institucionet e administratës shtetërore*) për planifikimin dhe aplikimin për vendet vakante të vitit 2017. Nga analiza e të dhënave të aplikimeve rezulton se ato kanë një shpërndarje jo të rregullt ku më të theksuara paraqiten dy intervale të muajve të parë të vitit (mungesa e planit të miratuar) si dhe periudha korrik-gusht (periudhë e pushimeve). Fenomeni i mësipërm ka një impakt negativ në procesin e plotësimit të vendeve vakante	qëllim koordinimin e hartimit të Planit vjetor të pranimit në shërbimin civil (jo më vonë se mesi i muajit janar) me atë të miratimit të Buxhetit të Shtetit.

4. QENDRA KOMBËTARE E BIZNESIT - QKB.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: Qendrën Kombëtare të Biznesit

Përgatitur:

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 550/2, datë 31.05.2018

Auditimi është kryer nga:

1. Brunilda Zeneli, Përgjegjëse Grupi
2. Elira Cukalla, Audituese e Lartë
3. Benard Haka, Auditues i Parë
4. Bledi Dervishaj, Auditues i Parë
Periudha e Auditimit: 01.01.2017 deri në 31.12.2017

Afati i auditimit: 01.06.2018 deri në datë 18.07.2018

ÇFARË KEMI AUDITUAR
Fushat e auditimit

- "Auditimi i Marrëveshjeve të Nivelit të Shërbimit (MNSH)"
- "Auditimi i Operacioneve në TIK";
- "Auditimi i Sigurisë së Informacionit"
- "Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output dhe shkalla e sigurisë së përdoruesve".

Auditimi ka përfunduar dhe është evaduar subjekti ka dërguar përgjigje në afat për ndjekjen e rekomandimeve

PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Projekti i auditimit, për auditimin e Sistemeve të Teknologjisë së Informacionit, në Qendrën Kombëtare të Biznesit, është pjesë e Planit Vjetor të auditimit të KLSH-së, si dhe e Planit Mujor, Qershor 2018. Projektimi i këtij auditimi, është bërë bazuar në një analizë risku, si gjatë hartimit të planit vjetor, po ashtu edhe gjatë hartimit të Programit të Projektit të Auditimit, ku KLSH, ka vlerësuar si të rëndësishëm auditimin e QKB-së, për shkak të rëndësisë së veçantë të shërbimit që ofron, administrimit të Regjistrit Elektronik Tregtar dhe Regjistrit Elektronik të Lejeve dhe Licencave në nivel kombëtar

Qendra Kombëtare e Biznesit në vijim (QKB) është institucion në varësi të Ministrit të Financave dhe Ekonomisë, i krijuar në bazë të Ligjit nr. 131/2015 "Për Qendrën Kombëtare të Biznesit", si rezultat i bashkimit të dy institucioneve, Qendrës Kombëtare të Licencimit dhe Qendrës Kombëtare të Regjistrimit.

QKB është institucioni i vetëm përgjegjës për regjistrimin e biznesit dhe të lejeve/licencimit dhe autorizimeve në Shqipëri dhe shërben si sportel me një ndalesë ku kryhen të gjitha proceset e regjistrimit, lejeve, licencimit dhe autorizimeve të biznesit, duke përfshirë dhe regjistrimin për efekt të taksave në nivel kombëtar dhe vendor, sigurimin shëndetësor e shoqëror dhe inspektoratin e punës, leje, licencave dhe autorizimeve për kategori të ndryshme.

QKB-ja, funksionon në bazë të një sistemi elektronik të integruar të dhënash që realizon lidhjen ndërmjet sporteleve të shërbimit në rrethe me zyrën qendrore të QKB-së në Tiranë. Sistemi i regjistrimit u krijon mundësinë bizneseve të regjistrohen brenda 24 orëve dhe koordinon të dhënat duke ju dhënë mundësinë subjekteve të interesuara të informohen në kohë reale, për sa i përket statusit të aplikimit të tyre. Sistemi në fjalë është bazë të dhënash shtetërore dhe është i regjistruar pranë ARK me nivel sigurie L-D3I1K0.

Nisur nga rëndësia e të dhënave që përpunon dhe menaxhon QKB por dhe nga impakti që ka shërbimi i ofruar nga QKB kundrejt bizneseve, u propozus që ky subjekt të merret në konsideratë për tu audituar për vitin 2018.

Në përfundim të auditimit për 22 gjetjet u lanë rekomandimet përkatëse dhe u hartua opinioni i auditimit.

Më hollësisht:

<u>OPINIONI I AUDITIMIT:</u>

Opinioni mbi funksionimin e Sistemeve të Teknologjisë së Informacionit në Qendrën Kombëtare të Biznesit, është bazuar në ligjin nr. 154/2014, "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit", ISSAI 5300, Manualin e Auditimit TIK, praktikat më të mira si dhe në Standardet e Auditimit ISSAI 400.

Nga auditimi i funksionimit të Sistemeve të Teknologjisë së Informacionit, sa i takon shkallës së zbatueshmërisë nga subjekti "Qendra Kombëtare e Biznesit", të ligjeve dhe rregulloreve, politikave, standardeve të vendosura u konkludua se, janë marrë masa rregullative dhe organizative për garantimin e shërbimeve dhe funksionaliteteve për të garantuar disponibilitetin e sistemeve të informacionit që disponon, në shërbim të biznesit, por ka edhe mangësi të cilat nuk rezultojnë materiale përsa i përket rëndësisë, konkretisht:

- mbivendosje të akteve ligjore, duke sjellë gjenerim të të dhënave parësore për të njëjtin qëllim nga dy institucionet QKB dhe DPT, në kundërshtim me ligjin "Për bazat e të dhënave shtetërore", si dhe duke ndikuar negativisht në lehtësimin e procedurave për biznesin;

- mungesë të komunikimit me sistemin e Drejtorisë së Përgjithshme të Tatimeve dhe njësitë vendore për shkëmbimet e të dhënave në kohë reale, të cilat rezultojnë si arsyet kryesore, për një volum të lartë të përpunimit të të dhënave, përqendruar në zyrat qendrore;

- është dakordësuar që kodet NVE (Nace) të dërgohen elektronikisht nga DPT në QKB-së, të azhurnuara në rast verifikimi dhe konstatimi nga Administrata Tatimore, në një kohë që këto të dhëna në Regjistrin Tregtar reflektohen si të dhëna parësore që i përkasin themelimit dhe veprimtarisë së subjekteve tregtare kodet NVE (NACE), referuar VKM nr. 863, datë 21.10.2015 "Për krijimin e bazës të të dhënave shtetërore të qendrës kombëtare të regjistrimit, regjistri tregtar";

- një nivel të gabimit të inputit, si rezultat i mosfunksionimit në masën e duhur të sistemit të kontrollit të brendshëm;

Nr.	Gjetje nga auditimi	Rekomandimi
1	Nga auditimi lidhur me Planin Strategjik të Teknologjisë së Informacionit rezulton se, Qendra Kombëtare e Biznesit nuk ka të ndërtuar një Plan Strategjik të Teknologjisë së Informacionit, çfarë sjell mos pasqyrimin të qartë të objektivave të QKB, lidhur me sigurinë institucionale dhe infrastrukturën TIK, objektivat strategjikë për burimet njerëzore të strukturës së TIK në QKB, si dhe në degët rajonale në lidhje me burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen e tyre.	QKB në bashkëpunim me Drejtorinë e Inovacionit dhe Regjistrave si dhe me strukturat këshilluese mbi TIK, të marrë masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit, duke marrë në konsideratë kohën, burimet e nevojshme dhe rishikimin vjetor të indikatorëve të performancës së ecurisë së objektivave.
2	Nga auditimi lidhur me Planin e Rimëkëmbjes nga Katastrofat, QKB si institucion që administron të dhëna me rëndësi për regjistrimin dhe licencimin në dy sisteme informacioni (QKR dhe QKL), përcaktuar në ligjin organik që rregullon regjistrimin dhe licencimin e biznesit, rezulton se nuk ka qendër të rimëkëmbjes nga katastrofat (DRC) për	QKB, duke marrë në konsideratë kohën dhe burimet e nevojshme të marrë masa për ndërtimin dhe hartimin e Planeve të Vazhdimësisë së Institucionit, duke përfshirë planet për backup dhe rimëkëmbjen nga katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat, hartimin e planit të sigurisë së informacionit dhe implementimin e tij,

	serverat e sistemeve QKR dhe QKL të cilët hostohen tek data centeri i AKSHI-t, si dhe nuk ka të hartuar një plan të politikave të vazhdueshmërisë së biznesit (BCP) dhe dokumentim mbi planin e rimëkëmbjes nga katastrofa (DRC).	duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TIK. Planifikimi dhe testimi i sistemeve TIK të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen
3	Nga auditimi mbi dokumentimin e regjistrit elektronik të Licencave, Lejeve dhe Autorizimeve si bazë të dhënash shtetërore rezulton se, ky regjistër është i pa miratuar me akte ligjore.	AKSHI të marrë masa për nxjerrjen e akteve ligjore për miratimin e Regjistrit elektronik të Licencave, Lejeve dhe Autorizimeve si autoritet rregullator koordinues, përgjegjës për përpunimin, përditësimin dhe standardizimin e procedurave dhe rregullave për krijimin, regjistrimin, përfundimin e funksionimit, administrimin, ndërveprimin dhe sigurinë e bazave të të dhënave shtetërore dhe elementëve të tjerë specifikë që lidhen me këto procese
4	Rregullorja e Teknologjisë së Informacionit është e pa miratuar, ndërkohë që Drejtoria e Inovacionit dhe Regjistrave e ka mbështetur aktivitetin e saj në këtë rregullore. Me miratimin dhe futjen në fuqi të VKM nr. 673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit", rregulloret e miratuara nga QKB nuk janë efiçente dhe efektive për t'u përdorur dhe do të duhet t'u nënshtrohen një rishikimi të hollësishëm, duke reflektuar ndryshimet që do të ndodhin në strukturë, në përshkrimet e punës dhe në ndarjen e përgjegjësive të gjithsecilit, për t'u përshtatur me kërkesat e kësaj VKM-je. Drejtoria e Inovacionit dhe Regjistrave	QKB të marrë masa për hartimin e një Rregulloreje të Përgjithshme mbi Teknologjinë e Informacionit në QKB, në të cilën të identifikikohen të gjitha operacionet TIK në institucion, afatet dhe burimet e nevojshme për çdo veprimtari. Hartimi i kësaj Rregulloreje të marrë në konsideratë të gjitha rregulloret e miratuara dhe kërkesat që vijnë si rezultat i futjes në fuqi të VKM-s 673, datë 22.11.2018 si dhe legjislacionin e Teknologjisë, Informacionit dhe Komunikimit në Shqipëri.

