REPUBLIKA E SHQIPËRISË
KONTROLLI I LARTË I SHTETIT
Drejtoria e Auditimeve IT

Adresa: Rr "Abdi Toptani", nr.1, Tiranë; *E-mail: klsh.org.al; Web-site: www.klsh.org.al*

Nr.864/5Prot. Tiranë, më 14.12.2018

V E N D I M

Nr. 197, Datë 14.12.18

PËR

AUDITIMIN E USHTRUAR NË BASHKINË ELBASAN MBI
"Auditimin e Sistemeve të Teknologjisë së Informacionit"
për periudhën nga data 01.01.2017 deri më datën 30.06.2018.

Nga auditimi i ushtruar në Bashkinë Elbasan rezultoi që, në bazë të programit të auditimit nr.864/1.prot, datë 11.09.2018 me objekt: "Auditimi i Sistemeve të Teknologjisë së Informacionit" për periudhën 01.01.2017 deri në 30.06.2018, Bashkia Elbasan ka zhvilluar sisteme të Teknologjisë së Informacionit në funksion të përmbushjes së objektivave të institucionit duke shfrytëzuar burimet e vëna në dispozicion si dhe kryer thithjen e investimeve të konsiderueshme nga donatorët e huaj për zhvillimin dhe mirëmbajtjen e infrastrukturën së TI.
Pasi u njoha me Raportin Përfundimtar të Auditimit dhe Projektvendimin e paraqitur nga Grupi i Auditimit të Drejtorisë së Auditimit IT, shpjegimet e dhëna nga subjekti i audituar, si dhe vlerësimet mbi objektivitetin dhe cilësinë e auditimit nga Drejtori i Drejtorisë së mësipërme, Drejtori i Drejtorisë së Standardeve dhe Sigurimit të Cilësisë si 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",

VENDOSA:

I. Të miratoj Raportin Përfundimtar të Auditimit "Për Auditimin e Sistemeve të Teknologjisë së Informacionit" të ushtruar në Bashkinë Elbasan sipas programit të auditimit nr 864/1 prot, datë 11.09.2018 për veprimtarinë nga *data 01.01.2017* deri më datën *30.06.2018.*

II. Të miratoj rekomandimet për përmirësimin e gjendjes dhe të kërkoj marrjen e masave sa vijon;

A. OPINION I AUDITIMIT:

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

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

Rezultatet e arritura janë të kompromentuar nga mungesa e Strategjisë për Teknologjinë e Informacionit, duke mbartur riskun e keq adresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së Bashkisë Elbasan.

B. MASA ORGANIZATIVE:

1. Gjetje nga Auditimi: *Nga auditimi u konstatua se Struktura IT ka një bazë rregullative të plotësuar (*rregullorja e strukturës IT dhe ndarja e detyrave, rregullore për sigurinë dhe komunikimet elektronike, manuale të aplikacioneve të përfituara si rezultat i donacioneve, dokumentacion mbi procedurat e backup etj*...), por kjo bazë rregullative është e pa miratuar.*

(Më hollësisht trajtuar në pikën VI.1, faqet nr. .10-13. të raportit të Auditimit.)

1.1 Rekomandimi: Strukturat drejtuese të Bashkisë Elbasan të marrin masa për 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 të përfituara si rezultat i donacioneve, dokumentacion mbi procedurat e backup).*

Menjëherë dhe në vijimësi

2. Gjetje nga Auditimi: Nga auditimi u konstatua se nuk ka plan trajnimi vjetor për vitet 2017-2018 për burimet njerëzore të sektorit të Teknologjisë e Informacionit. Nuk dokumentohet procesi i kërkesave, nevojave dhe analizimi i tyre. Trajnimet e përfituara nga donatorët dhe zhvilluesit e sistemeve janë të pa mjaftueshme e nuk plotësojnë nevojat për trajnim mbi sistemet, sigurinë dhe teknologjinë e informacioni për stafin IT.

(Më hollësisht trajtuar në pikën VI.1, faqen nr. 13. të raportit të Auditimit.)

2.1 Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan në bashkëpunim me Drejtorinë e Burimeve Njerëzore dhe Sektorin e Inovacionit IT dhe mbrojtjes Kibernetike 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.

