REPUBLIKA E SHQIPËRISË
KONTROLLI I LARTË I SHTETIT
DEPARTAMENTI I AUDITIMIT TË TEKNOLOGJISË SË INFORMACIONIT
KRYETARI

Adresa: *Rruga "Abdi Toptani" nr.1, Tiranë; Tel: 04251-267,* ***e-mail:*** *klsh@klsh.org.al,* ***web-site*** *www.klsh.org.al*

Nr.702/32 Prot. Tiranë, më 13.11.2020

V E N D I M

Nr. 123, Datë 13.11.2020

PËR
EVADIMIN E MATERIALEVE TË AUDITIMIT TË USHTRUAR NË: AUTORITETIN E KOMUNIKIMEVE ELEKTRONIKE DHE POSTARE (AKEP), AGJENCINË KOMBËTARE TË SHOQËRISË SË INFORMACIONIT (AKSHI), AUTORITETIN E MEDIAVE AUDIOVIZIVE (AMA), AUTORITETIN E MBIKËQYRJES FINANCIARE (AMF), MINISTRINË E BUJQËSISË DHE ZHVILLIMIT RURAL (MBZHR), MINISTRINË E DREJTËSISË (MD), MINISTRINË E KULTURËS (MK), BASHKINË FIER, BASHKINË KORÇË, BASHKINË LEZHË, BASHKINË VLORË, FONDIN E SIGURIMIT TË DETYRUESHËM TË KUJDESIT SHËNDETËSOR (FSDKSH), KORPORATËN ELEKTROENERGJITIKE SHQIPTARE SH.A (KESH), MINISTRINË E FINANCAVE DHE EKONOMISË (MFE), UJËSJELLËS KANALIZIME BERAT KUÇOVË (UKBK), UJËSJELLËS KANALIZIME LUSHNJE SH.A (UKL),
" PËR ZBATIMIN E REKOMANDIMEVE TË LËNA NË AUDITIMET E MËPARSHME TË EVADUARA NË VITIN 2019."

Në mbështetje të kërkesave të Udhëzimit nr. 1, datë 04.11.2016 të Kryetarit të Kontrollit të Lartë të Shtetit "*Mbi procedurat për ndjekjen dhe dokumentimin e punës në auditimin e verifikimit të zbatimit të rekomandimeve të Kontrollit të Lartë të Shtetit*" dhe në zbatim të Programit të auditimit nr. 702, datë 17.07.2020 "Për zbatimin e rekomandimeve të lëna në auditimet e mëparshme të evaduara në vitin 2019", të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit, u kryen auditime në 16 subjekte, për ecurinë e zbatimit të rekomandimeve të lëna gjatë vitit 2019 dhe në përfundim rezultoi:

Në **16** subjekte të audituara, janë rekomanduar nga KLSH gjithsej **224** masa, nga të cilat janë pranuar **221** masa ose **99** % dhe nuk janë pranuar 3 masa ose **1%**. Janë zbatuar plotësisht 73 prej tyre ose **33**%, janë në proces zbatimi **97** masa ose **44 %**, janë zbatuar pjesërisht **16** ose **7%** dhe nuk janë zbatuar **35** masa ose **16%.** Analiza sipas llojit të rekomandimeve të dhëna paraqitet:

A-<u>MASA ORGANIZATIVE</u>, janë rekomanduar nga KLSH gjithsej **222** masa, nga të cilat janë pranuar **220** masa ose **99** % dhe nuk janë pranuar 2 masa ose **1%**. Janë zbatuar plotësisht 72 prej tyre ose **33**%, janë në proces zbatimi **97** masa ose **44 %**, janë zbatuar pjesërisht **16** ose **7%** dhe nuk janë zbatuar **35** masa ose **16%**

B-<u>MASA PËR ELEMINIMIN E EFEKTEVE NEGATIVE TË KONSTATUARA NË ADMINISTRIMIN E FONDEVE PUBLIKE DHE PËR MENAXHIMIN ME EKONOMICITET, EFICENCE DHE EFEKTIVITET TË FONDEVE PUBLIKE ËSHTË REKOMANDUAR 1 MASË, E CILA ËSHTË PRANUAR DHE ZBATUAR,</u> është rekomanduar nga KLSH gjithsej **1** masë, është pranuar 1 masë **100%** dhe është zbatuar **1** mase **100%.**

Në përputhje me kërkesat e nenit 15, shkronja "j", të ligjit nr. 154/2014 datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit", 2 prej subjekteve nuk kanë kthyer përgjigje brenda 20 ditëve në KLSH, mbi masat e marra për zbatimin e rekomandimeve të lëna në raportet përfundimtare të auditimit nga KLSH, sipas afateve të përcaktuara, konkretisht: (*Bashkia Lezhë dhe Minisria e Financës dhe Ekonomisë*)

Gjithashtu konstatohet se, nga auditimet e kryera, 9 prej subjekteve nuk kanë kthyer përgjigje në KLSH mbi ecurinë e zbatimit të rekomandimeve brenda afatit 6 mujor në zbatim të pikë 2, të nenit 30, të Ligjit nr. 154/2014 datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit", konkretisht:
(Autoriteti i Mbikëqyrjes Financiare, Ministria e Bujqësisë dhe Zhvillimit Rural, Ministria e Drejtësisë, Ministria e Kulturës, Ministria e Financave dhe Ekonomisë, Bashkia Lezhë, Bashkia Vlorë, Korporata Elektroenergjitike Shqiptarë, Ujësjellës Kanalizime Berat-Kuçovë Sh.a)

Bazuar në rezultatet e mësipërme mbi ecurinë e zbatimit të rekomandimeve të lëna, 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 subjektet e audituara, si dhe vlerësimet mbi objektivitetin dhe cilësinë e auditimit nga Drejtori i Departamentit të mësipërm, Drejtori i Drejtorisë së Standardeve dhe Sigurimit të Cilësisë dhe Drejtori i Përgjithshëm, në mbështetje të neneve 10, 15, 25 dhe 30, të ligjit nr. 154/2014 miratuar në datën 27.11.2014 "*Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit*",

V E N D O S A :

I. Të miratoj Raportin Përfundimtar të Auditimit "Për zbatimin e rekomandimeve të lëna në auditimet e mëparshme të evaduara në vitin 2019", të ushtruar në Autoritetin e Komunikimeve Elektronike dhe Postare (AKEP), Agjencinë Kombëtare të Shoqërisë së Informacionit (AKSHI), Autoritetin e Mediave Audiovizive (AMA), Autoritetin e Mbikëqyrjes Financiare (AMF), Ministrinë e Bujqësisë dhe Zhvillimit Rural (MBZHR), Ministrinë e Drejtësisë (MD), Ministrinë e Kulturës (MK), Bashkinë Fier, Bashkinë Korçë, Bashkinë Lezhë, Bashkinë Vlorë, Fondin e Sigurimit të Detyrueshëm të Kujdesit Shëndetësor (FSDKSH), Korporatën Elektroenergjitike Shqiptare sh.a (KESH), Ministrinë e Financave dhe Ekonomisë (MFE), Ujësjellës Kanalizime Berat Kuçovë (UKBK), Ujësjellës Kanalizime Lushnje Sh.a (UKL), sipas Programit të Auditimit

nr. 702, datë 17.07.2020, miratuar nga Kryetari i Kontrollit të Lartë të Shtetit, për periudhën e aktivitetit e vitit 2019, me afat auditimi nga 20.07.2020-07.08.2020.

II. Të miratoj rikërkërkimin e zbatimit të rekomandimeve të pa zbatuara, të zbatuara pjesërisht, në proces zbatimi ose të papranuara sa vijon:

1. Ministria e Financave dhe Ekonomisë
2. Fondi i Sigurimit të Detyrueshëm të Kujdesit Shëndetësor
3. Korporata Elektroenergjitike Shqiptarë
4. Ujësjellës Kanalizime Berat-Kuçovë Sh.a
5. Ujësjellës Kanalizime Lushnje Sh.a
6. Ministria e Drejtësisë
7.Ministria e Bujqësisë dhe Zhvillimit Rural
8.Ministria e Kulturës
9.Bashkia Vlorë
10.Bashkia Lezhë
11. Bashkia Korçë
12. Bashkia Fier
13. Autoriteti i Mbikëqyrjes Financiare
14.Autoriteti i Mediave Audiovizive
15. Agjencisa Kombëtare e Shoqërisë së Informacionit

Në kushtet kur të gjitha rekomandimet e KLSH janë pranuar dhe zbatuar plotësisht nuk do të rikërkoj zbatimin e rekomandimeve, në subjektet si më poshtë:

1. Autoriteti i Komunikemeve Elktronike dhe Postare

Në mënyrë më të detajuar, më poshtë po paraqesim gjetjet dhe rekomandimet për subjektet e audituara:

1. Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit AKEP me shkresën Nr. 779/42 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Janë rekomanduar 5 masa organizative. Nga masat organizative janë pranuar plotësisht 5 masa, nga të pranuarat janë zbatuar 5 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 0 masa organizative, 0 masa organizative nuk janë zbatuar.

A. MASA ORGANIZATIVE

Nga auditimi rezultoi se AKEP ka zbatuar plotësisht 5 rekomandime.

2. Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit AKSHI me shkresën Nr. 779/38 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Janë rekomanduar 9 masa organizative. Nga masat organizative janë pranuar plotësisht 9 masa, nga të pranuarat janë zbatuar 2 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 7 masa organizative, 0 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që AKSHI të marrë masa të zbatojë të gjitha rekomandimet që rezultuan në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Nga auditimi u konstatua se, nuk monitorohet ofrimi i shërbimit të internetit për institucionet e varësisë të cilat nuk janë në rrjetin GOVNET. Gjithashtu, në dy vitet 2018-2019, referuar parashikimit të fondeve buxhetore për shërbimin e internetit, shpërndarja e tyre është bërë tek institucionet e varësisë edhe pse këto fonde duhet të ishin rialokuar në buxhetin e AKSHI-t si institucioni përgjegjës për kryerjen e procedurës së prokurimit dhe lidhje se kontratës, në kundërshtim me VKM Nr. 673, datë 22.11.2017 "Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit", i ndryshuar.
1.1 Rekomandimi: AKSHI në bashkëpunim me institucionet e varësisë të cilat nuk bëjnë pjesë në rrjetin GOVNET, të marrin masa për monitorimin e shërbimit të internetit si dhe ndjekjen e hapave të nevojshëm si institucion qendror, për ofrimin e shërbimit të internetit.
Masat e marra nga subjekti për zbatimin e rekomandimit
Shërbimi internetit institucionet e varësisë të cilat nuk bëjnë pjesë në rrjetin GOVNET monitorohet nëpërmjet kontratave individuale me secilin institucion, duke dorëzuar raporte periodike mbi shërbimin e internetit. Komunikimi me institucionet është i pandërprerë nga ndjekësit e kontratës të cilët kujdesen për vijueshmërinë e shërbimit për këto institucione.
Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga Auditimi: Nga auditimi u konstatua se AKSHI nuk disponon mekanizma për verifikimin dhe marrjen e masave në kohë reale mbi administrimin e sulmeve strategjike të avancuara kibernetike ose edhe të dëmtimeve në pjesët e pajisjeve.
2.1 Rekomandimi: AKSHI të marri masat për ndërtimin e mekanizmave për administrimin në kohë reale të sulmeve të ndryshme të sigurisë ndaj proceseve që AKSHI ofron.
Masat e marra nga subjekti për zbatimin e rekomandimit
AKSHI ka implementuar mekanizma teknik për monitorimin, alertimin dhe reagimin ndaj incidenteve specifike në lidhje me sigurinë e sistemeve apo faqeve të hostuara pranë infrastrukturës së DC.
Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

3. Gjetje nga Auditimi: Nga auditimi u konstatua se vendosja nga AKSHI e kritereve kushtëzuese që një Operator Ekonomik i cili plotëson kriterin e vendosur nga AKSHI për stafin teknik me 10 inxhiniere në njërin nga lotet, nuk mund të marrë pjesë në lotin e dytë me të njëjtët inxhiniere.

Nisur nga fakti që Loti 1 është shërbim i përqendruar pranë AKSHIT, nuk është domosdoshmërisht kritike që po këta inxhiniere mos të marrin pjese për procedurën e Lotit 2.

3.1 Rekomandimi: AKSHI për procedura të të njëjtit profil dhe pavarësisht madhësisë së shërbimit, duhet të kërkoj kritere të cilat nuk ndikojnë në kushtëzimin e operatoreve ekonomike edhe pse këto shërbime janë të nivelit masiv.

Masat e marra nga subjekti për zbatimin e rekomandimit

Në zbatim të rekomandimit AKSHI do të marrë masa gjatë hartimit të termave dhe kritereve të reja në momentin e përfundimit të kontratës aktuale.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

4. Gjetje nga Auditimi: Nga auditimi u konstatua se AKSHI ka nën administrim një linjë fizike me institucionet që bëjnë pjesë në Govnet. Në rastin e një problematike të dëmtimit të fibrës optike, këto institucione do të mbeten pa shërbim interneti.

4.1 Rekomandimi: AKSHI të marri masa për sigurimin dhe vazhdimësinë e ofrimit të shërbimit të internetit me qëllim garantimin pa ndërprerje të këtij shërbimi.

Masat e marra nga subjekti për zbatimin e rekomandimit

AKSHI ka një kontratë mirëmbajtje për rrjetin fizik me fibër optike, e cila mbulon çdo dëmtim apo shtrim të ri në rast të shtimit të institucioneve të reja në këtë rrjet. Kjo kontratë funksionon me nivele urgjence të cilat kanë kohën respektive të reagimit.

Ky rekomandim është në proces ***Menjëherë***

5. Gjetje nga Auditimi: Nga auditimi u konstatua se vendosja nga AKSHI e kërkesave në specifikimet e procedurës në Shërbimet e ndërlidhjes së DPGJC me zyrat e saj Rajonale "lidhja e diplomave të specialistëve me certifikatat e sigurisë" si dhe numrit të madh të tyre, është i tepërt dhe i pa nevojshëm, pasi certifikimet ndërkombëtare garantojnë AKSHIN lidhur me këtë procedurë.

5.1 Rekomandimi: AKSHI për projektet që kanë të bëjnë me sigurinë e informacionit të marrë në konsideratë certifikimet ndërkombëtare dhe jo numrin e diplomave, pasi në këtë mënyrë garantohet ofrimi i standardeve më të mira ndërkombëtare.

Masat e marra nga subjekti për zbatimin e rekomandimit

Në zbatim të rekomandimit AKSHI do të marrë masa gjatë hartimit të termave dhe kritereve të reja në momentin e përfundimit të kontratës aktuale.

Ky rekomandim është në proces ***Në vijimësi***

6.Gjetje nga Auditimi: Nga auditimi u konstatua se AKSHI nuk ka staf të mjaftueshëm në kryerjen e detyrave të caktuara. Nuk ka zhvilluar trajnime lidhur me Teknologjinë e Informacionit në mënyrë që të garantohet realizimi me sukses i objektivave të institucionit.

6.1 Rekomandimi: Strukturat drejtuese të AKSHI-t të marrin masa për menaxhimin e burimeve njerëzore duke plotësuar nevojat për staf si dhe për zhvillimin e trajnimeve në lidhje me objektivat e këtij institucioni në fushën e Teknologjisë së Informacionit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Në lidhje me këtë rekomandim AKSHI me anë të shkresës nr. Prot. 3490 dt. 22.07.2020 i është drejtuar Ministrisë së Financave dhe Ekonomisë si dhe Departamentit për Administratën Publike për rritjen e strukturës se institucionit me 20 pozicione të reja. Ndërkohe nevojat për trajnime do të trajtohen në marrëveshjen e re Qeveritare me Microsoft, nisur nga fakti se kjo marrëveshje

mbulon të gjitha fushat e veprimit të AKSHI-t në Teknologjinë e Informacionit. Për sa më sipër, grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

7. Gjetje nga Auditimi: Nga auditimi u konstatua se në subjektet AKSHI, AMA dhe AMF nuk dokumenton operacionet IT (Help desk) për shërbimet e brendshme dhe të jashtme në lidhje me problematika në fushën e sigurisë. Në rastin e një problematike ose ndryshimeve nuk ka një historik të konfigurimeve ku do të ndihmonte në rastin e një problematike për kthimin e shërbimeve sa më shpejtë. Komunikimet në rastin e problematikave, kërkesave kryhen nëpërmjet postës elektronike dhe dokumentet dhe konfigurimet ruhen në kompjuter.

7.1 Rekomandimi: AKSHI, AMA dhe AMF të marrin masat për analizimin e nevojave mbi ofrimin e shërbimeve Helpdesk të tyre, ku çdo departament të ketë akses për problematikat dhe kërkesat e tyre si dhe departamenti IT të procedoje me hedhjen e të gjitha konfigurimeve në këtë sistem.

Masat e marra nga subjekti për zbatimin e rekomandimit

Aktualisht AKSHI është në procesin e lidhjes së Marrëveshjes së re Qeveritare me Microsoft, tek e cila do të përfshihet edhe Sistemi i Helpdeskut (Ticket Management) për portalin eAlbania dhe operacionet IT rutinë të pjesës tjetër të stafit në AKSHI.

Ky rekomandim është në proces ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë, të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

3. Autoriteti i Mediave Audiovizive (AMA)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit AMA me shkresën Nr. 779/39 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Janë rekomanduar 8 masa organizative. Nga masat organizative janë pranuar plotësisht 8 masa, nga të pranuarat është zbatuar 1 masë, është zbatuar pjesërisht 0 masë, dhe janë në proces zbatimi 6 masa organizative, 1 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që AMA të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Nga auditimi u konstatua se për linjën e dytë të internetit e cila përdoret për back up, AMA nuk kishte zhvilluar një procedurë prokurimi por ky shërbim ishte i kontraktuar në mënyrë të drejtpërdrejtë, në kundërshtim me nenin 4 "Fusha e zbatimit" të ligjit nr. 9643, datë 20.11.2006 "Për prokurimin publik", i ndryshuar.

1.1 Rekomandimi: AMA të marrë masa për zhvillimin e procedurës së prokurimit, me qëllim përfitimin e një vlere ekonomike sa më të favorshme, duke nxitur konkurrencën ndërmjet operatorëve ekonomikë.

Masat e marra nga subjekti për zbatimin e rekomandimit

Kontrata e lidhur me shoqërinë Albtelecom sh.a për shërbimin e internetit për linjën back-up përfundon më 04.08.2020. Në përfundim të kësaj kontrate, AMA do të procedojë me zhvillimin e procedurës së prokurimit për këtë shërbim, për periudhën 05.08.2020-31.12.2020. Për sa më sipër, grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga Auditimi: Nga auditimi u konstatua se menaxhimi dhe konfigurimi routerit për ofrimin e shërbimit wireless në AMA nuk është i konfiguruar me kufizime në lidhje me aksesin e jashtëm dhe të brendshëm të rrjetit.

2.1 Rekomandimi: AMA të marrë masa për ndërtimin e kufizimeve të aksesimit të shërbimit wireless, për parandalimin e sulmeve ose hyrjeve të pa autorizuara në pajisjet e institucionit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Pajisja CiscoFirepower ASA 5506-x është jashtë funksioni pasi ka pësuar defekt dhe rrjeti i brendshëm i AMA-s ka kaluar në RouterMicrotik (pajisje backup). Në këto kushte AMA ka hequr nga përdorimi shërbimin wireless të ofruar nga pajisjet Albtelecom.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

3.**Gjetje nga Auditimi:** Aktualisht domain controller është në një server fizik. Po në këtë server është i instaluar edhe sistemi i virtualizimeve vMware Workstation ku janë të krijuara 2 makina virtuale që shërbejnë për programin e menaxhimit të brendshëm për AMA. Në rastin e një problematike nuk ka një server të dyte backup si dhe pjesë të garantuara.

3.1 Rekomandimi: AMA të marri masat për analizimin e nevojave për vendosjen e një server backup me parametrat optimal si serveri i parë nga ku të konfigurohet failover.

Masat e marra nga subjekti për zbatimin e rekomandimit

Drejtoria e Planifikimit të Frekuencave dhe TIK në AMA, ka parashikuar në buxhetin e vitit 2020 blerjen e një serveri back-up replikimi me serverin kryesor. Zhvillimi i procedurës së prokurimit e cila isht parashikuar për t'u realizuar brenda gjashtë mujorit të parë të vitit 2020, për shkak të situatës së krijuar nga pandemia COVID-19 nuk është bërë i mundur realizimi i kësaj procedure.
Aktualisht AMA është në fazë të hartimit të specifikimeve teknike të serverit back-up

Ky rekomandim është në proces ***Në vijimësi***

4. Gjetje nga Auditimi: Nga auditimi u konstatua se AMA nuk disponon raporte monitorimi mbi shërbimin e internetit. Komunikimet mbi menaxhimin e user-ave (hapje, mbyllje) menaxhohen me anë të komunikimeve verbale pa u dokumentuar procesi përkatës, duke mos realizuar identifikimin e risqeve, çka mbart riskun e përsëritjes së incidenteve. Nuk ka regjistër të menaxhimit të

incidenteve por ka procedura për menaxhimin e incidenteve të pajisjeve fundore, për monitorimin e mirëmbajtjen e sistemeve dhe rrjetit.

4.1 Rekomandimi: AMA të marri masa për hartimin e regjistrit të risqeve mbi infrastrukturën TIK, dokumentimin e monitorimit të incidenteve dhe menaxhimin e ndryshimeve.

Masat e marra nga subjekti për zbatimin e rekomandimit

AMA ka konfiguruar filtra të cilët bllokojnë faqe adult dhe faqe të tjera të rrezikshme që dëmtojnë dhe rrezikojnë pajisjet dhe rrjetin TIK në AMA, në pajisjen CiscoFirepower ASA 5506-x. Duke qenë se kjo pajisje është jashtë funksioni, të njëjtat konfigurime janë kryer në pajisjen RouterMicrotik (pajisje back-up).

Lidhur me procedurën për ruajtjen dhe analizimin e log-eve AMA ka miratuar një udhëzues të posaçëm me nr. Prot 1472, datë11.06.2020.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

5.Gjetje nga Auditimi: Nga auditimi u konstatua se në subjektet AKSHI, AMA dhe AMF nuk dokumenton operacionet IT (Help desk) për shërbimet e brendshme dhe të jashtme në lidhje me problematika në fushën e sigurisë. Në rastin e një problematike ose ndryshimeve nuk ka një historik të konfigurimeve ku do të ndihmonte në rastin e një problematike për kthimin e shërbimeve sa më shpejtë. Komunikimet në rastin e problematikave, kërkesave kryhen nëpërmjet postës elektronike dhe dokumentet dhe konfigurimet ruhen në kompjuter.

5.1 Rekomandimi: AKSHI, AMA dhe AMF të marrin masat për analizimin e nevojave mbi ofrimin e shërbimeve Helpdesk të tyre, ku çdo departament të ketë akses për problematikat dhe kërkesat e tyre si dhe departamenti IT të procedoje me hedhjen e të gjitha konfigurimeve në këtë sistem.

Ky rekomandim është i pazbatuar ***Në vijimësi***

6. Gjetje nga Auditimi: Nga auditimi u konstatua se AMA dhe AMF nuk kryejnë analizim të nevojës për sasinë dhe cilësinë e shërbimit të interneti, në lidhje me veprimet operacionale që kryen përdoruesi fundor.

6.1 Rekomandimi: AMA dhe AMF të analizojnë nevojat mbi sasinë dhe cilësinë e shërbimit të interneti, nisur nga sasia e veprimeve operacionale që kryejnë përdoruesit fundor.

Masat e marra nga subjekti për zbatimin e rekomandimit

Monitorimi lidhur me përdorimin e sasisë së internetit vijon të kryhet në mënyrë periodike nga Sektori Teknik në AMA.

Ky rekomandim është në proces ***Në vijimësi***

7. Gjetje nga Auditimi: Nga auditimi u konstatua se subjektet e audituara AKEP dhe AMA nuk ka elementë të teknologjisë së informacionit në regjistrin e riskut, në kundërshtim me ligjin nr. 10 296, datë 08.07.2010 "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar, si dhe Udhëzimin nr. 30 datë 27.12.2011 "*Për menaxhimin e aktiveve në Njësitë e Sektorit Publik*".

7.1. Rekomandimi: Strukturat drejtuese në AKEP dhe AMA të marrin masat e nevojshme për hartimin dhe dokumentimin në regjistrin e risqeve të elementëve të identifikuara si risqe të teknologjisë së informacionit me qëllim vlerësimin, kontrollin e risqeve që mund të vënë në rrezik arritjen e objektivave institucionalë.

Masat e marra nga subjekti për zbatimin e rekomandimit

Sektori Teknik ka hartuar draft-regjistrin me të gjitha pajisjet elektronike që ndodhen në institucion. Ky regjistër përmban kodin e artikullit, emrin e artikullit, njësinë, çmimin dhe vlerën

e mbetur duke zbatuar normën e amortizimin 25% në vit. Për shkak të situatës së krijuar nga pandemia COVID-19, AMA është duke verifikuar pajisjet dhe të dhënat e tjera të përcaktuara në këtë regjistër për çdo pajisje. Grupi i auditimit konstatoi se regjistri është hartuar por është i pa miratuar dhe nuk është dokumentuar regjistër i regjistrimit të incidenteve, masave të marra në raste incidentesh dhe masat për parandalimin e incidenteve të ngjashme në të ardhmen.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi dhe të pa zbatuar,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

4. Autoriteti i Mbikëqyrjes Financiare (AMF)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit AMF me shkresën Nr. 779/34 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se AMF, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 8 masa organizative. Nga masat organizative janë pranuar plotësisht 8 masa, nga të pranuarat janë zbatuar 6 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 2 masa organizative, 0 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që AMF të marrë masa të zbatojë të gjitha rekomandimet që rezultuan në proces zbatimi si më poshtë:

A MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Nga auditimi u konstatua se AMA dhe AMF nuk kanë politika për kufizimet në përdorimin e internetit si dhe nuk disponojnë procedura për analizimin e log-eve.