	në QKB është një nga strukturat që preket nga miratimi dhe futja në fuqi e VKM-s nr. 673 ku sipas së cilës, stafi TI dhe pajisjet kalojnë në varësi të ASKHI-it.	
5	Nga auditimi lidhur me identifikimin dhe menaxhimin e risqeve në teknologjinë e informacionit rezulton se regjistri i riskut në QKB nuk është i përditësuar (update) me risqet e reja të brendshme dhe të jashtme që mund të jenë shfaqur, si dhe nuk ka identifikuar ndikimin e këtyre risqeve në institucion. Regjistri i riskut ka të pasqyruara të njëjtat fusha të përsëritura për tre vitet e fundit duke e bërë jo efektiv dhe jo efiçent reduktimin e risqeve, në mospërputhje me nenet 19-21 të ligjit nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar, udhëzimi nr. 30, datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik", i ndryshuar, udhëzimi nr. 21, datë 25.10.2016 "Për nëpunësit zbatues të të gjitha niveleve", Udhëzimi i Ministrit të Financave nr. 16, datë 20.07.2016 "Për përgjegjësitë dhe detyrat e koordinatorit të menaxhimit financiar dhe kontrollit dhe koordinatorit të riskut në njësitë publike".	QKB në bashkëpunim me Drejtorinë e Inovacionit dhe Regjistrave si dhe me strukturat këshilluese mbi TIK, të marrin masat e nevojshme për përditësimin dhe dokumentimin e regjistrit të risqeve dhe të marrin masa për hartimin dhe dokumentimin e një plani veprimi për minimizimin/ parandalimin e risqeve të identifikuara, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave.
6	Nga auditimi mbi veprimet operacionale rezulton se, thjeshtimi i veprimeve në sportel ka deleguar fluksin tek regjistruesit, që aktualisht duhet të kalojnë çdo veprim në miratim edhe kur risku është i ulët, ose i pa konsiderueshëm. Në ndërtimin e	QKB të analizojë nevojën për miratim të veprimeve operacionale me risk të ulët, për të gjitha llojet e sporteleve përfshirë dhe shërbimin online të e-albania, për kalimin me miratim të thjeshtë në sportel, në funksion të një menaxhimi më të mirë të kërkesave nga biznesi, si

	sistemeve QKB nuk ka marrë në konsideratë miratimin e thjeshtë (simple aprove), në momentin e aplikimit për krijime, apo ndryshime të elementëve të caktuar të regjistrit që janë lehtësisht të verifikueshëm që në sportel.	dhe të burimeve njerëzore që vetë institucioni disponon.
7	Nga auditimi mbi hartimin e marrëveshjes për komunikimin elektronik rezulton se, ndërmjet QKB dhe DPT marrëveshja për ndërveprimin e të dhënave, është nënshkruar pa përfshirjen e Autoritetit Rregullator Koordinues, si institucioni përgjegjës për përpunimin, përditësimin dhe standardizimin e procedurave dhe rregullave për krijimin, regjistrimin, përfundimin e funksionimit, administrimin, ndërveprimin dhe sigurinë e bazave të dhënave shtetërore dhe elementëve të tjerë specifikë që lidhen me këto procese bazuar në nenin10/pika 1,2 të ligjit nr. 10325, datë 23.09.2010 "Për bazat e të dhënave shtetërore". Gjithashtu, ndërmjet QKB dhe DPT ende nuk rezulton të jetë zyrtarizuar ndonjë protokoll komunikimi apo ndërveprimi të dhënash për lehtësimin e procedurave, konsultimin si dhe leximin në mënyrë të ndërsjellët në zbatim të objektit të marrëveshjes neni 3, pika 3.2 në të cilën citohet se: ".....nëpërmjet hapave të detajuar në Protokollin e Shkëmbimit Elektronik i cili është pjesë përbërëse e kësaj marrëveshje".	Nga ana e QKB dhe DPT të merren masa për rishikimin e marrëveshjes me nr. 12420/1, datë 07.09.2017 në lidhje me ndërtimin e protokollit të komunikimit në një kohë sa më të shkurtër, për përmirësimin në kohë të afateve të përgjigjes së institucioneve tek njëri-tjetri, si dhe përfshirjen e autoriteti rregullator koordinues në rishikimin e saj.
8	Nga auditimi ka rezultuar se QKB-së, nuk i është mundësuar leximi i	DPT, si palë në marrëveshjen e lidhur me QKB, të marrë masa që në zbatim të

	detyrimeve tatimore në kohë reale në sistemin e DPT, në kundërshtim me objektin e marrëveshjes me nr. 12420/1, datë 07.09.2017. Konkretisht, në lidhje me leximin e të dhënave në DPT për situatën aktuale tatimore të subjekteve që aplikojnë për çregjistrim, rezulton se aplikimet për çregjistrim nga QKB dërgohen në kohë reale në DPT dhe me shkresë zyrtare në njësitë vendore. DPT dhe njësitë vendore i përgjigjen kërkesës së QKB në lidhje me detyrimet e subjektit që ka aplikuar për çregjistrim me shkresë zyrtare dhe jo nëpërmjet sistemit.	marrëveshjes me QKB nr. 12420/1, datë 07.09.2017, të mundësojë QKB-së, nëpërmjet ndërveprimit të të dhënave, leximin në kohë reale, të situatës aktuale tatimore.
9	Në marrëveshjen ndërmjet palëve është dakordësuar që kodet NVE (Nace) të dërgohen elektronikisht nga DPT në QKB-së, të azhurnuara në rast verifikimi dhe konstatimi nga Administrata Tatimore, në një kohë që këto të dhëna në Regjistrin Tregtar reflektohen si të dhëna parësore që i përkasin themelimit dhe veprimtarisë së subjekteve tregtare kodet NVE (NACE), referuar VKM nr. 863, datë 21.10.2015 “Për krijimin e bazës të të dhënave shtetërore të qendrës kombëtare të regjistrimit, regjistri tregtar”.	QKB në bashkëpunim me DPT, të marrë masa për rishikimin e pikës 4.4 të Marrëveshjes me nr. 12420/1, datë 07.09.2017, në të cilën të cilësohet se e drejta e DPT për kodet NACE është reklamimi pranë QKB, i rasteve të konstatuara gjatë kontrolleve në terren nga Administrata Tatimore, ku ushtrimi i aktivitetit nga ana e subjekteve është në ndryshim nga ai i deklaruar. Pasqyrimi i ndryshimit të objektit të veprimtarisë së subjektit (kodi NACE) është detyrim i QKB, pasi është e dhënë parësore në sistemin e regjistrit të biznesit, ndryshim i cili nga QKB nëpërmjet ndërveprimit të sistemeve automatikisht ti pasqyrohet DPT-së.
10	Nga auditimi i ndërveprimit për elementë të rëndësishëm rezultoi se DPT nuk merr nga QKB të dhëna në kohë reale, por nëpërmjet postës elektronike me komunikime periodike javore për:	QKB në bashkëpunim me DPT të përfshijnë në protokollin e komunikimit elektronik dhe të realizojë shkëmbimin në kohë reale ndërmjet sistemeve, të dhënat që marrin periodikisht, për një

	Aplikimet për aktivizim; Fillimin e procedurave për likuidim; Bashkim me përthithje; Ndarjen e shoqërisë; Shndërrimin e shoqërisë.	pasqyrim sa më të saktë dhe në një afat të shkurtër për: Aplikimet për aktivizim; Fillimin e procedurave për likuidim; Bashkim me përthithje; Ndarjen e shoqërisë; Shndërrimin e shoqërisë.
11	Nga trajtimi i incidenteve dhe gabimeve ka rezultuar se, QKB nuk ka të dokumentuar dhe implementuar një procedurë të standardizuar për kontrollin e ndryshimeve në infrastrukturë dhe në sistemet e TIK në institucion. Situata në QKB dhe në degët rajonale, për periudhën nën auditim, menaxhohet mbi baza ngjarjesh. Gjithashtu, nuk disponohet procedurë për inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve (update, upgrade, etj.), struktura kontrolli për verifikimin e efektivitetit të ndryshimeve të kryera, procedura për ndryshimet emergjente si dhe dokumentimin e të gjithë procesit të ndryshimeve, duke përfshirë dhe incidentet që vijnë nga ndërveprimi i të dhënave. Nga auditimi rezulton se mungon formati kur çështja hapet nga vetë punonjësit në zbatim të urdhrave apo vendimeve të ndryshme që janë detyruese për zbatim.	QKB të marrë masa organizative lidhur me hartimin dhe vënien në funksion të rregullores për trajtimin e incidenteve dhe gabime, masave shtesë, personat përgjegjës si dhe afatet për ngjarje të të pa parishikuara, të cilat mund të ndodhin gjatë punës me veprime operacionale. Në rregullore të përfshihen dhe veprimet, që vijnë si rezultat i vendimeve të ndryshme detyruese për ekzekutim, si dhe ndryshimet që ndodhin brenda për brenda TIK.
12	Nga auditimi u konstatuan disa parregullsi në inputet e QKL. Për vitet 2015-2017, në fushën “Tipi i Subjektit”, plotësimi i fushës nuk është i unifikuar.	QKB të marrë masa për analizimin e anomalive të konstatuara nga auditimi i inputeve të të dhënave në QKL, duke përcaktuar përgjegjësitë, si dhe të marrë

	Saktësisht kjo fushë është plotësuar me statusin "*Shoqeri Aksionare*" si dhe "*Shoqëri Aksionare*". Gjithashtu kjo fushë është plotësuar me statusin "*Shoqëri me përgjegjësi të kufizuar*" si dhe e shkurtuar "*Shpk*". Edhe pse për rastet e cituara, në thelb statusi juridik mbetët i njëjtë, kjo qasje rrit mundësinë në deklarimin e statistikave të gabuara nga ana e institucionit të Qendrës Kombëtare të Biznesit. - Për vitet 2015-2017, në 19 raste mosha e aplikantit për marrjen e licencës është nën 18 vjeç, *pra pa zotësi të plotë juridike për të vepruar*. Saktësisht u konstatuan 12 raste për vitin 2015, 6 raste për vitin 2016 dhe 1 rast për vitin 2017. Gjithashtu në 10 raste u konstatua se data e lindjes së aplikantit i përket së ardhmes. Saktësisht 5 raste për vitin 2015 dhe 5 raste për vitin 2016. - Një pjesë e fushave të plotësuara kanë vlerën "NULL". Saktësisht fushat: "Adresa e e-mail", "Gjinia", "TechDirector Name", "Economic Activity", "Description of Activity". Pra fushat nuk kanë të dhënat e kërkuara, e për pasojë informacioni i plotë për këto raste nuk ekziston. - Për vitin 2016, në 3831 raste nga 4095 në total, fusha "Sasia e paguar" rezulton datë. Normalisht kjo fushë duhet të jetë e plotësuar me vlerat "100", "50" ose "NULL". - Për vitet 2015-2018, u konstatua se fusha "NID" nuk është plotësuar gjithnjë në mënyrë korrekte, pasi në mjaft raste	masa për krijimin e kontrolleve parandaluese në të ardhmen me qëllim regjistrimin, mbajtjen dhe raportimin e saktë të të dhënave. -QKB të marrë masa për përcaktimin e fushave "Mandatory fields", apo shtimin në këtë kategori të fushave të përmendura, të cilat në opinion të grupit të auditimit janë të rëndësishme për dhënien e një pasqyre sa më të plotë të bizneseve.

