REPUBLIKA E SHQIPËRISË
KONTROLLI I LARTË I SHTETIT
Departamenti i Auditimit të Teknologjisë së Informacionit

Adresa: Rruga *"Abdi Toptani" Nr.1 Tiranë* E-mail: klsh.org.al; web-site ëëë.klsh.org.al

Nr. 1229 /10 Prot. Tiranë, më 19.12.2018

V E N D I M

Nr. 213, Datë 19.12.2018

PËR

AUDITIMIN E USHTRUAR NË 4 SUBJEKTE PËR VERIFIKIMIN E ZBATIMIT TË REKOMANDIMEVE TË LËNA NË AUDITIMET E TREMUJORIT IV- TË VITIT 2017, DHE 4-MUJORI (JANAR-PRILL) 2018: DREJTORIA E UJËSJELLËS KANALIZIME TIRANË, INSITITUTI I SIGURIMEVE SHOQËRORE, INSTITUTI I STATISTIKAVE, DREJTORIA E PËRGJITHSHME E TAKSAVE DHE TARIFAVE VENDORE, TIRANË"

Nga auditimi i ushtruar në 4 subjekte Drejtoria e Ujësjellës Kanalizime Tiranë, Insitituti i Sigurimeve Shoqërore, Instituti i Statistikave, Drejtoria e Përgjithshme e Taksave dhe Tarifave Vendore, Tiranë".
Pasi u njoha me Raportin Përfundimtar të Auditimit dhe projektvendimin e paraqitur nga Grupi i Auditimit të Departamentit të Auditimit të Teknologjisë së Informacionit, shpjegimet e dhëna nga subjekti i audituar, mendimin për vlerësimin mbi objektivitetin dhe për cilësinë e auditimit nga Drejtori i Departamentit të mësipërm, mendimin nga Drejtori i Departamentit të Metodologjisë, Standardeve dhe Sigurimit të Cilësisë së Auditimit dhe nga Drejtori i Përgjithshëm, në mbështetje të neneve 10, 15 dhe 30, të ligjit 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",

VENDOSA:

I. Të miratoj Raportin Përfundimtar të Auditimit "*Mbi Verifikimin e zbatimit të rekomandimeve të lëna në auditimet e mëparshme të evaduara në 3-mujorin e fundit të vitit 2017 dhe 4-mujori (Janar-Prill) 2018",* të ushtruar në 4 Subjekte: Drejtoria e Ujësjellës Kanalizime, Tiranë, Instituti i Sigurimeve Shoqërore, Instituti i Statistikave, Drejtoria e Përgjithshme e Taksave dhe Tarifave Vendore", sipas programit të auditimit nr. 1229 prot, datë 02.11.2018, të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit .

II. Të miratoj rekomandimet e përcaktuara dhe të kërkoj marrjen e masave, për sa vijon:
Nga 4 subjektet e verifikuara rezulton se Instituti i Sigurimeve Shoqërore, Instituti i

Statistikave, Drejtoria e Përgjithshme e Taksave dhe Tarifave Vendore**,** kanë kthyer përgjigje në KLSH, brenda afatit ligjor prej 20 ditëve, duke hartuar dhe planet e veprimit (*programet e punës).* DPTTV dhe INSTAT kanë raportuar në KLSH me shkrim mbi ecurinë e zbatimit rekomandimeve brenda afatit 6 mujor, ndërsa ISSH nuk ka raportuar mbi këtë ecuri.
UKT, nuk ka kthyer përgjigje për hartimin e planit të veprimit për vënien në zbatim të rekomandimeve në respektim të afatit 20 ditë kalendarike, në kundërshtim me pikën 15 shkronja (j) të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit". UKT nuk ka kthyer përgjigje edhe mbi ecurinë e zbatimit të rekomandimeve të lëna në respektim të afatit ligjor prej 6 muajsh, në kundërshtim me pikën 2 të nenit 30 të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit".
Nga auditimi i realizuar në 4 subjektet e verifikuara për zbatimin e *detyrave dhe masave të rekomanduara në auditimin e kryer në në 3-mujorin e fundit të vitit 2017 dhe 4-mujori (Janar-Prill) 2018,* rezultoi një nivel i lartë pranueshmërie në **masën 100%, ku 65 masa organizative** të rekomanduara janë pranuar plotësisht. Nga një total prej 65 masash organizative të rekomanduara, janë zbatuar plotësisht 26 masa, nuk janë zbatuar 14 masa, janë zbatuar pjesërisht 8 masa, ndërsa 17 masa janë në proces zbatimi.