1.1 Rekomandimi: Strukturat drejtuese në AMA dhe AMF të marrin masat për monitorimin e kufizimeve në internet si dhe të ndërtojnë procedura lidhur me ruajtjen dhe analizimin e log-eve.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga AMF aktualisht janë marrë këto masa për kufizimin e internetit: antenat wifi në ambjentet e AMF jane konfiguruar që të kenë shpejtësi të kufizuar si dhe të cilët kufizojnë aksesin në internet për kompjuterat apo pajisje inteligjente të tjera të lidhura në wifi për sa i përket faqeve që nuk lidhen me objektin e punës së përditshme. Kufizime të ngjashme të faqeve ndiqen gjithashtu përmes DNS së Active Directory.

IT e AMF është në fazë analize për implementimin e një Web Proxy, me qëllim lehtësimin dhe mundësi më të mëdha në kufizimin e faqeve që përdoren nga punonjësit e AMF, gjithashtu dhe mbrojtie më të mirë kibernetike. Zbatimi i Web Proxy pritet në fillim të 2021 pasi të jetë alokuar fondi përkatës në buxhetin e 2021. Ndërkohë AMF ka krijuar një procedurë Kodi: TI-PRO-003 e

cila cilëson se eksporti i logeve kryhet manualisht në një disk të jashtëm dhe njëkohësisht bëhet analizimi i tyre periodik për evidentimin e ndonjë incidenti. Gjithashtu IT-ja e AMF është në proces të analizës për ndërtimin e një sistemi administrimi log-es, implementimi i të cilit është shtyrë për shkak të pandemisë dhe mendohet të zbatohet në fillim të 2021. Ky sistem do të shërbej për të qëndërzuar dhe analizuar në mënyrë të automatizuar log-et në një vend të përbashkët duke bërë të mundur uljen e kohës dhe rritjen e cilësisë së monitorimit të log-eve e për rrjedhojë identifikimin e hershëm të ndonjë incidenti potencial që mund të ndodh në sistemet e AMF-së duke i parandaluar ato përmes masave të marra në kohë. Nga AMF është planifikuar që ky sistem mos të funksionoj vetëm për loget e aksesit në internet por do përfshihen pajisje të ndryshme gjithashtu si (server, storage, rrjeti), sisteme operimi të ndryshme (Linux, Windows), baza të dhënash të ndryshme (Oracle, SQL, My SQL) si dhe aplikacione të ndryshme të programuar me gjuhë programimi të ndryshme (Java, .Net, PHP, etj.), ku kryesisht qëndrojnë mbi ambjente të virtualizuara me Hyper-V. Deri në finalizimin e procesit AMF do të viojë me ruajtien dhe dokumentimin manual të logeve si dhe gjatë muajve në vijim do përfundohet analiza paraprake. Për sa më sipër, grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

2.Gjetje nga Auditimi: Nga auditimi u konstatua se në subjektet AKSHI, AMA dhe AMF nuk dokumenton operacionet IT (Help desk) për shërbimet e brendshme dhe të jashtme në lidhje me problematika në fushën e sigurisë. Në rastin e një problematike ose ndryshimeve nuk ka një historik të konfigurimeve ku do të ndihmonte në rastin e një problematike për kthimin e shërbimeve sa më shpejtë. Komunikimet në rastin e problematikave, kërkesave kryhen nëpërmjet postës elektronike dhe dokumentet dhe konfigurimet ruhen në kompjuter.

2.1 Rekomandimi: AKSHI, AMA dhe AMF të marrin masat për analizimin e nevojave mbi ofrimin e shërbimeve Helpdesk të tyre, ku çdo departament të ketë akses për problematikat dhe kërkesat e tyre si dhe departamenti IT të procedoje me hedhjen e të gjitha konfigurimeve në këtë sistem.

Masat e marra nga subjekti për zbatimin e rekomandimit

AMF ka marr masa për analizimin e nevojave për sistemin helpdesk dhe ka nisur ndërtimin e një sistemi Intranet për AMF, i cili do përbëhet nga disa module dhe ndër to është dhe moduli Helpdesk me qëllim adresimin e çështjes së hedhjes dhe administrimit të komunikimeve dhe dokumentacioneve që adresojnë drejtorinë e TI dhe jo vetëm. Moduli i parë është menaxhimi i aseteve i cili aktualisht është funksional dhe do shërbej për të lidhur asetet IT me Helpdesk ku çdo aseti mund ti hapet nje ticket dhe informacioni i nevojshëm sipas rastit. Për sa i përket adresimit të ketij moduli AMF është në proces zhvillimi për shkak të pandemisë dhe kompleksitetit të tij.

Ky rekomandim është në proces ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

5. Ministria e Bujqësisë dhe Zhvillimit Rural (MBZHR)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit MBZHR me shkresën Nr. 779/35 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se MBZHR, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 9 masa organizative. Nga masat organizative janë pranuar plotësisht 9 masa, nga të pranuarat janë zbatuar 7 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 2 masa organizative, 0 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që MBZHR të marrë masa të zbatojë të gjitha rekomandimet që rezultuan në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Mungesa e treguesve mbi monitorimin e shërbimit të internetit të ofruar nga AKSHI për Ministritë, nuk i mundëson sektorit të IT pranë ministrive monitorimin mbi cilësinë dhe vazhdimësinë e këtij shërbimi.
1.1 Rekomandimi: Ministria e Drejtësisë në bashkëpunim me AKSHI-n të hartojë dhe miratojë MNSH, ku të pasqyrohen dhe vlerat e parametrave kryesor të ofrimit të shërbimit të internetit nga AKSHI, ndërsa MKdhe MBZHR të marrin masa për pasqyrimin e tyre në MNSH-të ekzistuese.
Masat e marra nga subjekti për zbatimin e rekomandimit
Ministria e Bujqësisë dhe Zhvillimit Rural ka dërguar në AKSHI shkresën nr. Prot 2580, datë 27.03.2020*"Kërkesë për përditësimin e Marrëveshjes në Nivel Shërbimi midis AKSHI-t dhe MBZHR-së, në zbatim të rekomandimeve të Kontrollit të Lartë të Shtetit"*, por nuk ka marrë përgjigje. Është në pritje të dërgimit të MNSH-së të ndryshuar nga AKSHI.
Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga Auditimi: Nga auditimi u konstatua seMarrëveshjet e Nivelit të Shërbimit (*Service Level Agreement*), të lidhura midis AKSHI-t me MBZHR dhe MK, nuk janë hartuar përputhje me kërkesat e Udhëzimit nr. 1159, datë 17.3.2014 për Hartimin e Marrëveshjes së Nivelit të Shërbimit.
2.1. Rekomandimi: MBZHR dhe MK në bashkëpunim me AKSHI-n të konsiderojnë ndryshime në marrëveshjet e bashkëpunimit, në të cilën të përcaktohet detyrimi mbi kohën e raportimit, të përgjigjes dhe afatin e vlefshmërisë, etj.
Masat e marra nga subjekti për zbatimin e rekomandimit
Ministria e Bujqësisë dhe Zhvillimit Rural brenda datës 31.03.2020 ka dërguar në AKSHI shkresën nr. Prot 2580, datë 27.03.2020 *"Kërkesë për përditësimin e Marrëveshjes në Nivel Shërbimi midis AKSHI-t dhe MBZHR-së, në zbatim të rekomandimeve të Kontrollit të Lartë të Shtetit",* por nuk ka marrë përgjigje. Është në pritje të dërgimit të MNSH-së të ndryshuar nga AKSHI.
Ky rekomandim është në proces ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021.

Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

6. Ministria e Drejtësisë (MD)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit Ministria e Drejtësisë me shkresën Nr. 779/36 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se Ministria e Drejtësisë, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 11 masa organizative. Nga masat organizative janë pranuar plotësisht 11 masa, nga të pranuarat janë zbatuar 5 masa, është zbatuar pjesërisht 1 masë, dhe janë në proces zbatimi 5 masa organizative, 0 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që Ministria e Drejtësisë të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të zbatuara pjesërisht dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë, Ministria e Kulturës dhe Ministria e Bujqësisë dhe Zhvillimit Rural, nuk disponojnë rregullore për Politikat e Sigurisë së Informacionit.
1.1 Rekomandimi: Strukturat Drejtuese në MD, MK dhe MBZHR të marrin masa për hartimin dhe miratimin e një Rregullore për Politikat e Sigurisë së Informacionit, si dhe vënien e saj në dispozicion të gjithë punonjësve përgjegjës për sigurinë e informacionit, përfshirë përdoruesit e sistemeve të cilët kanë rol në mbrojtjen e informacionit.
Masat e marra nga subjekti për zbatimin e rekomandimit
Ministria e Drejtësisënë kuadër të rekomandimit të lënë nga KLSH ka hartuar rregulloren *"Rregullore për Sigurinë e Informacionit në Ministrinë e Drejtësisë"*,e cila është draft i pa miratuar. Për sa më sipër, grupi i auditimit e konsideron rekomandimin në proces zbatimi.
Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

2. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë, Ministria e Kulturës dhe Ministria e Bujqësisë dhe Zhvillimit Rural nuk disponojnë procedura mbi administrimin e incidenteve dhe problemeve, këto institucione nuk kanë të dokumentuar një plan masash për trajtimin e problemeve dhe incidenteve që mund të ndodhin. Në mungesë të këtyre procedurave të shkruara, problemet dhe incidentet për periudhën nën auditim menaxhoheshin mbi bazë ngjarjesh të cilat raportoheshin nëpërmjet email-it. Gjithashtu këto subjekte nuk kanë realizuar identifikimin e problemeve dhe incidenteve, si dhe nuk disponojnë një bazë të të dhënave të gabimeve të njohura dhe historikun e incidenteve të mëparshme, siç edhe kërkohet në MNSH-t respektive.

2.1 Rekomandimi: Strukturat Drejtuese në MD, MK dhe MBZHR në bashkëpunim me Sektorin e IT-së të atashuar pranë tyre, të marrin masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve mbi infrastrukturën TIK.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ministria e Drejtësisënë kuadër të rekomandimit të lënë nga KLSH ka hartuar *"Planin e Menaxhimit të Inicidenteve TIK në Ministrinë e Drejtësisë",* e cila është në formën e një drafti, të pa miratuar. Për sa më sipër, grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

3. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë, Ministria e Kulturës, Ministria e Bujqësisë dhe Zhvillimit Rural nuk disponojnë procedura të standardizuara për menaxhimin e ndryshimeve në sistem, aplikacioneve IT apo ndryshimeve të tjera. Nuk disponojnë procedurë për inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve.

3.1 Rekomandimi: Strukturat Drejtuese në MD, MK dhe MBZHR në bashkëpunim me Sektorin IT atashuar pranë tyre, të marrin masat e nevojshme për menaxhimin dhe dokumentimin e të gjithë procesit të ndryshimeve që do kryejnë në vazhdimësi.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga ana e Ministrisë së Drejtësisë janë ndërmarë masa duke hartuar rregullore të cilat janë në formën e një drafti, të pa miratuar. Referuar afateve të rekomandimit grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

4. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë, Ministria e Kulturës, Ministria e Bujqësisë dhe Zhvillimit Rural nuk kryejnë administrimin e përdoruesve në Active Directory mbështetur në politika të mirë përcaktuara, procedurat zhvillohen pa një akt rregullativ (rregullore).

4.1 Rekomandimi: MD, MK dhe MBZHR në bashkëpunim me AKSHI-n të marrin masa për hartimin dhe miratimin e një rregulloreje ku të përcaktohen qartë procedurat që do të ndiqen për administrimin e përdoruesve si dhe llojet e kufizimeve që aplikohen për çdo përdorues fundor.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ministria e Drejtësisë në kuadër të rekomandimit të lënë nga KLSH ka hartuar *" Politikat e Administrimit të Përdoruesve të Sistemeve TIKnë Ministrinë e Drejtësisë",* e cila është në formën e një drafti, të pa miratuar. Për sa më sipër, grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

5. Gjetje nga Auditimi: Mungesa e treguesve mbi monitorimin e shërbimit të internetit të ofruar nga AKSHI për Ministritë, nuk i mundëson sektorit të IT pranë ministrive monitorimin mbi cilësinë dhe vazhdimësinë e këtij shërbimi.

5.1 Rekomandimi: Ministria e Drejtësisë në bashkëpunim me AKSHI-n të hartojë dhe miratojë MNSH, ku të pasqyrohen dhe vlerat e parametrave kryesor të ofrimit të shërbimit te internetit nga AKSHI, ndërsa MK dhe MBZHR të marrin masa për pasqyrimin e tyrenë MNSH-të ekzistuese.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ministria e Drejtësisë me anë të shkresës përcjellëse nr. Prot. 3317, datë 02.06.2020 i ka dërguar AKSHI-t kërkesa për përditësimin e "Marrëveshjes në Nivel Shërbimi midis AKSHI-t dhe MD-

së", në zbatim të rekomandimeve të KLSH-së, por AKSHI me anë të shkresës nr. 2759/1, datë 10.06.2020, protokolluar ne MD me nr. 3317/2, datë 12.06.2020 nga AKSHI, ka refuzuar kërkesën.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë dhe në vijimësi***

6. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë dhe Ministria e Bujqësisë dhe Zhvillimit Rural nuk disponojnë regjistër risku për identifikimin, kategorizimin, ndjekjen dhe minimizimin e risqeve që lidhen me teknologjinë e informacionit.

6.1 Rekomandimi: Ministria e Drejtësisë dhe Ministria e Bujqësisë dhe Zhvillimit Rural në bashkëpunim me AKSHI-n të hartojnë dhe miratojnë regjistrin e riskut mbi sistemet IT.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ministria e Drejtësisënë kuadër të rekomandimit të lënë nga KLSH ka hartuar *"Regjistrin e Riskut Për Teknologjinë e Informacionit në Ministrinë e Drejtësisë",* e cila është në formën e një drafti, të pa miratuar. Për sa më sipër, grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

7. Ministria e Kulturës (MK)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit Ministria e Kulturës me shkresën Nr. 779/37 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se Ministria e Kulturës, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 8 masa organizative. Nga masat organizative janë pranuar plotësisht 8 masa, nga të pranuarat janë zbatuar 2 masa, janë zbatuar pjesërisht 2 masa, dhe janë në proces zbatimi 4 masa organizative, 0 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që Ministria e Kulturës të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të zbatuara pjesërisht dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë, Ministria e Kulturës dhe Ministria e Bujqësisë dhe Zhvillimit Rural, nuk disponojnë rregullore për Politikat e Sigurisë së Informacionit.

1.1 Rekomandimi: Strukturat Drejtuese në MD, MK dhe MBZHR të marrin masa për hartimin dhe miratimin e një Rregullore për Politikat e Sigurisë së Informacionit, si dhe vënien e saj në dispozicion të gjithë punonjësve përgjegjës për sigurinë e informacionit, përfshirë përdoruesit e sistemeve të cilët kanë rol në mbrojtjen e informacionit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ministria e Kulturë është në proces hartimi për rregulloren e përdorimit të sistemit Web- based (HRMIS, SIFQ, E-AKTET), në bashkepunim me IT e atashuar pranë MK. Kjo rregullore do të dërgohet për miratim dhe unifikim pranë Akshit, brenda vitit 2020.

Ky rekomandim është në proces ***Menjëherë***

2. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë, Ministria e Kulturës, Ministria e Bujqësisë dhe Zhvillimit Rural nuk disponojnë procedura të standardizuara për menaxhimin e ndryshimeve në sistem, aplikacioneve IT apo ndryshimeve të tjera. Nuk disponojnë procedurë për inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve.

2.1 Rekomandimi: Strukturat Drejtuese në MD, MK dhe MBZHR në bashkëpunim me Sektorin IT atashuar pranë tyre, të marrin masat e nevojshme për menaxhimin dhe dokumentimin e të gjithë procesit të ndryshimeve që do kryejnë në vazhdimësi.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga ana e Ministrisë së Kulturës janë ndërmarë masa duke hartuar rregullore të cilat janë në formën e një drafti, të pa miratuar.Referuar afateve të rekomandimit grupi i auditimit e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

3. Gjetje nga Auditimi: Nga auditimi u konstatua se Ministria e Drejtësisë, Ministria e Kulturës, Ministria e Bujqësisë dhe Zhvillimit Rural nuk kryejnë administrimin e përdoruesve në Active Directory mbështetur në politika të mirë përcaktuara, procedurat zhvillohen pa një akt rregullativ (rregullore).

3.1 Rekomandimi: MD, MK dhe MBZHR në bashkëpunim me AKSHI-n të marrin masa për hartimin dhe miratimin e një rregulloreje ku të përcaktohen qartë procedurat që do të ndiqen për administrimin e përdoruesve si dhe llojet e kufizimeve që aplikohen për çdo përdorues fundor.

Masat e marra nga subjekti për zbatimin e rekomandimit

MK ka dërguar shkresën nr. 495/1 prot., datë 27.01.2020 drejtuar AKSHI-t, në të cilën kërkohet bashkëpunimi i tyre për realizimin e këtij rekomandimi, për hartimin e rregullores.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

4. Gjetje nga Auditimi: Nga auditimi mbi testet e zhvilluara nga grupi i auditimit mbi faqet web të Ministrisë së Drejtësisë dhe Ministrisë së Kulturës, u konstatua se ato nuk përdorin një lidhje të sigurt si dhe ridrejtojnë kërkesat për akses në portal në dy module të ndryshme Http (*Not secure status*) dhe Https (*Hyper text transfer protocol secure*), që do të thotë se serveri i faqes së internetit nuk përdor një certifikatë sigurie për të vërtetuar identitetin e internetit në shfletues. Mungesa e kësaj certifikate mbart riskun e cënimit të privatësisë dhe shkëmbimit të informacionit që merret ose jepet me anë të këtij portali.

4.1 Rekomandimi: Ministria e Drejtësisë dhe Kulturës në bashkëpunim me AKSHI-n 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.

Masat e marra nga subjekti për zbatimin e rekomandimit
MK ka dërguar shkresën nr. 495/1 prot., datë 27.01.2020 drejtuar AKSHI-t si dhe email drejtuar përgjegjësit IT të atashuar pranë MK.
Ky rekomandim është në proces ***Në vijimësi***

5. Gjetje nga Auditimi: Mungesa e treguesve mbi monitorimin e shërbimit të internetit të ofruar nga AKSHI për Ministritë, nuk i mundëson sektorit të IT pranë ministrive monitorimin mbi cilësinë dhe vazhdimësinë e këtij shërbimi.
5.1 Rekomandimi: Ministria e Drejtësisë në bashkëpunim me AKSHI-n të hartojë dhe miratojë MNSH, ku të pasqyrohen dhe vlerat e parametrave kryesor të ofrimit të shërbimit te internetit nga AKSHI, ndërsa MKdhe MBZHR të marrin masa për pasqyrimin e tyre në MNSH-të ekzistuese.
Masat e marra nga subjekti për zbatimin e rekomandimit
MK ka dërguar shkresën nr. 495/1 prot., datë 27.01.2020 drejtuar AKSHI-t, në të cilën kërkohet bashkëpunimi i tyre. Nuk kanë nje kthim përgjigje nga AKSHI.
Ky rekomandim është zbatuar pjesërisht ***Në vijimësi***

6. Gjetje nga Auditimi: Nga auditimi u konstatua se Marrëveshjet e Nivelit të Shërbimit (*Service Level Agreement*), të lidhura midis AKSHI-t me MBZHR dhe MK, nuk janë hartuar përputhje me kërkesat e Udhëzimit nr. 1159, datë 17.3.2014 për Hartimin e Marrëveshjes së Nivelit të Shërbimit.
6.1 Rekomandimi: MBZHR dhe MK në bashkëpunim me AKSHI-n të konsiderojnë ndryshime në marrëveshjet e bashkëpunimit, në të cilën të përcaktohet detyrimi mbi kohën e raportimit, të përgjigjes dhe afatin e vlefshmërisë, etj.
Masat e marra nga subjekti për zbatimin e rekomandimit
MK ka dërguar shkresën nr. 495/1 prot., datë 27.01.2020 drejtuar AKSHI-t, në të cilën kërkohet bashkëpunimi i tyre. Nuk kanë nje kthim përgjigje nga AKSHI.
Ky rekomandim është zbatuar pjesërisht ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimidhe zbatuar pjesërisht,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

8. Bashkia Fier

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit Bashkia Fier me shkresën Nr. 779/43 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Janë rekomanduar 7 masa organizative. Nga masat organizative janë pranuar plotësisht 7 masa, nga të pranuarat janë zbatuar 4 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 3 masa organizative, 0 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që Bashkia Fier të marrë masa të zbatojë të gjitha rekomandimet që rezultuan në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi u konstatua se nga Bashkia Fier nuk kryen kontrolle mbi aktivitetin e përdoruesve. Log-et nuk janë të ruajtura as nga Bashkia dhe as nga operatorët ekonomikë. Gjithashtu ky institucion nuk kanë marrë masat për krijimin e një *active directory* dhe *Domani controller* për menaxhimin e user-ave.
Grupi i auditimit vlerëson se kjo qasje rrit riskun e pasigurisë në përdorimin e internetit si dhe ndërhyrjeve të mundshme në rrjetin e Bashkisë.
1.1 Rekomandim: Bashkia Fier të marrë masat e nevojshme për krijimin e një *active directory* dhe *Domain controller* për menaxhimin e user-ave, si dhe ruajtjen dhe monitorimin e vazhdueshëm të log-eve, me qëllim rritjen e sigurisë në përdorimin e shërbimit të internetit.
Masat e marra nga subjekti për zbatimin e rekomandimit
Bashkia Fier është në fazë studimi (për arsye munges fondesh) dhe zbatimi në vijimësi të krijimit të një activ directorie si dhe një Domain Controller duke parashikuar në Buxhetin e vitet pasardhës edhe fondet përkatëse për realizimin e tyre.
Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Fier nuk ka politika të mirë përcaktuara mbi sigurinë e informacionit, apo plane për sigurinë e sistemeve të teknologjisë së informacionit në përgjithësi dhe në drejtim të rrjetit në veçanti. Në këtë drejtim, mungon një rregullore mbi aksesin e përdoruesve në internet, veprim i cili ka ndikuar në akses të pakufizuar.
2.1 Rekomandim: Bashkia Fier të marrë masat për hartimin e politikave të mirë përcaktuara mbi sigurinë e informacionit, si dhe plane për sigurinë e sistemeve të teknologjisë së informacionit në drejtim të rrjetit.
Masat e marra nga subjekti për zbatimin e rekomandimit
Aktualisht Bashkia Fier ka vleresuar rekomandimin e lënë në lidhje me sigurinë e informacionit, sistemeve dhe rrjetit elektronik duke:
a) Studiuar dhe Planifikuar krijimin e Active Directory për userat në Administratën qëndrore, duke kufizuar përdoruesit në qasjet në internet kundrejt faqeve dhe rrjeteve që nuk kanë lidhje me detyrat funksionale.
b) Parashikimin për blerje të një pajisje firewall profesional për të ndalur sulmet të mundshme nga jashtë rrjetit, si dhe blerjen e licensave antivirus për çdo pc për të rritur sigurine e rrjetin dhe mbrojtjen nga viruse të mundshme .
c) Për sistemet (softwaret) që zotëron aktualisht institucioni do të parshikoj kontrata mirëmbajtje në përputhje me legjislacionin e parashikuar /sygjeruar nga AKSHI.
d) Po bashkëpunojmë me specialist IT për sigurine të AKSHI, si një nga institucionet referuese për Teknologjinë e informacionit, për të rritur sa më shumë nivelin e sigurisë së informacionit, sistemeve dhe rrjetit elektronik të Bashkisë Fier.
Ky rekomandim është në proces ***Në vijimësi***

3. Gjetje nga auditimi: Nga penetration test zhvilluar nga grupi i auditimit mbi faqen web të Bashkisë Fier, u konstatua se nuk përdorin një lidhje e sigurt (*connection security*) HTTPS (*Hyper Text 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. Në mungesë të kësaj certifikate mund të ndodhë humbja e privatësisë, ndryshimit të informacionit që merret ose jepet me anë të këtij portali.

3.1 Rekomandim: Bashkia Fier të marrë 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.

Masat e marra nga subjekti për zbatimin e rekomandimit

Bashkia Fier me qëllim përdorimin me efektivitet dhe siguri më të lartë të shërbimeve të hostimit të faqes web dhe të postës elektronike, në bashkëpunim me AKSHI-n ka siguruar hostimin e tyre pranë kësaj agjensie. Ende faqja e web-it përdor lidhje të pasigurt (*Not secure status)*.

Ky rekomandim është në proces ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

9. Bashkia Korçë

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit Bashkia Korçë me shkresën Nr. 779/42 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Janë rekomanduar 8 masa organizative. Nga masat organizative janë pranuar plotësisht 8 masa, nga të pranuarat janë zbatuar 3 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 4 masa organizative, 1 masë organizative nuk është zbatuar.

Për sa më sipër *<u>rikërkoj</u>* që Bashkia Korçë të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Nga auditimi u konstatua se specialistët e IT në Bashkitë e audituara janë të pozicionuar në Drejtorinë e Burimeve Njerëzore. Në vlerësimin tonë, ky pozicionim nuk është i përshtatshëm, pasi përveç faktit që teknologjia e informacionit nuk ka qasje të përbashkët me burimet njerëzore, gjithashtu tendenca aktuale në zhvillimet teknologjike në administratën publike e më gjerë, kërkon një afrimitet të strukturës IT sa më afër vendimmarrjes.