	është plotësuar me numrin e letërnjoftimit apo numrin e pasaportës. - Për vitet 2015- 2018, u konstatuan 241 raste të veprimeve të dublikuara. Saktësisht për vitin 2015 rezultojnë 33 veprime të dublikuara, për vitin 2016 rezultojnë 19 raste, për vitin 2017 rezultojnë 122 raste dhe 2018 rezultojnë 67 raste.	
13	Nga auditimi u konstatuan disa parregullsi në inputet e Regjistrit Tregtar. Për vitet 2015-2018, u konstatuan 52 raste në të cilat forma ligjore nuk është e përcaktuar. Saktësisht për vitin 2015 rezultojnë 18 raste, për vitin 2016 rezultojnë 13 raste, për vitin 2017 rezultojnë 8 raste dhe 2018 rezultojnë 13 raste. - Për vitet 2015-2018, u konstatuan 197 raste në të cilat fusha "NACE_ID" si dhe "NACE_PARENT" nuk janë të përcaktuara. Saktësisht për vitin 2015 rezultojnë 156 raste, për vitin 2016 rezultojnë 7 raste, për vitin 2017 rezultojnë 26 raste dhe 2018 rezultojnë 8 raste.	QKB të marrë masa për analizimin e anomalive të konstatuara nga auditimi i inputeve të të dhënave në Regjistrin Tregtar, duke përcaktuar përgjegjësitë, si dhe të marrë masa për krijimin e kontrolleve parandaluese në të ardhmen me qëllim regjistrimin, mbajtjen dhe raportimin e saktë të të dhënave.
14	Nga auditimi i menaxhimit të shërbimeve TIK dhe dhënies së sportit, ka rezultuar se, në mungesë të strukturës/sektorit Help Desk në QKB, nuk sigurohet menaxhimi i shërbimeve TIK dhe plotësimi i kërkesave të përdoruesve të institucionit si dhe degëve rajonale. Duke parë rëndësinë e QKB-së, në dhënien e shërbimeve për biznesin, duhej të gjendej mënyra për dhënie sporti, ku të përcaktoheshin	QKB, duke marrë në konsideratë kohën dhe burimet e nevojshme, të marrë masa për dhënien e sportit, për plotësimin e kërkesave të përdoruesve të institucionit dhe degëve rajonale për të siguruar cilësinë e shërbimeve ndaj biznesit dhe qytetarëve.

	detyrat dhe përgjegjësitë e gjithsecilit për të garantuar dhe siguruar cilësinë e shërbimeve ndaj biznesit dhe qytetarëve.	
15	Mungesa e trajnimeve dhe planifikimi i trajnimeve. Nga auditimi i burimeve njerëzore në strukturën e TIK dhe menaxhimi i kapaciteteve të personelit që ka akses në asetet e informacionit të QKB në mënyrë që të jetë i vetëdijshëm për rregullat dhe standardet e sigurisë dhe të jenë të aftë t'i zbatojnë dhe ndjekin ato gjatë punës së tyre u konstatua se: - Drejtoria e Inovacionit dhe Regjistrave ka mungesa në personel; - QKB dhe Drejtoria e Inovacionit dhe Regjistrave nuk ka një analizë të nevojave për trajnim të stafit të drejtorisë dhe nuk ka plan për trajnime. Stafi i Drejtorisë së Inovacionit dhe Regjistrave nuk ka kryer asnjë ditë trajnim për sistemet, sigurinë dhe teknologjinë e informacionit, etj	QKB të marrë masa për menaxhimin e burimeve njerëzore, duke plotësuar nevojat për trajnime të stafit të Drejtorisë së Inovacionit dhe Regjistrave, si dhe të hartojë plane dhe politika për zhvillimin e trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit.
16	Nga auditimi u konstatuan mungesa në kapacitetet e serverëve si më poshtë: - Serverat kanë mungesë në hapësirat fizike dhe logjike, duke ndikuar në performancën dhe mbarëvajtje e sistemeve, si dhe duke rrezikuar në humbjen e të dhënave. Transactional backup nuk bëhet për shkak të mungesës së hapësirave në serverin e databazës. - Backup-i i sistemit të regjistrit të biznesit, realizohet në mënyrë manuale nga punonjësit e Drejtorisë së	QKB në bashkëpunim me Drejtorinë e Inovacionit dhe Regjistrave si dhe me strukturat këshilluese mbi TIK, të marrin masa për: - analizimin dhe dokumentimin e situatës së krijuar dhe krijimin e kushteve optimale mbi rritjen e kapaciteve (hapësirave storage) të serverave të sistemeve për të siguruar mbarëvajtjen e sistemeve dhe vazhdimësinë e ofrimit të shërbimeve pa ndërprerje; - kryerjen backup-it të particioneve të konsideruara kritike dhe klasifikimin e të

	Inovacionit dhe Regjistrave. - Disa nga volumet Hdd nuk janë të konfiguruar në redundant RAID, gjë e cila mund të sjellë humbje të dhënash në raste aksidentesh apo në raste të dështimit të një Hdd, etj. - Serverat e sistemit QKL për shkak të mungesës së suportit nga ana e prodhuesit kanë kaluar në status "retired". - Upgrade-imi i SQL Servers në versione më të reja nuk mund të realizohet, për arsye të mungesës së kapaciteteve të vetë serverave dhe kushteve të tjera optimale, që kërkohen për të kaluar në versione më të reja.	dhënave të rëndësishme; - kryerjen e konfigurimeve përkatëse të Hdd-ve ose volumeve që nuk janë të konfiguruar si redundant RAID.
17	Nga auditimi i portalit rezultoi se, nuk përdoret një lidhje e sigurt (connection security) HTTPS (HyperText Transfer Protocol Secure**)** (Not secure status) që do të thotë se serveri i faqes së internetit nuk përdor një certifikatë sigurie për të vërtetuar identitetin e internetit në shfletues, si Chrome. Në mungesë të kësaj certifikate mund të ndodhë humbja e privatësisë, ndryshimit të informacionit që merret ose jepet me anë të këtij portali.	QKB në bashkëpunim me strukturat përgjegjëse për mbarëvajtjen e faqes web, të marrin masa për përmirësimin e faqes web me elementët përkatës të sigurisë (certifikatën e sigurisë) së navigimit online për të rritur sigurinë dhe ndihmesën ndaj qytetarëve. Të kihet parasysh që në të ardhmen të shtohen elementë inovativ në faqen web për ta bërë atë sa më interaktive dhe ndihmëse për qytetarët.
18	Nga auditimi mbi diagramat e rrjedhës së informacionit rezulton se, nuk janë përfshirë statuset e aplikimit për të gjitha rastet nga vjen aplikimi, duke qenë se aplikimet vijnë jo vetëm nga sporteli, por dhe nga portali e-albania, si dhe hapat që duhet të ndiqen kur: Regjistruesi refuzon miratimin e një	QKB të pasqyrojë veprimet e pa dokumentuara që ndodhin gjatë rrjedhës së informacionit, që menaxhohet nëpërmjet sistemit, si dhe të kryejë pasqyrimin e ndryshimeve në të gjithë manualet apo udhëzuesit që disponon për përdorimin e sistemeve.

	veprimi duke kërkuar nga sporteli i QKB të bëhen plotësimet e nevojshme. Aplikimi vjen nga portali qeveritar E-albania	
19	Nga auditimi rezultojnë të pa standardizuar formularët për 56 shërbime për regjistrin e biznesit, si dhe 6 shërbime për regjistrin e Licencave/Lejeve dhe Autorizimeve	QKB të analizojë të gjitha mundësitë operacionale dhe ato financiare duke renditur grupimin e formularëve nga prioriteti me i lartë, për standardizimin e formularëve që kanë numër të madh aplikimesh.
20	Nga auditimi ka rezultuar se komisionet përgjegjëse për mbikëqyrjen e zbatimit të kontratave, nuk kanë dokumentuar kryerjen e matjeve në lidhje me cilësinë e shërbimit. Nga strukturat përgjegjëse për mbikëqyrjen e zbatimit të kontratës, nuk u paraqit asnjë dokument, apo e dhënë, ku të vërtetohej se nga ana e tyre është përmbushur kjo detyrë. Gjithashtu, ka rezultuar se nuk janë mbajtur Procesverbale të kontrolleve të kryera për zbatimin e kontratës dhe të pranimit të shërbimit.	QKB, në cilësinë e Autoritetit Kontraktor, si dhe struktura përgjegjëse për zbatimin e kontratave të marrin masa për dokumentimin e të gjithë hapave, kontrolleve, testimeve të kryera gjatë mbikëqyrjes së zbatimit të kontratave.
21	Nga auditimi rezultoi se ka mospërputhje midis stafit të deklaruar nga operatori ekonomik fitues në dokumentet tenderit, me stafin i cili realisht ka kryer mirëmbajtjen e sistemit. Kjo ka ndodhur pasi, nga strukturat përgjegjëse për mbikëqyrjen e zbatimit të kontratave, nuk është kryer verifikim mbi stafin e kontraktuesit, i cili ka kryer mirëmbajtjen e shërbimit, sipas kontratave përkatëse. Konkretisht, konfirmimin e marrëdhënies së punës me kontraktuesin si, kontrata pune,	QKB në cilësinë e Autoritetit Kontraktor, si dhe struktura përgjegjëse për zbatimin e kontratës, duhet të marrë masa që nga ana e subjektit kontraktues, i cili do të realizojë MNSH, të deklarohet përbërja e stafit që do të kryejë mirëmbajtjen e sistemeve TIK, me qëllim verifikimin e tij, në lidhje me marrëdhënien e punës me kontraktuesin si dhe kapacitetin tekniko-profesional, në raport me atë të deklaruar në dokumentet e tenderit nga operatori ekonomik i shpallur fitues (kontraktuesi).

	formulari E-sig; kapacitetin tekniko-profesional si, diploma dhe certifikata, në raport me atë të deklaruar në DT nga (kontraktuesi), me qëllim marrjen e sigurisë se shërbimi i kontraktuar do të kryhet me cilësi.	
22	Nga auditimi u konstatua se personeli kompanive kontraktuese, i cili është caktuar për kryerjen e këtij shërbimi, nuk është dokumentuar ruajtja e kofidencialitetit të të dhënave, pavarësisht se në kontratat e lidhura në nenet përkatëse është cilësuar domosdoshmëria e ruajtjes së të dhënave nga të dy palët. Nga këqyrja e dokumentacionit rezultoi se, nuk ka asnjë dokument i cili vërteton përmbushjen e këtij kushti të kontratave, nga ana e stafit të kontraktuesve, të cilët kanë akses në sistem, për shkak të detyrës.	QKB, në cilësinë e Autoritetit Kontraktor, të marrë masa që për të gjithë personat e deklaruar nga Kontraktuesi, se do të jenë pjesë e stafit që do të zbatojë Marrëveshjet e Nivelit të Shërbimit, të kërkojë të paraqesin paraprakisht deklaratë për ruajtjen e konfidencialitetit të të dhënave të kontraktorit (QKB).