I. DREJTORIA E UJËSJELLËS KANALIZIME, TIRANË - UKT

KLSH në përfundim të Auditimit, për përmirësimin e gjendjes ka lënë *15 rekomandime si masa organizative*, me shkresën nr. 479/6, datë 25.09.2017 sipas Vendimit nr.119, datë 25.09.2017 të Kryetarit të KLSH-së, ka dërguar Raportin Përfundimtar të Auditimit dhe rekomandimet për auditimin e ushtruar me programin nr. 479/1, datë 05.06.2017**.**
UKT nuk ka kthyer përgjigje mbi hartimin e planit të veprimit për vënien në zbatim të rekomandimeve në respektim të afatit 20 ditë kalendarike, në kundërshtim me pikën 15 shkronja (j) të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit". UKT nuk ka kthyer përgjigje mbi ecurinë e zbatimit të rekomandimeve të lëna në respektim të afatit ligjor prej 6 muajsh, në kundërshtim me pikën 2 të nenit 30 të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit".
Nga *15 rekomandime si masa organizative, të cilat janë pranuar plotësisht, janë zbatuar plotësisht 2, nuk janë zbatuar 8 dhe janë zbatuar pjesërisht 5 rekomandime.*

KLSH kërkon intensifikimin e veprimeve për përfundimin e rekomandimeve që rezultuan në proces si dhe marrjen e masave të menjëhershme për zbatimin e rekomandimeve që rezultuan të pazbatuara, si vijon:

A. MASA ORGANIZATIVE:

1. Gjetje nga auditimi. 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.
1.1 Rekomandimi: 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.

2. Gjetje nga auditimi. Nga auditimi i procedurave të prokurimit zhvilluar për projektet e teknologjisë së informacionit për:
- Krijimi i një mjedisi të ri dhomë serverash për drejtorinë e Ujësjellës Kanalizime Tiranë sh.a,
- Blerje pajisje monitorimi, licenca, software financiar dhe faturimi (SMI) sistem menaxhimi informacioni për UKT sh.a,
- Infrastrukturë TI Server, pajisje Data Center për UKT sh.a, u konstatuan të njëjtat mangësi, si më poshtë:

- 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".
- 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".
- 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).
- 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 në të gjitha procedurat, duke sjellë në këtë mënyrë një kufizim në pjesëmarrje.
- 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.

2.1 Rekomandimi: 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 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.

f. 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".

3. Gjetje nga auditimi. 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.

c. Në kontratën e shërbimit nënshkruar midis palëve, UKT dhe JV "BNT Electronics" & "Jehona Softëare", 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.

3.1 Rekomandimi:

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 hapësirë për kosto të paparashikuara.

d. 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 JV "BNT Electronics" & "Jehona Softëare", për mirëmbajtje dhe zhvillim të mëtejshëm të sistemit të faturimit Al-Billing.

4. Gjetje nga auditimi: 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.

4.1 Rekomandimi: 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.

5. Gjetje nga auditimi. 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 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.

e) 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.

5.1 Rekomandimi: UKT dhe STI të hartojnë, miratojë e zbatojë rregulla për hapjen dhe mbylljen e përdoruesve në sistemet e teknologjisë së informacionit si dhe për vendosjen dhe ndërimin 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**.**

6. Gjetje nga auditimi. 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 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.

6.1 Rekomandimi: 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.

7. Gjetje nga auditimi. Nga auditimi i bazës rregullatore të sektorit IT u konstatua se UKT nuk ka rregullore të veçantë për Teknologjinë e Informacionit.
7.1 Rekomandimi: UKT të marrë masa për hartimin e një Rregulloreje të Përgjithshme mbi Teknologjinë e Informacionit, në të cilën të përfshihen të gjitha operacionet IT, 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.