Brenda 6 mujorit të parë të vitit 2019 dhe në vijimësi

3. Gjetje nga Auditimi: Nga auditimi u konstatua se Organizimi i Strukturës IT në nivel sektori nën Drejtorinë e Politikave Strategjike e Inovacionit dhe Medias, nuk i përgjigjet shtrirjes së teknologjisë së informacionit në Bashkinë Elbasan dhe institucionet e vartësisë duke zbehur ndikimin e varësisë direkt nga menaxhimi i lartë. Nga auditimi i procesit të identifikimit të nevojave për investime në fushën e teknologjisë së informacionit dhe priorizimit të tyre konstatohet se Strukturat e IT që marrin pjesë aktive në procesin e identifikimit të nevojave nuk përfshihen në procesin e menaxhimit të tyre si rezultat i statusit organizativ në nivel sektori nën Drejtorinë e Politikave Strategjike e Inovacionit dhe Medias. *(Më hollësisht trajtuar në pikën VI, faqet nr. 13-14 të raportit të Auditimit.)*

3.1 Rekomandimi: Strukturat drejtuese të Bashkisë Elbasan të analizojnë mundësinë e ndryshimeve strukturore të strukturës ekzistuese IT me qëllim rritjen e rolit të saj dhe përfshirjen në procesin e menaxhimit të identifikimit të nevojave për investimet në fushën e teknologjisë së informacionit

Brenda Vitit 2019 dhe në vijimësi

4. Gjetje nga Auditimi: Nga auditimi u konstatua se Bashkia Elbasan nuk ka Strategji për Teknologjinë e Informacionit, mungesa e të cilës sjell mos pasqyrimin e objektivave lidhur me infrastrukturën, burimet dhe instrumentet e nevojshëm për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keq adresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së Bashkisë Elbasan

(Më hollësisht trajtuar në pikën VI.4, faqet nr. 24-25. të raportit të Auditimit.)

4.1 Rekomandimi: Strukturat drejtuese të Bashkisë Elbasan, 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.

Brenda Vitit 2019 dhe në vijimësi

5. Gjetje nga Auditimi: Standardet e Praktikat me të mira rekomandojnë që Qeverisja TIK duhet të vendosi politika në fushën e IT. Këto politika vendosin kërkesat për mbrojtjen e aseteve të informacionit dhe mund t'i referohen procedurave ose mjeteve të tjera në mënyrën sesi këto do të mbrohen. Politikat duhet të jenë të disponueshme ndaj të gjithë punonjësve përdorues të IT. Bashkia Elbasan nuk ka vendosur politika e parime mbi sigurinë dhe vazhdueshmërinë e punës së institucionit. Bashkia Elbasan nuk ka krijuar facilitetet e nevojshme për vënien në dispozicion të rregulloreve dhe politikave për të gjithë punonjësit përgjegjës mbi sigurinë e informacionit, përfshirë përdoruesit e sistemeve të cilët kanë rol në mbrojtjen e informacionit me qëllim që të gjithë punonjësit të familjarizohen dhe ta bëjnë pjesë të mënyrës së të menduarit dhe të veprimtarisë së tyre të përditshme.

(Më hollësisht trajtuar në pikën VI.4, faqet nr. 25-26 të raportit të Auditimit.)

5.1 Rekomandimi: Strukturat drejtuese të Bashkisë Elbasan, të marrin masa për familjarizimin me rregulloret dhe politikat TIK për të gjithë punonjësit përgjegjës mbi

sigurinë e informacionit, përfshirë përdoruesit e sistemeve të cilët kanë rol në mbrojtjen e informacionit.

Brenda Vitit 2019 dhe në vijimësi

6. Gjetje nga Auditimi: *Rregullorja e Brendshme, lidhur me strukturën IT në* Bashkinë Elbasan, nuk është në përputhje me rekomandimet e AKSHIT, rregullorja nuk përmban elementët e nevojshëm për të siguruar funksionimin e përshtatshëm të strukturës IT në institucion.

(Më hollësisht trajtuar në pikën VI.4, faqet nr. 25-26 të raportit të Auditimit.)

6.1 Rekomandimi: Bashkia Elbasan të hartojë, dhe miratojë *Rregulloren e Brendshme, lidhur me strukturën IT* në përputhje me rekomandimet e AKSHIT. Për hartimin e kësaj Rregulloreje të marret në konsideratë vendosja e kontrolleve të brendshme lidhur me menaxhimin e riskut, përputhshmërinë me procedurat dhe rregullat e brendshme aktuale të sektorit si dhe me legjislacionin e Teknologjisë së Informacionit dhe Komunikimit në Shqipëri.