5. TAKSAT VENDORE BASHKIA ELBASAN.

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: ***Bashkia Elbasan***

Përgatitur: 15.10.2018

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 864/1, datë 11/09/2018

Auditimi është kryer nga:

1. Kozma Kondakçiu, përgjegjës grupi
2. Meald Habazaj, anëtar
3. Aldo Kita, anëtar

Periudha e Auditimit: 01.01.2017 – 30.06.2018
Afati i auditimit: 03.09.2018 – 15.10.2018

ÇFARË KEMI AUDITUAR

Fushat e auditimit

- Vlerësimi i burimeve njerëzore në strukturën e TIK
- Verifikimi i Strategjisë, politikave dhe procedurave TIK
- Identifikimi dhe menaxhimi i risqeve në TIK
- Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet
- Auditimi i projekteve e investimeve të teknologjisë së informacionit
- Identifikimi, hartimi i nevojave dhe kritereve të vendosura për mallra dhe shërbime
- Verifikimi i shkallës së sigurisë së aplikacioneve

PSE ËSHTË I RËNDËSISHËM KY AUDITIM

Më hollësisht:

OPINIONI I AUDITIMIT:

Grupi i auditimit KLSH duke vlerësuar rolin e teknologjisë së informacionit në përmbushjen e misionit të Bashkisë Elbasan, duke mbështetur auditimin në Standardet Kombëtare dhe Ndërkombëtare të Auditimit (ISSAI 1 Neni 22, Ligjin e KLSH Nr.154/2014 Neni 3 dhe 14, Manualin e Auditimit të Teknologjisë së Informacionit (WGITA), COBIT 4.1, ISSAI 5300.6, 8 dhe 12.2, 16.19, 21.1, 23, ISSAI 100.36,48, ISSAI 5310), pas shqyrtimit të të dhënave dhe dokumentacionit TI të vënë në dispozicion nga Bashkia Elbasan, arriti në konkluzionin se:

Bashkia Elbasan ka zhvilluar sisteme të Teknologjisë së Informacionit në funksion të përmbushjes së objektivave të institucionit duke shfrytëzuar burimet e vena në dispozicion si dhe kryer thithjen e investimeve të konsiderueshme nga donatoret e huaj për zhvillimin dhe mirëmbajtjen e infrastrukturën TI. Investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht problemet e sigurisë së informacionit, sigurimin e Vazhdueshmërisë së Biznesit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat. Zhvillimi i shërbimeve dhe infrastrukturës duhet të mbështetet në praktikat më të mira si dhe rekomandimet e AKSHIT.

Rezultatet e aritura janë të kompromentuara nga mungesa e Strategjisë për Teknologjinë e Informacionit, duke mbartur riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së Bashkisë Elbasan.

Nr.	Gjetje nga auditimi	Rekomandimi
1	Bashkia Elbasan nuk disponon strategji dhe regjistër risku për teknologjinë e informacionit në mospërputhje me ligjin nr.	

	10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar, Udhëzimi nr. 30, datë 27.12.2011 "Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik".	
2	Struktura TI ka një bazë rregullative të plotësuar (rregulloja e strukturës TI dhe ndarja e detyrave, rregullore për sigurinë dhe komunikimet elektronike, manuale të aplikacioneve të perfituara si rezultat i donacioneve, dokumentacion mbi procedurat e backup etj), por kjo bazë rregullative është e pa miratuar.	
3	Nuk ka plan trajnimi vjetor për vitet 2017-2018 për burimet njerëzore të sektorit të Teknologjine e informacionit . Nga ana e burimeve njerezore dhe Sektorit të Inovacionit TI dhe mbrojtjes Kibernetike nuk dokumentohet procesi i kërkesave, nevojave dhe analizimi i tyre. Trajnimet e përfituara nga donatorët dhe zhvilluesit e sistemeve janë të pa mjaftueshme e nuk plotësojnë nevojat për trajnim mbi sistemet, sigurinë dhe teknologjinë e informacioni për stafin TI.	
4	Organizimi i strukturës TI-së në nivel sektori nën Drejtorinë e Politikave Strategjike e Inovacionit dhe Medias, nuk i përgjigjet shtrirjes së teknologjisë së informacionit në Bashki dhe institucionet e vartësisë duke zbehur ndikimin e varësisë direkte nga menazhimi i lartë.	
5	Nga auditimi u konstatua se Bashkia Elbasan nuk ka Strategji për Teknologjinë e Informacionit, mungesa e të cilës sjell mos pasqyrimin e objektivave lidhur me infrastrukturën, burimet e nevojshme si dhe instrumentave të nevojshëm për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së Bashkisë Elbasan.	
6	Standartet e Praktikat me të mira të rekomandojnë që Qeverisja TIK duhet të vendosi politika në fushën e TI. Këto politika vendosin kërkesat për mbrojtjen e aseteve të informacionit dhe mund ti referohen procedurave ose mjeteve të tjera në mënyrën sesi këto do të mbrohen. Politikat duhet të jenë të disponueshme ndaj të gjithë punonjësve përdorues të TI.	

	Bashkia Elbasan nuk ka vendosur politika e parime mbi sigurinë dhe Vazhdueshmerisë së Punës së Institucionit. Bashkia Elbasan nuk ka krijuar facilitetet e nevojshme për vënien në dispozicion rregulloreve dhe politikave të gjithë punonjësve përgjegjës mbi sigurinë e informacionit, përfshirë përdoruesit e sistemeve të cilët kanë rol në mbrojtjen e informacionit me qëllim që të gjithë punonjesit të familjarizohen dhe ta bëjnë pjesë të menyrës së të menduarit dhe të veprimtarisë së tyre të përditshme.	
7	*Rregullorja e Brendshme, lidhur me strukturën TI në* Bashkinë Elbasan, nuk është në përputhje me rekomandimet e AKSHIT, rregullorja nuk përmban elementët e nevojshëm për të siguruar funksionim e përshtatshëm të strukturës TI në institucion.	
8	Bashkia Elbasan nuk ka politika të ruajtjes së dokumenteve dhe nuk ka të dokumentuar një plan masash për identifikimin, trajtimin e gabimeve dhe incidenteve që mund të ndodhin në infrastrukturën TI, në mungesë të procedurave të shkruara, risqet menaxhohet mbi bazë ngjarjesh. Jepet suport, mbështetje teknike dhe logjike për operacionet TI që ndihmojnë mbarëvajtjen e strukturave të institucionit. Procedurat kryhen nëpërmjet shkëmbimeve verbale dhe nëpërmjet e-mail-eve, duke mos realizuar identifikimin e risqeve, mbart riskun e përseritjes së incidenteve. Identifikimi i risqeve çon në gjetjen e zgjidhjeve për t'i trajtuar ato dhe për të parandaluar ndodhjen e incidenteve të ngjashme në të ardhmen dhe në mënyrë që funksionet e institucionit të jenë të mbrojtura.	
9	Bashkia Elbasan nuk rezulton të ketë plan të miratuar emergjence dhe politika të miratuara për vazhdimësinë e biznesit. Politika organizative mbi vazhdimësinë e ofrimit të shërbimeve duke marrë në konsideratë: rolet dhe përgjegjësitë, fushëveprimin, kërkesat për trajnim, orarin e mirëmbajtjes, orarin e testimit, nivelet e miratimit dhe palët e përfshira në këtë proces. Nuk jane përcaktuar Objektivat e Kohës së Rimëkëmbjes dhe Objektivat e Punës së Ripërtëritjes për çdo proces kritik.	

10	Bashkia Elbasan nuk ka kryer analizë risku lidhur me Sigurinë e të dhënave, identifikimin e të dhënave kritike si dhe kërcënimet e mundshme në ndikim të sistemeve , aplikacioneve ku zhvillohet aktiviteti i Bashkisë Elbasan.	
11	Siguria e infrastrukturës network në Bashkinë Elbasan është e kompromentuar si rezultat i mungesës së: Active Directory dhe Domain Controller për menaxhimin e userave, paisjeve dhe aplikacioneve dhe për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhimin e shërbimeve në përputhje me standardet. - server të dedikuar per CA (Certificate Authority) - Server i dedikuar për mail server (Exchange server) - Firewall Hardware - Switch të menaxhueshëm	
12	Nga auditimi i rrjetit kompjuterik qe lidh Bashkine Elbasan me qendrat administrative rezultoi se: a. Përdoruesit në këto qendra janë lidhur nga fibra optike dhe marrin shërbimin në një Swich të pa menaxhueshëm. b. Konfigurimet në rrjet të PC janë si administratorë. c. Në të njëjtin swich marrin shërbime disa institucione.	
13	Nuk dokumentohet procesi i hapjes dhe mbylljes së përdoruesve në sisteme.	
14	Ambienti fizik i dhomës së rrjetit nuk është në përputhje me standardet e përcaktuara në Rregulloren për Ndërtimin e Dhomës së Serverëve (Versioni 1.0, datë 02.12.2008) miratuar nga AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit) përkatësisht: a. Pika 4.3. Parandalimi i zjarrit**.** Dhoma duhet të jetë e pajisur me një sistem të përshtatshëm kundër zjarrit Dhoma duhet të jetë rezistente ndaj zjarrit nëse kabllot dhe	

	sistemet e ftohjes kombinohen në të njëjtën hapësire sipër tavanit ose nën dysheme b. Pika 4.5. Sistemi Elektrik. Instalimi elektrik i dhomës së serverëve nuk është veçmas instalimit të përgjithshëm. c. Pika 4.6. Sistemi i Alarmit. Mungon sistemi i alarmit. Duhet të jenë të tillë që të sinjalizojnë problemet me rrymën elektrike, me ambientin fizik, sensor për rrjedhjen e ujit, sensor për parandalimin e dëmtimeve fizike të strukturës së dhomës.	
15	Mungon Siguria e Hyrjes në dhomë. Duhet të jetë e siguruar me anë të një sistemi elektronik dhe natyrisht duhet të ketë dhe sistem alarmi në rast thyerje. **Testimi i Web të Bashkisë Elbasan për dobësi** . Për testimin e performancës së faqes së internetit të Bashkisë Elbasan *http://www.elbasani.gov.al* u krye një testim i sigurisë dhe mangësive.	
16	Komunikimi ndërmjet Web Browser-it dhe serverit kryeht duke përdorur protokollin HTTP, i cili i merr dhe jep informacion në mënyrë jo të sigurt në rrjet. Kjo sjell që, një sulmues i jashtëm, i cili arrin të hyj në rrjeti, ka mundësi të lexojë dhe ndryshojë informacionin i cili aksesoret nga rrjeti, duke përfshirë (fjalëkalimet-et, të dhëna sekret si dhe të tjera të dhëna sensitive). Nëse ndodh një sulm, tipit të software-ve dhe versioni i përdorur identifikohen lehtësisht dhe mund të përdoren për sulme specifike. Mbrojtësi X-XSS i HTTP dikton shfletuesin (browserin) të mos hap faqe webi të cilat kapin sulme Cross-Site Scripting (XSS) të reflektuar. Për shkak të këtij mbrojtësi, web siti ekspozohen përdoruesit tek sulmuesit e XSS, nëse faqia web i ka këto dobësi.	
17	Nga auditimi i procesit të identifikimit të nevojave për investime në fushën e teknologjisë së informacionit dhe priorizimit të tyre konstatohet se Strukturat e TI që marrin pjesë aktive në procesin e identifikimit të nevojava nuk përfshihen në	

	procesin e menaxhimit të tyre si rezultat i statusit organizativ në nivel sektori nën Drejtorinë e Politikave Strategjike e Inovacionit dhe Medias.	
18	Bashkia Elbasan përgjatë periudhës 01/01/2017-30/06/2018 ka realizuar 3 prokurime në fushën e TI dhe një MNSH. Grupi i auditimit konstaton: Për vitin 2017 2018 U kontrolluan këto Kontrata prokurimesh: • Nr. Kontrate 8796 "Elbasan Virtual Tour 360" • Nr. Kontrate 9756 "Projekti i monitorimit të ambientit në qytetin e Elbasanit" • Nr. Kontrate 472 "Mirëmbajte e platformës: Transport Inteligjent" • Nr. Kontrate 2474"Shërbim Interneti për Bashkinë Elbasan dhe njësitë e vartësisë"	
19	Nga auditimi i Kontratës nr.2474 "Shërbim Interneti për Bashkinë Elbasan dhe Njësitë e vartësisë" rezultoi se grupi i marrjes në dorëzim grupi i marrjes në dorëzim nuk ka një raport të marrjen në dorëzim të punimeve të kryera (në këtë rast shërbimin e Internetit) nga OE në kundërshtim me VKM Nr. 914, datë 29.12.2014,Neni 77, Pika 3. *Mbikëqyrja e kontratës.* Në disa nga faturat Tatimore, të sjella nga Operatori Ekonomik X SH.A., Blerësi në këtë rast Autoriteti Kontraktor (Bashkia Elbasan), ka firmosur këto fatuar vetëm me emrin "Bashkia Elbasan" dhe jo grupi i marrjes në dorëzim të shërbimit të internetit. Përkatësisht në faturat nr.90726620, nr.90735561. Ndërsa faturat e tjera janë firmosur vetëm nga një përfaqësues i grupit të marrjes në dorëzim. *MNSH* U kontrolluan këto Kontrata për MNSH (Marrëveshje Nivel Shërbimi):	