8 Gjetje nga auditimi. 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.
8.1 Rekomandimi: 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 IT dhe çdo përdoruesi të sistemeve IT për sistemet, sigurinë dhe teknologjinë e informacionit. Te hartoje e miratoje planet trajnimit si dhe zhvillojë ato.

9. Gjetje nga auditimi. 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.
9.1 Rekomandimi: Strukturat Drejtuese në UKT në bashkëpunim me Sektorin e 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 Drejtorinë e Auditimit të Brendshëm të marrin masa për përfshirjen e Sektorit i Teknologjisë së Informacionit në procesin e auditimit.

10. Gjetje nga auditimi. 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 bazë ngjarjesh, d.m.th jepet suport, mbështetje teknike dhe logjike për operacionet IT 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 IT.
10.1 Rekomandimi: 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, dokumentimin dhe monitorimin e incidenteve. Gjithashtu të marren masa për menaxhimin e ndryshimeve dhe dokumentimin e të gjithë procesit të ndryshimeve.

11. Gjetje nga auditimi. 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 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.

11.1 Rekomandimi: 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 shmangien, adresimin, transferimin apo pranimin e risqeve të identifikuara, si dhe monitorimin periodik për zbatimin e masave të marra nga sektori përgjegjës.

12. Gjetje nga auditimi 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 si dhe veprimet e rekomandimet e ndërmarra. UKT nuk ka listë të artikujve të vlerësuar prioritare për proceset emergjente

b) Mbajtja e Rrjetit netëork i UKT ndodhet në dhomën e vjetër të serverave janë jashtë çdo standardi përbën risk për funksionimin e sistemit TI të UKT.

c) Institucioni nuk ka politika në lidhje me aksesin në rast emergjence në qendrën e të dhënave.

12.1 Rekomandimi: 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 IT. Planifikimi dhe testimi i sistemeve IT të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen.

13. Gjetje nga auditimi. 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 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.

h. 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.

13.1 Rekomandimi:

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 dispeçerie 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.

INSTITUTI I SIGURIMEVE SHOQËRORE - ISSH

KLSH në përfundim të Auditimit, për përmirësimin e gjendjes ka lënë *21 rekomandime si masa organizative*, me shkresën nr. 1222/5, datë 18.06.2017 sipas Vendimit nr.65, datë 18.06.2017 të Kryetarit të KLSH-së, ka dërguar Raportin Përfundimtar të Auditimit dhe rekomandimet për auditimin e ushtruar me programin nr. 1222/1, datë 26.01.2017**.**

ISSH ka kthyer përgjigje me shkresën nr.723/14, datë 18.07.2018 mbi hartimin e planit të veprimit për vënien në zbatim të rekomandimeve në respektim të afatit 20 ditë kalendarike, në zbatim të pikës 15 shkronja (j) të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit". Nga ana e insititucionit nuk është kthyer përgjigje mbi ecurinë e zbatimit të rekomandimeve të lëna në respektim të afatit ligjor prej 6 muajsh, pika 2 e nenit 30 të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit".

Nga *21 rekomandime, si masa organizative, të cilat janë pranuar plotësisht, janë zbatuar plotësisht 5, zbatuar pjesërisht 3, nuk janë zbatuar 6 dhe janë në proces zbatimi 7 rekomandime.*

KLSH kërkon intensifikimin e veprimeve, për përfundimin e rekomandimeve që rezultuan në proces si dhe marrjen e masave të menjëhershme për zbatimin e rekomandimeve që rezultuan të pazbatuara, si vijon:

A. MASA ORGANIZATIVE:

1 Gjetje nga auditimi: 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.

1.1 Rekomandimi: 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

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.