1.1 Rekomandimi: Bashkitë Fier, Korçë, Lezhë e Vlorë, të marrin masat për krijimin e një strukture të veçantë të Teknologjisë së Informacionit, së paku në nivel sektori apo drejtorie, me qëllim rritjen e rëndësisë së këtij sektori dhe afrimin e tij me vendimmarrjet institucionale.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me vendimin e Këshillit Bashkiak nr. 173 datë 26.12.2019 "mbi miratimin e buxhetit vjetor 2020 të Bashkisë Korçë" është miratuar numri i punonjësve për vitin 2020, më pas bazuar në numrin e punonjësve të miratuar është hartuar struktura e vitit 2020 në të cilën nuk ishte e mundur krijimi i një strukture të veçantë të teknologjisë së informacionit në nivel sektori apo drejtorie. Do rishikohet mundësia e krijimit të kësaj strukture në miratimin e buxhetit të vitit 2021.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

2. Gjetje nga Auditimi: Nga auditimi u konstatua se asnjë nga Bashkitë audituara nuk kryen kontrolle mbi aktivitetin e përdoruesve. Në Bashkitë Fier, Lezhë e Vlorë, log-et nuk janë të ruajtura as nga Bashkitë dhe as nga operatorët ekonomikë. Ndërsa në Bashkinë e Korçës, log-et ruhen në mikrotik, por edhe në këtë rast ruhen vetëm log-et e IP-ve statike të cilat po ashtu humbasin në rast rindezje të pajisjes. Gjithashtu këto institucione nuk kanë marrë masat për krijimin e një active directory dhe Domani controller për menaxhimin e user-ave.
Grupi i auditimit vlerëson se kjo qasje rrit riskun e pasigurisë në përdorimin e internetit si dhe ndërhyrjeve të mundshme në rrjetin e Bashkive.
2.1 Rekomandimi: Bashkitë Fier, Korçë, Lezhë e Vlorë, të marrin masat e nevojshme për krijimin e një *active directory* dhe *Domain controller* për menaxhimin e user-ave, si dhe ruajtjen dhe monitorimin e vazhdueshëm të log-eve, me qëllim rritjen e sigurisë në përdorimin e shërbimit të internetit.
Masat e marra nga subjekti për zbatimin e rekomandimit
Janë marrë masat dhe janë përcaktuar në buxhetin e vitit 2020 fonde te nevojshme për blerjen e një serveri i cili do të shërbejë për krijimin e një *activedirectory* dhe *domaincontroller* për menaxhimin e user-ave, si dhe ruatjen dhe monitorimi ne vazhdueshëm të log-eve, me qëllim rritjen e sigurisë në përdorimin e shërbimit të internetit.
Ky rekomandim është në proces ***Në vijimësi***

3.Gjetje nga Auditimi: Nga auditimi u konstatua se Bashkitë Fier, Korçë, Lezhë e Vlorë nuk kanë politika të mirë përcaktuara mbi sigurinë e informacionit, apo plane për sigurinë e sistemeve të teknologjisë së informacionit në përgjithësi dhe në drejtim të rrjetit në veçanti. Në këtë drejtim, mungon një rregullore mbi aksesin e përdoruesve në internet, veprim i cili ka ndikuar në akses të pakufizuar.
3.1 Rekomandimi: Bashkitë Fier, Korçë, Lezhë e Vlorë, të marrin masat për hartimin e politikave të mirë përcaktuara mbi sigurinë e informacionit, si dhe plane për sigurinë e sistemeve të teknologjisë së informacionit në drejtim të rrjetit.
Masat e marra nga subjekti për zbatimin e rekomandimit
Është hartuar regjistri i riskut për teknologjinë e informacionit ku në mënyrë mujore evidentohen ngjarjet që kanë efekte negative në mbarëvajtjen e punës. Në regjistrin e riskut janë evidentuar si mëposhtë:
-Mirëmbajtje e programit të menaxhimit të taksave- kontrata e lidhur në datën 28.02.2020 me afat deri në31.12.2020;
-Suport për hostimin, mailserver dhe domain me afat deri në 31.12.2020;
-Abonim internet ADSL dhe Central Telefonik, kontrata është lidhur në datën 27.01.2020 me afat 12 muaj;
-Mirëmbatje e sistemit"Qytetiim"31.12.2020;
-Mirëmbajtje e"Platformes WEBGIS31.12.2020;
-Mirëmbajtje e programit Onestop shop 31.12.2020;
-Rinovimi i licensave vjetorepër të gjithë Antiviruset për një periudhë1 vjeçare;
-Ndryshimi i teknologjisë për kompiuterat të cilët kanë kaluar afatin për një periudhë 4 vjeçare
Ky rekomandim është në proces ***Në vijimësi***

4. Gjetje nga Auditimi: Nga penetration test zhvilluar nga grupi i auditimit mbi faqen web të Bashkive Fier, Korçë, Lezhë e Vlorë, u konstatua se nuk përdorin 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. Në mungesë të kësaj certifikate mund të ndodhë humbja e privatësisë, ndryshimit të informacionit që merret ose jepet me anë të këtij portali.

4.1 Rekomandimi: Bashkitë Fier, Korçë, Lezhë e Vlorë, 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.

Masat e marra nga subjekti për zbatimin e rekomandimit

Në procedurën që do të kryhet për vitin 2020 përsai përket faqës web dhe mirëmbajtjes së saj do të merren masa për përmirësimin e saj dhe shtimin e çertifikatavetë sigurisë të navigimit online. Kjo procedurë do të kryhet në momentin e rinovimit të kontratës me operatorin që do shpallet fitues për mirëmbajtjen e website.

Ky rekomandim është në proces ***Në vijimësi***

5. Gjetje nga Auditimi: Nga auditimi u konstatua se Bashkitë Korçë, Lezhë dhe Vlorë kanë lidhur kontrata në vlerat respektive 79,000 lekë, 114,000 lekë dhe 149,000 lekë me TVSH me operatorë ekonomik, për hostimin e email-eve dhe web-eve. Ndërsa Bashkia Fier i hoston pranë Agjencisë Kombëtare të Shoqërisë së Informacionit (AKSHI).

5.1. Rekomandimi: Bashkitë Korçë, Lezhë dhe Vlorë në bashkëpunim me AKSHI-n të marrin masat e nevojshme që në vazhdimësi të sigurojnë hostimin e faqes web dhe postës elektronike pranë AKSHI-t me qëllim përdorimin me efektivitet dhe siguri më të lartë të këtij shërbimi.

Masat e marra nga subjekti për zbatimin e rekomandimit

Për vitin 2020 do të merren masa që hostimi do të bëhet pranë AKSHI-t dhe posta elektronike për të rritur sigurinë e shërbimeve. Kjo procedurë do të bëhet në momentin e rinovimit të kontratës me operatorin që do shpallet fitues për mirëmbajtjen e website.

Ky rekomandim është në proces ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi dhe të pa zbatuara,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

10. Bashkia Lezhë

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit Bashkia Lezhë me shkresën Nr. 779/41 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 20 ditor për hartimin e plan veprimit (Hartimin e Programit), konstatojmë se Bashkia Lezhë, nuk e ka përmbushur detyrimin e afatit 20 ditor të kthimit të përgjigjes në KLSH.

Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se Bashkia Lezhë, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 10 masa organizative. Nga masat organizative janë pranuar plotësisht 10 masa, nga të pranuarat janë zbatuar 2 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 2 masa organizative, 6 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që Bashkia Lezhë të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi u konstatua se email-et nuk janë individual por në nivel drejtorie. Gjithë stafi i drejtorive ka akses tek e njëjta adresë, me të njëjtat kredenciale, duke rritur pasigurinë e komunikimit dhe duke vështirësuar ndarjen e punëve dhe përgjegjësive.
1.1 Rekomandim: Bashkia Lezhë te marrë masat e nevojshme për administrimin e email-eve për çdo përdorues me qëllim përmirësimin e komunikimit dhe ndjekjen sipas përgjegjësive individuale në detyrat e çdo punonjësi.
Masat e marra nga subjekti për zbatimin e rekomandimit
Nga ana e Bashkisë Lezhë është bërë kërkese të Agjensia Kombetare e Shoqerisë së Informacionit për adresa zyrtare ër punonjësit e Bashkisë Lezhë dhe nga ana e AKSH-it janë dërguar adresat zyrtare individuale për përsonelin e administratës së Bashkisë Lezhë të cilat përdoren për komunikimin zyrtar të administratës.
Ky rekomandim është në proces ***Menjëherë***

2.Gjetje nga auditimi: Nga auditimi u konstatua se specialistët e IT në Bashkinë Lezhë janë të pozicionuar në Drejtorinë e Burimeve Njerëzore. Në vlerësimin tonë, ky pozicionim nuk është i përshtatshëm, pasi përveç faktit që teknologjia e informacionit nuk ka qasje të përbashkët me burimet njerëzore, gjithashtu tendenca aktuale në zhvillimet teknologjike në administratën publike e më gjerë, kërkon një afrimitet të strukturës IT sa më afër vendimmarrjes.
2.1 Rekomandim: Bashkia Lezhë të marrë masat për krijimin e një strukture të veçantë të Teknologjisë së Informacionit, së paku në nivel sektori apo drejtorie, me qëllim rritjen e rëndësisë së këtij sektori dhe afrimin e tij me vendimmarrjet institucionale.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

3. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Lezhë nuk kryen kontrolle mbi aktivitetin e përdoruesve. Në Log-et nuk janë të ruajtura as nga Bashkia dhe as nga operatori ekonomik. Gjithashtu nuk janë marrë masat për krijimin e një *active directory* dhe *Domani controller* për menaxhimin e user-ave.
Grupi i auditimit vlerëson se kjo qasje rrit riskun e pasigurisë në përdorimin e internetit si dhe ndërhyrjeve të mundshme në rrjetin e Bashkisë.
3.1 Rekomandim: Bashkia Lezhë të marrë masat e nevojshme për krijimin e një *active directory* dhe *Domain controller* për menaxhimin e user-ave, si dhe ruajtjen dhe monitorimin e vazhdueshëm të log-eve, me qëllim rritjen e sigurisë në përdorimin e shërbimit të internetit.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

4. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Lezhë nuk ka një regjistër risku për teknologjinë e informacionit, ku të jenë evidentuar ato ngjarje të mundshme të cilat mund të kenë efekt negativ në mbarëvajtjen e punës institucionale. Edhe pse ky institucion ka një regjistër risku i cili përditësohet çdo vit, aty nuk ka elemente të teknologjisë së informacionit.
4.1 Rekomandim: Bashkia Lezhë të marrë masat për hartimin e një regjistri risku për teknologjinë e informacionit ku të jenë evidentuar ato ngjarje të mundshme të cilat mund të kenë efekt negativ në mbarëvajtjen e punës institucionale, me qëllim krijimin e një plani pune në rastet e shfaqjes së problematikave të ndryshme në fushën e teknologjisë së informacionit.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

5. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Lezhë nuk ka politika të mirë përcaktuara mbi sigurinë e informacionit, apo plane për sigurinë e sistemeve të teknologjisë së informacionit në përgjithësi dhe në drejtim të rrjetit në veçanti. Në këtë drejtim, mungon një rregullore mbi aksesin e përdoruesve në internet, veprim i cili ka ndikuar në akses të pakufizuar.
5.1 Rekomandim: Bashkia Lezhë të marrë masat për hartimin e politikave të mirë përcaktuara mbi sigurinë e informacionit, si dhe plane për sigurinë e sistemeve të teknologjisë së informacionit në drejtim të rrjetit.

Ky rekomandim nuk është zbatuar **Në vijimësi**

6. Gjetje nga auditimi: Nga penetration test zhvilluar nga grupi i auditimit mbi faqen web të Bashkisë Lezhë, u konstatua se nuk përdor një lidhje të 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. Në mungesë të kësaj certifikate mund të ndodhë humbja e privatësisë, ndryshimit të informacionit që merret ose jepet me anë të këtij portali.
6.1 Rekomandim: Bashkia Lezhë të marrë 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.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

7. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Lezhë ka lidhur kontratë në vlerën 114,000 lekë me TVSH me operator ekonomik, për hostimin e email-eve dhe web-eve.
7.1 Rekomandim: Bashkia Lezhë në bashkëpunim me AKSHI-n të marrin masat e nevojshme që në vazhdimësi të sigurojë hostimin e faqes web dhe postës elektronike pranë AKSHI-t me qëllim përdorimin me efektivitet dhe siguri më të lartë të këtij shërbimi.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

8. Gjetje nga auditimi: Nga auditimi i procedurës së prokurimit të shërbimit të internetit në Bashkinë Lezhë, u konstatua se:
a. Mungon dokumenti për përllogaritjen e fondit limit, në kundërshtim me pikën 2, neni 57, VKM 914 datë 29.12.2014 "Për miratimin e rregullave të prokurimit publik", i ndryshuar.

b. Nuk ka dokumentacion që të vërtetojë se operatori fitues plotëson kriteret e vendosura në procedurën e prokurimit, veprim në kundërshtim me pikën 16 të Udhëzimit nr. 3, datë 08.01.2018 "Mbi përdorimin e procedurës së prokurimit me vlerë të vogël dhe zhvillimin e saj me mjete elektronike", i ndryshuar.
c. Nuk dokumentohet procesi i marrjes në dorëzim të shërbimit të internetit si dhe raportet e kolaudimit të shërbimit.
d. Nuk ka dokumentacion mbi deklaratën e konfliktit të interesit të njësisë së prokurimit, në kundërshtim me neni 16, VKM 914 datë 29.12.2014 "Për miratimin e rregullave të prokurimit publik", i ndryshuar.
e. Kërkesat për kualifikim në këtë procedurë nuk janë të argumentuara, në kundërshtim me nenin 61, pika 2, VKM 914 datë 29.12.2014 "Për miratimin e rregullave të prokurimit publik", i ndryshuar.
8.1 Rekomandim: Në vijimësi, Titullari i Autoritetit Kontraktor, Njësia e prokurimit dhe KVO, të marrin masa për respektimin e të gjithave kërkesave të legjislacionit mbi këto procedura, me qëllim dhënien e sigurisë së arsyeshme për mirë përdorimin e fondeve publike.
Masat e marra nga subjekti për zbatimin e rekomandimit
Verifikimi i detajuar i këtij rekomandimi do të bëhet në auditimin e ardhshëm.
Ky rekomandim është në proces ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi dhe të pa zbatuara,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

11. Bashkia Vlorë

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit Bashkia Vlorë me shkresën Nr. 779/40 prot, datë 31.12.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:
Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se Bashkia Vlorë, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 9 masa organizative. Nga masat organizative janë pranuar plotësisht 9 masa, nga të pranuarat është zbatuar 1 masë, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 2 masa organizative, 6 masa organizative nuk janë zbatuar.
Për sa më sipër *rikërkoj* që Bashkia Vlorë të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Vlorë nuk ka kryer asnjë analizë të nevojave institucionale në lidhje me shërbimin e internetit, për sa i përket cilësisë, parametrave, kohës së përgjigjes apo bandwith-it të nevojshëm për përmbushjen e detyrave funksionale. Kjo mund të ndikojë në marrjen e shërbimit të internetit nën kriteret e nevojshme për përmbushjen e

detyrave institucionale ose shpenzimit pa efektivitet të fondeve në rastet e marrjes së parametrave më të mira nga sa është e nevojshme.

1.1 Rekomandim: Në vijimësi Bashkia Vlorë të marrë masa për analizimin e nevojave reale të institucionit mbi cilësitë e duhura të shërbimit të internetit për kryerjen e detyrave funksionale, para kryerjes së procedurës së prokurimit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga ana e sektorit të IT janë vlerësuar nevojat e institucionit për shërbimin e internetit. Por ende nuk ka një miratim për këtë analizë. Ky proces do të konkretizohet në procedurën e ardhshme që do të zhvillohet për përfitimin e internetit.

Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Vlorë nuk ka dokumentacion mbi zbatimin e kontratës MNSH-s. Nuk ka plane, përgjegjësi, dhe procedura të mirë përcaktuara ndaj incidenteve të mundshme në drejtim të ofrimit të shërbimit të internetit. Gjithashtu nuk janë të përfshirë të gjithë elementët e MNSH-së, sipas Udhëzimit Nr. 1159, datë 17.3.2014 "Për hartimin e marrëveshjes së nivelit të shërbimit". Bashkia Vlorë, nuk ka ngritur grup për marrjen në dorëzim të shërbimit të internetit apo grup për monitorim të kontratës.

2.1 Rekomandim: Bashkia Vlorë, të marrë masat për ngritjen e grupeve të punës për monitorimin dhe marrjen në dorëzim të shërbimit të internetit, me qëllim dhënien e sigurisë së arsyeshme të zbatimit me rigorozitet të kontratës. Gjithashtu, në kontratat e ardhshme të marrin masa për implementimin e elementëve të MNSH sipas Udhëzimit Nr. 1159, datë 17.3.2014 "Për hartimin e marrëveshjes së nivelit të shërbimit", të cilat përputhen me këtë shërbim.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ky proces do të konkretizohet në hartimin e kontratës në procedurën e ardhshme që do të zhvillohet për përfitimin e internetit.

Ky rekomandim është në proces ***Në vijimësi***

3. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Vlorë nuk kryen kontrolle mbi aktivitetin e përdoruesve. Log-et nuk janë të ruajtura as nga Bashkia dhe as nga operatori ekonomik. Gjithashtu nuk janë marrë masat për krijimin e një *activedirectory* dhe *Domani controller* për menaxhimin e user-ave.

Grupi i auditimit vlerëson se kjo qasje rrit riskun e pasigurisë në përdorimin e internetit si dhe ndërhyrjeve të mundshme në rrjetin e Bashkisë.

3.1 Rekomandim: Bashkia Vlorë, të marrë masat e nevojshme për krijimin e një *activedirectory* dhe *Domaincontroller* për menaxhimin e user-ave, si dhe ruajtjen dhe monitorimin e vazhdueshëm të log-eve, me qëllim rritjen e sigurisë në përdorimin e shërbimit të internetit.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

4. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Vlorë nuk ka një regjistër risku për teknologjinë e informacionit, ku të jenë evidentuar ato ngjarje të mundshme të cilat mund të kenë efekt negativ në mbarëvajtjen e punës institucionale. Edhe pse ky institucion kanë një regjistër risku i cili përditësohet çdo vit, aty nuk ka elemente të teknologjisë së informacionit.

4.1 Rekomandim: Bashkia Vlorë të marrë masat për hartimin e një regjistri risku për teknologjinë e informacionit ku të jenë evidentuar ato ngjarje të mundshme të cilat mund të kenë efekt negativ

në mbarëvajtjen e punës institucionale, me qëllim krijimin e një plani pune në rastet e shfaqjes së problematikave të ndryshme në fushën e teknologjisë së informacionit.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

5. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Vlorë nuk ka politika të mirë përcaktuara mbi sigurinë e informacionit, apo plane për sigurinë e sistemeve të teknologjisë së informacionit në përgjithësi dhe në drejtim të rrjetit në veçanti. Në këtë drejtim, mungon një rregullore mbi aksesin e përdoruesve në internet, veprim i cili ka ndikuar në akses të pakufizuar.
5.1 Rekomandim: Bashkia Vlorë të marrë masat për hartimin e politikave të mirë përcaktuara mbi sigurinë e informacionit, si dhe plane për sigurinë e sistemeve të teknologjisë së informacionit në drejtim të rrjetit.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

6. Gjetje nga auditimi: Nga penetration test zhvilluar nga grupi i auditimit mbi faqen web të Bashkisë Vlorë, u konstatua se nuk përdori një lidhje të sigurt (*connection security*) HTTPS (*HyperTextTransferProtocolSecure*) (*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. Në mungesë të kësaj certifikate mund të ndodhë humbja e privatësisë, ndryshimit të informacionit që merret ose jepet me anë të këtij portali.
6.1 Rekomandim: Bashkia Vlorë të marrë 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.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

7. Gjetje nga auditimi: Nga auditimi u konstatua se Bashkia Vlorë ka lidhur kontratë në vlerën 149,000 lekë me TVSH me operator ekonomik, për hostimin e email-eve dhe web-eve.
7.1 Rekomandim: Bashkia Vlorë në bashkëpunim me AKSHI-n të marrë masat e nevojshme që në vazhdimësi të sigurojë hostimin e faqes web dhe postës elektronike pranë AKSHI-t me qëllim përdorimin me efektivitet dhe siguri më të lartë të këtij shërbimi.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

8. Gjetje nga auditimi: Nga auditimi u konstatua së Bashkia Vlorë nuk ka asnjë kontratë të nënshkruar ndërmjet saj dhe operatorit ekonomik ofrues të shërbimit "Nisatel". Bashkëpunimi ndërmjet tyre ka nisur në vitin 2012, pa procedurë prokurimi dhe pa rënë dakord juridikisht (me kontratë). Për këtë arsye, ky shërbim nuk është pjesë e regjistrit të parashikimeve dhe regjistrit të realizimit të procedurave të prokurimit. Marrja e shërbimit të internetit në mënyrë të drejtpërdrejtë, pa zhvillimin e një procedure prokurimi është në kundërshtim me nenin 4 "*Fusha e zbatimit*" të ligjit Nr. 9643, datë 20.11.2006 "Për prokurimin publik", i ndryshuar.
8.1 Rekomandim: Bashkia Vlorë të marrë masa për zhvillimin e procedurës së prokurimit, me qëllim përfitimin e një vlere ekonomike sa më të favorshme, duke nxitur konkurrencën ndërmjet operatorëve ekonomikë.

Ky rekomandim nuk është zbatuar ***Menjëherë***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi dhe të pa zbatuara,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

12. Fondi i Sigurimit të Detyrueshëm të Kujdesit Shëndetësor (FSDKSH)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit FSDKSH me shkresën Nr. 63/8 prot, datë 08.08.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Janë rekomanduar 37 masa organizative. Nga masat organizative janë pranuar plotësisht 37 masa, nga të pranuarat janë zbatuar 11 masa, janë zbatuar pjesërisht 10 masa, dhe janë në proces zbatimi 11 masa organizative, 5 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që FSDKSH të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara, të zbatuara pjesërisht dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: Nga auditimi u konstatua se FSDKSH nuk menaxhon ndryshimet në sistemet IT pasi mungojnë procedura për inicimin, prioritarizimin, rishikimin dhe aprovimin e tyre, nuk kryhet verifikimi i efektivitetit të ndryshimeve të kryera, procesi i ndryshimeve nuk dokumentohet.
1.1 Rekomandimi: FSDKSH të hartojë procedura për menaxhimin e ndryshimit, verifikimin e efektivitetit dhe dokumentimin e ndryshimeve në sistemet IT.
Masat e marra nga subjekti për zbatimin e rekomandimit
FSDKSH në vijim të rekomandimit në bashkëpunim me Bankën Botërore dhe Ministrinë e Shëndetësisë dhe Mbrojtjes Sociale janë duke përgatitur specifikimet teknike për një sistem suporti (CRM) për menaxhimin e ndryshimeve dhe dokumentin e tyre. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.
Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga Auditimi: Gjatë vitit 2018 struktura e DIAS rezulton me mungesa në personel në sektorë të rëndësishëm si Sektori i Programimit dhe Menaxhimit të databazave si dhe Sektorin e Suportit Teknik dhe Administrimit të rrjetit.
2.1 Rekomandimi: FSDKSH të marrë masa për:
a. plotësimin e burimeve njerëzore në DIAS
b. hartimin e politikave për menaxhimin e ndryshimeve për pozicionet kritike.
Masat e marra nga subjekti për zbatimin e rekomandimit

DIAS aktualisht është i plotësuar me staf sipas strukturës. Në lidhje me hartimin e politikave për menaxhimin e ndryshimeve për pozicionet kritike FSDKSH është në vijimësi të rekomandimit. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Brenda vitit 2020, në vijimësi***

3. Gjetje nga Auditimi: Nisur nga objektivat strategjikë të FSDKSH, nga shtrirja e teknologjisë së informacionit në institucion si dhe nga rëndësia kombëtare e të dhënave që ruhen dhe përpunohen në FSDKSH nga DIAS, grupi i auditimi gjykon që Sektori i Analizës Statistikore është përfshirë në mënyrë të papërshtatshme brenda Drejtorisë.

3.1 Rekomandimi: FSDKSH të marrë masa në zbatim të praktikave me të mira të fushës për analizimin e situatës me objektiv ndryshimet e nevojshme strukturore në drejtorine DIAS 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.

Masat e marra nga subjekti për zbatimin e rekomandimit

FSDKSH nuk ka vënë dokumentacion në dispozicion.Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

4.Gjetje nga Auditimi: Në FSDKSH nuk ekziston një procedurë e dokumentuar për identifikimin, trajtimin dhe raportimin gabimeve e incidenteve, procedurë e cila redukton kohën e zgjidhjes në rast përsëritje të të njëjtit incident si dhe ul riskun e ndodhjes së incidenteve në të ardhmen. Procedurat kryhen me anë të shkëmbimeve verbale dhe komunikimeve me e-mail. Mungesa e një procedure të menaxhimit të incidenteve sjell paqartësi në:

- njohjen e nivelit të riskut që kërcënime të ndryshme mund mbartin për FSDKSH -në;
- nivelin e impaktit të incidenteve të ndodhur në veprimtarinë e FSDKSH -së;
- dokumentimin dhe mos lënien e gjurmëve për trajtimin e incidenteve dhe zgjidhjen e tyre nga punonjësit.

Në opinionin e grupit të auditimit, mbajtja e korrespondencës midis niveleve të punonjësve brenda institucionit për incidentet e ndodhura, është e pamjaftueshme për trajtimin në kohë dhe në mënyrë efektive të incidenteve, pasi FSDKSH-ja nuk ka politika për ruajtjen e këtyre dokumenteve. 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 nga punonjësit.

4.1 Rekomandimi: Strukturat Drejtuese dhe zbatuese në FSDKSH të marrin masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve në përputhje me kërkesat e Ligjit nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar, Udhëzimit nr. 30, datë 27.12.2011 "Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik", i ndryshuar.

Masat e marra nga subjekti për zbatimin e rekomandimit

Drejtori i Përgjithshëm në FSDKSH ka ngritur grupin e punës me anë të urdhrit Nr.569, datë 07.10.2019 "*Mbi hartimin e rregullores për sigurine teknike dhe organizative në fushën kibernetike si dhe propozimin e ekipit përgjegjës për incidentet kibernetike (CSIRT)".* Grupi punës është duke u këshilluar për hartimin e kësaj rregullore me AKCESK (Autoriteti Kombëtare për Certifikimin Elektronik dhe Sigurinë Kibernetike). Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

5. Gjetje nga Auditimi: FSDKSH për sistemin e DRC Durrës (Disaster Recovery Centre), duke filluar që nga muaji Janar 2017, nuk ka një marrëveshje për nivelin e shërbimit, SLA-Service Level Agreement në kundërshtim me VKM Nr. 710, datë 21.8.2013 "Për Krijimin dhe Funksionimin e Sistemeve të Ruajtjes së Informacionit, Vazhdueshmërisë së Punës dhe Marrëveshjeve të Nivelit të Shërbimit" (Ndryshuar me VKM nr.755, datë 26.10.2016).