	• Nr. Kontrate 8796 "Elbasan Virtual Tour 360" • Nr. Kontrate 9756 "Projekti i monitorimit të ambientit në qytetin e Elbasanit" • Nr. Kontrate 472 "Mirëmbajte e platformës: Transport Inteligjent"	
20	Nga auditimi i këtyre procedurave rezultoi se të gjitha marrëveshjet e nivel shërbimit (MNSH), që janë me afat 4 vjeçar, grupi i marrjes në dorëzim nuk ka një raport të marrjen në dorëzim të punimeve të kryera nga OE në kundërshtim me VKM Nr. 914, datë 29.12.2014,Neni 77, Pika 3. *Mbikëqyrja e kontratës* *Për t'u siguruar nëse cilësia e punëve, shërbimeve ose e mallrave është e njëjtë me cilësinë për të cilën është shpallur fitues kontraktori, autoriteti kontraktor duhet të monitorojë zbatimin e kontratës dhe në rast të shkeljes së kushteve të kërkuara zbaton penalitetet e parashikuara në kontratë. "Autoriteti kontraktor, gjatë kryerjes së kontrolleve mban procesverbal me shkrim në prani të kontraktorit, sipas përcaktimeve në legjislacionin në fuqi" Procesverbali i marrjes në dorëzim. Raporti i komisionit që merr në dorëzim.*	
21	Nga auditimi i Kontratës Nr. 8796 "Elbasan Virtual Tour 360" rezultoi se, kjo kontratë nuk ka MNSH (Marrëveshje Nivel Shërbimi) në kundërshtim me pikën 3 të Udhëzimit Nr. 1159, datë 17.3.2014 për Hartimin E Marrëveshjes Së Nivelit Të Shërbimit i cili citon*: "Institucionet, të cilat janë duke zhvilluar sisteme të reja në fushën e TIK-ut, detyrimisht, të parashikojnë MNSH-në, si pjesë të procedurës së realizimit të investimit për këto sisteme. Kohëzgjatja e kësaj marrëveshjeje duhet të jetë jo më e shkurtër se 4 (katër) vjet."* c)U konstatua se në të gjitha MNSH nuk përfshihen: *koha e raportimit; koha e përgjigjes; prioriteti; përshkallëzimi* Kjo në kundërshtim me pikën 7 të Udhëzimit Nr. 1159, datë 17.3.2014 për Hartimin E Marrëveshjes së Nivelit të Shërbimit e cila citon: *Të drejtat dhe detyrimet e ofruesit të shërbimit Ky seksion*	

	duhet të përcaktojë të drejtat dhe detyrimet që ofruesi i shërbimit ka ndaj institucionit, në lidhje me ofrimin e shërbimit. Për sa u përket detyrimeve, duhet të përcaktohen metodologjitë dhe specifikat e suportit të ofruesit të shërbimit të MNSH-së; për sa i përket ndërmarrjes së të gjitha veprimeve në kohën e duhur. Në lidhje me shërbimet që do të përcaktohen në marrëveshje, ofruesi i shërbimeve duhet t'u përgjigjet dhe të zgjidhë kërkesat ose incidentet e paraqitura nga institucioni. Gjithashtu, ofruesi i shërbimit duhet të ofrojë dokumentacionin e plotë për komponentët e shërbimit; të garantojë personel të kualifikuar dhe në numër të mjaftueshëm për realizimin e shërbimit; të ofrojë sigurimin e pjesëve të këmbimit (kur është e aplikueshme) dhe në sasinë që do të duhen për t'u ndërruar brenda harqeve kohore të përcaktuara.	
22	Siguria e aplikacioneve si rezultat i mos dokumentimit të procesit të hapjes dhe mbylljes së kredencialeve të përdoruesve në aplikacionet është e kompromentuar.	
23	Bashkia Elbasan nuk ka infrastukturën e nevojshme për të siguruar aplikacionet e zhvilluara, ambienti fizik kompromenton sigurine e aplikacioneve. Bashkia Elbasan nuk ka ambient të veçantë për testime përpara kalimit të ndryshimeve në sistemin Live për aplikacionet mungesa e të cilit komprometon sigurinë e sistemit, të dhënave si dhe vazhdimësinë e ofrimit të shërbimeve.	
24	Sistemi i Administrimit të Taksave (TAIS) nuk ndërvepron me sistemin QKB për të marrë automatikisht të dhënat e bizneseve me impakt mos informimin në kohë për bizneset e reja të regjistruara.	
25	Sistemi i Administrimit të Taksave (TAIS) nuk disponon sisteme kontrolli për parandalimin e inputeve të pa sakta në bazën e të dhënave, nga auditimi u konstatuan paregullsi në fushat e rëndësishme të bazës së të dhënave si "NIPT", "Adresa" "Emërtimi i Biznesit".	
26	1. Siguria e vazhdimësisë së punës së aplikacioneve është e	

	cënuar nga: a. Mungesa e testeve të Back-up dhe Resotre b.Mos përcaktimin në rregullore të frekuencës së kryerjes së Back-up dhe testimit te tij c. Mos përcaktimi i afatit të ruajtjes së informacionit në Backup d. Ruajtjes të Back-up në të njëjtin ambient me bazën e të dhënave primare (dhoma e serverave).	

6. AGJENCIA E PROKURIMIT PUBLIK (APP)

Titulli: "*Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit*"

Subjekti: Agjencia e Prokurimit Publik

Përgatitur: 21.10.2018

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 865/2, datë 11.09.2018

Auditimi është kryer nga:

– Kozma Kondakçiu, Përgjegjëse Grupi
– Elira Cukalla, Audituese e Lartë
– Bledi Dervishaj, Auditues i Parë
Periudha e Auditimit: 01.01.2017 – 30.06.2018

Afati i auditimit: 03.09.2018 – 08.10.2018

ÇFARË KEMI AUDITUAR

Fushat e auditimit

Auditimi i funksionimit të Qeverisjes TIK

a. Verifikimi i Strategjisë, politikave dhe procedurave TIK, vlerësimi i performancës së procedurave të prokurimit publik

b. Vlerësimi i burimeve njerëzore në strukturat TIK

2. Auditimi i projekteve e investimeve të teknologjisë së informacionit

a. Identifikimi, hartimi i nevojave dhe kritereve të vendosura për mallra dhe shërbime në TIK

3. Auditimi i Sigurisë së Informacionit

a. Identifikimi dhe menaxhimi i risqeve në TIK

4. Auditimi i Aplikacioneve

a. Verifikimi i shkallës së sigurisë së aplikacioneve

PSE ËSHTË I RËNDËSISHËM KY AUDITIM

APP është organ qendror, person juridik publik në varësi të Kryeministrit, që financohet nga Buxheti i Shtetit.

Veprimtaria e saj bazohet në Ligjin Nr. 9643/2006 "Për Prokurimin Publik", i ndryshuar, Ligjin Nr. 125/2013 "Për koncesionet dhe partneritetin publik privat" dhe Ligjin Nr. 9874/2008 "Për ankandin publik", i ndryshuar.

Detyrat dhe kompetencat e Agjencisë së Prokurimit Publik fokusohen kryesisht në:

- Përgatitjen e projekt-propozimeve për rregullat e prokurimit publik, ankandeve publike dhe atyre në fushën e koncesioneve/partneriteteve publike private, hartimin e Dokumentave Standarte të Tenderit dhe nxjerrja e udhëzimeve të nevojshme në ndihmë të autoriteteve që ndërmarrin këto procedura;

- Verifikimin e zbatimit të procedurave të prokurimit publik, procedurave të koncesionit dhe ankandit publik pas fazës së nënshkrimit të kontratës dhe në rast shkeljesh të dispozitave ligjore dhe nënligjore, vendosjen e gjobave ose propozimin e marrjes së masave administrative;

- Monitorimin e mbarëvajtjes së sistemit të prokurimit publik, si dhe zbatimin e masave dhe aktiviteteve në mënyrë që të arrijë dhe të ruajë një sistem plotësisht transparent dhe efikas të koncesioneve/partneriteteve publike private;

- Hartimin dhe nxjerrjen e Buletinit të Njoftimeve Publike;

- Përjashtimin e operatorëve ekonomikë nga pjesëmarrja në prokurimet publike, koncesionare apo të ankandit publik për një periudhë nga një deri në tre vjet;

- Nxitjen dhe organizimin e kualifikimit të punonjësve të qeverisjes qendrore dhe vendore, të përfshirë në veprimtaritë e prokurimit publik;

Duke pasur parasysh rëndësinë e këtij institucioni në procesin e Prokurimeve Publike sidhe faktin që në këtë institucion është kryer një auditim TI, u ndermor ky auditim TI me përdorim të teknikave CAAT në analizimin e bazave të të dhënave.

Më hollësisht:

OPINIONI I AUDITIMIT:

Grupi i auditimit mbështetur në Standartet ndërkombëtare të Auditimit përkatësisht në ISSAI 100, ISSAI 5300, ISSAI 5310 si dhe nenet 3 dhe 14 të ligjit 154 "Për Organizimin dhe Funksionimin e KLSH " datë 27.11.2014 konstaton:

-Agjencia e Prokurimit Publik, ka marrë masa rregullative dhe organizative, për të garantuar disponibilitetin e sistemeve të informacionit, masat e marra për rritjen e transparencës dhe efektivitetit të procedurave të prokurimit kanë rezultuar të suksesshme duke frenuar përdorimin e procedurës së prokurimit "negocim pa shpallje paraprake të njoftimit të kontratës" gjatë vitit 2018 në krahasim me treguesit e vitit 2017.

-Ndryshimet e strukturave të TI në APP (dhe jo vetëm) mbartin riskun e dobësimit të Qeverisjes TI duke ulur rolin e tyre në drejtim të mbledhjes së kërkesave, analizimit të nevojave, dhënies së zgjidhjeve dhe pjesëmarjes në vendimarje.

-Rezultatet e aritura janë të kompromentuara nga mungesa e Strategjisë për Teknologjinë e Informacionit, duke mbartur riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së APP.