Brenda vitit 2019 dhe në vijimësi

7. Gjetje nga Auditimi: Bashkia Elbasan nuk disponon regjistër risku për teknologjinë e informacionit në mospërputhje me ligjin nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar, Udhëzimi nr. 30, datë 27.12.2011 "Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik".

7.1. Gjetje nga Auditimi Bashkia Elbasan nuk ka politika të ruajtjes së dokumenteve dhe nuk ka të dokumentuar një plan masash për identifikimin, trajtimin e gabimeve dhe incidenteve që mund të ndodhin në infrastrukturën 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 në mënyrë që funksionet e institucionit të jenë të mbrojtura. *(Më hollësisht trajtuar në pikën VI.3., faqet nr. 18-19 të raportit të Auditimit.)*

7.2. Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan në bashkëpunim me Sektorin e Inovacionit IT dhe mbrojtjes Kibernetike të marrin masa për:

a. identifikimin e risqeve IT dhe hartimin e regjistrit të risqeve.

b. dokumentimin dhe monitorimin e incidenteve.

c. menaxhimin e ndryshimeve dhe dokumentimin e tyre.

Brenda 6 mujorit të parë të vitit 2019 dhe në vijimësi

8. Gjetje nga Auditimi: Bashkia Elbasan nuk rezulton të ketë plan të miratuar emergjence dhe politika të miratuara për vazhdimësinë e biznesit. Politika organizative mbi vazhdimësinë e ofrimit të shërbimeve duke marrë në konsideratë: rolet dhe përgjegjësitë, fushëveprimin,

kërkesat për trajnim, orarin e mirëmbajtjes, orarin e testimit, nivelet e miratimit dhe palët e përfshira në këtë proces. Nuk janë përcaktuar Objektivat e Kohës së Rimëkëmbjes dhe Objektivat e Punës së Ripërtëritjes për çdo proces kritik.

(Më hollësisht trajtuar në pikën VI.3., faqet nr. 19-20. të raportit të Auditimit).

8.1. Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan në bashkëpunim me Sektorin e Inovacionit IT dhe mbrojtjes Kibernetike të marrin masa për miratimin e një plani për emergjenca dhe politika mbi vazhdimësinë e biznesit.

Brenda 6 mujorit të parë të vitit 2019 dhe në vijimësi

9.a Gjetje nga Auditimi: Siguria e infrastrukturës *network* në Bashkinë Elbasan është e kompromentuar si rezultat i mungesës së:
a. Active Directory dhe Domain Controller për menaxhimin e userave, pajisjeve dhe aplikacioneve dhe për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhimin e shërbimeve në përputhje me standardet.
b. server të dedikuar për CA (Certificate Authority)
c. Server i dedikuar për mail server (Exchange server)
d. Firewall Hardware
e. Switch të menaxhueshëm

9.b. Gjetje nga Auditimi: Nga auditimi i rrjetit kompjuterik që lidh Bashkinë Elbasan me njësitë administrative rezultoi se:
a. Përdoruesit në këto qendra janë lidhur nga fibra optike dhe marrin shërbimin në një Swich të pa menaxhueshëm.
b. Konfigurimet në rrjet të PC janë si administratorë.
Në të njëjtin swich marrin shërbime disa institucione

9.c. Gjetje nga Auditimi: Nuk dokumentohet procesi i hapjes dhe mbylljes së logarive të përdoruesve në sisteme.

(Më hollësisht trajtuar në pikën VI.3., faqen nr. 20 të raportit të Auditimit.)

9.1. Rekomandimi: Bashkia Elbasan për mbarëvajtjen e punës dhe për të pasur siguri në rrjet duhet të marri masat për t'u pajisur me: Active Directory dhe Domain Controller për menaxhimin e userave, pajisjeve dhe aplikacioneve dhe 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.

Brenda vitit 2020 dhe në vijimësi

10. Gjetje nga Auditimi: Ambienti fizik i dhomës së rrjetit nuk është në përputhje me standardet e përcaktuara në Rregulloren për Ndërtimin e Dhomës së Serverëve (Versioni 1.0, datë 02.12.2008) miratuar nga AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit) përkatësisht:

a. Pika 4.3. Parandalimi i zjarrit**.**

Dhoma duhet të jetë e pajisur me një sistem të përshtatshëm kundër zjarrit

Dhoma duhet të jetë rezistente ndaj zjarrit nëse kabllot dhe sistemet e ftohjes kombinohen në të njëjtën hapësire sipër tavanit ose nën dysheme

b.Pika 4.5. Sistemi Elektrik. Instalimi elektrik i dhomës së serverëve nuk është veçmas instalimit të përgjithshëm.
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.