5.1. Rekomandimi: FSDKSH të kryejë analizimin e situatës në DRC Durrës (Disaster Recovery Centre), dhe mbulimin me MNSH në përputhje me **VKM Nr. 710, datë 21.8.2013 "**Për Krijimin dhe Funksionimin e Sistemeve të Ruajtjes së Informacionit, Vazhdueshmërisë së Punës dhe Marrëveshjeve të Nivelit të Shërbimit" (Ndryshuar me VKM nr.755, datë 26.10.2016).

Masat e marra nga subjekti për zbatimin e rekomandimit

Sistemet bazike që FSDKSH ka si përfituese të shërbimit janë të hostuar pranë AKSHI-t në bazë të marrëveshjes nënshkruar ndërmjet palëve me shkresën nr. 3450 Prot., datë 25.06.2019 protokolluar në AKSHI-t dhe me nr. 3023 Prot., datë 25.06.2019 protokolluar në FSDKSH, për *"Ofrimin e hapësirës fizike në Data Center-in Qeveritar - RACK/ Hapësirë 'U' Në RACK"*, për hostimin e sistemeve.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

6. Gjetje nga Auditimi: Sistemi eFarmacia nuk ka mekanizma kontrolli për veprimet e kryera. Nga auditimi i të dhënave për vitin 2018 të sistemit e-Farmacia, gjithësej 91386 rekorde u konstatuan disa parregullsi:

- 1341 raste të ekzekutimit të recetave për të cilët nuk rezultojnë mjekë të regjistruar për aprovimin e saj (Tabela bashkëlidhur në aneks)
- 9 raste të rimbursimit të recetës me vlerë negative (Tabela bashkëlidhur në aneks)
- 56 rekorde me vlera negative në diferenca të datave (Tabela bashkëlidhur në aneks)

6.1. Rekomandimi: FSDKSH të marri masa për vendosjen e mekanizmave të kontrollit për veprimet e kryera në sistem me qëllim rritjen e efektivitetit, eficiencës dhe ekonomicitetit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Sistemi eFarmacia nuk është më në përdorim, funksioni i këtij sistemi është zëvendësuar me sistemin e Recetës elektronik e-Rx i cili ndërvepron me sistemet e tjera qeveritare. *)".* Grupit të auditimit nuk iu vu në dispozicion dokumentacion mbështetës lidhur me rekomandimin për marrjen e masave për vendosjen e mekanizmave të kontrollit për veprimet e kryera në sistem me qëllim rritjen e efektivitetit, eficiencës dhe ekonomicitetit. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

7. Gjetje nga Auditimi: Nga auditimi i aplikacionit receta elektronike u konstatua se:

- Nuk ka mekanizma kontrolli për aktivitetin e kryer në sistem, rast specifik paraqitet vijimi i punës së farmacive në sistem edhe kur u ka mbaruar afati i kontratës me FSDKSH. Nga raportet e BI rezulton se farmacitë kanë ushtruar aktivitet edhe pas përfundimit të afatit të vlefshmërisë së kontratës me FSDKSH.
- Nuk ka një kontroll të logeve të serverave dhe analizim të tyre, të gjithë loge-eve HW ose SW
- Sistemi nuk paralajmëron për statisktika të storage (Used disk space etj)
- Nuk janë dokumentuar kontrolle të statisktikave të storage (Used disk space etj)
- Nuk ka një raport mbi rishikim të të dhënave mbi performancën e serverave
- Nuk është kryer testim apo kontroll i kompletuar i pjesëve më kritike të infrastrukturës

- Nuk ka një raport mbi gjendjen aktuale dhe propozim për upgrade të mundshem HW
- Sistemi nuk ndërvepron me një e-shërbim web me sistemin e sigurimeve shoqërore për konsultimin e pensionistëve.

Pikat e mësipërme janë të përfshira në kontratën e lidhur me OE.

7.1. Rekomandimi: FSDKSH të marrë masa që të identifikojë origjinën dhe sistemimin e të gjitha problematikave lidhur me mungesën e mekanizmave të kontrollit në sistemin eReceta, dokumentimin e të gjitha ndryshimeve dhe kryerjen e testimeve periodike me qëllim rritjen e integritetit të sistemit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Sistemi i recetës elektronike e-Rx është një kontratë e Ministrisë së Shëndetësisë dhe Mbrojtjes Sociale me OE, FSDKSH është përfituese e këtij shërbimi. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

8. Gjetje nga Auditimi: FSDKSH 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.

8.1. Rekomandimi:

a. FSDKSH duke analizuar mjetet financiare, kohën dhe burimet njerëzore të kryejë investime në drejtim të përdorimit të informacionit që ruhet në sistemet e tij për rritjen e efektivitetit, eficencës dhe ekonomicitetit në administrimin e skemës së rimbursimeve.

b. FSDKSH të rrisë bashkëpunimin me institucionet përgjegjëse në menaxhimin e skemës së sigurimeve shëndetësore (Institutin e Sigurimeve Shoqërore, Ministrinë e Shëndetësisë dhe Mbrojtjes Sociale, Institutin e Statistikës) me qellim përdorimin e big data dhe analizimit të tyre në hartimin e politikave kombëtare të kujdesit shëndetësor.

Masat e marra nga subjekti për zbatimin e rekomandimit

FSDKSH është në komunikime të vazhdueshme ndër-institucionale me AKSHI-n, MshMS, INSTATdhe me të gjithë aktorët e shërbimit shëndetësor. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

9. Gjetje nga Auditimi: Nga auditimi u konstatua se mungesa e bashkëveprimit të sistemit të Kostove Spitalore me sistemin e Shpenzimeve Spitalore (i cili është i shtrirë në të gjithë spitalet bashkiake) mbart riskun e saktësisë në përgatitjen e buxhetit dhe strategjisë nga ana e degëve të FSDKSH dhe njëkohësisht financimin e spitaleve nga FSDKSH.

9.1. Rekomandimi: FSDKSH të analizojë dhe implementojë ndryshimet e nevojshme në sistemin e Kostove Spitalore me qëllim integrimin me sistemet e tjera.

Masat e marra nga subjekti për zbatimin e rekomandimit

DIAS ka parashikuar në PBA 2020-2022 suport shërbim mirembajtje për sistemin e Shpenzimeve Spitalore ku do të bëjë të mundur realizimin e ndryshimeve të nevojshme për integrimin e tij me sistemin e Kostove spitalore dhe me sistemet e tjera. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

10. Gjetje nga Auditimi: Nga auditimi konstatohet se sistemi i Depove farmaceutike:

- Sistemi nuk kryen hedhjen në kohë reale të faturave hyrëse dhe dalëse të depove.
- Sistemi nuk kryen shkëmbim të dhënash me sistemin e recetës elektronike për të dhënat e farmacive (për daljet nga depot dhe hyrjet në farmaci për të dhënat e hyrjeve të inventarëve të farmacive)
- Sistemi nuk kryen shkëmbim të dhënash të depove me njëra-tjetrën
- Sistemi nuk kryen shkëmbim të dhënash me sistemin e regjistrit të barnave përsa i përket të dhënave të barnave të rimbursueshme

Si pasojë, regjistrimi i faturave hyrëse e dalëse mbart riskun e gabimeve njerëzore.

10.1. Rekomandimi: FSDKSH të analizojë dhe implementojë ndryshimet e nevojshme në sistemin e DEPO-ve me qëllim integrimin me sistemet e tjera dhe rritjen e integritetit të tij.

Masat e marra nga subjekti për zbatimin e rekomandimit

Referuar kontratës së AKSHI-t me Nr.Prot 1023 datë 26.02.2019 *"Zhvillim software moduli i depove farmaceutike"*, ku FSDKSH është përfituese e këtij shërbimi është në fazë implementimi në Depot Farmaceutike të sistemit online e DEPO. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

11. Gjetje nga Auditimi: Auditimi i brendshëm në FSDKSH **nuk**:

- ka akses dhe nuk shfrytëzon për auditim informacion nga sistemet informatike të FSDKSH.
- përdor teknika të auditimit të bazuara në teknologji informacioni.
- ka një plan auditimi të bazuar në rrezik për të përcaktuar përparësitë e aktivitetit të auditimit të brendshëm, në linjë me objektivat e FSDKSH-së.
- vlerëson nëse qeverisja e teknologjisë së informacionit në FSDKSH mbështet strategjitë dhe objektivat institucionale.
- përdor teknologjinë për zbulimin e mashtrimit dhe vlerësimin e mundësisë e ngjarjes së tij.

11.1. Rekomandimi: DIAS ne funksion te kryerjes se detyrimeve ligjore ti siguroj Auditit te brendshëm akses në sistemet informatike të FSDKSH.

Masat e marra nga subjekti për zbatimin e rekomandimit

FSDKSH me shtimin e pozicionit specialist IT në Drejtorinë e Auditit të Brendshëm, me rekrutimin e stafit përkatës do të mundësohoj aksesin e nevojshëm në modulin Audit Vault të sistemit e-RX. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

12. Gjetje nga Auditimi:

a. Në planin strategjik konstatohet se nuk adresohet në mënyrë të përshtatshme roli kritik i sigurisë së informacionit dhe nuk merren në konsideratë planet e IT, klasifikimi i të dhënave, standardet teknologjike, politikat e kontrollit dhe menaxhimi i riskut.

b. Në planin e sigurisë së TI-së konstatohet se nuk identifikohen qartë detyrat dhe përgjegjësitë (menaxhimit ekzekutiv, menaxhimit të linjës, personelit dhe të gjithë përdoruesve të sistemeve IT të FSDKSH), kërkesat e stafit, ndërgjegjësimi dhe trajnimi mbi sigurinë, zbatimi i praktikave, nevoja për investime në burimet e kërkuara të sigurisë. Nuk janë të hartuara dokumentet e raportimit të incidenteve të sigurisë dhe ndjekja e tyre për të përcaktuar se çfarë veprimesh ndërmerren në rastet kur individët abuzojnë me politikat e sigurisë. Plani i sigurisë konstatohet se nuk ka marrë në konsideratë zbatimin e detyrimeve ligjore të përcaktuara në dispozitat e ligjit nr. 2/2017 "Për Sigurinë Kibernetike".

c. Në Rregulloren për organizimin, funksionimin dhe përshkrimet e punës të FSDKSH, në seksionin që i referohet DIAS nuk janë të përcaktuara detyrat dhe përgjegjësitë e qarta të TI-së lidhur me Politikat e Sigurisë së Informacionit (referuar ISO 27001) dhe politikat e sigurisë së informacionit nuk janë implementuar në përputhje me klasifikimin e të dhënave sensitive të FSDKSH-së.

12.1. Rekomandimi: Strukturat drejtuese në FSDKSH, duke marrë në konsideratë kohën dhe burimet e nevojshme të marrin masa për hartimin e planit të sigurisë së informacionit dhe implementimin e tij ku të pasqyrohet ndarja e detyrave/përgjegjësive të sigurisë në TI, në respektim të praktikave më të mira mbi sigurinë e informacionit dhe të dhënave që sistemet e saj përpunojnë.

Masat e marra nga subjekti për zbatimin e rekomandimit

FSDKSH ka ngritur grupin e punës me urdhër nr. 569, datë 07.10.2019 *"Mbi hartimin e rregullores për sigurinë teknike dhe organizative në fushën kibernetike si dhe propozimin e ekipit përgjegjës për incidentet kibernetike (CSIRT)".* Grupit të auditimit nuk iu vu në dispozicion dokumentacion mbështetës lidhur me rekomandimin për hartimin e planit të sigurisë së informacionit dhe implementimin e tij ku të pasqyrohet ndarja e detyrave/përgjegjësive të sigurisë në TI, në respektim të praktikave më të mira mbi sigurinë e informacionit dhe të dhënave që sistemet e saj përpunojnë. Për këtë arsye grupi i auditimit e konsideron rekomandimin si pjesërisht të zbatuar.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë dhe në vijimësi***

13. Gjetje nga Auditimi:Për te gjitha drejtoritë rajonale, nuk ka te konfiguruar asnjë log për të monitoruar veprimtaritë input/output në aksesimin e routerave. Të gjitha routerat e drejtorive rajonale janë te konfiguruara në VPN IPSEC me zyrën qëndrore.

13.1. Rekomandimi:DIAS në bashkëpunim me IT e zyrave rajonale të konfigurojë pajisjet për ruajtjen e logeve në rrjetin kompjuterik të drejtorive rajonale për të monitoruar veprimtarinë në aksesimin e routerave dhe në mënyrë periodike të analizojë dhe dokumentojë ato.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ruajta e logeve në routerat Juniper është aktivizuar por nuk bëhet për një kohë të gjatë. DIAS ka parashikuar në PBA 2020-2022 suport shërbim mirembajtje për sistemin e rrjetit WAN në FSDKSH. Pajisjet e infrastrukturës së rrjetit nuk janë në shërbim mirëmbajtje. Janë bërë procedura për kalimin e tyre në regjism mirëmbajtje, por janë evidentua se këto pajisje janë endofflife service nga vetë prodhuesi. Për sa më sipër grupi i auditimit e konsideron rekomandimin si të zbatuar pjesërisht.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë***

14. Gjetje nga Auditimi: Nga auditimi i logeve të sigurisë, në routerin e zyrës qendrore, të cilat mundësojnë ruajtjen e informacionit, u konstatua se loget janë të çaktivizuara.

Referuar konfigurimit, routeri nuk ruan asnjë informacion mbi hyrjet input/output. Në këtë mënyrë nuk mund të analizohen dhe të detektohen në kohë reale ndërhyrje në sisteme, sulme apo tentativa për krime kibernetike.

14.1. Rekomandimi: DIAS të konfigurojë pajisjet duke aktivizuar loget e sigurisë në routerin e zyrës qendrore për të monitoruar veprimtarinë në aksesimin e routerave dhe në mënyrë periodike të analizojë dhe dokumentojë ato.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ruajta e logeve në routerat Juniper është aktivizuar por ruajtja nuk bëhet për një kohë të gjatë. DIAS ka parashikuar në PBA 2020-2022 suport shërbim mirembajtje për sistemin e rrjetit WAN në FSDKSH.Pajisjet e infrastrukturës së rrjetit nuk janë në shërbim mirëmbajtje, pajisje janë

endofflife service nga vetë prodhuesi. Për sa më sipër grupi i auditimit e konsideron rekomandimin si të zbatuar pjesërisht.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë***

15. Gjetje nga Auditimi: Nga auditimi i konfigurimeve për detektimin e sulmeve dhe ruajtjen në loge të informacionit që rrjedh prej tyre (konfiguruar nga DIAS për krijimin e sigurisë për protokollet e konfiguruara në rrjet), u konstatua se filet e logeve sipas konfigurimeve të mëposhtme janë fshire pa kryer me pare procedurën e analizimit dhe dokumentimit te tyre si dhe evidentimin e rasteve kritike për rrjetin e FSDKSH.

15.1. Rekomandimi:DIAS në mënyrë periodike të analizojë dhe dokumentojë loget e sigurisë me qëllim detektimin e sulmeve dhe rasteve kritike në rrjetin e FSDKSH.

Masat e marra nga subjekti për zbatimin e rekomandimit

Është aktivizuar ruajta e logeve në routerat Juniper, por ruajtja nuk bëhet për një kohë të gjatë. DIAS ka parashikuar në PBA 2020-2022 suport shërbim mirembajtje për sistemin e rrjetit WAN në FSDKSH.Pajisjet e infrastrukturës së rrjetit nuk janë në shërbim mirëmbajtje, pajisje janë endofflife service nga vetë prodhuesi. Për sa më sipër grupi i auditimit e konsideron rekomandimin si të zbatuar pjesërisht.

Ky rekomandim është zbatuar pjesërisht ***Në vijimësi***

16. Gjetje nga Auditimi: Nga auditimi i routerit të zyrës qendrore u konstatua se konfigurimet e gjetura lejojnë kompromentime të sigurisë si me poshtë:

a) Router ka të konfiguruar me të gjitha drejtoritë rajonale një VPN të bazuar në protokollin IPSEC. Nga auditimi i logeve u konstatua se lidhjet mbi protokollin VPN nuk mundësojnë asnjë informacion si dhe status të monitorimit të tyre.

b) Paregullsi ne konfigurimet për direktimin e paketave nga IP-te e jashtme drejt rrjetit te brendshëm, vërehet qe ka DST-NAT (Destination NAT) me source ..... pra lejimin e te gjitha IP-ve nga jashtë drejt shërbimeve te brendshme ne portat ..... prej dy IP statike te jashtme .....dhe .....

16.1. Rekomandimi: DIAS të konfigurojë pajisjet për ruajtjen e logeve në routerin qendror në mënyrë që të mundësohet status i monitorimit të tyre dhe të kufizohen direktimet e paketave specifike drejt rrjetit të brendshëm.

Masat e marra nga subjekti për zbatimin e rekomandimit

Është aktivizuar ruajta e logeve në routerat Juniper, por ruajtja nuk bëhet për një kohë të gjatë. DIAS ka parashikuar në PBA 2020-2022 suport shërbim mirembajtje për sistemin e rrjetit WAN në FSDKSH.Pajisjet e infrastrukturës së rrjetit nuk janë në shërbim mirëmbajtje, pajisje janë endofflife service nga vetë prodhuesi. Për sa më sipër grupi i auditimit e konsideron rekomandimin si të zbatuar pjesërisht.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë***

17. Gjetje nga Auditimi: Nga auditimi u konstatua se:

Rule HR-nat-..... përdor një pool me IP të brendshme .....dhe Rule fin-..... përdor një pool me IP te brendshme ..... Nga auditimi i këtyre konfigurimeve u konstatua se çdo IP-interneti mund te lidhet ne portën ..... e cila sipas konfigurimit te pool përkatës redirect ne IP-te e rrjetit të brendshëm (..... dhe .....) dhe filet e logeve për këto lidhje janë fshirë pa kryer me pare procedurën e analizimit dhe dokumentimit te tyre si dhe evidentimin e rasteve kritike për rrjetin e FSDKSH.

17.1. Rekomandimi: DIAS të konfigurojë pajisjet për ruajtjen e logeve në routerin qendror në mënyrë që të mos lejohet redirekt të cdo IP interneti në rrjetin e brendshëm. Loget të analizohen dhe dokumentohen.

Masat e marra nga subjekti për zbatimin e rekomandimit

Është aktivizuar ruajta e logeve në routerat Juniper, por ruajtja nuk bëhet për një kohë të gjatë. DIAS ka parashikuar në PBA 2020-2022 suport shërbim mirembajtje për sistemin e rrjetit WAN në FSDKSH.Pajisjet e infrastrukturës së rrjetit nuk janë në shërbim mirëmbajtje, pajisje janë endofflife service nga vetë prodhuesi. Për sa më sipër grupi i auditimit e konsideron rekomandimin si të zbatuar pjesërisht.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë***

18. Gjetje nga Auditimi: Nga konfigurimet e ERX konstatohet se është e konfiguruar një rregull e cila lejon çdo IP të internetit të lidhet me ERX në portën .....

Nga auditimi i ketyre konfigurimeve u konstatua se çdo IP-interneti mund të lidhet në portën ..... e cila sipas konfigurimit te pool përkatës redirect në IP e rrjetit të brendshëm (.....) dhe rezulton se filet e logeve për këto lidhje janë fshire pa kryer me parë procedurën e analizimit dhe dokumentimit të tyre si dhe evidentimin e rasteve kritike për rrjetin e FSDKSH.

18.1. Rekomandimi: DIAS të konfigurojë pajisjet për ruajtjen e logeve në routerin qendror në mënyrë që të mos lejohet redirekt të çdo IP interneti në rrjetin e brendshëm përmes IP statike specifike. Loget të analizohen dhe dokumentohen.

Masat e marra nga subjekti për zbatimin e rekomandimit

Referuar marrëveshjes midis AKSHI-t dhe FSDKSH, nënshkruar ndërmjet palëve me shkresën nr. 3450 Prot., datë 25.06.2019 protokolluar në AKSHI-t dhe me nr. 3023 Prot., datë 25.06.2019 protokolluar në FSDKSH, për *"Ofrimin e hapësirës fizike në Data Center-in Qeveritar - RACK/ Hapësirë 'U' Në RACK"*, mbi hostimin e shërbimeve pranë Datacenterit Qeveritar edhe Receta Elektronike është zhvendosur pranë AKSHI-t.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë dhe në vijimësi***

19. Gjetje nga Auditimi: Nga auditimi u konstatua se FSDKSH:

- Nuk ka Rregullore të Teknologjisë së Informacionit (IT) ku të mbështesë aktivitetin e saj.
- Nuk ka dokumentuar dhe implementuar politika mbi sigurinë e informacionit duke patur parasysh disa elementë si:
- 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 sistemeve të FSDKSH;
- Planet e sigurisë;
- Loget e të dhënave të audit trial nuk gjenden dhe nuk ruhen në kundërshtim me "Rregulloren për menaxhimin e log-eve digjitale në administratën publike", miratuar me Urdhrin nr. 109 datë 10.06. 2016 të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT);
- Nuk ka dokumentim për procedurat e testimit të back up-it dhe restore-it. {Kopjet (backup) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme;

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.}

19.1.Rekomandimi: FSDKSH, 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. Planifikimi dhe testimi i sistemeve TIK të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen.

Masat e marra nga subjekti për zbatimin e rekomandimit

Referuar marrëveshjes midis AKSHI-t dhe FSDKSH, nënshkruar ndërmjet palëve me shkresën nr. 3450 Prot., datë 25.06.2019 protokolluar në AKSHI-t dhe me nr. 3023 Prot., datë 25.06.2019 protokolluar në FSDKSH, për *"Ofrimin e hapësirës fizike në Data Center-in Qeveritar - RACK/ Hapësirë 'U' Në RACK"*, mbi hostimin e shërbimeve pranë Datacenterit Qeveritar të gjitha sistemet bazike janë zhvendosur pranë AKSHI-t. Grupit të auditimit nuk iu vu në dispozicion dokumentacion mbështetës lidhur me rekomandimin 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. Për këtë arsye grupi i auditimit e konsideron rekomandimin si pjesërisht të zbatuar.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë dhe në vijimësi***

20. Gjetje nga Auditimi: DRC nuk plotëson standardet e miratuara nga AKSHI "Për ndërtimin e dhomës së serverëve" dhe nuk është ndërtuar bazuar në praktikat më të mira për ndërtimin e DRC.

20.1. Rekomandimi: Të merren masa për ndërtimin e ambienteve DRC mbështetur në praktikat më të mira ndërkombëtare dhe në zbatim të kërkesave të Rregullores për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK.

Masat e marra nga subjekti për zbatimin e rekomandimit

Referuar marrëveshjes midis AKSHI-t dhe FSDKSH, nënshkruar ndërmjet palëve me shkresën nr. 3450 Prot., datë 25.06.2019 protokolluar në AKSHI-t dhe me nr. 3023 Prot., datë 25.06.2019 protokolluar në FSDKSH, për *"Ofrimin e hapësirës fizike në Data Center-in Qeveritar - RACK/ Hapësirë 'U' Në RACK"*, mbi hostimin e shërbimeve pranë Datacenterit Qeveritar të gjitha sistemet bazike janë zhvendosur pranë AKSHI-t. Për sa më sipër grupi i auditimit e konsideron rekomandimin si pjesërisht të zbatuar.

Ky rekomandim është zbatuar pjesërisht ***Në vijimësi***

21. Gjetje nga Auditimi: DRC Durrës nuk e kryen funksionin për të cilin është ndërtuar.

Nga kontrolli i kryer në DRC Durrës rezultoi si më poshtë:

- Sistemet nuk ndër veprojnë në kohë reale me njëri tjetrin.
- Nga UPS-ët e vendosur, njëri prej tyre rezulton i fikur.
- Switch Juniper SRX240 është jofunksional.
- Blade server 1 dhe 3 janë në gjendje alarmi.
- Serveri nuk arrin të aksesohet dhe kompania nuk ka të dokumentuar dokumentacion teknik për ndërhyrje në raste problematikash.
- Nga analizimi i logeve të DRC konstatohet se:
- Ka errore të shpeshta për fikje/ndezje të shasive brenda blade me status kritik
- Ka shkëputje të shpeshta të energjisë për të gjitha blloqet e ushqimit
- 4 nga slotet janë me statusin error aktiv

21.1. Rekomandimi: FSDKSH të marrë masa për vënien në punë të DRC sipas standardeve për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe rimëkëmbjes nga katastrofat.

Masat e marra nga subjekti për zbatimin e rekomandimit

Referuar marrëveshjes midis AKSHI-t dhe FSDKSH, nënshkruar ndërmjet palëve me shkresën nr. 3450 Prot., datë 25.06.2019 protokolluar në AKSHI-t dhe me nr. 3023 Prot., datë 25.06.2019 protokolluar në FSDKSH, për *"Ofrimin e hapësirës fizike në Data Center-in Qeveritar - RACK/ Hapësirë 'U' Në RACK",* mbi hostimin e shërbimeve pranë Datacenterit Qeveritar të gjitha sistemet bazike janë zhvendosur pranë AKSHI-t. Për sa më sipër grupi i auditimit e konsideron rekomandimin si pjesërisht të zbatuar.

Ky rekomandim është zbatuar pjesërisht ***Menjëherë***

22.Gjetje nga Auditimi:

a.Nga auditimi u konstatua se Strategjia për Teknologjinë e Informacionit në FSDKSH përfshin vitet 2014-2017, është miratuar nga Këshilli Administrativ me vendim nr. 13 datë 26.02.2014 është e pa përditësuar.

b. FSDKSH po zhvillon teknologjinë e informacionit pa strategji, duke mos pasqyruar në zhvillimet TIK objektivat institucionale lidhur me infrastrukturën, burimet e nevojshme si dhe instrumenteve të nevojshëm për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keq adresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së FSDKSH.

22.1 Rekomandimi: FSDKSH në bashkëpunim me DIAS dhe me strukturat këshilluese mbi TIK, duke marrë në konsideratë kohën, burimet e nevojshme të marrë masa për:

a. Hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit,

b. Rishikimin periodik të indikatorëve të performancës për matjen e ecurisë së objektivave institucionalë.