Nr.	Gjetje nga auditimi	Rekomandimi
1	Nga auditimi mbi përmbajtjen e Buletinit që publikon APP bazuar në VKM nr. 176 datë 29.03.2006 rezulton se janë pjesë e tij dhe njoftimeve si Vende të Lira Pune, Shkollat e Larta dhe nga DAP, të cilat nuk janë në përputhje me objektin e aktivitetit të saj përcaktuar në ligjin 9643, datë 20.11.2006 "Për prokurimin publik" i ndryshuar, ndërkohë që në VKM janë lënë jashtë publikimit njoftime që lidhen me Koncensionet/PPP. Së pari publikimi i njoftimeve në kategoritë përmendur më sipër nuk orienton drejt të interesuarit dhe së dyti data e dorëzimit mund të ketë përfunduar përpara se të publikohet njoftimi pasi afati i publikimit të Buletinit është cdo 5 ditë.	KM dhe APP të konsiderojnë ndryshime në VKM nr. 176 datë 29.03.2006 "Për botimin e buletinit të njoftimeve" duke garantuar që përmbajtja e Buletinit të jetë në përputhje me objektin e aktivitetit përcaktuar në Ligj dhe publikimet e kategorive që nuk janë në përputhje me objektin e APP të delegohen në institucione përgjegjëse.

2	Nga auditimi u konstatua se: a. Përshkrimet e punës ku janë transferuar specialistët TI, nuk kanë ndryshuar shumë nga detyrat e mëparshme që po të njëjtët specialist kryenin. b. Në asnjë përshkrim pune nuk janë pasqyruar përgjegjësitë që lidhen me sigurinë rregullorja e sigurisë paragrafi 5.1 "Rregullorja për organizimin e punës në APP". c. Nuk rezultojnë të dokumentuara detyrat e përkohshme që kryejnë deri në plotësimin e strukturës me specialist TI nga AKSHI. d. Detyra të përcaktuara në rregulloren e sigurisë si prsh "**Administrator"** nuk adresohen në përputhje me përshkrimin e punës së punonjësve. e. Specialistët e TIK jo vetëm që nuk kanë kryer trajnime për periudhën object auditimi, por APP nuk ka marrë as përgjigje për ndonjë pjesëmarrje në të ardhmen nga insitucionet të cilave ju është drejtuar AKSHI-t dhe AKSK.	APP të rishikojë përshkrimin e punës për çdo punonjës, për të përcaktuar sa më afër detyrave reale që specialistët e saj kryejnë ku të përcaktojë dhe detyrat funksionale që dhe të identifikojë detyrat e përkohshme, të cilat kryhen aktualisht nga specialistët e saj por që do të transferohen tek AKSHI në zbatim të VKM nr. 673, datë 22.11.2017 "Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit".
3	Nga auditimi rezultoi se pozicioni i kërkuar për Oficer Sigurie nga APP nuk është miratuar në strukturën e saj gjatë periudhës objekt auditimi. APP nuk disponon as ndonjë përgjigje zyrtare në lidhje me këtë kërkesë e cila ka qenë një rekomandim nga KLSH në auditimin e mëprashëm.	APP nën përgjegjësinë që i jep ligji për administrimin dhe mbrojtjen e të dhënave të prokurimit publik, të rikërkojë ndryshim të strukturës për pozicionin Oficer Sigurie i cili edhe pse formimin mund ta ketë të bazuar në Teknologjinë e Informacionit nuk është pjesë e strukturës së TIK, por raportimi i tij duhet jetë në nivelin më të lartë drejtues të APP bazuar në standartet ndërkombëtare, pasi vetëm në këtë

		mënyrë mund të garantohet pavarësia dhe mund të shmanget konflikti i interesit, për arsye të ushtrimit të kompetencave të tij.
4	Nga auditimi rezulton se numri prej 4 specialistësh në teknologjinë e informacionit për vitin 2017 ka qenë shumë i vogël, për ofrimin e asistencës teknike për probleme të ndryshme që mund të hasin autoritetet kontraktore si dhe garantimin e disponibilitetit të sistemit të prokurimit që është 24 orë në 7 ditë të javës.	APP te identifikojë të gjitha detyrat lidhur me asistencën teknikë që janë realizuar nga specialistët e saj, që të parashikojë saktë delegimin e tyre tek specialistët e TIK që do të vihen në dispozicion nëpërmjet AKSHI-t.
5	Deri në momentin e kryerjes së auditimit, procedura e prokurimit "Pajisje elektronike për sistemin TI", e cila pritet të finalizohet nga AKSHI, nuk ka përfunduar ende, duke vënë në rrezik ecurinë normale të punës, kryesisht lidhur me procesin e backup-it (mungesa e Tape-ve). Grupi i auditimit e vlerëson këtë situatë me risk të lartë, pasi procesi i backup-t është një proces mjaft i rëndësishëm për ruajtjen periodike të të dhënave. Arsyet që kanë ndikuar në këtë vonesë, në opinionin tonë, krahas vonesave në kryerjen e procedurës nga AKSHI, të cilat grupi i auditimi për efekt të objektit të auditimit nuk mund ti auditojë, lidhen me kërkesën e vonuar të APP kundrejt AKSHI-t. Gjithashtu, edhe procedurat tjera të trajtuara nga grupi i auditimit, janë zhvilluar në muajin dhjetor, duke rrezikuar humbjen e fondeve të vitin ushtrimor në rast anullimi/shtyrjeje të përkohshme të procedurave.	Në vazhdimësi APP të marrë masa që procedurat e prokurimit, sidomos ato që lidhen me procese të rëndësishme të ecurisë së punës, të nisin sa më shpejtë gjatë vitit, duke mos rrezikuar gjendjen në situata të paparashikuara.

	Grupi i auditimit shpreh opinionin se procedurat e prokurimit, sidomos ato që lidhen me procese të rëndësishme të ecurisë së punës, duhet të nisin sa më shpejtë gjatë vitit, duke mos rrezikuar gjendjen në situata të paparashikuara	
6	Nisur nga eksperienca e grupit të auditimit si dhe gabimit të konstauar në procedurën e mësipërme "Blerje pajisje komjuterike, UPS dhe fotokopje 2017", për arsye të ndryshme, ka mjaft raste ku ana shkresore nuk përputhet me atë elektronike. Gjithashtu mbajtja e dokumentave shkresor, pa i bërë pjesë të dosjes elektronike të procedurave të prokurimit, rrit riskun e tjetërsimit të tyre me kalimin e kohës. Grupi i auditimit vlerëson se është e nevojshme përditësimi i faqes së APP, duke krijuar mundësinë e hedhjes apo ngarkimit të të gjithë dokumentacionit të procedurave të prokurimit, duke rritur besueshmërinë e gjurmës së auditimit të këtyre procedurave.	APP të shqyrtojë mundësinë e shtimit të opsionit të hedhjes së të gjithë dokumentacionit të tenderit me qëllim rritjen e besueshmërisë në procedurat e prokurimit duke e plotësuar elektronikisht të gjithë gjurmën e auditimit.
7	Nga auditimi mbi risqet në TIK, rezultoi se: -Risqet e identifikuara për vitin 2017 si dhe prioriteti dhe probabiliteti janë të njëjta me 3 risqet e identifikuara në vitin 2018, në mospërputhje me nenet 19-21 të ligjit nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar, udhëzimin nr. 30, datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik", i ndryshuar. -Në të dy regjistrat e viteve 2017 dhe 2018 nuk rezulton që gjatë vitit të ketë patur përditësime me risqe të reja të	APP të marrë masa për Informimin e AK me listën e kodeve CPV që përcaktojnë saktë kategorinë e produktit. Njëkohësisht APP të bëjë ndryshimet e nevojshme në listën e kategorive të produktit duke hequr nga mundësia e zgjedhjes kodin 000000 si dhe të garantojë suportin për ndryshime apo shtime në listën e kategorive.

	identifikuara gjatë periudhës. -Nuk janë analizuar dhe dokumentuar si pjesë e regjistrit të riskut hapat që duhen ndërmarrë nga specialistët e TIK, për minimizimin e çdo risku të identifikuar për teknologjinë e informacionit. - Nuk janë identifikuar risqe në lidhje me: *sigurinë, disponibilitetin dhe integritetin e sistemit dhe të dhënave që gjenerohen nëpërmjet sistemit të prokurimit publik* si dhe palët e treta që janë kontraktuar për ofrimin e shërbimit të mirëmbajtjes së sistemit të prokurimit elektronik dhe fizik. -Nuk janë identifikuar risqe të mundshme që lidhen me plotësimin e saktë të të dhënave për procedurat e parashikuara nga autoritet kontraktore, për tu zhvilluar në vitin kalendarik, proces ky i cili është informatizuar dhe ka përfunduar fazën e testimit. -Nuk janë identifikuar risqet në burimet njerëzore të TIK, të cilat duhen adresuar për të siguruar mirëfunksionimin dhe mbarëvajtjen e procesit të prokurimit. -Ndarja ose transferimi i risqeve së bashku me asetet tek AKSHI, dhe për cilat risqe ndjekja dhe minimizimi i tyre do të administrohen nga APP. -Nuk janë analizuar dhe identifikuar mbivendosjet ligjore, si dhe hapat që do të ndërmerren për minimizimin e problemeve që mund të ndodhin në sistemin e prokurimit si dhe përgjegjësitë ndërmjet e AKSHI-t dhe APP. -Nuk janë identifikuar rrisqe që lidhen me hapa të procedurës së prokurimit që janë ende të painformatizuar për	

	përmirësim të sistemit të prokurimit si prsh, të dhënat që lidhen me nënkontraktimin të cilin autoritet kontraktore aktualisht e administrojnë në letër.	
8	APP me transferimin e aseteve dhe burimeve njerëzore te AKSHI, në bashkpunim me këtë të fundit të analizojë dhe të konsiderojë risqet që lidhen me Teknologjinë duke bërë një ndarje sa më reale midis atyre që do të administroje vetë dhe atyre që për shkaqe teknike i delegohen AKSHI-t. Të dokumentohen përgjegjësit dhe hapat që duhen ndjekur për cdo risk të identifikuar. APP të përditësojë regjistrin me risqe të reja të identifikuara gjatë periudhës dhe të mbajë në monitorim të vazhdueshëm ecurinë e risqeve, ku theksi duhet të jetë në garantimin e sigurisë, disponibilitetit dhe integritetit të sistemit dhe të dhënave që gjenerohen nga sistemi i prokurimit publik.	Nga auditimi rezulton se lista e kodeve edhe pse është konfiguruar dhe plotësimi në sistem është bërë i detyrueshëm, në web nuk është publikuar, për ti dhënë mundësi autoriteteve kontraktore që të studjojnë listën e kategorive, përpara plotësimit të saj.
9	: Portali i APP nuk përdor një lidhje të sigurtë *(connection security)* HTTPS *(HyperText Transfer Protocol Secure)* (*Not secure status*) që do të thotë se serveri i faqes së internetit nuk përdor një certifikatë sigurie për të vërtetuar identitetin e internetit në shfletuesit e ndryshëm. Në mungesë të kësaj certifikate ekziston risku për humbjen e privatësisë, ndryshimit të informacionit që merret ose jepet me anë të këtij portali.	APP në bashkëpunim me strukturat përgjegjëse për mbarëvajtjen e faqes Web, të marrin masa për përmirësimin e faqes Web me elementët përkatës të sigurisë *(certifikatën e sigurisë)* së navigimit online për të rritur sigurinë dhe ndihmesën ndaj përdoruesve.
10	APP disponon politika të shkruara mbi vazhdimësinë e punës (business continuity), si dhe politika të shkruara	Nga APP të merren masat e nevojshme për testimin e politikave mbi vazhdimësinë e punës (business