2. Gjetje nga auditimi: Nga auditimi u konstatua se:
a. 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.
b. Nuk ka të afishuar procedurat se si një qytetar mund ta transferojë pensionin nga një qytet në tjetrin , ku duhet ta bëjë kërkesën , cilat janë procedurat që duhet të ndiqen.
c. 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.
d. 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.
e. 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.
f. Nuk ka rregullore për faqen e webit si dhe mungon shërbimi i intranetit.
g. 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;
h. Lista e kompensimeve nuk është e plotë në faqe, aty gjenden vetëm 2 lloje kompensimesh;
i. 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 web nuk janë funksional;
j. Mungon shërbimi i intranetit.
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 broëserave (shfletuesave),
- Nuk ka dokumentacionë administruar nëse janë bëre modifikime të përmbajtjes të faqes web.

2.1 Rekomandimi: 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 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.

3. Gjetje nga auditimi: 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 IT në institucion.
3.1 Rekomandimi: ISSH në bashkëpunim me Drejtorinë e Burimeve të Informacionit dhe me strukturat këshilluese mbi IT, 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 IT në institucion duke hartuar plane veprimi për incidentet e mundshme si dhe për menaxhimin e ndryshimeve.

Krahas Rregullores së Përgjithshme të IT, 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.

4. Gjetje nga auditimi: 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.
4.1 Rekomandimi: 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.

5. Gjetje nga auditimi: 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 regjistrin e personave që kanë ndërruar jetë.
- 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.
- 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.
- 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:
- Për llogaritjen e kontributeve shoqërore për punëmarrësin
- Për llogaritjen 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).

5.1 Rekomandimi: 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.

6. Gjetje nga auditimi: 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 sistem 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.
6.1 Rekomandimi: 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.

7. Gjetje nga auditimi: 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 IT.
7.1 Rekomandimi: 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.

8. Gjetje nga auditimi: Nga auditimi u konstatua se:
- 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.
8.1 Rekomandimi: 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. Gjetje nga auditimi: 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).
9.1 Rekomandimi: 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).

10. Gjetje nga auditimi: 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.
10.1 Rekomandimi: 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.

11. Gjetje nga auditimi: Nga auditimi i Menaxhimit të Incidenteve dhe Problemeve në ISSH dhe DBI u konstatua se nuk janë hartuar rregulla mbi menaxhimin e incidenteve dhe institucioni nuk ka të dokumentuar një plan masash për trajtimin e gabimeve dhe incidenteve që mund të ndodhin në infrastrukturën IT. Mungesa e këtij plani masash bën që institucioni të

mos ketë të identifikuar risqet me efekt negativ në IT 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.
11.1 Rekomandimi: Strukturat Drejtuese në ISSH në bashkëpunim me Drejtorinë e Burimeve të Informacionit të marrë masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve. Gjithashtu të marren masa për menaxhimin e ndryshimeve dhe dokumentimin e të gjithë procesit të ndryshimeve.

12. Gjetje nga auditimi: 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 IT të ISSH-së pika 4.4 "Analiza e riskut dhe ndryshimit të dokumenteve". Gjithashtu u konstatua:
a. Nuk ka kryer vlerësime të risqeve dhe 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.
b. Nuk ka një mekanizëm efektiv dhe të mire dokumentuar të vlerësimit të riskut të sigurisë së informacionit. Përsa 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.
12.1 Rekomandimi: Strukturat drejtuese në ISSH në bashkëpunim me Drejtorinë e Burimeve të Informacionit të bëjnë përditësimin dhe dokumentimin e regjistrit të risqeve IT 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.

13. Gjetje nga auditimi: 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", 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;

e. Listë të artikujve të vlerësuar prioritare për proceset emergjente.

13.1 Rekomandimi: 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 IT. Planifikimi dhe testimi i sistemeve IT të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen.

14. Gjetje nga auditimi: 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 mëtejshëm të tij. Në asnjë rast nuk është raportuar në Drejtorinë e Burimeve të Informacionit, ndonjë problem i konstatuar me sistemin.

14.1 Rekomandimi: ISSH të përfshijë në përshkrimet e punës për specialistët IT 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.