Ky rekomandim nuk është zbatuar ***Menjëherë dhe në vijimësi***

23. Gjetje nga Auditimi: Nga auditimi i sistemit e-Receta konstatohet se nuk janë hartuar politika adekuate të sigurisë së informacionit që të mbrojnë të gjithë informacionin konfidencial lidhur me palët e brendshme dhe të jashtme. DIAS nuk ka hartuar një rregullore specifike për "Mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale" në përputhje me dispozitat e ligjit nr. 9887/2008 "Për mbrojtjen e të dhënave personale" dhe Udhëzimin nr. 47, datë 14.9.2018 të Komisionerit "Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha".

23.1. Rekomandimi:DIAS në bashkëpunim me strukturat drejtuese në FSDKSH duke marrë në konsideratë kohën dhe burimet e nevojshme të marrin masa për hartimin e një dokumenti politikash mbi sigurinë e sistemit e-Receta duke marrë në konsideratë edhe kërkesat e ligjit nr. 9887/2008 "Për mbrojtjen e të dhënave personale".

Ky rekomandim nuk është zbatuar ***Menjëherë***

24. Gjetje nga Auditimi: Nga auditimi konstatohet se Drejtoria e Informacionit dhe Analizës Statistikore në FSDKSH nuk ka akses në bazën e të dhënave të sistemit e-Receta (as me të drejta lexuesi) dhe as në modulin audit vault. Aksesi në bazën e të dhënave mbahet vetëm nga kompania "Infosoft

Systems sh.p.k" duke kompromentuar kështu sigurinë e sistemit i cili përpunon të dhëna sensitive dhe ka rëndësi të lartë kombëtare.

24.1. Rekomandimi: Strukturat drejtuese në FSDKSH dhe DIAS të marrin masa për marrjen e të drejtave të plota të administratorit e të pronarit të sistemit eReceta.

Ky rekomandim nuk është zbatuar ***Menjëherë***

25. Gjetje nga Auditimi: Pas shqyrtimit të dokumentacionit të vënë në dispozicion, pjesë e të cilit janë edhe Rregulloret, Udhëzimet dhe Manualet e sistemeve të Teknologjisë së Informacionit nën administrimin e FSDKSH grupi i auditimit konstatoi se:

- Nuk ka dokumentacion të procedurave që ndiqen për hapjen dhe mbylljen e llogarive së përdoruesve.
- Sistemet e Teknologjisë së Informacionit në FSDKSH funksionojnë pa rregullore të miratuara ku të jenë të përcaktuara nivelet e aksesit, të drejtat dhe përgjegjësitë e ndara të përdoruesve në mënyrë që të reduktohen mundësitë për aksesin e paautorizuar.
- Nuk ka raporte të hartuara dhe analizë mbi gjendjen e përdoruesve të çelur në sistem.
- Si shkak i mos dokumentimit të procedurave, funksionimit pa rregullore të miratuara dhe mos kryerjes së analizave, llogaritë e përdoruesve nuk mbyllen edhe pas largimit të tyre nga puna.

Çështjet e mësipërme cenojnë sigurinë e të dhënave që mbrohen nga Ligji Nr. 2/2017, datë 26.01.2017 "Për Sigurinë Kibernetike".

25.1. Rekomandimi: FSDKSH 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 sistemeve me qëllim uljen e riskut të dhënies së të drejtave mbi përdorimin e sistemeve, racionalizimin e privilegjeve si dhe dokumentimin e ndryshimeve.

Ky rekomandim nuk është zbatuar ***Menjëherë dhe në vijimësi***

26. Gjetje nga Auditimi: Nga auditimi u konstatua se në shërbimin e gjenerimit të kartës së shëndetit që u ofrohet qytetarëve në platformën e-albania, i cili merr të dhëna nga sistemi e-Regjistër, në disa raste qytetarëve i mungon kodi i pacientit. Plotësimi i të dhënave të sistemit e-Regjistër është një detyrim i funksionimit të shërbimit të gjenerimit të kartës së shëndetit.

Grupi i auditimit konstaton se regjistri elektronik i banorëve në ndërveprimin me sisteme të tjera për ofrimin e shërbimit të kartës së shëndetit mbart risqet e keqadresimit të problematikave që këto sisteme mbartin.

26.1. Rekomandimi: FSDKSH të marrë masa për analizimin e të dhënave për përcaktimin e të dhënave detyruese për tu plotësuar dhe vendosjen e mekanizmave të kontrollit në mënyrë që të rrisë cilësinë e shërbimeve që ofrohen nga ky sistem.

Ky rekomandim nuk është zbatuar ***Menjëherë dhe në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *të zbatuara pjesërisht, në proces zbatimi dhe të pa zbatuara,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

13. Korporata Elektroenergjitike Shqiptare sh.a (KESH)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit KESH me shkresën Nr. 370/10 prot, datë 16.09.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se KESH, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 23 masa organizative. Nga masat organizative janë pranuar plotësisht 23 masa, nga të pranuarat janë zbatuar 10 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 11 masa organizative, 2 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që KESH të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi u konstatua se në planin strategjik të miratuar pasqyrohen objektivat e shoqërisë dhe misioni i saj, por nuk ka përmbajtje apo identifikim të nevojave teknologjike që ndihmojnë shoqërinë të realizojë arritjen e objektivave. Departamenti i Automatizimit dhe Teknologjisë së Informacionit (DATI) nuk ka Strategji për Teknologjinë e Informacionit, mungesa e të cilës sjell mos pasqyrimin e objektivave lidhur me infrastrukturën, burimet e nevojshme si dhe instrumenteve të nevojshëm për matjen e objektivave dhe arritjen e këtyre objektivave.

1.1 Rekomandimi: KESH sh.a 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 adresohet qartë mënyra se si teknologjia e informacionit do të ndihmojë në arritjen e objektivave të vetë institucionit.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. në kuadër të rekomandimit të lënë nga KLSH ka ndërmarrë hapa mbi hartimin e Planit Strategjik të Teknologjisë së Informacionit, e cila është në formën e një drafti, të pa miratuar.

Ky rekomandim është në proces ***Në vazhdimësi***

2. Gjetje nga auditimi: Nga auditimi rezulton se për të gjithë sistemet që disponon KESH, nuk ka hartuar/miratuar rregullore të përdorimit të tyre, me qëllim adresimin e qartë të proceseve të informatizuara. Mungesa e rregulloreve krijon mundësinë për mos përdorimin e sistemeve, e si rezultat dhe mos adresimin e përgjegjësive për mungesë efektiviteti dhe sigurie të çdo hapi të informatizuar.

2.1 Rekomandimi: KESH sh.a. të marrë masa për hartimin e rregulloreve për secilin prej sistemeve, duke identifikuar pozicionet që e kanë përdorimin e sistemit një detyrim si dhe procesit që cdo sistem dhe të dhënat e tij i shërbejnë. Në rregullore të përfshihet menaxhimin i ndryshimeve përfshirë dhe rastet e emergjencës.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. ka hartuar dhe miratuar rregulloret për sistemet:

- Sistemi i videomonitorimit,

- Sistemi i monitorimit Sizmik,
- Sistemi i monitorimit të sigurisë së digave.

Gjithashtu janë ndërmarë masa duke hartuar rregullore për *"Politikat për sigurinë e informacionit"* dhe*"Sistemi i monitorimit hidro-gjeologjik"* të cilat janë në formën e një drafti, të pa miratuar.

Ky rekomandim është në proces ***Menjëherë***

3. Gjetje nga auditimi: Departamenti i Automatizimit dhe Teknologjisë së Informacionit nuk ka procedura pune, apo dokumenta të tjera ligjore për të përcaktuar procedurat e punës. Dokumenti i vetëm zyrtar janë përshkrimet e punës dhe skema organizative e Departamentit të Automatizimit dhe Teknologjisë së Informacionit.

3.1 Rekomandim: KESHsh.a të marrë masa për hartimin dhe miratimin e bazës rregullative për funksionimin e DATI, ku të përcaktohet ndarja detyrave dhe përgjegjësive specifike të roleve, punëve dhe veprimeve operacionale brenda Departamentit të Automatizimit dhe Teknologjisë së Informacionit.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. ka hartuar *"Rregulloren e funksionimit të DATI"*, e cila është në formën e një drafti, të pa miratuar.

Ky rekomandim është në proces ***Menjëherë***

4. Gjetje nga auditim: Nga auditimi u konstatua se departamenti i Automatizimit dhe Teknologjisë së Informacionit nuk ka një analizë të nevojave për trajnim të stafit të departamentit dhe nuk ka një plan specifik për trajnime. Stafi i Departamentit të Automatizimit dhe Teknologjisë së Informacionit nuk ka kryer asnjë ditë trajnim për sistemet, sigurinë dhe teknologjinë e informacionit.

4.1Rekomandim: KESH sh.a. në bashkëpunim meDATI të marrin masa, për hartimin e politikave të trajnimit të Burimet Njerëzore, duke analizuar, identifikuar dhe planifikuar nevojat për trajnim të stafit të Departamentit të Automatizimit dhe Teknologjisë së Informacionit, si dhe të hartojë e miratojë plane dhe politika për zhvillimin e trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit për çdo funksion kryesor të lidhur me realizimin me sukses të objektivave të korporatës.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. ka ndërmarrë hapa për përcaktimin e nevojave për trajnime të stafit. KESH sh.a. ka përgatitur listën e trajnimeve së bashku me urdhrin nr. 117, datë 04.12.2019 , por është bllokuar per efekt të situatës së pandemisë.

Ky rekomandim është në proces ***Në vazhdimësi***

5. Gjetje nga auditimi: Nga auditimi mbi identifikimin dhe vlerësimin e risqeve në IT rezulton se, KESH sh.a nuk disponon regjister risku në asnjë drejtim që lidhet me Teknologjinë e Informacionit si dhe të dhënat që gjenerohen prej përdorimit të saj në kundërshtim me Nenin 11, pika 2 të 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". Nuk ka një proces identifikimi, ndjekje, raportimi dhe prioritarizimi të çështjeve me impakt negativ mbi përdorimin, sigurinë, adresimin dhe ndjekjen deri në zgjidhje.

Nga auditimi rezulton se nuk janë identifikuar dhe prioritarizuar risqe për:

- disponibilitetin dhe integritetin e sistemeve, të dhënave, si dhe palët e treta që janë kontraktuar

- humbjen e të dhënave
- dhënia e informacionit të paautorizuar dhe konfidencialiteti i informacionit
- humbjet apo perfitimet nga automatizimi i proceseve të punës nëpërmjet sistemeve IT

5.1 Rekomandimi: KESH sh.a të marrë masa për ndërtimin e rregjistrit të rriskut në Teknologjinë e informacionit duke identifikuar, vlerësuar, kategorizuar dhe ndjekur dhe raportimin e çështjeve me impakt negativ.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. ka hartuar *"Rregulloren e funksionimit të DATI"*, e cila është në formën e një drafti, të pa miratuar

Ky rekomandim është në proces ***Menjëherë***

6. Gjetje nga auditimi: KESH ka të gjeneruar *user admin* me të drejta Admin në sisteme.

6.1 Rekomandim:Të bllokohen në të gjitha paisjet e menaxhueshme userat "admin" dhe privilegjet e Administratorit të konfigurohen me userat e tjerë.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. ka zbatuar rekomandimin dhe angazhohet të vijojë zbatimin në vazhdimësi.

Ky rekomandim është në proces ***Në vazhdimësi***

7. Gjetje nga auditimi: *Firewall* ka të konfiguruar që të gjitha log-et input/output si dhe procesimin e vetë routerave ti shkruajë në një sistem *ArchsighLogger*, i cili ruan loget të gjitha loget për një periudhe 6 mujore. Nga verifikimet e kryera me stafin IT, sistemi ofron vetëm storage për loget dhe jo analiza risku ose mundësi konfigurimi të alerteve dhe bën të pamundur analizimin e risqeve në kohë reale.

7.1 Rekomandim: Të kryhen auditime ditore mbi loget e firewall input/output. Sektori IT duhet të bëjë kontrolle ditore si dhe të mbajë procesverbale në rastin e një logu i cili është rregjistruar si pasojë e sulmeve.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. ka zbatuar rekomandimin dhe angazhohet të vijojë zbatimin në vazhdimësi

Ky rekomandim është në proces ***Në vazhdimësi***

8. Gjetje nga auditimi: Tek routeri në Tiranë janë të konfiguruar përdorues VPN tetra dhe tetra1. Këto përdorues kanë akses VPN nga rrjeti public me akses të plotë në rrjetin e KESH,cfarë bën të mundur kompromentimin e informacionit si dhe të gjitha aplikimeve që KESH ka në përdorim.

8.1 Rekomandim: Të konfigurohen *policy për subnetet e VPN* vetëm për lejimin e shërbimit që kompania është kontraktuar dhe të bllokohen akseset për të gjitha shërbimet e tjera.

Masat e marra nga subjekti për zbatimin e rekomandimit

KESH sh.a. ka zbatuar rekomandimin dhe angazhohet të vijojë zbatimin në vazhdimësi.

Ky rekomandim është në proces ***Në vazhdimësi***

9. Gjetje nga auditimi: KESH nuk ka të instaluar një sistem qendror i cili komunikon me sistemet e tjera të monitorimit në rastin e matjeve, problematikave.

9.1 Rekomandim: Të merren masa urgjente për instalimin e paisjes BMS e cila duhet të lidhet me sistemin elektrik, antizjarr dhe sistemin e kondicionimit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga KESH sh.a. është kërkuar të implementohet në projektin :

1. Ndërtimi i dhomës së serverave (BCC Site) në Vaun e Dejës dhe krijimi i kushteve teknike në HEC,Vau i Dejës, HEC Koman dhe HEC Fierzë.
Parashikuar në buxhet për vitin 2020, por shtyrë për vitin 2021 për shak të rishikimit të buxhetit në zërin:
1. Përmirësimi i dhomës së serverave në godinën qendrore të KESH sh.a.
Ky rekomandim është në proces ***Në vazhdimësi***

10. Gjetje nga auditimi: KESH sh.a. nuk përdor sistem të informatizuar për shitblerjen e Energjisë i vlerësuar si i nevojshëm edhe nga ana e tij për të siguruar përputhje me parimet e barazisë, konkurrencës, transparencës dhe parimet e ruajtjes së konfidencialitetit. Procesi i prokurimit nga KESH sh.a., është anulluar me arsyen e mungesës së fondeve.
10.1 Rekomandim: KESH sh.a. të marrë masa për ngritjen e nje sistemi të informatizuar të procedurave të blerjes dhe shitjes së energjisë elektrike, ky sistem të ndërveprojë me sistemet ekzistuese të prodhimit dhe parashikimit të burimeve hidrike.
Masat e marra nga subjekti për zbatimin e rekomandimit
KESH sh.a. ka kërkuar si modul ne implementimin e projektit *"Implementimi i aplikimeve dhe funksioneve ERP në KESH SH.A"*, e cila është në fazë prokurimi Korrik 2020.
Ky rekomandim është në proces ***Në vazhdimësi***

11. Gjetje nga auditimi: Nga auditimi mbi: dokumentacionin dërguar me shkresën nr.2431/4, datë 24.06.2019 vënë në dispozicion grupit të auditimit, draft strategjisë, draft planit e DRC "Konfigurimi i VMware Site Recovery Manager – KESH", përgatitur nga departamenti IT gjatë periudhës së auditimit si dhe intervistave me nivelin drejtues rezulton se KESH **nuk disponon** një plan vazhdimësie dhe plan rikuperimi për garantimin e vazhdimësisë së ofrimit të shërbimit duke lënë pa vlerësuar impaktin në element shumë të rëndësishëm si:

- Identifikimi dhe prioritarizimi i aplikacioneve, i të dhënave dhe i veprimtarive kritike
- Identifikimi i personave relevantë duke përfshirë dhe nivelin e lartë drejtues në proces
- Identifikimi i risqeve, dhe vlerësimi mbi ndikimin e biznesit, kontrollet parandaluese në drejtim të mjedisit dhe të sistemeve që gjenerojnë të dhëna, dokumentimi, testimi i planit të vazhdueshmërisë si dhe trajnimi i punonjësve mbi të cilët mbështetet implementimi i planit të vazhdimësisë.

Gjatë testimit u vu re se siti që KESH e quan DRC nuk shërben si e tillë, por thjesht si një qendër të dhënash që ndodhet jashtë godinës qendrore.
11.1 Rekomandim: KESH sh.a. të marrë masa për hartimin e një plani vazhdimësie ku të ketë të identifikuar rendësinë e sistemeve, të dhënave dhe proceset më prioritare, personat relevantë si dhe risqet e ndikimi i tyre në ushtrimin e veprimtarisë në rastin e një nevoje për që lidhet me vazhdimësinë. Gjithashtu, DATI të marrë masa për plotësimin e konfigurimeve të nevojshme të rrjetit në funksion të garantimit të vazhdimësisë, duke qenë se disponon softëare dhe pajisje për të garantuar shërbim pa ndërprerje.
Masat e marra nga subjekti për zbatimin e rekomandimit
KESH sh.a. ka hartuar dokumentin *"Procedura e Ruajtjes se të Dhënave të Institucionit dhe e Rikuperimit të tyre"*, e cila është në formën e një drafti, të pa miratuar.
Ky rekomandim është në proces ***Menjëherë***

12. Gjetje nga auditimi: Nga auditimi rezulton se edhe pse është kërkuar një automatizim mbi dërgimin e njoftimeve automatike, procesi vazhdon të jetë ende manual, për arsye se në tabelën

"*sentmails*" nuk u gjet asnje gjurmë për emailet e dërguara cfarë tregon se parametrizimi mbi njoftimet automatike është konceptuar të realizohet në "kodit", duke krijuar vështirësi që konfigurimet në kod të kryhen nga IT në kushte kur nuk ka një mirëmbajtje me OE.
Gjithashtu, rekrutimet nuk rezulton të jenë bërë pjesë e sistemit të burimeve njerëzore edhe pse kërkesat për këtë janë përfshirë në modulin "Menaxhimi i trajnimeve, rekrutimeve". Në sistem regjistrohen trajnimet, por nuk u konstatuan rekorde që kanë të bëjnë me rekrutime, të paktën asnjë aplikim për punë nuk rezulton i regjistruar në sistem edhe pse moduli i zhvilluar për rekrutimet ka qenë pjesë e kërkesave në specifikimeve teknike.
12.1 Rekomandim: Strukturat drejuese në KESH Sh.a në bashkëpunim me Drejtorinë DATI të marrin masa për të adresuar problematikat që lidhen me realizimin e njoftimeve automatike dhe rekrutimeve si kërkesa që duheshin plotësuar nga OE, kërkuar në specifikimet teknike për të cilat nuk u gjet asnjë gjurmë realizimi në sistem.

Ky rekomandim nuk është zbatuar ***Menjëherë***

13. Gjetje nga auditimi: Njohuritë mbi Teknologjinë e Informacionit të burimeve njerëzore në Auditin e Brendshëm janë të pamjaftueshme, për të realizuar misione të auditimit në sistemet e TI-së, në përputhje me nenet 14 dhe 8 të ligjit nr. 114/2015 "*Për Auditimin e Brendshëm në sektorin publik*".
13.1 Rekomandim: KESH sh.a. të marri masa për zhvillimin e burimeve njerëzore të Auditit të Brendshëm me njohuri të mjaftueshme mbi teknologjinë e informacionit me qëllim kryerjen e auditimit të teknologjisë së informacionit si dhe përdoruesit e sistemeve informatike në përputhje me përcaktimet ligjore.

Ky rekomandim nuk është zbatuar ***Menjëherë***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi dhe të pa zbatuara,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

14. Ministria e Financave dhe Ekonomisë (MFE)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit MFE me shkresën Nr. 357/12 prot, datë 16.09.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 20 ditor për hartimin e plan veprimit (Hartimin e Programit), konstatojmë se MFE, nuk e ka përmbushur detyrimin e afatit 20 ditor të kthimit të përgjigjes në KLSH
Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se MFE, nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.

Janë rekomanduar 19 masa organizative. Nga masat organizative janë pranuar plotësisht 17 masa, nga të pranuarat është zbatuar 1 masë, janë zbatuar pjesërisht 2 masa, dhe janë në proces zbatimi 7 masa organizative, 7 masa organizative nuk janë zbatuar. Është rekomanduar 1 masë propozim për ndryshime apo përmirësime në legjislacionin në fuqi, e cila nuk është marrë parasysh.

Për sa më sipër *rikërkoj* që MFE të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara, të zbatuara pjesërisht dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi u konstatua se Marrëveshjet në Nivel Shërbimi në MFE, 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 VKM nr. 710, datë 21.08.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdimësisë së punës dhe marrëveshjeve të nivelit të shërbimit*", i ndryshuar, pika 2, germa c, dhe 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 Udhëzimi, ndër të tjera duhet të përcaktohen 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.

1.1 Rekomandimi: MFE dhe AKSHI në vijimësi të marrin masa për përfshirjen e plotë të elementëve të Marrëveshjeve në Nivel Shërbimi sipas përcaktimeve ligjore dhe nënligjore në fuqi, me qëllim kontrollin e plotë të shërbimit të ofruar nga ana e operatorëve ekonomik.

Masat e marra nga subjekti për zbatimin e rekomandimit

Janë amenduar 2 kontrata, saktësisht mirëmbajtja e sistemit Alpha dhe kontrata e dhomës së monitorimit. Për sa i përket kontratave të tjera do të veprohet me ribërjen e kontratave.

Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga auditimi: Nga auditimit u konstatua se Drejtoria TIK aktualisht e ushtron aktivitetin e saj me 9 punonjës, edhe pse struktura e miratuar është e përbërë nga 13 punonjës. Duke u nisur nga rëndësia specifike e Drejtorisë TIK në MFE konstatohen mungesa në staf në disa pozicione të rëndësishme të sektorëve të drejtorisë TIK, duke rritur riskun e mos përmbushjes së detyrave.
Drejtoria TIK pranë MFE nuk kryen trajnime në fusha specifike dhe nuk ka vendosur standarde të cilat do të çonin në rritjen profesionale dhe kualifikimin e stafit të TI.

2.1 Rekomandimi: Strukturat drejtuese të AKSHI-t në bashkëpunim me MFE të marrin masa për mirë menaxhimin e burimeve njerëzore duke plotësuar vendet vakante dhe të hartojnë politika për zhvillimin e tyre nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit, me qëllim përmbushjen e nevojave në fushën TIK në MFE.

Masat e marra nga subjekti për zbatimin e rekomandimit

Drejtorisë TIK në MFE ka marrë masa për një plan trjanimesh, dhe gjithashtu ka shpallur vendet vaktante për plotësimin e strukturës së miratuar.
Ky rekomandim është në proces ***Në vijimësi***

3. Gjetje nga auditimi: Nga auditimi u konstatua se, MFE nuk ka regjistër të menaxhimit të incidenteve. Risqet menaxhohen mbi bazë ngjarjesh. Jepet suport, mbështetje teknike dhe logjike për operacionet IT 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 përsëritjes së incidenteve. Ekzistenca e një regjistri të menaxhimit të incidenteve bazohet në Objektivat e Kontrollit të Teknologjisë së Informacionit COBIT, Manualin e Auditmit IT si dhe praktikave më të mira.
3.1 Rekomandimi: Strukturat Drejtuese në MFE në bashkëpunim me Drejtorinë e sistemeve dhe Teknologjinë e Informacionit atashuar pranë MFE-s të marrin masa për:
-identifikimin e risqeve IT dhe hartimin e regjistrit të risqeve mbi infrastrukturën TIK;
-dokumentimin dhe monitorimin e incidenteve;
-menaxhimin e ndryshimeve dhe dokumentimin e tyre.
Masat e marra nga subjekti për zbatimin e rekomandimit
Strukturat Drejtuese në MFE në bashkëpunim me Drejtorinë e sistemeve dhe Teknologjinë e Informacionit atashuar pranë MFE kanë krijuar një regjistër risku draft.
Ky rekomandim është në proces ***Në vijimësi***

4. Gjetje nga auditimi: Nga auditimi u konstatua se, Drejtoria e TIK e atashuar pranë MFE nuk ka hartuar raporte monitorimi dhe shërbimi në kundërshtim me pikën 4 të marrëveshjes në nivel shërbimit ndërmjet dy institucioneve protokolluar me nr. 420 prot., (AKSHI) dhe nr. 653/1 prot., (MFE), datë 24.01.2018.
4.1 Rekomandimi: Drejtoria e TIK pranë MFE në vijimësi të kryejë analizimin, prioritarizimin dhe ofrimin e shërbimeve të përcaktuara në MNSH-në ndërmjet institucioneve (MFE dhe AKSHI), hartimin e raporteve javore dhe mujore të shërbimeve të ofruara, me qëllim dhënien e sigurisë së arsyeshme për kryerjen me rigorozitet të suportit.
Masat e marra nga subjekti për zbatimin e rekomandimit
Ky rekomandim do të verifikohet nga auditimiet e mëvonshme.
Ky rekomandim është në proces ***Në vijimësi***

5. Gjetje nga auditimi: Për periudhën e audituar, procedurat e prokurimit si dhe lidhja e kontratave për mallrat apo shërbimet në fushën e teknologjisë së informacionit, janë zhvilluar dhe nënshkruar nga AKSHI, ndërsa vetë investimi si dhe detyrimi financiare kalojnë për MFE. VKM Nr. 673, datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*", i ndryshuar, saktësisht në pika 18, citon: "*Institucionet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave duhet të dorëzojnë pranë AKSHI-t 1 (një) kopje të dokumentacionit të plotë të çdo sistemi dhe infrastrukture TIK ekzistuese dhe kodin e burimit. Sistemet dhe infrastruktura TIK ekzistuese kalojnë nën administrimin dhe inventarin e AKSHI-t, së bashku me të drejtat dhe detyrimet juridiko-civile përkatëse brenda datës 30 shtator 2018*".
Me Urdhër të përbashkët të Sekretarit të Përgjithshëm të MFE dhe Drejtorit të Përgjithshëm të AKSHI-t, me nr. 5762 prot, datë 21.03.2018 (MFE) dhe nr. 1311 prot, datë 16.03.2018 (AKSHI), janë ngritur grupet e punës për evidentimin e sistemeve IT dhe infrastrukturave hardware të MFE,

si dhe përcaktimin e listës së aktiveve të qëndrueshme të trupëzuara dhe të patrupëzuara objekt kalimi kapital.
Edhe pse ka kaluar rreth 1 vit e 4 muaj nga nxjerrja e urdhrit të përbashkët për kalimin e kapitalit, si dhe rreth 10 muaj nga afati i vendosur në VKM Nr. 673, ky proces ende nuk ka përfunduar. Aktualisht sistemet e IT dhe infrastruktura hardware e MFE, janë ende pjesë e inventarit të MFE, e për pasojë edhe detyrimet juridike dhe financiare mbi këto sisteme, në kundërshtim me pikën 18 të VKM nr. 673, datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit*", i ndryshuar.
5.1 Rekomandimi: Organet drejtuese të MFE dhe AKSHI-t të marrin masat e nevojshme për përfundimin e procesit të kalimit të aktiveve të sistemeve të informacionit nga MFE tek AKSHI, si dhe të përcaktojnë përgjegjësitë për vonesat e shkaktuara të zbatimit të kërkesave ligjore lidhur me këtë çështje.
Masat e marra nga subjekti për zbatimin e rekomandimit
Ende ka aktive të cilat nuk kanë kaluar nga MFE tek AKSHI.
Ky rekomandim është në proces ***Në vijimësi***