	mbi rimëkëmbjet nga katastrofat (disaster recovery). Nga auditimi u konstatua se APP nuk disponon dokumentacion për ngritjen e grupit të punës apo të testimeve zhvilluara për funksionimin e këtyre dy politikave mjaft të rëndësishme për sistemin e APP, në kundërshtim me pikën 9.1 të Planit të Sigurisë së Rishikuar me nr. 8904/7 prot, datë 10.04.2017. Këto testime duhet të kryhen në mënyrë periodike dhe me theks të lartë sa herë të ketë ndryshime thelbësore, me qëllim dhënien e sigurisë së arsyeshme se sistemi do të funksionojë në të gjitha situatat hipotetike, dhe se burimet njerëzore janë të mirënjohura me zbatimin e hapave që duhen ndjekur. Për këtë arsye grupi i auditimit shprehet me rezervë mbi funksionimin apo jo të dy politikave të mësipërme mbi vazhdimësinë e punës dhe rimëkëmbjen nga katastrofat, në rast se do të jetë e nevojshme. Gjithashtu plani i fundit i rekuperimit nga katastrofa i vënë në dispozicion të grupit të auditimit është me datë 07.04.2017, në kundërshtim me pikën nr. 9.3 të Planit të Sigurisë së Rishikuar me nr. 8904/7 prot, datë 10.04.2017, sipas së cilës këto plane duhet të rishikohen të paktën një herë në vit.	continuity) dhe mbi rimëkëmbjen nga katastrofat (disaster recovery) sa herë që ato azhornohen apo ndryshojnë, me qëllim dhënien e sigurisë së arsyeshme se do të funksionojë në të gjitha situatat hipotetike, dhe se burimet njerëzore janë të mirënjohura me zbatimin e hapave që duhen ndjekur. Nga APP të merren masat e nevojshme për përditësimin e planeve të rimëkëmbjes nga katastrofat dhe vazhdimësisë së punës të paktën një herë në vit me qëllim të qënurit gjithnjë në koherent me ndryshimet e ndodhura, në përputhje me Planin e Sigurisë së Rishikuar me nr. 8904/7 prot, datë 10.04.2017.
11	Grupi i auditimit e testoi faqen e APP në disa “free page security test”, nga ku rezultuan mjaft raste ku shfaqeshin “malware” si dhe pika të dobëta dhe jo të sigurta të faqes. Për arsye sigurie dhe konfidencialiteti, grupi i auditimit nuk do ti bëjë pjesë të materialit, por do ti	APP të marrë masa për ngritjen e një grupi pune për analizimin e rasteve të konstatuara nga grupi i auditimit, si dhe verfikimin periodik dhe të shpeshtë të sigurisë së faqes Web, me qëllim minimizimin e kërcënimeve dhe rritjen e

	komunikojë ato me stafin përgjegjës të APP.	sigurisë së faqes Web.
12	Nga auditmi u konstatua se nuk ka një rregullore apo dokument tjetër shkresor ku të përcaktohet qartë lidhja përdoues-punonjës i APP. Përdoruesit dhe të drejtat e tyre përcaktohen rast pas rasti, në varësi të burimeve njerëzore dhe të volumit të punës duke krijuar një risk potencial të akordimit subjektiv të të drejtave mbi përdorimin e sistemit, si dhe akumulimin e privilegjeve, në kundërshtim me pikën 3.2.2.1 të Planit të Sigurisë së Rishikuar me nr. 8904/7 prot, datë 10.04.2017.	APP të marrë masa për hartimin e një rregulloreje ku të përcaktohet qartë lidhja ndërmjet pozicionit të punës dhe të drejtave që ky pozicion duhet të ketë si user i sistemit me qëllim uljen e riskut të akordimit subjektiv të të drejtave mbi përdorimin e sistemit, si dhe akumulimin e privilegjeve.
13	Agjencia e Prokurimit Publik ka lejuar Autoritetet Kontraktore nëpërmjet një llogarie administratori të hapë llogari të tjera sipas nevojave të institucionit për të aksesuar në sistemin e APP. Nga auditimi u konstatua se hapja e këtyre përdoruesve mbetet pothuajse e pamonitoruar, pasi vetë APP nuk kryen monitorime që lidhen me këtë veprim, duke rritur riskun e krijimit të përdoruesve të paautorizuar, e për pasojë humbjen e konfidencialitetit të të dhënave apo keqpërdorimin e tyre.	Në vazhdimësi APP të marrë masa për verifikimin e përdoruesve të hapur nga llogaritë administratore të Autoriteteve Kontraktore, duke ulur riskun e humbjes së konfidencialitetit të të dhënave si dhe keqpërdorimit të tyre.
14	Nga auditimi u konstatua se APP nuk ka Strategji për Teknologjinë e Informacionit, mungesa e të cilës sjell mos pasqyrimin e objektivave lidhur me infrastrukturën, burimet e nevojshme si dhe instrumentave të nevojshëm për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së APP.	

15	App nuk ka menazhuar ndryshimin e strukturave të burimeve njerëzore në përputhje me Vendimin e Komisionit të Ristrukturimit të Agjencisë së Prokurimit Publik nr, prot 3285 datë 19.03.2018 duke mos updatuar ndryshimet në rregulloret, ndarjen e detyrave të njesisë së Teknologjinë e Informacionit në përputhje me organizimin, strukturën e re. Standartet e Praktikat me të mira të rekomandojnë që Qeverisjes TIK duhet të vendosi politika në fushën e TI. Këto politika vendosin kërkesat për mbrojtjen e aseteve të informacionit dhe mund ti referohen procedurave ose mjeteve të tjera në mënyrën sesi këto do të mbrohen. Politikat duhet të jenë të disponueshme ndaj të gjithë punonjësve perdorues te TI. APP ka vendosur politika e parime në planin e sigurisë (version 3 datë 10.04.2017) si dhe në Politikat e Vazhdueshmerisë së Punës së Institucionit.	
16	Nga auditimi u konstatua se APP nuk ka krijuar facilitetet e nevojshme për vënien në dispozicion të gjithë punonjësve përgjegjës për sigurinë e informacionit, përfshirë përdoruesit e sistemeve të cilët kanë rol në mbrojtjen e informacionit në kundështim me pikën 2 të planit të sigurisë "Qëllimi dhe fusha e zbatimit ku thuhet: "ky udhezim do të behet efektiv duke u zbatuar në mënyrë të detyrueshme nga çdo punonjës i APP .Të gjithë punonjesit duhet të familjarizohen me përmbajtjen e tij dhe ta bëjnë pjesë të menyrës së të menduarit	

	dhe të veprimtarise se tyre të perditshme. Në vijim të VKM Nr. 673, datë 22.11.2017 sipas së cilës strukturat TI kalojnë në varësi nga AKSHI-t (të APP-së dhe jo vetëm). APP në vijim të këtyre ndryshimeve me Vendimin e Komisjonit të Ristrukturimit të Agjencisë së prokurimit Publik nr, prot 3285 date 19.03.2018 i drejtohet DAP për propozimin e transferimit të përhershëm të nënpunësve civile në kuadër të ristrukturimit i kërkon transferimin e përhershëm të drejtorit të Drejtorisë së Teknollogjisë së informacionit dhe publikimit si dhe 7 specialistëve, të APP nga Drejtoria, e Informacionit dhe Publikimit në Drejtorinë e Informacionit dhe Publikimit.	
17	Me ndryshimet e strukturave APP i cënohet pjesa e rëndësishme e Qeverisjes TI. Roli i strukturës TI nuk duhet dhe mund të zevendesohet me struktura të tjera pasi struktura TI luan një rol të rëndesishëm në drejtim të mbledhjes së kërkesave, analizimit të nevojave, dhënies së zgjidhjeve dhe pjesëmarjes në vendimarje për problemet e TI.	
18	Autoritetet Kontraktore me gjithe përmirësimet gjatë vitit 2018 kanë vazhduar të përdorin në një shkallë të lartë procedurën me negocim pa shpallje paraprake e cila zë 31.8% të numrit total të procedurave të prokurimit, të zhvilluara gjatë vitit 2017 apo 8.3% të vlerës totale. Konstatohet se në 67% e rasteve të	

	përdorimit të kësaj procedure janë për mbulimin e nevojave të fillim vitit për blerjen e mallrave dhe shërbimeve. Përdorimi i kësaj metode për të "mbuluar nevojat" e fillimit të vitit për blerjen e mallrave dhe shërbimeve mbart risqet: keqplanifikimet e nevojave dhe shmangien e konkurrencës, me pasojë efektivitet shumë të ulët të prokurimit.	
19	Sistemi i prokurimit publik nuk ka filtrat e nevojshëm për mos lejimin e hedhjes të të dhënave gabim, apo lejuar lidhjen e kontratave pa pasur fondin limit të nevojshëm në 14 raste fondi i prokuruar (609,887,131 lekë) është më i madh se fondi limit (395,611,677 lekë) në vlerën -214,275,454 lekë.	
20	Nga krahasimi me vendet e rajonit konstatohet se megjithë eksperiencën dhe punën e bërë, niveli i përdorimit të prokurimit elektronik gjatë vitit buxhetor 2017 është relativisht i ulët. - tregues nën mesataren e vendeve të rajonit të fondit të prokuruar ndaj PBB. - tregues mbi mesataren e vendeve të rajonit të fondit të prokuruar ndaj shpenzimeve buxhetore.	
21	Nga analiza krahasimore e përdorimit të procedurës "Me Negocim pa Shpallje Paraprake" nga Autoritetet Kontraktore gjatë tremujoreve të parë të viteve 2017 dhe 2018 tregojnë se megjithë uljen e fondit të përdorur me këtë procedurë gjatë tremujorit të parë të vitit 2018 niveli i efektivitetit të prokurimit mbetet i ulët.	
22	Procedurat e Prokurimit të shpallura kanë një shkallë të lartë prej 19% të anullimit, duke treguar se puna e AK për	

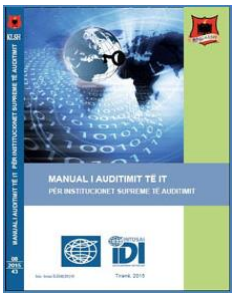
	përgatitjen e procedurave (përcaktimi i nevojave, studimi i tregut, hartimi i dokumentacionit në përputhje me legjislacionin) është e pa mjaftueshme dhe ka nevojë për përmirësim. Mos kryerja në kohë e investimeve duhet të kosiderohet jo vetëm si mos efektivitet në përdorimin e burimeve por impakti negativ i tyre ka një spektër me të gjërë.	
23	Nga analiza e procedurave të publikuara dhe të kryera me përfundim lidhje kontrate rezultojnë me risk 393 procedura me fond të prokuruar 8,767,669,428 lekë të cilat janë lidhur në muajt janar-shkurt si rrjedhojë e kohës së limituar në përgatitjen e dokumentacionit përkatës si dhe zhvillimit të procedurave të prokurimit. Paraqesin risk të lartë në lidhje me kohën e nevojshme për zbatimin e kontratave 435 procedura me fond 8,248,475,384 të cilat janë lidhur në muajin dhjetor 2017.	
24	Treguesit e pritshëm të procedurave të prokurimit publik për vitit 2018 mbartin risqet e: - mos menaxhimit të ndryshimeve nga strukturat e caktuara për përqendrimin e prokurimeve - kohës së limituar të hyrjes në fuqi të përqendrimeve	