15. Gjetje nga auditimi: 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.

15.1 Rekomandimi: 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.

16. Gjetje nga auditimi: 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.

16.1 Rekomandimi: 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.

II. INSTITUTI I STATISTIKAVE - INSTAT

KLSH në përfundim të Auditimit, për përmirësimin e gjendjes ka lënë 7 *rekomandime si masa organizative*, me shkresën nr. 833/7, datë 29.12.2017 sipas Vendimit nr.199, datë 28.12.2017 të Kryetarit të KLSH-së, ka dërguar Raportin Përfundimtar të Auditimit dhe rekomandimet për auditimin e ushtruar me programin nr. 1222/1, datë 10.10.2017**.**

INSTAT me marrjen e raportit përfundimtar të Kontrollit dhe rekomandimeve ka hartuar dhe planin e veprimit në lidhje me masat e marra për hartimin e programit, afatet dhe persona/struktura përgjegjëse, i janë përcjellë brenda afatit 20 ditor, për kthimin e përgjigjes për zbatimin e rekomandimeve Kontrollit të Lartë të Shtetit me shkresën nr. 1106/11 Prot., datë 23.01.2018. INSTAT ka përcjellë në KLSH brenda afatit ligjor prej 6 muajsh dhe raportimin përmbledhës mbi zbatimin e rekomandimeve të lëna, me shkresë nr. 1074 Prot., datë 02.07.2018 "Raportim mbi zbatimin e rekomandimeve të lëna".
Nga ana e KLSH me shkresat përcjellëse në auditimin e mëparshëm, për përmirësimin e gjendjes janë lënë *7 rekomandime, si masa organizative, të cilat janë pranuar dhe zbatuar plotësisht.*

III. DREJTORIA E PËRGJITHSHME E TAKSAVE DHE TARIFAVE VENDORE - DPTTV

KLSH në përfundim të Auditimit, për përmirësimin e gjendjes ka lënë *22 rekomandime si masa organizative*, me shkresën nr. 619/7, datë 08.01.2018 sipas Vendimit nr. 224, datë 31.12.2017 të Kryetarit të KLSH-së, ka dërguar Raportin Përfundimtar të Auditimit dhe rekomandimet për auditimin e ushtruar me programin nr. 619/1, datë 26.09.2017**.**

DPTTV me marrjen e raportit përfundimtar të Kontrollit dhe rekomandimeve ka hartuar dhe planin e veprimit në lidhje me masat e marra për hartimin e programit, afatet dhe persona/struktura përgjegjëse, i janë përcjellë brenda afatit 20 ditor, për kthimin e përgjigjes për zbatimin e rekomandimeve Kontrollit të Lartë të Shtetit me shkresën nr. 1241/1 Prot., datë 31.01.2018. DPTTV ka dërguar informacion në KLSH për zbatimin e rekomandimeve me shkresën nr.1241/2, datë 27.07.2018, duke përfshirë detaje mbi rekomandimet e lëna nga auditimi për një periudhë 6 mujore.
Nga *22 rekomandime, si masa organizative, janë pranuar plotësisht nga ana e subjektit të audituar, nga të cilat 10 janë zbatuar plotesisht, 2 janë zbatuar pjesërisht dhe 10 janë në proces zbatimi.*
KLSH kërkon intensifikimin e veprimeve, për përfundimin e rekomandimeve që rezultuan në proces si dhe marrjen e masave të menjëhershme për zbatimin e rekomandimeve që rezultuan të pazbatuara, si vijon:

IV. A. MASA ORGANIZATIVE:

1. Gjetje nga auditimi. DPTTV nuk ka një Plan Strategjik të shkruar e miratuar për Teknologjinë e Informacionit duke mos bërë planifikime strategjike mbi sigurinë institucionale dhe infrastrukturën IT 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.
1.1 Rekomandimi: 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. Gjetje nga auditimi: *Rregullorja e Brendshme, lidhur me strukturën IT në DPTTV,* nuk është në përputhje me rekomandimet e AKSHIT, rregullorja nuk përmban elementët e nevojshëm për të siguruar funksionim e përshtatshëm të strukturës IT në institucion.
2.1 Rekomandimi: DPTTV në bashkëpunim me Bashkinë Tiranë dhe strukturat këshilluese mbi IT, 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.

3. Gjetje nga auditimi: *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 IT 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 IT.
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 IT 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.

3.1 Rekomandimi: Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e IT 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 IT dhe veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura.