6. Gjetje nga auditimi: Nga auditimi mbi sigurinë e aksesit të network-ut u konstatua se:
-Nga konfigurimet nuk shikohen bllokime të *subneteve* të këtyre bankave drejt *subneteve* të MFE çka përbën risk për hyrje dhe skanime të rrjetit të MFE nga këto lidhje;
-Pajisja *firewall* ka të aktivizuar log çka bën të mundur për të verifikuar një sërë procesesh që routeri kryen si edhe ruajtjen e tyre. Routeri ka një memorie të vogël dhe këto log-e nuk mund të ruhen ose të analizohen live duke bërë të mundur detektimin në kohë reale të një sulmi ose të një hyrje të paautorizuara;
-Nuk ka të krijuar group users me nivele të ndara menaxhim/monitorim. Çdo veprim bëhet nga useri admin;
-Nuk janë marrë masa për të bërë *disable* userin admin dhe për të krijuar një user tjetër me të drejta admini. Kjo gjë do të parandalonte sulme nga scripte/viruse që mund të merren brenda serverave ose pc-ve në MFE. Shumica e viruseve që bëjnë DDoS, përdorin si username "admin";
-Në routerin me IP private .....dhe IP publike .....vërehet se ka usera të krijuar për shoqërinë INTECH+ dhe usera oracle të cilët mund të aksesojnë edhe nga jashtë rrjetin e brendshëm si edhe shërbimet e MFE. Këta usera mund të logohen nëpërmjet VPN edhe nga jashtë MFE.
-Për routerin me ID .....shikohet që faza IKE për *ipsec* ka një *pre shared key* me 3 karaktere "....." për të gjitha lidhjet VPN të MFE me zyrat e rretheve si dhe me site të tjera. Passwordi që është përdorur nuk përmbush parametrat e sigurisë dhe përbën rrezik për akses nga palë të treta dhe të pa autorizuara.
6.1 Rekomandim: Drejtoria TIK e AKSHI-t pranë MFE të marrë masa për:
-Krijimin e konfigurimeve përkatëse bllokuese për të gjitha lidhjet VPN nga Bankat e nivelit të dytë drejt rrjetit privat të MFE;
-Krijimin e grupeve dhe usera-ve admin/monitorim;
-Useri admin të bëhet *disable* dhe të krijohet një user me emërtim ndryshe me të drejta administratori për të gjitha routerat/switchet e menaxhueshëm;
-Konfigurimin e një *script-i* në firewall i cili bllokon për 24 orë IP-në nëse nga kjo IP provohet me shumë se 3 here logimi të gabuar;
-Marrjen e masave për krijimin e një platforme të centralizuar për gjenerimin e alerteve sipas riskut për mbajtjen e log-eve për të gjitha pajisjet. Pasja e një platforme të centralizuar, parandalon në

kohë reale sulme, dëmtime të pajisjeve si dhe ndihmon në ecurinë e shërbimeve TIK që MFE disponon.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ky rekomandim do të verifikohet nga auditimiet e mëvonshme.

Ky rekomandim është në proces ***Në vijimësi***

7. Gjetje nga auditimi: Nga auditimi u konstatua se në sistemin e thesarit ndodhin në mënyrë të përsëritur bug-e (error-e) të natyrave të ndryshme, si në vijim:

- Bankës së Shqipërisë, pas rakordimit me bankat e nivelit të dytë, e dërgon atë ditën e nesërme në sistemin e thesarit me anë *Swift Server* (*me data encryption*). Gjatë shpërndarjes së postës, ndodh që posta e një dege të caktuar i kalon një dege tjetër që nuk i përket asaj. Pasi sinjalizohet nga punonjësit e degës së thesarit, kryhet riparimi i kësaj anomalie (bug-u) me anë të një skripti i cili e dërgon postën në degën përkatëse në mënyrë që të kryhet rakordimi i degës së thesarit. Ky bug është akoma prezent në sistemin e thesarit duke krijuar një anomali të tilla.
- U konstatua 1 rast ku sistemi i thesarit nuk i ka dhënë vlerë fushës së numrit rendor të veprimit të kryer, "*DOC SEQUENCE VALUE*", fushë e cila duhet të plotësohet automatikisht nga sistemi (*vlerë default*).

Bug-e të tilla me natyrë të ngjashme janë krijuar edhe në periudha të mëparshme, edhe pse janë raste të izoluara.

- Bugs të natyrave të ndryshme ndodhin në procese të tjera të sistemit të thesarit gjatë plotësimit të transaksioneve PO nga një përdorues të cilit i ndërpritet procesi i punës duke i nxjerrë error.

7.1 Rekomandimi: Nga MFE dhe AKSHI të analizohen të gjitha rastet e bug-eve të ndryshme të sistemit, si dhe të merren masat e nevojshme për trajtimin dhe eliminimin e tyre në të ardhmen.

Masat e marra nga subjekti për zbatimin e rekomandimit

Në lidhje me sa më sipër është hapur proces në Oracle dhe janë rregulluar. Verifikimi i detajuar i këtyre bug-eve dhe të tjera do të verifikohet në auditimin e ardhshëm.

Ky rekomandim është në proces ***Menjëherë***

8. Gjetje nga auditimi: Nga verifikimi analitik i 374 userave aktiv të sistemit të SIFQ, u konstatua:

a) usera të cilët edhe pse e kanë përfunduar objektin për të cilin janë çelur, janë ende aktiv. Ky fakt mbart një risk të lartë për ndërhyrje të paautorizuara në sistem duke mos lënë gjurmë mbi aktivitetin që kanë kryer. Saktësisht: Oracle, Oracle3, Oracle5, Oracle7, Oracle9. Gjithashtu user-at nuk kanë një "End Date", pra edhe pas shkëputjes së marrëdhënieve të punës, punonjësve nuk u është mbyllur ende account-i.

b) useri FADMIN përdoret nga disa punonjës të cilat gjithashtu kanë userin e tyre, duke mos lënë gjurmë se cili punonjës ka kryer një veprim të caktuar me këtë user. Ky user ka 127 lloje të drejtash (atribute) në sistem, duke bërë që risku i përdorimit të tij nga shumë punonjës të jetë i lartë.

c) Nuk ka një rregullore/ manual ku të përcaktohen atributet që secili user duhet të gëzojë në varësi të pozicionit të punës që ka.

8.1 Rekomandimi: MFE në bashkëpunim me AKSHI-n të analizojë problematikat e konstatuar nga grupi i auditimit në lidhje me user-at e sistemit të SIFQ, duke marrë masat e nevojshme për çaktivizimin e user-ave të cilëve u ka përfunduar objekti i krijimit të tyre, fshirjen e useri-it FADMIN, i cili nuk i përket asnjë punonjësi në veçanti.

MFE në bashkëpunim me AKSHI-n të marrin masat e nevojshme për hartimin e një rregulloreje ku të përcaktohet qartë lidhja ndërmjet atributeteve të user-t me pozicionin e punës.

Masat e marra nga subjekti për zbatimin e rekomandimit
Janë bërë disable userat: Oracle, Oracle3, Oracle5, Oracle7, Oracle9. Nuk është bërë disable useri FADMIN. Nuk ka ende një rregullore/ manual ku të përcaktohen atributet që secili user duhet të gëzojë në varësi të pozicionit të punës që ka.
Ky rekomandim është zbatuar pjesërisht ***Në vijimësi***

9. Gjetje nga auditimi: Nga auditimi u konstatua se:
- Nga Sekretari i Përgjithshëm i MFE janë nxjerrë urdhra për ngritjen e grupeve të punës, ku pjesë përbërëse e grupit janë punonjës të AKSHI-t. Një veprim i tillë nuk citohet në asnjë pikë të marrëveshjes në nivel shërbimi ndërmjet dy institucioneve protokolluar me nr. 420 (AKSHI) dhe nr. 653/1 (MFE), ku t'i jepet e drejtë titullarit të një institucioni të ngrejë urdhra me punonjës/specialist të një institucioni tjetër. Gjithashtu këto institucione nuk janë në varësi të njëra tjetrës, për pasojë grupi i auditimit i vlerëson këto urdhra të pabazuara juridikisht.
- Në disa nga urdhrat e marrjes në dorëzim të aktiveve apo shërbimeve në fushën e teknologjisë së informacionit, pjesë e grupit të marrjes në dorëzim janë punonjës jo specialistë të fushës, veprim në kundërshtim me pikën 43 të Udhëzimit Nr. 30 Datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik", i ndryshuar, ku citohet "*Komisioni përbëhet nga specialistë të fushës sipas llojit të aktiveve dhe, në rast nevoje, edhe nga ekspertë të jashtëm. Në komision bëjnë pjesë jo më pak se tre veta, duke përfshirë edhe punonjësin me përgjegjësi materiale*".

9.1 Rekomandimi: Organet drejtuese të MFE dhe AKSHI-t në të ardhmen të marrin masat e nevojshme për ngritjen e grupeve të punës me punonjës brenda institucioneve përkatëse, përcaktimin e përgjegjësive individuale si dhe në përputhje me kërkesat e Udhëzimit nr. 30, për vendosjen e specialistëve të fushës sipas llojit të aktiveve.
Masat e marra nga subjekti për zbatimin e rekomandimit
MFE para se të përfshijë punonjësit e AKSHI-t në grupet e punës, merr paraprakisht miratimin e AKSHI-t. Për sa i përket vendosjes së specialistëve të fushës sipas llojit të aktiveve, do t verifikohet në auditimin e ardhshëm.
Ky rekomandim është zbatuar pjesërisht ***Në vijimësi***

10. Gjetje nga auditimi: Nga auditimi i "*Process Order*" për vitin 2018, u konstatuan 33903 raste ku fusha "*Bill Amount*" është e barabartë me fushën "Shuma" (pra kontrata është mbyllur), por nuk ka marrë statusin "*Closed*", me qëllim mbylljen e procesit.
Gjithashtu u konstatuan 2 raste ku fusha "*Bill Amount*" është më e madhe se fusha "*Shuma*". Ky veprim do të thotë se furnitori është paguar më shumë se vlera e kontratës. Për pasojë, rezulton se sistemi i thesarit në këto raste nuk ka mekanizmat e duhur parandalues për mos lejim të tejkalimit të vlerës së kontratës.
10.1 Rekomandimi: MFE dhe AKSHI të analizojnë rastet e konstatuara të tejkalimit të vlerave të kontratave dhe më gjerë. Administruesit e sistemit të marrin masat e nevojshme për parandalimin automatik nga vetë sistemi të kësaj problematike.

Ky rekomandim nuk është zbatuar ***Menjëherë***

11. Gjetje nga auditimi: Nga auditimi i Marrëveshjeve të Nivelit të Shërbimit në Ministrinë e Financave dhe Ekonomisë, si dhe duke patur në konsideratë ndryshimet e fundit të akteve ligjore dhe nënligjore, mënyrën e organizimit të funksionimit të strukturave dhe sistemeve të teknologjisë

së informacionit në MFE, u konstatua se sipas VKM Nr. 673, datë 22.11.2017 "*Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit*", i ndryshuar, procesin e ofrimit të shërbimit duhet ta mbulojë vetë AKSHI, pasi ka aftësitë e nevojshme profesionale për ofrimin e këtyre shërbimeve.
Në marrëveshjen e nivelit të shërbimit datë 24.01.2018, ndërmjet Agjencisë Kombëtare të Shoqërisë së Informacionit dhe Ministrisë së Financave dhe Ekonomisë, protokolluar me nr. 420 (AKSHI) dhe nr. 653/1 (MFE), përcaktohen elementët që do të mbulohen nga AKSHI.
Gjithashtu mbështetur edhe në përshkrimet e punës të stafit të drejtorisë TIK të AKSHI-t atashuar pranë MFE, përkatësisht "*Sektori i Zhvillimit dhe Mirëmbajtjes dhe Sigurisë së Infrastrukturës*" ka detyra kryesore të përcaktuara për mirëmbajtjen dhe suportin në kategori të ndryshme.
Nga sa më sipër konstatohet se zërat e përfshira në këto marrëveshje në nivel shërbimi, gjenden të pasqyruara në kompetencat e përcaktuara nga VKM nr. 673 datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*", i ndryshuar dhe në marrëveshjen e nivelit të shërbimit datë 24.01.2018, ndërmjet Agjencisë Kombëtare të Shoqërisë së Informacionit dhe Ministrisë së Financave dhe Ekonomisë.
11.1 Rekomandimi: MFE dhe AKSHI të analizojnë nevojën e adresimit të shërbimeve të cilat janë pjesë e MNSH-ve aktuale dhe de-jure i janë ngarkuar në mënyrë të drejtpërdrejtë AKSHI-t. Në përputhje me aktet ligjore dhe nënligjore në fuqi, të identifikohen problematikat dhe të merren masat për zgjidhjen e tyre.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

12. Gjetje nga auditimi: Teknologjia e informacionit zhvillohet pa Plan Strategjik, duke sjellë mos pasqyrim të qartë të objektivave të MFE lidhur me sigurinë institucionale dhe infrastrukturën TI, objektivat strategjikë për burimet njerëzore të strukturës së TI pranë MFE, në kundërshtim me strategjinë kombëtare të zhvillimit të dixhitalizimit.
12.1 Rekomandimi: Strukturat drejtuese në MFE dhe AKSHI, duke marrë në konsideratë kohën, burimet e nevojshme si dhe rëndësinë e të dhënave që institucioni zotëron dhe përpunon, të marrin masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit duke patur parasysh ndryshimet e ndodhura me aktet ligjore dhe nënligjore.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

13. Gjetje nga auditimi: Nga auditimi u konstatua se nga DPTH nuk është mbajtur një regjistër gabimesh (*hedhje gabim, korrigjime nëpër TDO apo edhe në MFE*) funksionale që bëhen nga userat e SIFQ, me qëllim trajtimin dhe hartimin e masave parandaluese e tyre në të ardhmen.Ekzistenca e një regjistri gabimesh bazohet në Objektivat e Kontrollit të Teknologjisë së Informacionit COBIT, Manualin e Auditmit IT si dhe praktikave më të mira.

13.1 Rekomandimi: DPTH të marrë masa për krijimin e një regjistri gabimesh me qëllim trajtimin dhe hartimin e masave parandaluese në të ardhmen.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

14. Gjetje nga auditimi: Nga DPT merren të dhëna vetëm për të ardhurat. DPT dërgon ne MFE

informacionin elektronik nëpërmjet file.txt i cili i korrespondon kontabilizimit të transaksioneve mbi të ardhurat tatimore të file-it txt dërguar paraprakisht nga MFE ne DPT mbi arkëtimin e këtyre të ardhurave. Çdo file ka një emër unik dhe një file nuk mund të ngarkohet më shumë se një here në SIFQ, në të kundërt SIFQ refuzon automatikisht ngarkimin e të njëjtit file më shumë se një herë. Në rastin e korrigjimeve kontabile që DPT dërgon në MFE lidhur me kontabilizime të të ardhurave dërguar me file-t e mëparshme, DPT dërgon një file të ri i cili përmban korrigjimet kontabile, ku çdo transaksion korrigjimi kontabil përmban numrin e referencës së pagës në SIFQ të cilës i referohet ky korrigjim. DPT file txt e upload-on në serverin FTP të mundësuar nga MFE. në momentin që në serverin FTP dërgohet një file txt, nga drejtoria IT në MFE dërgohet me email tek Drejtoria e Operacioneve të Thesarit vetëm emri i filet.txt dërguar nga DPT dhe punonjësi ne Drejtorinë Operacionale kryen ekzekutimin e programit të ngarkimit të këtij file në SIFQ. Pra shkëmbimi i drejtpërdrejtë i të dhënave ndërmjet sistemit të DPT dhe sistemit të thesarit (SIFQ) nuk kryhet në mënyrë automatike.

14.1 Rekomandimi: MFE, AKSHI në bashkëpunimin me DPT të marrin masat për krijimin e mekanizmave të nevojshëm për automatizimin dhe ndërveprimin e hedhjes së të dhënave ndërmjet sistemeve DPT dhe SFIQ.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

15. Gjetje nga auditimi: Në sistemin SIFQ janë të implementuara metodat e sigurimit të kontrollit të inputit me qëllim sigurimin e një produkti cilësor final, por nuk ka raporte mbi saktësinë e outputit. Nga auditimi u konstatua se mungojnë kontrollet periodike të outputit. Kontrollet kryhen vetëm në rastet kur ka sinjalizime për ndonjë parregullsi. Në rastin e fushës *PERIOD_NAME* nuk ka funksion të kontrollit të inputit. Grupi i auditimit testoi inputin në këtë fushë duke vendosur vitin 2022, e cila nuk përbën vlerë logjike për këtë fushë. Kjo vlerë u pranua nga sistemi.
15.1 Rekomandimi: MFE dhe AKSHI të analizojë rastin e konstatuar nga grupi i auditimit duke e shtrirë verifikimin edhe në fushat e tjera, duke dhënë zgjidhje të cilat të shërbejnë jo vetëm për rregullimet momentale të problematikës, por gjithashtu për krijimin e një kontrolli paraprak të këtyre inputeve edhe në vazhdimësi.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

16. Gjetje nga auditimi: Nga auditimi me zgjedhje të rastësishme të ambienteve të serverave të 4 degëve të thesarit, saktësisht Vlora, Fieri, Lezha dhe Shkodra, u konstatuan problematika të tilla si:
-mungesë e UPS për rastet e luhatjes apo ndërprerjes së energjisë elektrike;
-gjeneratorë jashtë funksionit;
-pajisjet IT (pc, printera all in one, etj) ishin të amortizuara
-kondicioneri për dhomën e serverave ishte jashtë funksionit duke rritur riskun e mbinxehjes së pajisjeve dhe serverit;

16.1 Rekomandimi: MFE dhe AKSHI të marrin masa për pajisjen dhe standardizimin e infrastrukturës IT të degëve të thesarit, me qëllim sigurimin e kushteve optimale për ofrimin e shërbimit dhe mbarëvajtjen e punës pa ndërprerje.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *të zbatuara pjesërisht, në proces zbatimi dhe të pa zbatuara,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

15. Ujësjellës Kanalizime Berat Kuçovë (UKBK)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit UKBK me shkresën Nr. 1436/6 prot, datë 26.07.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Nga auditimi i zbatimit të afatit 6 mujor për raportimin e ecurisë së zbatimit të rekomandimeve, konstatojmë se UKBK, *nuk e ka përmbushur detyrimin e afatit 6-mujor të raportimit.*

Janë rekomanduar 23 masa organizative. Nga masat organizative janë pranuar plotësisht 23 masa, nga të pranuarat janë zbatuar 8 masa, është zbatuar pjesërisht 1 masë, dhe janë në proces zbatimi 8 masa organizative, 5 masa organizative nuk janë zbatuar. Për eliminimin e efekteve negative të konstatuara në administrimin e fondeve publike dhe për menaxhimin me ekonomicitet, eficence dhe efektivitet të fondeve publike është rekomanduar **1 masë,** e cila është pranuar dhe zbatuar.

Për sa më sipër *rikërkoj* që UKBK të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara, të zbatuara pjesërisht dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi. Nga auditimi se si UKBK SHA identifikon dhe menaxhon risqet në teknologjinë e informacionit, u konstatua se UKBK SHA nuk disponon një regjistër risku për minimizimin e risqeve që lidhen me 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 auditimi konstatohet se nuk janë identifikuar risqe që i përkasin teknologjisë së informacionit në lidhje me: sigurinë, disponibilitetin dhe integritetin e sistemeve dhe të dhënave që gjenerohen nëpërmjet tyre si dhe palëve të treta që janë kontraktuar për ofrimin e shërbimit të mirëmbajtjes. Sa i përket riskut të rritur të adresimit të shqetësimeve të qytetarëve me impakt ofrimin e shërbimit, grupi i auditimit konstatoi se mungesa e dhënies së zgjidhjeve dhe regjistrimit të përgjigjeve në sistemin Al Billing nuk i shërben informimit të qytetarëve të cilët përgjigjen e marrin fizikisht në pikat e UKBK SHA.
1.1 Rekomandimi: Strukturat drejtuese të UKBK SHA 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.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi. Aktualisht ka nisur puna për harimin e regjistrit të riskut, por nuk ka përfunduar ende.

Ky rekomandim është në proces ***Menjëherë***

2. Gjetje nga auditimi. Kriteret e veçanta të procedurës së prokurimit "Zhvillime shtesë, licensa si dhe shërbimi i mirëmbajtjes" në opinion të grupit të auditimit janë hartuar në mënyrë të tillë që kanë ndikuar negativisht në pjesëmarrjen e gjerë të operatorëve ekonomik. Gjithashtu specifikimet teknike në rastin e dimensioneve të pajisjeve PDA konsiderohen të tepruara pasi janë dhënë fikse dhe jo me tolerancë, duke ndikuar negativisht në varietetin e pajisjeve të ofruara nga operatorët ekonomik. Këto veprime janë në kundërshtim me nenin 23, të Ligjit Nr. 9643, datë 20.11.2006, i ndryshuar.

2.1 Rekomandimi: Ujësjellës Kanalizime Berat Kuçovë të marrë masa për vendosjen e kritereve të cilat janë të domosdoshme për realizimin e kontratave, duke eleminuar kërkesa të cilat mund të ndikojnë negativisht në pjesëmarrjen masive të operatorëve ekonomik, si një nga parimet kryesore të përdorimit të procedurave të prokurimit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi. Verifikimi i detajuar do të bëhet në auditimet e ardhshme.

Ky rekomandim është në proces ***Në vijimësi***

3. Gjetje nga auditimi. Në pikën 5 të kontratës me Nr. 883 Prot, datë 25.07.2018 ndërmjet UKBK sha dhe "Jehona Software", konstatohet se mungojnë disa nga elementet e marrëveshjeve në nivel shërbimi të cituara në Udhëzimin të Ministrisë së Shtetit për Inovacion dhe Administratën Publike Nr. 1159, datë 17.03.2014 "Për hartimin e marrëveshjes së nivelit të shërbimit", i ndryshuar. Saktësisht mungojnë elementët:

-disponueshmëria e shërbimeve, koha mesatare e ndërprerjeve të shërbimeve (1/b)
-koha mesatare e rekuperimit (1/c)
-nivelet e suportit, përgjegjësitë dhe kufizimet (1/ç)
-qëllimi dhe objektivat (aneksi 1 pika 2)
-matja e cilësisë së shërbimit (aneksi 1 pika 8/ç)
-kërkesat e shërbimit (aneksi 1 pika 8/d)
-raporti i shërbimit dhe vlerësimet periodike (aneksi 1 pika 8/dh)
-menaxhimi i vazhdueshmërisë së shërbimit (aneksi 1 pika 8/e)

Këto mangësi, në opinion të grupit të auditimit kanë si pasojë monitorimin e cunguar të marrëveshjes së nivelit të shërbimit.

3.1 Rekomandimi: Ujësjellës Kanalizime Berat Kuçovë në vijimësi të marrë masat përplotësimin me të gjithë elementët e nevojshëm në marrëveshjet në nivel shërbimi, për një monitorim sa më të saktë dhe më produktiv të ofrimit të shërbimeve.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi. Verifikimi i detajuar do të bëhet në auditimet e ardhshme.

Ky rekomandim është në proces ***Në vijimësi***

4. Gjetje nga auditimi. Nga auditimi i kryer rezultoi se:

- Kopjet e Backup-eve ruhen automatikisht në të njëjtën makinë (server) ku ndodhet dhe kopja primare, por në një particion të veçantë, si dhe manualisht nga ana e strukturës IT në një makinë (desktop) me vendndodhje në zyrat e UKBK SHA, ç'ka përmban risk të lartë për humbjen e të dhënave në rastet e incidenteve të mundshëm.
- Ujësjellës Kanalizime Berat Kuçovë disponon aktualisht 2 servera me anë të të cilëve kryen menaxhimin e sistemeve që janë në përdorim. Ambienti fizik ku janë vendosur këta servera është jashtë çdo standarti dhe në mospërputhje me standardet e përcaktuara në Rregulloren për Ndërtimin e Dhomës së Serverëve miratuar nga AKSHI, si dhe nga data 13.07.2018 në kundërshtim me Nenin 13 dhe 14 të Rregullores për 'Mbrojtjen, Perpunimin, Ruajtjen dhe Sigurinë e të Dhënave Personale'
- UKBK merr shërbimin e ofruar të internetit, dhe nuk kryen asnjë filtrim të komunikimit c'ka sjell që rrjeti netëork i UKBK, me anë të të cilit ndërveprojnë sistemet në përdorim, është i ekspozuar dhe vulnerabël ndaj risqeve kibernetike, pasi lidhja me internetin kryhet pa asnjë lloj filtrimi ç'ka mbart risk të lartë për funksionimin sistemeve TI të UKBK SHA.