ANEKSE

METODOLOGJIA E AUDITIMIT TË TEKNOLOGJISË SË INFORMACIONIT

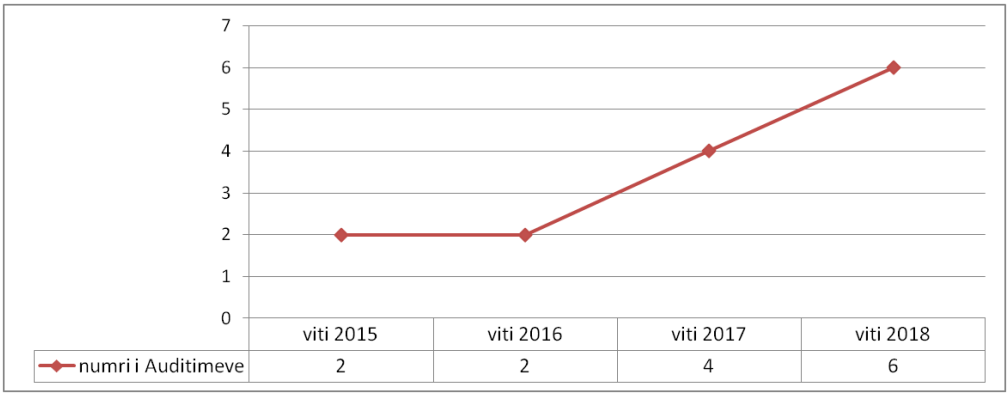
KLSH zhvillon Auditimin e Teknologjisë së Informacionit dhe mbështetur në Standardet Kombëtare dhe Ndërkombëtare të Auditimit:

- Mandati për kryerjen e Auditimit mbështetet në ISSAI 1 Neni 22 dhe Ligjin e KLSH Nr.154/2014 Neni 3 dhe 14
- Manualin e Auditimit të Teknologjisë së Informacionit (WGITA) dhe Manuali Aktiv i TI. COBIT 4.1 Objektivat e Kontrollit të Teknologjisë së Informacionit.
- Udhëzime mbi Auditimet Teknologjinë e Informacionit, ISSAI 5300.6, 8 dhe 12.2, 16.19, 21.1, 23.
- ISSAI 100.36,48 Udhëzime për të gjitha auditimet e sektorit publik .
- ISSAI 5310 - udhëzues për shqyrtimin e sigurisë së sistemit të informacionit (ISS) në organizatat qeveritare.
-Legjislacionin dhe Standartet Shqiptare të fushës.

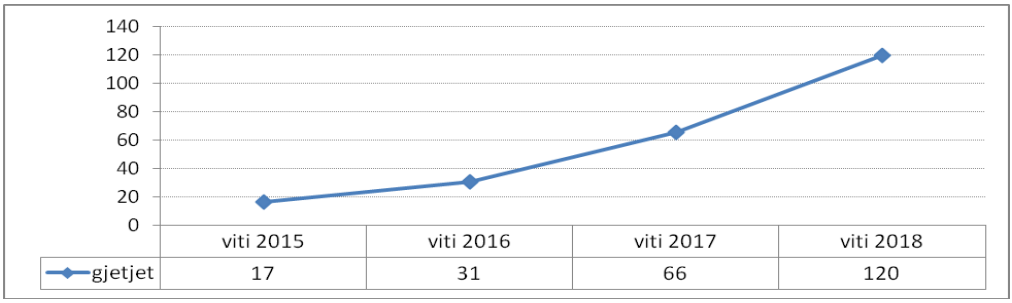
COBIT		
Control Objectives for Information and related Technology (COBIT®) siguron praktika të mira përgjatë një strukure dhe operimi, si dhe paraqet aktivitetet në një strukturë të menaxhueshme edhe logjike.		
	34 PROCESE NË 4 FUSHA TË MËDHA Planifikim dhe Organizim Disponim dhe Implementim Dorëzim dhe Mbështetje Monitorim dhe Vlerësim	**PËR ÇDO PROCES REKOMANDON:** Objektiva kontrolli Qëllime dhe matje Grafikun Raci Inpute dhe Outpute Model maturiteti
Manualin e Auditimit të TI (WGITA) dhe Manuali Aktiv i TI.		
	**Manuali i auditimit TI përmban:** Shtatë çështje të mëdha auditimi: - Qeverisja dhe Politikat TI - Zhvillimi/Prokurimi i zgjidhjeve TI - Operacionet TI - Nënkontraktimi - BCP dhe DRP - Siguria e Informacionit - Kontrollet e Aplikacioneve	Matricat e auditimit-të bazuara mbi pyetje auditimi. Përcaktimin dhe përshkrimin e tyre, Elementët kyç të këtyre çështjeve, Risqet TI të subjekteve, pyetësorët e auditimit

Auditimet e TI-së në vitet 2015-2018

Numri i Auditimet të TI-së të zhvilluara



Gjetjet nga Auditimet e TI-së



Lista e subjekteve të Audituara.

Nr	Viti/Nr.		Subjekti
1.	2018	1.	Agjencia Kombëtare e Shoqërisë së Informacionit.
2.		2.	Drejtoria e Përgjithshme e Gjendjes Civile.
3.		3.	Departamenti i Administratës Publike.
4.		4.	Qendra Kombëtare e Biznesit.
5.		5.	Bashkia Elbasan.
6.		6.	Agjencia e Prokurimit Publik.
7.	2017	1.	Drejtoria e Përgjithshme të Taksave dhe Tarifave Vendore.
8.		2.	Instituti i Statistikave.
9.		3.	Drejtorinë e Ujësjellës Kanalizimeve, Tiranë.
10.		4.	Instituti i i Sigurimeve Shoqërore.
11.	2016	1.	Drejtoria e Përgjithshme të Thesarit dhe Drejtoria e Shërbimeve dhe Teknologjisë së Informacionit në Ministrinë e Financave.
12.		2.	Fondi i Sigurimit të Detyrueshëm të Kujdesit Shëndetësor.
13.	2015	1.	Agjencia e Prokurimit Publik.
14.		2.	Agjencia e Kontrollit të Barnave dhe Pajisjeve Mjekësore

FJALORI I SHKURTIMEVE

AK	**A**utoriteti **K**ontraktor
AKBPM	**A**gjencia e **K**ontrollit të **B**arnave dhe **P**ajisjeve **M**jekësore
AKSHI	**A**gjencia **K**ombëtare e **Sh**oqërisë së **I**nformacionit
APP	**A**gjencia e **P**rokurimit **P**ublik
BCC	**B**usiness **C**ontinuity **C**entre
BCP	**B**usiness **C**ontinuity **P**lan
BE	**B**ashkimi **E**vropian
CAAT	**C**omputer **A**ssisted **A**uditing **T**echniques
CEF	**C**enter of **E**xcellence in **F**inance
CMIS	**C**ontent **M**anagement **I**nteroperability **S**ervices
COBIT	**C**ontrol **Ob**jectives for **I**nformation and related **T**echnology
DAP	**D**epartamenti i **A**dministratës **P**ublike
DAQ,	**D**rejtoria e **A**rkivës **Q**endrore
DBI	**D**rejtoria e **B**urimeve të **I**nformacionit
DPD	**D**rejtoria e **P**ërgjithshme e **D**oganave
DPGJC	**D**rejtoria e **P**ërgjithshme e **Gj**endjes **C**ivile.
DPT	**D**rejtoria e **P**ërgjithshme e **T**atimeve
DPTH	**D**rejtoria e **P**ërgjithshme e **Th**esarit
DSTI	**D**rejtoria e **S**hërbimeve dhe **T**eknologjisë së **I**nformacionit
DPTTV	**D**rejtoria e **P**ërgjithshme të **T**aksave dhe **T**arifave **V**endore
DRC	**D**isaster **R**ecovery **C**entre
DRP	**D**isaster **R**ecovery **P**lan
EUROSAI	**Eur**opean **O**rganisation of **S**upreme **A**udit **I**nstitutions
FSDKSH.	**F**ondi i **S**igurimit të **D**etyrueshëm të **K**ujdesit **Sh**ëndetësor
HRMIS	**H**uman **R**esources **M**anagement **I**nformatics **S**ystem
IDEA	**I**nteractive **D**ata **E**xtraction and **A**nalysis
IDI	**I**ntosai **D**evelopment **I**nitiative
INSTAT	**In**stitutin e **Stat**istikave.
INTOSAI	**Int**ernational **O**rganisation of **S**upreme **A**udit **I**nstitutions
IPA	**I**nstrument for **P**re-Accession **A**ssistance
ISSAI	**I**nternational **S**tandards of **S**upreme **A**udit **I**nstitutions
ISSH	**I**nstitutin e **S**igurimeve **Sh**oqërore
ITASA	**IT A**udit **S**elf-**A**ssessment

ITSA	**IT S**elf-**A**ssessment
KLSH	**K**ontrolli i Lartë i **Sh**tetit
MB	**M**inistria e **B**rendshme
MF	**M**inistria e **F**inancave
MNSH	**M**arrëveshje **N**ivel **Sh**ërbimi
MTQ	**M**anaging **T**otal **Q**uality
NjP	**Nj**esia e **P**rokurimit
QKB	**Q**endra **K**ombëtare e **B**iznesit
QKR	**Q**endra **K**ombëtare e **R**egjistrimit
RKGJC	**R**egjistrit **K**ombëtar të **Gj**endjes **C**ivile
SAI	**S**upreme **A**udit **I**nstitution
SIFQ	**S**istemi **I**nformatik **F**inanciar i **Q**everisë
SIGMA	**S**upport for **I**mprovement in **G**overnance and **M**anagement
SLA	**S**ervice-**L**evel **A**greement
T.I.	**T**eknologjia e **I**nformacionit
TIK	**T**eknologjia e **I**nformacionit dhe **K**omunikimit
TVSH.	**T**atimi i **V**lerës së **Sh**tuar
UFSH	**U**rdhri i **F**armacistëve të **Sh**qipërisë
UKT	**U**jësjellës **K**analizime **T**iranë
UMF	**U**dhëzimin i **M**inistrisë së **F**inancave
USAID.	**U.S**. **A**gency for **I**nternational **D**evelopment
VKM	**V**endim i **K**ëshillit të **M**inistrave
WAN	**W**ide **A**rea **N**etwork
WGITA	**W**orking **G**roup on **IT A**udit

CIP Katalogimi për botim BK Tiranë

RSH. Kontrolli i Lartë i Shtetit

Auditimi i teknologjisë së informacionit 2014-2018 /

RSH. Kontrolli i Lartë i Shtetit. – Tiranë : KLSH, 2018

198 f. ; 16.5 x 23.5 cm.

ISBN 978-9928-159-77-9

1.Kontrolli i Lartë i Shtetit 2.Teknologjia e informacionit

3.Kontrolli 4.Raporte 5.Shqipëri

351.95(496.5)(047)

Shtypur në Shtypshkronjën
MORAVA

ISBN 978-9928-159-77-9

Kontrolli i Lartë i Shtetit
Rruga "Abdi Toptani", Nr. 1
Tiranë Tel/Fax 04/228485, Tel.04/251267
Web-site: www.klsh.org.al; e-mail: klsh@klsh.org.al