4. Gjetje nga auditimi: 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 IT dhe Statistikës.

- *DPTTV nuk ka kërkesa dhe analiza të nevojave për trajnim të stafit të Sektorit të IT dhe Statistikës;*
- *DPTTV nuk ka plan dhe nuk ka zhvilluar trajnime për sistemet, sigurinë dhe teknologjinë e informacioni për stafin e Sektorit të IT dhe Statistikës gjatë vitit 2016.*

4.1 Rekomandimi: Strukturat drejtuese të DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e IT dhe Statistikës të marrin masa për identifikimin e nevojave për trajnimin e stafit IT dhe të çdo përdoruesi të sistemeve IT si dhe të hartojë e miratojë plane dhe politika për zhvillimin e trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit.

5. Gjetje nga auditimi: 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.
5.1 Rekomandimi: 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.

6. Gjetje nga auditimi: 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.
6.1 Rekomandimi: Strukturat drejtuese të DPTTV me Sektorin IT, 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.

7. Gjetje nga auditimi: 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.
7.1 Rekomandimi: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.

8. Gjetje nga auditimi: 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 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.
- Paswordi 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 pasëordin 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.

8.1 Rekomandimi: 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.

9. Gjetje nga auditimi: 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

9.1 Rekomandimi: Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e IT 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 së "Regular Expression" për kontrolle për inputin e informacionit në këto fusha.

10. Gjetje nga auditimi:-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 grumbullimit të informacionit, përcaktimin e parametrave të subjekteve prej të cilave pritet të gjenerohen detyrimet.
10.1 Rekomandimi:-Strukturat Drejtuese në DPTTV në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Shërbimeve Mbështetëse dhe Sektorin e IT dhe Statistikës dhe strukturat e DPTTV në teren duke vlerësuar burimet të marrin masa për plotësimin e informacioneve mbi subjektet.

11. Gjetje nga auditimi: 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 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".
11.1 Rekomandimi: Strukturat drejtuese të DPTTV në bashkëpunim me Drejtorinë e Auditit të Brendshëm, Drejtorinë e Burimeve Njerëzore dhe me Sektorin e IT dhe Statistikës të marrë 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, si dhe monitorimin periodik për zbatimin e masave të marra nga sektori përgjegjës.

12. Gjetje nga auditimi: Nga auditimi i trigera-ve që popullojnë tabelën e auditimit, rezultoi se:
a. Ndryshimet në të dhëna, 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 (neë 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**.**
12.1 Rekomandimi: Të analizohen të gjitha mundësitë, për të siguruar gjurmën e auditimit lidhur me të dhënat më të rëndësishme që DPTTV 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.

Shënim: *Bashkëlidhur Aneksi Nr. 1, për paraqitjen tabelare të zbatimit rekomandimeve për 4 subjektet e verifikuara për zbatimin e rekomanduar.*

Departamenti Auditimit të Teknologjisë së Informacionit
Verifikimi i zbatimit të rekomandimeve në 4 subjekte të evaduara në 3-mujorin e fundit të vitit 2017 dhe 4-mujori (Janar-Prill) 2018

Aneksi nr. 1 . Masa Organizative:

Nr	Emërtimi i Subjekteve	Reko manduar	Pa pranuar	Pranuar	Nga rekomandimet e pranuara :			
					Zbatuar	Zbatuar Pjesërisht	Në proces	Pa zbatuar
a	**b**	**1**	**2**	**3 (1-2)**	**4**	**5**	**6**	**7**
1	Ujësjellës Kanalizime, Tiranë	15	0	15	2	5	0	8
2	Institutin e Sigurimeve Shoqërore (ISSH)	21	0	21	5	3	7	6
3	Instituti i Statistikave (INSTAT)	7	0	7	7	0	0	0
4	Drejtoria e Përgjithshme e Taksave dhe Tarifave Vendore, Tiranë- DPTTV	22	0	22	12	0	10	0
	GJITHSEJ	65	0	65	26	8	17	14
	Në %		0%	100%	40%	12%	26%	22%

BUJAR LESKAJ

KRYETAR