4.1 Rekomandimi:

- Struktura e Teknologjisë së Informacionit në UKBK SHA të marrë masa për ruajtjen e kopjeve të backup në një ambient të dytë të ndryshëm nga serveri primar ku ruhen të dhënat e sistemeve që UKBK SHA ka në përdorim.
- Strukturat drejtuese të UKBK SHA në bashkëpunim me strukturën e Teknologjisë së Informacionit të marrin masa për analizimin e situatës së ambientit fizik ku janë të vendosur serverat e institucionit, dhe të marrin hapat e nevojshëm për vendosjen e tyre në një ambient që të përmbushi parametrat dhe kushtet teknike për ruajtjen dhe mirëfunksionimin e sistemeve të teknologjisë së informacionit.
- Strukturat drejtuese të UKBK SHA në bashkëpunim me strukturën e Teknologjisë së Informacionit të marrin masa për t'u pajisur me mjete teknologjike për të kryer filtrimin e shkëmbimit të informacionit në internet me qëllim mbrojtjen e të dhënave nga risqet e mundshëm që paraqet ky shkëmbim informacioni.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi.

Realizimi i këtij rekomandimi kërkon kohë dhe financim, për këtë arsye zbatimi i plotë do të verifikohet në auditimin e ardhshëm.

Ky rekomandim është në proces ***Në vijimësi***

5. Gjetje nga auditimi. Nga auditimi mbi plotësinë dhe saktësinë e të dhënave u konstatua gjithashtu se:

- Në afërsisht 495 raste janë faturuar abonentë me më pak se 12 fatura gjatë vitit 2018, të cilat kërkojnë verifikim nga ana e UKBK rast pas rasti.
- Shumë abonentë, për një kohë të gjatë faturohen me një konsum gati të papërfillshëm nga 0-4 m3 ujë në muaj. Totali i përllogaritur nga të dhënat e vëna në dispozicion shkon afërsisht në 70,000 faturime në gjithë vitin 2018.

- Afërsisht 426 kontrata në tipin Aforfe, për kategorinë Biznes nga 2,375 kontrata që shoqëria disponon për këtë kategori, pra afërsisht 15%.
- Nga të dhënat u konstatuan dhe afërsisht 59 raste të kontratave të cilat kanë një NIPT, edhe në kategorizimin e tipit "*familjar*".
- Nga krahasimi i të dhënave në dispozicion të ujësjellësit me listën e fundit që dispononin tatimet vendore të bashkisë Berat-Kucovë, rezultuan se për afërsisht 700 biznese UKBK nuk disponon kontratë abonenti. SHA UKBK, nuk u konstatua se ka ngritur ndonjë praktikë kontrolli apo verifikimi me drejtorinë e tatim taksave vendore të Berat-Kucovës, për bizneset e reja që krijohen në këtë qark.

5.1 Rekomandimi: Ujësjellës Kanalizime Berat Kucovë të marrë masat e nevojshme organizative për verifikimin në terren rast pas rasti të problematikave të konstatuara nga auditimi dhe të marrë masa administrative në rastet e identifikuara si kundravajtje të furnizimit me ujë/kanalizime, për zonën Berat Kuçovë.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi. Janë verifikuar rastet, dhe po verifikohen në vazhdimësi.

Ky rekomandim është në proces ***Menjëherë***

6. Gjetje nga auditimi. Nga auditimi mbi numrin e leximit të kontratave me matje që kanë si detyrimi 10 faturues të cilët janë pajisur me lexues PDA si rezultat i projektit të zhvillimit të sistemit AL Billing, krahasuar me leximet që kanë kryer për 3 muaj e fundit të vitit 2018, u konstatua se ka një diferencë në lexime ku afërsisht 30 % e leximeve lexohen manualisht dhe jo me PDA.

6.1 Rekomandimi: Ujësjellës Kanalizime Berat Kucovë të marrë masa organizative për maksiminizimin deri në masën 100% të leximit me anë të pajisjeve PDA, duke rritur në këtë mënyrë efektivitetin e investimit si dhe garantimin e shërbimit të leximit për të gjithë abonentët leximet e të cilëve kryhen me këto pajisje.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi. UKBK Sh.A është në përpjekje të vazhdueshme për maksimizimin e leximit me anë të pajisjeve PDA.

Ky rekomandim është në proces ***Menjëherë***

7. Gjetje nga auditimi. Nga të dhënat e eksportuara nga sistemi u konstatua se:
- Fusha të cilat plotësohen manualisht, por që janë numra identifikimi unik si prsh numër kontrate apo NIPT janë të shkruara në disa raste edhe me hapësira ndërmjet karaktereve alfanumerike çfarë tregon se nuk ekziston parametrizimi i tyre me anë të së cilës të standartizohen dhe ndërtohen kontrolle automatike për plotësimin e tyre sipas një maske. Në disa raste u konstatua se Nipti është e dhënë e vendosur tek adresa e abonentit dhe jo tek NUIS.
- Kontrolli mbi regjistrimin e fushave me përmbajtje unike gjatë inputit mungon në systemin e Billing-ut. Në mungesë të këtij kontrolli në input, numrat unik mund të regjistrohen me gjatësi karakteresh me shumë se sa vetë numri, por njëkohësisht edhe me me pak se sa vetë numri.
- Institucioni nuk u konstatua të ishte në dijeni për ndonjë kontroll automatik nëpërmjet sistemit për serinë tatimore, por dhe manualisht ky kontroll është realizuar nga OE.

Nga auditimi i të dhënave të detajuara dhe të detyrueshme në sistemin e faturimit u konstatuan disa raste kur:

- Adresa e abonentit në afërsisht 5,626 kontrata nuk është plotësuar si e dhënë. UKBK nuk ka iniciuar asnjë process lidhur me popullimin e kësaj fushe.
- Adresa e abonentit nuk rezultoi të jetë konfiguruar si e dhënë e detyrueshme, apo e pandryshueshme në rastet kur kontrata amendohet në elementët që ndryshimet lejohen si prsh: emri i abonentit, faturisti, matësi, tipi i abonentit etj.

Nga verifikimi mbi regjistrimin, ndryshimin e abonentit në sistem u konstatua se nuk ka fusha të tjera të konfiguruara si të detyrueshme si:

- Numri i matësit kur abonenti është i kategorizuar me matje
- Nipti si e dhënë e detyrueshme në rastin kur abonenti është Biznes

7.1 Rekomandimi: Ujësjellës Kanalizime Berat Kucovë të marrë masat e nevojshme për saktësimin dhe plotësimin e të dhënave, identifikimin e të dhënave të detyrueshme si dhe analizimin e mundësisë për parametrizimin e fushave si të tilla, për të garantuar plotësinë dhe saktësinë e tyre.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi.

Ky është një proces i cili ka nisur dhe është i vazhdueshëm.

Ky rekomandim është në proces ***Menjëherë***

8. Gjetje nga auditimi. Nga auditimi i zbatimit të 2 kontratave në fushën e Teknologjisë së informacionit, saktësisht "Zhvillime shtesë, licensa si dhe shërbimi i mirëmbajtjes" dhe implementimi i sistemeve "Alpha Waterbill" dhe "Alpha Biznes", u konstatua se mungon dokumentacioni i nevojshëm për vërtetimin e kryerjes së plotë të kontratave. Mungesa e dokumentacionit justifikues mbi kryerjee e trajnimeve të stafit dhe raportet e kryerjes së shërbimit të mirëmbajtjes, kanë krijuar mangësi në mbajtjen e dokumentacionit të plotë vërtetues për realizimin e detyrimeve kontraktualenë kundërshtim mepikën 36 të udhëzimit nr.30, datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik" dhe në kundërshtim me aneksin 1 të udhëzimit nr.1159, datë 17.03.2014, "Për hartimin e marrëveshjen në nivel shërbimi" i ndryshuar.

8.1 Rekomandim: Ujësjellës Kanalizime Berat Kuçovë të administrojë me përgjegjësi dokumentacionin vërtetues të zbatimit të kontratave të teknologjisë së informacionit me qëllim garantimin e gjurmës audituese për realizimin e plotë dhe në kohë të tyre.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi.

Verifikimi i detajuar do të bëhet në auditimet e ardhshme.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

9. Gjetje nga auditimi. Nga auditimi i kryer rezultoi se:

- UKBK SHA nuk ka hartuar plane për garantimin e ofrimit të shërbimit dhe vazhdimësisë së proceseve të lidhura me shwrbimet.
- Struktura IT e UKBK SHA nuk disponon dokumentacione në lidhje me: procedurat e testimit, listë të testeve të kryera për vitin 2018, procedura të pasqyruara qartë të backup-it.

- UKBK SHA nuk ka procedura të dokumentuara dhe të miratuara për procesin e hapjes dhe mbylljes së përdoruesve të sistemeve.
- Sistemet e Teknologjisë së Infromacionit në UKBK SHA funksionojnë pa rregullore të miratuar ku të jenë të përcaktuara nivelet e aksesit dhe të drejtat e përdoruesve.

9.1 Rekomandimi: Strukturat drejtuese të UKBK SHA në bashkëpunim me strukturën e Teknologjisë së Informacionit të marrin masa për ndërtimin dhe hartimin e një strategjie për garantimin e ofrimit të shërbimit si dhe të një plani të përcaktuar në lidhje me vazhdueshmërinë e proceseve ku të përfshihet ndarja e detyrave/përgjegjësive në lidhjë me këtë çështje.

- Gjithashtu, nga ana e strukturave drejtuese të UKBK SHA të merren masa për hartimin, miratimin e një rregulloreje per funksionimin e sistemeve të teknologjisë së informacionit, ku të përcaktohen qartë detyrat, përgjegjësitë, nivelet e aksesit si edhe procedurat per procesin e hapjes dhe mbylljes së përdoruesve të sistemeve.

Masat e marra nga subjekti për zbatimin e rekomandimit

Me urdhrin e Titullarit nr. 292 me nr. 1628 prot, datë 07.08.2019, është ngritur grupi i punës për zbatimin e këtij rekomandimi. Është hartuar rregullorja, por nuk janë marrë masat për ndërtimin dhe hartimin e një strategjie për garantimin e ofrimit të shërbimit si dhe të një plani të përcaktuar në lidhje me vazhdueshmërinë e proceseve ku të përfshihet ndarja e detyrave/përgjegjësive në lidhjë me këtë çështje

Ky rekomandim është zbatuar pjesërisht ***Në vijimësi***

10. Gjetje nga auditimi. Nga auditimi i procedurave të prokurimit, u konstatuan mangësitë e mëposhtme:

- Një pjesë e dokumentcaionit është pa numër protokolli, veprim i cili nuk jep siguri të arsyeshme mbi gjurmën e auditimit
- Për përcaktimin e fondit limit jo në të gjitha rastet ofertat janë të vërtetuara me dokumentacionin përkatës veprim në kundërshtim me udhëzimin Nr. 30 datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik", i ndryshuar
- Kriteret e veçanta të kualifikimit nuk janë të argumentuara, veprim në kundërshtim me nenin 61 pika 2 të VKM Nr. 914, datë 29.12.2014 "Për miratimin e regullave të prokurimit publik", i ndryshuar, përcaktohet: "*Në çdo rast, hartimi i kritereve për kualifikim dhe specifikimet teknike duhet të argumentohen dhe të dokumentohen në një procesverbal të mbajtur nga personat e ngarkuar për përgatitjen e tyre*".
- Në provedurën e prokurimit prokurimit "Zhvillime shtesë, licensa si dhe shërbimi i mirëmbajtjes" janë ftuar për të marrë pjesë 5 operatorë ekonomik, por përzgjedhja e tyre nuk është e argumentuar, veprim në kundërshtim me nenin 39 Kërkesa për propozime, pika 4 të VKM Nr. 914, datë 29.12.2014 "Për miratimin e regullave të prokurimit publik", i ndryshuar, ku citohet: "*Pavarësisht nga publikimi i njoftimit të kontratës, sipas pikës 2, të këtij neni, autoriteti kontraktor fton për të marrë pjesëdhe të paktën 5 (pesë) operatorë ekonomikë. Në çdo rast, autoriteti kontraktor duhet të argumentojë dhe të dokumentojë përzgjedhjen e operatorëve ekonomikë që do të ftojë*".

10.1 Rekomandimi: Administratori i UKBK të analizojë problematikat e konstatuara nga grupi i auditimit, të evidentojë përgjegjësitë si dhe të marrë masa për trajnimin e stafit për njohjen më të mirë me procedurat e prokurimeve publike, me qëllim uljen e riskut të përsërtijes së mangësive të mësipërme.

Ky rekomandim nuk është zbatuar ***Menjëherë dhe në vijimësi***

11. Gjetje nga auditimi. Nga auditimi i rregullores së brendshme dhe udhëzimit në lidhje me përdorimin e sistemit të faturimit AL Billing u konstatua se:

- Institucioni nuk disponon rregullore mbi përdorimin e sistemit me anë të të cilit administrohen abonentët, matësat, faturimi si dhe arkëtimi edhe pse proceset në lidhje më këto të dhëna janë automatizuar nëpërmjet sistemit në përdorim.
- Nuk disponon rregullore për administrimin e veprimeve operacionale
- Nuk disponon rregullore për sistemimin/korrigjimin e veprimeve në system
- Udhëzues sistemi është konsideruar vetëm manuali i përdorimit, i vënë në dispozicion nga OE Jehona Software, i cili është manuali i SHA Ujësjellës Kanalizime Tiranë pasi përmban dhe logon e kësaj shoqërie.
- Nuk është dokumentuar në asnjë formë se si të dhënat lëvizin nëpërmjet sistemit, si dhe klasifikim të transaksioneve të rëndësishme, për të cilat monitorimi / autorizimi i veprimeve kërkohet të jetë i vazhdueshëm.
- Institucioni nuk disponon udhëzime lidhur me parametrizime të ndryshme të sistemit apo dhe hapat që duhen ndjekur nga ana operacionale në rastin e anulimit/ndryshimit të një fature për të cilën është verifikuar një pasaktësi në matje, apo veprime të tjera të nevojshme për korrigjim.
- Mungon përcaktimi i personit përgjegjës për komunikimin me OE, për mbarëvajtjen e çështjeve që lindin gjatë punës në sistem si dhe për çështje që lidhen me nevojat për përmirësim/ndryshim në sistemin e Billing-ut.

11.1 Rekomandimi: Ujësjellës Kanalizime Berat Kucovë në bashkëpunim me OE si administrator i vetëm i sistemit, të marrë masa për dokumentimin e diagramave të rrjedhës së informacionit, hartimin e rregulloreve mbi përdorimin e sistemit dhe administrimin e veprimeve operacionale, manual të përdoruesit për të gjitha veprimet që krijohen apo ndryshohen nëpërmjet sistemit.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

12. Gjetje nga auditimi. Nga auditimi mbi të dhënat e ruajtura në formën e logeve, për garantimin e gjurmës së auditimit u konstatua se:

- Institucioni nuk është në dijeni të strukturës dhe as të përmbajtjes të gjurmës audituese "audit trail", të gjeneruar nëpërmjet sistemit.
- Gjurma e auditimit e gjeneruar nëpërmjet sistemit nuk është e plotë dhe nuk përmban identifikues unikë për çdo record të ruajtur, por i vetmi numër me anë të të cilit mund të analizosh ndryshimet është ID e cila nuk është e dhënë unike, e vërtetuar kjo me anë të rekordeve të përsëritur me të njëjtin identifikues në më shumë se 1 herë.
- Nga auditimi mbi të dhënat u konstatuan fshirje të afërsisht 76 rekorde me të dhëna mbi konsumin të ruajtura në system si "DELETED", për muajt Tetor - Dhjetor 2018. Kjo sasi rekordesh të fshira nuk përfaqëson diferencën e ID që mungojnë në tabelën që ruan të dhëna mbi konsumin. Lejimi i fshirjes së rekordeve jo vetëm që cënon sigurinë e të dhënave nga ndërhyrjet e paautorizuara, por problemi konsiderohet me një rrisk tepër të lartë pasi këto fshirje as nuk monitorohen.
- Fshirja e rekordeve nuk rezulton si një process i dokumentuar me rregullore apo udhëzime që përcakton se cili veprim dhe nga kush mund të fshihet.

Nga auditimi mbi të dhënat e vëna në dispozicion në lidhje me detaje mbi përdoruesin, kohën e ndryshimit si dhe të dhënat mbi ndryshimet e kryera, u konstatua se edhe pse në sistemin e faturimit gjenerohen dhe ruhen gjurmë që lidhen me modifikime të të dhënave, kjo gjurmë elektronike nuk është e plotë, për arsye se:

- Në log-un për përdoruesin, nuk ruhen gjurmë mbi: krijimin e userit të ri apo mbylljen/c'aktivizimin e tij, disa rekorde kanë usercreated "*null*", çka pengon identifikimin mbi ndryshimet në këta përdorues.
- Institucioni nuk disponon asnjë dokumentacion mbi kërkesat për të hapur/mbyllur në system dhe asnjë gjurmë audituese, për ndryshimet e përdoruesve të cilët i ka krijuar/ndryshuar OE me përdoruesin "*Jehona*".
- Nga verifikimi mbi të drejtat e auditimit të software të cilat i janë dhënë disa përdoruesve, u konstatua se bëhet fjalë vetëm për një monitorim të kufizuar të aktivitetit të përdoruesit "*User Activity*", për arsye se nuk përmban detaje mbi përdoruesit, por vetëm hyrjen, daljen si dhe kohën që çdo përdorues ka kaluar në system. Nëpërmjet këtij monitorimi nuk është e mundur të identifikohet asnjë veprim më shumë i përdoruesve, cfarë rrit mundësinë e mos identifikimit të problematikave që mund të vijnë si rezultat i aksesimit të paautorizuar.

12.1 Rekomandimi: Ujësjellës Kanalizime Berat Kucovë në bashkëpunim me OE si administrator i vetëm i sistemit, të marrë masa për adresimin dhe zgjidhjen e problematikave të konstatuara në lidhje me plotësimin e gjurmës së auditimit dhe monitorimin e saj në përmbushje të detyrimit për garantimin e të dhënave të sakta dhe të plota.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

13. Gjetje nga auditimi. Nga auditimi mbi të dhënat e gjeneruara në trajtën e raporteve në sistemin Al Billing, për periudhën në auditim u konstatua se:

- Institucioni nuk disponon asnjë listë raportesh mbi të dhënat elektronike që gjenerohen nga sistemi.
- Mungesë kontrolli mbi plotësinë dhe zgjedhjen e të dhënave në raportet elektronike të gjeneruara nga sistemi Al Billing.
- Nuk janë ndërtuar raporte kontrolli në bazë ditore/mujore/periodike në lidhje me faturistin, matësat e regjistruar, debia e detajuar sipas vlerës së konsumit, taksës etj.
- Nga verifikimi mbi disa raporte nga të cilat konstatoi se dy raporte të ndryshme debitorësh, nuk tregojnë të njëjtin detyrim. "Raporti i debitorëve në datë të caktuar", i cili duhet të gjenerojë të dhëna për të gjitha detyrimet, nuk është i njëjtë me debinë që nxjerr raporti "Njoftimi i detyrimit", cfarë tregon për mangësi në përllogaritjen e saktë të këtij detyrimi. Grupi i auditimit verifikoi në periudha të ndryshme këto raporte duke patur në konsideratë dhe datën 28 të muajit pasardhës si datë maturimi, por në asnjë rast këto raporte nuk nxjerrin të njëjtën vlerë debitore.
- Mungonte argumentimi mbi elementët e debisë që merren në konsideratë në raporte të vëna në dsipozicion për ushtrimin e kontrollove apo vendimarrjeve të ndryshme si prsh "Debia për vitin 2018" etj.
- Raporte të cilat nuk nxjerrin asnjë të dhënë, duke vështirësuar marrjen e të gjithë informacionit të nevojshëm jo vetëm për audituesin, por dhe për vetë shoqërinë e cila mbi raporte bazon vendimarrjen, ku disa nga raportet janë:
    - Debia sipas faturave
    - Kontratat përkohësisht të pezulluara
    - Listat e Kontratave të mbyllura

13.1 Rekomandimi: Ujësjellës Kanalizime Berat Kucovë të marrë masat e nevojshme për adresimin tek administratori i sistemit AL Billing të problematikave të konstatuara në lidhje me gjenerimin e raporteve si dhe saktësimin e tyre për të garantuar një rezultat të saktë. Gjithashtu Ujësjellës Kanalizime Berat Kucovë të analizojë të gjitha mundësitë në ndërtimin e një monitorimi

të vazhdueshëm mbi vlefshmërinë e të dhënave të gjeneruara në trajtë raportesh që i shërbejnë analizave të ndryshme dhe vendimarrjes.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

14. Gjetje nga auditimi. Nga auditimi u konstatua se nuk janë ndërtuar:
- Rregullore dhe as skema testimi, por ndryshimet në sistem pasqyrohen direkt në Live, cka mbart një risk të lartë që mund të kenë këto ndryshime në mirëfunksionimin e sistemit si një i tërë.
- Ambjente testimi të sistemit në përdorim, vështirëson gjithashtu trajnimin e përdoruesve, testime të ndryshme në rritjen e njohurive si dhe në përvetësim të të gjitha opsioneve që ky sistem ofron.

14.1 Rekomandimi: Ujësjellës Kanalizime Berat Kucovë të marrë masat e nevojshme për krijimin e hapësirave minimale fizike dhe llogjike në krijimin e skemave të testimit, të cilat bazuar në praktikat më të mira do t'i shërbejnë testimit të funksionaliteteve, trajnimit të specialistëve IT si dhe gjithë përdoruesve të tjerë.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *të zbatuara pjesërisht**,** në proces zbatimi dhe të pa zbatuara,* inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

16. Ujësjellës Kanalizime Lushnje Sh.a (UKL)

Nga auditimi i zbatimit të rekomandimeve të dërguara subjektit UKL me shkresën Nr. 1435/7 prot, datë 26.07.2019, rezultoi se subjekti i ka trajtuar rekomandimet e lëna nga auditimi i KLSH dhe në lidhje me to ka zbatuar si më poshtë vijon:

Janë rekomanduar 29 masa organizative. Nga masat organizative janë pranuar plotësisht 29 masa, nga të pranuarat janë zbatuar 4 masa, janë zbatuar pjesërisht 0 masa, dhe janë në proces zbatimi 23 masa organizative, 2 masa organizative nuk janë zbatuar.

Për sa më sipër *rikërkoj* që UKL të marrë masa të zbatojë të gjitha rekomandimet që rezultuan të pazbatuara dhe në proces zbatimi si më poshtë:

A. MASA ORGANIZATIVE

1. Gjetje nga Auditimi: UKL Sh. A nuk ka rregullore për strukturën IT, rregullore për sigurinë dhe komunikimet elektronike, dokumentacion mbi procedurat e back up, dokumentacion mbi procedurat e veprimeve në sistem etj.

1.1 Rekomandimi: Strukturat drejtuese të Ujësjellës Kanalizime Lushnje Sh. A. të marrin masa për hartimin dhe miratimin e bazës rregullative të Teknologjisë së Informacionit (rregullorja e

strukturës IT dhe ndarja e detyrave, rregullore për sigurinë dhe komunikimet elektronike, manuale të aplikacioneve, dokumentacion mbi procedurat e back up etj.).

Masat e marra nga subjekti për zbatimin e rekomandimit

Në UKL SH.A. është në proces miratimi "*Rregullorja e brendshme mbi organizimin dhe funksionimin e strukturave dhe detyrat e tyre në Sh.a UKL për vitin 2020".*

Grupi i auditimit verifikoi dokumentacionin e vënë në dispozicion nga institucioni nga i cili në kuadër të rekomandimit të lënë nga KLSH ka marrë masa për miratimin me Vendim Nr.2, datë 10.01.2020 të Administratorit të shoqërisë mbi *"Miratimin e rregullores përPolitikat e Përdorimit të Rrjetit Kompjuterik & Sistemeve Elektronike"*. Gjithashtu miratiminme Vendim Nr.3, datë 10.01.2020të Administratorit të shoqërisë mbi *"Miratimin e rregullores për Politikat e Përdorimit të Shërbimit të Internetit dhe Postës Elektronike"*.

Ky rekomandim është në proces ***Në vijimësi***

2. Gjetje nga Auditimi: Nuk ka një analizë të nevojave për trajnim të stafit IT.

Nuk ka plan trajnimi vjetor për burimet njerëzore të sektorit të Teknologjisë e Informacionit.

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 IT.

2.1 Rekomandimi: Strukturat Drejtuese në Ujësjellës Kanalizime Lushnje Sh. A. në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe IT 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.

Masat e marra nga subjekti për zbatimin e rekomandimit

UKL SH.A. është në proçes zbatimi dhe në bashkëpunim me ASPA-n do të ndiqen të gjitha trajnimet e nevojshme nga Specialisti IT-së. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

3. Gjetje nga Auditimi: Nga auditimi u konstatua se Ujësjellës Kanalizime Lushnje Sh. A. nuk ka Strategji për Teknologjinë e Informacionit, mungesa e të cilës sjell mos pasqyrimin e objektivave lidhur me infrastrukturën, burimet e nevojshme si dhe instrumenteve të nevojshëm për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keq adresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së Ujësjellës Kanalizime Lushnje Sh. A.

3.1 Rekomandimi: Strukturat drejtuese të Ujësjellës Kanalizime Lushnje Sh. A., 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.

Masat e marra nga subjekti për zbatimin e rekomandimit

Grupit të auditimit nuk iu vu në dispozicion dokumentacion mbështetës lidhur me rekomandimin për hartimin e strategjisë së Teknologjisë së Informacionit ku të kenë parashikuar strategji zhvillimi të burimeve njerëzore IT në UKL Sh. A si një strukture të pa varur, pranë vendimmarrjes, të plotësuar me personel në vartësi të detyrave të ngarkuara në përputhje me praktikat më të mira si dhe standardet e AKSHI-t. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë***

4.Gjetje nga Auditimi: Ujësjellës Kanalizime Lushnje Sh. A. ka regjistër risku për teknologjinë e informacionit të pa miratuar dhe në mospërputhje me Ligjin nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", indryshuar, Udhëzimi nr. 30, datë 27.12.2011 "Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik".

4.1 Gjetje nga Auditimi Ujësjellës Kanalizime Lushnje Sh. A. 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 IT, në mungesë të procedurave të shkruara, risqet menaxhohet mbi bazë ngjarjesh.

Jepet suport, mbështetje teknike dhe logjike për operacionet IT 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 përsëritjes 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.

4.2 Gjetje nga Auditimi: Nuk dokumentohet procesi i hapjes dhe mbylljes së përdoruesve në sisteme.

4.3 Rekomandimi: Strukturat Drejtuese në Ujësjellës Kanalizime Lushnje Sh. A në bashkëpunim me specialistin e IT të marrin masa për:

a. Monitorimin e risqeve në infrastrukturën IT nëpërmjet identifikimit, prioritarizimit hartimit të një plan veprimi për minimizimin e tyre.

b. Dokumentimin dhe monitorimin e incidenteve në infrastrukturën IT.

c. Menaxhimin e ndryshimeve dhe dokumentimin e tyre.

rrjetit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Grupi i auditimit verifikoi dokumentacionin e vënë në dispozicion nga institucioni nga i cili në kuadër të rekomandimit të lënë nga KLSH ka marrë masa për miratimin me Vendim Nr.2, datë 10.01.2020 të Administratorit të shoqërisë mbi *"Miratimin e rregullores përPolitikat e Përdorimit të Rrjetit Kompjuterik & Sistemeve Elektronike"*. Gjithashtu miratiminme Vendim Nr.3, datë 10.01.2020të Administratorit të shoqërisë mbi *"Miratimin e rregullores për Politikat e Përdorimit të Shërbimit të Internetit dhe Postës Elektronike"*. Grupit të auditimit nuk iu vu në dispozicion dokumentacion mbështetës lidhur me rekomandimin për hartimin e një plan veprimi për risqet në infrastrukturën IT, dokumentimin dhe monitorimin e incidenteve, menaxhimin e ndryshimeve dhe dokumentimin e tyre. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Menjëherë***

5. Gjetje nga Auditimi: Strukturat e IT-së nuk janë përfshirë në procesin e identifikimit të nevojave si dhe nuk përfshihen në procesin e menaxhimit të tyre .

5.1 Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A. të marrë të gjitha masat e nevojshme për zhvillimin e strukturës IT, e cila (krahas kryerjes së detyrave funksionale) do të kryejë analizimin, prioritarizimin dhe planifikimin e nevojave për sistemet e reja dhe ekzistuese të Teknologjisë së Informacionit.

Masat e marra nga subjekti për zbatimin e rekomandimit

UKL SH.A. nuk ka mundur të marrë masat në kohë për zhvillimin e strukturës IT, e cila (krahas kryerjes së detyrave funksionale) të kryejë analizimin, prioritarizimin dhe planifikimin e nevojave

për sistemet e reja dhe ekzistuese të Teknologjisë së Informacionit. Grupi i auditimit duke patur parasysh afatet e konsideron rekomandimin në proces zbatimi.

Ky rekomandim është në proces ***Në vijimësi***

6. Gjetje nga Auditimi: Kontratat MNSH të lidhura nga UKL. Sh. A me OE "Invent" sh.p.k., OE "Instituti i Modelimeve në Biznes" sh.p.k dhe OE "Jehona Software" sh.p.k, për mirëmbajtjen e sistemeve respektivisht janë hartuar në mos përputhje me pikën **nr.6**të Udhëzimit nr. 1159, datë 17.03.2014 "*Për Hartimin e Marrëveshjeve të Nivelit të Shërbimit" (*Kontrata e MNSH nuk është aneks më vete dhe nuk përmban përcaktimet e udhëzimit të mësipërm për matjen e nivelit të shërbimit).

6.1. Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A. të hartojë e zbatojë në të ardhmen Marrëveshje të Nivelit të Shërbimit në fushën e Teknologjisë së Informacionit në përputhje me përcaktimet ligjore në fuqi.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ky rekomandim do të verifikohet nga auditimet e mevonshme.

Ky rekomandim është në proces ***Në vijimësi***

7. Gjetje nga Auditimi: Nga auditimi i tre kontratave të Marrëveshjes së Nivelit të Shërbimit (MNSH) respektivisht kontratën nr. 3 me fitues operatorin ekonomik "Invent" sh.p.k., kontratën nr.5 me fitues operatorin ekonomik "Instituti i Modelimeve në Biznes" sh.p.k. dhe kontratën nr. 640/6 me fituese Operatorin Ekonomik "Jehona Software" sh.p.k, ka një mangësi në proçesin e vlerësimit të shërbimit *(Kolaudimin)*kur dihet që përfundimi i implementimit të çdo projekti shoqërohet me kolaudime të pjesshme ose me një **analizë kosto-përfitim *(matja e cilësisë së shërbimit)***me përgjegjës z.F. Gj. për kontratën nr.3 dhe 5 si dhe z. E. DH. për kontratën nr. 640/6 sipas 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***dhe sipas ***pikës 8 (ç)***të Udhëzimit të Ministrit të Shtetit për Inovacionin dhe Administratën Publike nr. 1159, datë 17.03.2014 "*Për Hartimin e Marrëveshjeve të Nivelittë Shërbimit".*

7.1. Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A. në cilësinë e Autoriteti Kontrakor të ketë parasysh në të ardhmen:

-Në zbatimin e procedurave të prokurimitnë teknologjinë e informacionit, të marrë masa përkatëse për ngritjen e një strukture të posaçme që të bëjë të mundshme shoqërimin me kolaudime të pjesshme ose me një analizë kosto-përfitim të shërbimeve të përfituara për të bërë një vlerësim efikas mbi cilësinë dhe garantimin e vazhdueshmërisë së shërbimeve.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ky rekomandim do të verifikohet nga auditimet e mevonshme.

Ky rekomandim është në proces ***Në vijimësi***

8. Gjetje nga Auditimi: UKL Sh. A. në kontratat nr.5 me OE "Instituti i Modelimeve në Biznes sh.p.k. dhe nr.640/6 me OE "Jehona Software" sh.p.k, nuk ka zbatuar rregullat dhe procedurat e marrjes në dorëzim të shërbimit sipas *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***dhe sipas ***pikës 8 (dh***) të Udhëzimitnr. 1159, datë 17.03.2014 *"Për Hartimin e MNSH"*

8.1. Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A. në cilësinë e Autoriteti Kontrakor të ketë parasysh në të ardhmen:

-Në zbatimin e procedurave të prokurimit në teknologjinë e informacionit, të marrë masa ligjore për caktimin e personave përgjegjës dhe informacionin e kontaktimit të tyre për zbatimin dhe mbarëvajtjen e shërbimeve duke dokumentuar procesin monitorues.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ky rekomandim do të verifikohet nga auditimet e mevonshme.

Ky rekomandim është në proces ***Në vijimësi***

9. Gjetje nga Auditimi: Nga auditimi i Kontratës **nr.5**me fitues Operatorin Ekonomik "Instituti i Modelimeve në Biznes sh.p.k. me Administrator z.S. E. dhe **nr.640/6** me fituese Operatorin Ekonomik "Jehona Software" sh.p.k me administrator z. K. Z., u konstatua se nuk përfshihen: *koha e raportimit; koha e përgjigjes; prioriteti; përshkallëzimi.*Përgjegjës për hartimin dhe firmosjen e këtyre kontratave janë respektivisht për kontratën nr.5 z.. F.Gj. administrator i subjektit dhe për Kontratën nr.640/6 z. E. Dh. administrator i subjektit. Kjo në kundërshtim me **pikën 7**të Udhëzimit Nr. 1159, datë 17.3.2014 për "*Hartimin E Marrëveshjes së Nivelit të Shërbimit".*

9.1. Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A. në cilësinë e Autoriteti Kontrakor të ketë parasysh në të ardhmen:

-Në zbatimin e procedurave të prokurimit në teknologjinë e informacionit të marrë masat përkatëse për përfshirjen në kontrata të kohës së raportimin, kohës së përgjigjes, prioritetit dhe përshkallëzimeve në seksionin e të drejtave dhe detyrimeve në mënyrë që të zgjidhen kërkesat dhe të shmangen incidentet e mundshme që të zbatojë Marrëveshjen e Nivelit të Shërbimit sipas përcaktimeve ligjore në fuqi.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ky rekomandim do të verifikohet nga auditimet e mevonshme.

Ky rekomandim është në proces ***Menjëherë***

10. Gjetje nga Auditimi: Ujësjellës Kanalizime Lushnje Sh. A. nuk ka 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 janë përcaktuar Objektivat e Kohës së Rimëkëmbjes dhe Objektivat e Punës së Ripërtëritjes për çdo proces kritik.

10.1. Gjetje nga Auditimi: Ujësjellës Kanalizime Lushnje Sh. A. kryen back-up të bazës së të dhënave po në të njëjtin ambient me bazën e të dhënave primare (dhoma e serverëve).

10.2. Rekomandimi: Strukturat Drejtuese në Ujësjellës Kanalizime Lushnje Sh. A. në bashkëpunim me Specialistin e IT të marrin masa për miratimin e një plani për emergjenca dhe politika mbi vazhdimësinë e biznesit.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga dokumentacioni i vënë në dispozicion nga institucioni, UKL SH.A. ka marrë masa për miratimin me Vendim Nr.2, datë 10.01.2020 të Administratorit të shoqërisë mbi *"Miratimin e rregullores përPolitikat e Përdorimit të Rrjetit Kompjuterik & Sistemeve Elektronike", g*jithashtu miratiminme Vendim Nr.3, datë 10.01.2020të Administratorit të shoqërisë mbi *"Miratimin e rregullores për Politikat e Përdorimit të Shërbimit të Internetit dhe Postës Elektronike".*

Ky rekomandim është në proces ***Në vijimësi***

11. Gjetje nga Auditimi: Ujësjellës Kanalizime Lushnje Sh. A. 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 UKL Sh. A.

11.1. Gjetje nga Auditimi: Siguria e infrastrukturës network në Ujësjellës Kanalizime Lushnje Sh. A është e kompromentuar si rezultat i mungesës së:

a. Active Directory dhe Domain Controller për menaxhimin e userave, paisjeve dhe aplikacionevedhe për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhimin e shërbimeve në përputhje me standardet.

b. Server të dedikuar per CA (Certificate Authority)

c. Server i dedikuar për mail server (Exchange server)

d. Firewall Hardware

e. Switch të menaxhueshëm

11.2. Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A.për mbarëvajtjen e punës dhe për të pasur siguri në rrjet duhet të marri masat për t'u pajisur me: Active Directory dhe Domain Controllerpër menaxhimin e userave, pajisjeve dhe aplikacionevedhe për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhimin e shërbimeve në përputhje me standardet.;server të dedikuar për CA; Server i dedikuar për mail server, Firewall Hardware, Switch të menaxhueshëm.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga dokumentacioni i vënë në dispozicion nga institucioni, UKL SH.A. ka marrë masa për miratimin me Vendim Nr.2, datë 10.01.2020 të Administratorit të shoqërisë mbi *"Miratimin e rregullores përPolitikat e Përdorimit të Rrjetit Kompjuterik & Sistemeve Elektronike", g*jithashtu miratiminme Vendim Nr.3, datë 10.01.2020të Administratorit të shoqërisë mbi *"Miratimin e rregullores për Politikat e Përdorimit të Shërbimit të Internetit dhe Postës Elektronike".*

Ky rekomandim është në proces ***Në vijimësi***

12. Gjetje nga Auditimi: Hapja dhe ndalimi i aksesit të informacionit për personat e punësuar apo pushuar ose të transferuar nga puna monitorohet dhe nuk shoqërohet me një procesverbal për të vërtetuar që aksesi i informacionit është ndaluar në kohën e duhur për të shmangur humbjen ose keqpërdorimin e informacionit. Krijimi dhe fshirja e userave (përdoruesve) bëhet verbalisht nga administruesit e programeve përkatës.

12.1. Gjetje nga Auditimi: UKLSh. A. nuk ka procedura për të përcaktuar akseset dhe privilegjet e përdoruesve në mënyrë që përdorimi i informacionit të jetë në përshtatje me nivelin dhe pozicionin e punës, duke qenë se programet janë ndërtuar mbi arkitekturën multirole dhe multiuser duke pasur mundësi krijimi apo aksesi të informacionit në aplikacion.

12.2. Rekomandimi: UKL Sh. A.duhet të hartojë rregulla dhe procedura për krijimin dhe fshirjen e përdoruesve për personat e punësuar dhe ata të larguar ose transferuar**,** ndarjen e duhur të roleve në program për aksesin në informacion.

Masat e marra nga subjekti për zbatimin e rekomandimit

Nga dokumentacioni i vënë në dispozicion nga institucioni, UKL SH.A. ka marrë masa për miratimin me Vendim Nr.2, datë 10.01.2020 të Administratorit të shoqërisë mbi *"Miratimin e rregullores përPolitikat e Përdorimit të Rrjetit Kompjuterik & Sistemeve Elektronike", g*jithashtu miratiminme Vendim Nr.3, datë 10.01.2020të Administratorit të shoqërisë mbi *"Miratimin e rregullores për Politikat e Përdorimit të Shërbimit të Internetit dhe Postës Elektronike".*

Ky rekomandim është në proces ***Në vijimësi***

13. Gjetje nga Auditimi: Referuar ligjit nr. 9987, datë 10.03.2008 "Për mbrojtjen e të dhënave Personale" i ndryshuar, deklarata e Konfidencialitetit për përgjegjësinë dhe mbrojtjen e informacionit sensitiv nuk përkon me datën e fillimit të punës së punonjësve që kanë akses në të dhënat e sistemit.

13.1. Rekomandimi: Punonjësit e UKL Sh. A. duhet të firmosin deklaratat e konfidencialitetit në kohën që kanë akses në të dhënat e programeve që disponojnë.

Masat e marra nga subjekti për zbatimin e rekomandimit

UKL ka kryer firmosjen e deklaratave të punonjësve aktual dhe në proces për punonjësit të cilë do të punësohen në vazhdimësi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

14. Gjetje nga Auditimi: UKL Sh. A.përdor Sistemin e Faturimit "Al Billing"

a. Të paregjistruar si aset

b. Pa suport (kontrata nr. 640/6prot. datë 27.06.2018 ndërmjet UKL Sh. A.dhe OE "Jehona Software", për periudhën 27.06.2018 –26.06.2022 nuk ka përfshirë mirëmbajtjen e Sistemin e Faturimit "Al Billing").

14.1. Rekomandimi: Strukturat drejtuese të Ujësjellës Kanalizime Lushnje Sh.A të marrin masa për inventarizimin e Sistemit e Faturimit "Al Billing" si dhe zbatimin të procedurave ligjore për sigurimin e suportit të mirëmbajtjes nëpërmjet marrëveshjes së nivel shërbimit.

Masat e marra nga subjekti për zbatimin e rekomandimit

UKL SH.A. ka bërë inventarizimin e Sistemit Al Billing, por nuk ka realizuar një marrëveshje nivel shërbimi për suport mirëmbajtje.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

15. Gjetje nga Auditimi: Në Sistemin e Faturimit "Al Billing" janë kryer veprime për sistemime duke gjeneruar 458403 dublikata në fushën ID për të cilat nuk mbahet dokumentacion për argumentimin e tyre.

15.1. Rekomandimi: Strukturat drejtuese të Ujësjellës Kanalizime Lushnje Sh. A të marrin masa për dokumentimin e çdo procesi pune që sjell ndryshime në bazat e të dhënave të sistemeve TI.

Masat e marra nga subjekti për zbatimin e rekomandimit

Ky rekomandim do të verifikohet në auditimie të mëvonshme.

Ky rekomandim është në proces ***Në vijimësi***

16. Gjetje nga Auditimi: UKL Sh. A.nuk ka hartuar rregullore apo udhëzime mbi veprimet operacionale në Sistemin e "Al Billing" për parametrizime të ndryshme të sistemit apo dhe hapat që duhen ndjekur në rastin e anulimit/ndryshimit të rekordeve në bazën e të dhënave. Manuali i Sistemin e Faturimit "Al Billing" është i pa përditësuar në të përmbahen logo e përshkrime të institucioneve që nuk kanë lidhje me UKL Sh. A.

16.1. Rekomandimi: Strukturat drejtuese të Ujësjellës Kanalizime Lushnje Sh. A të marrin masa për hartimin dhe miratimin e bazës rregullative të Sistemit të Faturimit "Al Billing" dhe përditësimin e këtij manuali.

Masat e marra nga subjekti për zbatimin e rekomandimit

UKL SH.A. ka miratuar me Vendim Nr.33, datë 23.07.2020 të Administratorit të shoqërisë manuali mbi *"Përdorimin dhe administrimin e sistemit AL Billing dhe UK Reader",* dheështë në proçes pune dokumenti *"Politika të Sektorit të Shitjes"*.

Ky rekomandim është në proces ***Në vijimësi***

17. Gjetje nga Auditimi: UKL Sh. A nuk ka të drejta mbi kodin në burim në Sistemin e Faturimit "Al Billing" kompania "Jehona shpk" është pronare dhe administratore e këtij sistemi (përdoruesi Ariola Korreshi është user me të drejta të plota).

17.1. Rekomandimi: Strukturat Drejtuese në Ujësjellës Kanalizime Lushnje Sh. A. të ketë një punonjës si administrator të sistemit dhe të ketë të drejta të plota mbi kodin në burim të Sistemit të Faturimit.

Masat e marra nga subjekti për zbatimin e rekomandimit
UKL është në procesin e marrjes së të drejtës në burim të sistemi.

Ky rekomandim është në proces ***Menjëherë dhe në vijimësi***

18. Gjetje nga Auditimi: UKL Sh. A. nuk përdor sisteme inteligjente për menaxhimin e aktivitetit të saj me konkretisht në:
*1.1*Komunikimin, sinjalizimin, matjen e niveleve dhe shpërndarjes së ujit, siç janë matja e presioneve, matja e prurjeve dhe niveleve të ujit në depo.
*1.2.*Hartimin e bilancit total dhe pjesorë të prodhimit shpërndarjes dhe me qëllim minimizimin e humbjeve të ujit në rrjet.

18.1. Rekomandimi: UKL Sh. A. për të arritur objektivat e saj duhet të hartoj një plan strategjik IT për kryerjen e investimeve sisteme TI inteligjente për matjen epresioneve, prurjeve, nivelin e ujit në depo etj me objektiv krijimin e një strukture dispeçerie për menaxhimit e prodhimit, trajtimit, transportimit dhe shpërndarjes të ujit të pijshëm në sistem 24 orë/7.

Masat e marra nga subjekti për zbatimin e rekomandimit
Grupit të auditimit nuk iu vu në dispozicion dokumentacion mbështetës lidhur me rekomandimin për hartimin e një plan strategjik IT për kryerjen e investimeve me sisteme TI inteligjente për matjen epresioneve, prurjeve, nivelin e ujit në depo etj.

Ky rekomandim është në proces ***Në vijimësi***

19. Gjetje nga Auditimi: UKL Sh. A. nuk përdorë Teknologjinë e Informacionit në trajtimin e ujit (Pompat e shpërndarjes së klorit janë jashtë funksionit)
19.1. Rekomandimi: UKL Sh.A. duhet ti kushtojë vëmendje kryerjen e investimeve TI inteligjente në analizimin dhe trajtimin e ujit.

Masat e marra nga subjekti për zbatimin e rekomandimit
Janë në proces për realizimin e investimit për matësa teknologjik.

Ky rekomandim është në proces ***Në vijimësi***

20. Gjetje nga Auditimi: Ambientet e pompave, puseve dhe depove janë të rrethuara dhe të ruajtura me roje private por për të rritur sigurinë është e nevojshme përdorimi i sistemeve inteligjente survejimi.

20.1. Rekomandimi: Strukturat drejtuese të Ujësjellës Kanalizime Lushnje Sh. A. të kryejnë vlerësimin e sigurisë në sistemin e prodhimit, të shpërndarjes së ujit dhe duke vlerësuar kohën dhe mundësitë financiare të hartojnë plane investimi për rritjen e sigurisë nëpërmjet përdorimit të teknologjisë së Informacionit.

Masat e marra nga subjekti për zbatimin e rekomandimit
Janë në proces për realizimin e investimit për përdorimin e Teknologjisë së Informacionit në ambientet e pompave, puseve dhe depove të ujit.

Ky rekomandim është në proces ***Në vijimësi***

21. Gjetje nga Auditimi: Ambienti fizik i dhomës së rrjetit nuk është në përputhje me praktikat me te mira si dhe 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.
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.

21.1 Gjetje nga Auditimi: 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.

21.2. Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A.të marr masa për ndërtimin e ambienteve të dhomave të serverave në përputhje me praktikat me te mira si dhe standardet e përcaktuara në bazë të VKM nr. 248, datë 27.04.2007 "Për krijimin e Agjencisë Kombëtare të Shoqërisë së Informacionit" dhe Rregullorenpër 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.
Masat e marra nga subjekti për zbatimin e rekomandimit
Janë në proces për realizimin e investimit në ambientin fizik të dhomës së rrjetit.

Ky rekomandim është në proces ***Në vijimësi***

22. Gjetje nga Auditimi: Faqja e Web të Ujësjellës Kanalizime Lushnje Sh. A., nuk është e populluar me materialet dhe informacionet e nevojshme. Duke mos kryer funksionin e saj

22.1. Gjetje nga Auditimi: Komunikimi ndërmjet Web Browser-it dhe serverit kryhet 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.

22.2. Rekomandimi: Ujësjellës Kanalizime Lushnje Sh. A. të marri masat për të rikonfiguruar Web Server të përdor protokollin HTTPS, i cili kodon komunikimin ndërmjet Web Browserit dhe Serverit.
Masat e marra nga subjekti për zbatimin e rekomandimit
UKL SH.A. në pamundësi fondesh nuk ka mundur të marri masat për të rikonfiguruar Web Server.

Ky rekomandim është në proces ***Në vijimësi***

23. Gjetje nga Auditimi: Nga auditimi i bazës së të dhënave të Sistemit të Faturimit "Al Billing" për periudhën 01 janar 2018 deri më 31 dhjetor 2018 rezulton se janë kryer veprime duke krijuar 12247"Hendeqe"në fushën ID.(bashkëlidhur këtij akt konstatimi rekordet me hendeqe në fushën ID).

23.1. Rekomandimi: Strukturat drejtuese të Ujësjellës Kanalizime Lushnje Sh.A të analizojnë situatën dhe të marrin masa për të moslejuar kryerjen e sistemimeve në bazat e të dhënave nëpërmjet fshirjes së rekordeve.

Ky rekomandim nuk është zbatuar ***Në vijimësi***

24. Gjetje nga Auditimi: Sistemi i menaxhimit gjeospacial të aseteve (WebGis) i implementuar në UKL Sh. A. është populluar në një përqindje të ulët duke mos përfunduar identifikimin, pasqyrimin e aseteve të gjithë pjesët përbërëse të rrjetit të akumulimit dhe të shpërndarjes së ujit në UKL Sh. A. Të dhënat rreth stacioneve të pompimit, linjave, puseve, depove nuk janë regjistruar.

24.1. Rekomandimi: Strukturat drejtuese të UKL Sh. A. të marrin masa për analizimin e gjendjes dhe hartimin e një plan veprimi për vënien në eficencë të programit Web-Gis, të kryhet regjistrimi sistematik i aseteve dhe rezultatet të jenë të aksesueshme në përputhje me qëllimin e sistemit.

Ky rekomandim nuk është zbatuar ***Menjëherë dhe në vijimësi***

II. Për të gjitha rekomandimet e tjera, që konsiderohen *në proces zbatimi dhe të pa zbatuara*, inkurajohet përshpejtimi i realizimit të plotë të tyre brenda 3-mujorit të tretë të vitit 2020 dhe 3-mujorit të parë të vitit 2021. Në mbështetje të nenit 30, pika 2 të ligjit nr. 154/2014 datë 27.11.2014 "*Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit",* brenda 6 muajve nga përcjellja e rekomandimeve tona, të raportohet me shkrim pranë KLSH mbi ecurinë e zbatimit të tyre.

III. TË TJERA

Për të gjitha rekomandimet që konsiderohen në proces, të pazbatuara, të zbatuara pjesërisht, në proces zbatimi ose të papranuara inkurajoj përshpejtimin e realizimit të plotë të tyre brenda vitit 2020, verifikimi i zbatimit të të cilave do të kryhet në auditimin e rradhës që KLSH do kryejë në këto subjekte.

Për rekomandimet të cilat kanë rezultuar në proces, të pazbatuara, të zbatuara pjesërisht, në proces zbatimi ose të papranuara nga auditimi i ushtruar "Për zbatimin e rekomandimeve të lëna në auditimet e mëparshme", së bashku me pjesë nga Raporti Përfundimtar, do të përcillen për secilin subjekt gjatë muajit Nëntor 2020, sipas Vendimit të Kryetarit për këtë auditim.

Me ndjekjen dhe zbatimin e detyrave dhe masave të përcaktuara në këtë vendim ngarkohet Departamenti i Auditimit të Teknologjisë së Informacionit.

Arben SHEHU

K R Y E T A R

Departamenti i Auditimit të Teknologjisë së Informacionit
Verifikimi i zbatimit të rekomandimeve në 16 subjekte të evaduara në vitin 2019

Aneksi Nr. 1. Masat Organizative

Nr.	Emri i Insitucionit	Rekomanduar	Pranuar	Zbatuar Plotësisht	Zbatuar Pjesërisht	Në Proces	Pa zbatuar	
1	B Fier	**7**	**7**	**4**	**0**	**3**	**0**	
2	Akep	**5**	**5**	**5**	**0**	**0**	**0**	
3	AKSHI	**9**	**9**	**2**	**0**	**7**	**0**	
4	AMA	**8**	**8**	**1**	**0**	**6**	**1**	
5	AMF	**8**	**8**	**6**	**0**	**2**	**0**	
6	B Korce	**8**	**8**	**3**	**0**	**4**	**1**	
7	B Lezhe	**10**	**10**	**2**	**0**	**2**	**6**	
8	B Vlore	**9**	**9**	**1**	**0**	**2**	**6**	
9	FSDKSH	**37**	**37**	**11**	**10**	**11**	**5**	
10	KESH	**23**	**23**	**10**	**0**	**11**	**2**	
11	MiN BUQ	**9**	**9**	**7**	**0**	**2**	**0**	
12	MIN DREJ	**11**	**11**	**5**	**1**	**5**	**0**	
13	MFE	**20**	**17**	**1**	**2**	**7**	**7**	
14	M Kult	**8**	**8**	**2**	**2**	**4**	**0**	
15	UKBK	**22**	**222**	**8**	**1**	**8**	**5**	
16	UKL	**29**	**29**	**4**	**0**	**23**	**2**	
	Gjithësej	**222**	**220**	**72**	**16**	**97**	**35**	
	Në %		99%	33%	7%	44%	16%	