10.a 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.

(Më hollësisht trajtuar në pikën VI.4., faqet nr.27-28. të raportit të Auditimit.

10.1 Rekomandimi: Bashkia Elbasan të marrë masa për ndërtimin e ambienteve të dhomave të serverëve në bazë të VKM nr. 248, datë 27.04.2007 "Për krijimin e Agjencisë Kombëtare të Shoqërisë së Informacionit" dhe Rregulloren për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK dhe praktikat më të mira kombëtare dhe ndërkombëtare.

Brenda vitit 2019 Në vijimësi

11. 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 rrjet, ka mundësi të lexojë dhe ndryshojë informacionin i cili aksesohet nga rrjeti, duke përfshirë (fjalëkalimet-et, të dhëna sekret si dhe të tjera të dhëna sensitive).

Mbrojtësi X-XSS i HTTP mundëson shfletuesin (browserin) të mos hapë faqe webi të cilat kapin sulme Cross-Site Scripting (XSS) të reflektuar.

(Më hollësisht trajtuar në pikën VI.4., faqet nr. 28-29. të raportit të Auditimit.)

11.1 Rekomandimi: Drejtorinë e Politikave Strategjike e Inovacionit dhe Medias të marri masat për të rikonfiguruar Web Server të përdor protokollin HTTPS, i cili kodon komunikimin ndërmjet Web Browserit dhe Serverit.

Gjate vitit 2019 në vijimësi

12. Gjetje nga Auditimi: Nga auditimi i Kontratës nr.2474 "Shërbim Interneti për Bashkinë Elbasan dhe Njësitë e vartësisë" rezultoi se grupi i marrjes në dorëzim nuk ka një raport për marrjen në dorëzim të punimeve të kryera (në këtë rast shërbimin e Internetit) nga OE, në kundërshtim me VKM Nr. 914, datë 29.12.2014,Neni 77, Pika 3. *Mbikëqyrja e kontratës.*
Në disa nga faturat Tatimore, të sjella nga Operatori Ekonomik Albtelecom SH.A., blerësi në këtë rast Autoriteti Kontraktor (Bashkia Elbasan), ka firmosur këto fatura vetëm me emrin "Bashkia Elbasan" dhe jo "grupi i marrjes në dorëzim të shërbimit të internetit".
Përkatësisht në faturat nr. 90726620, nr. 90735561.
Ndërsa faturat e tjera janë firmosur vetëm nga një përfaqësues i grupit të marrjes në dorëzim.

4 MNSH
U kontrolluan këto Kontrata për MNSH (Marrëveshje Nivel Shërbimi):

- Nr. Kontrate 8796 “Elbasan Virtual Tour 360”
- Nr. Kontrate 9756 “Projekti i monitorimit të ambientit në qytetin e Elbasanit”
- Nr. Kontrate 472 “Mirëmbajte e platformës: Transport Inteligjent”

12.1 Gjetje nga Auditimi: Nga auditimi i këtyre procedurave rezultoi se në të gjitha marrëveshjet e nivel shërbimit (MNSH), që janë me afat 4 vjeçar, grupi i marrjes në dorëzim nuk ka një raport të marrjees në dorëzim të punimeve të kryera nga OE, në kundërshtim me VKM Nr. 914, datë 29.12.2014,Neni 77, Pika 3. *Mbikëqyrja e kontratës*

Për t'u siguruar nëse cilësia e punëve, shërbimeve ose e mallrave është e njëjtë me cilësinë për të cilën është shpallur fitues kontraktori, autoriteti kontraktor duhet të monitorojë zbatimin e kontratës dhe në rast të shkeljes së kushteve të kërkuara zbaton penalitetet e parashikuara në kontratë. "Autoriteti kontraktor, gjatë kryerjes së kontrolleve mban procesverbal me shkrim në prani të kontraktorit, sipas përcaktimeve në legjislacionin në fuqi" Procesverbali i marrjes në dorëzim. Raporti i komisionit që merr në dorëzim.

12.2. Gjetje nga Auditimi: Nga auditimi i Kontratës Nr. 8796 “Elbasan Virtual Tour 360” rezultoi se, kjo kontratë nuk ka MNSH (Marrëveshje Nivel Shërbimi) në kundërshtim me pikën 3 të Udhëzimit Nr. 1159, datë 17.3.2014 për Hartimin E Marrëveshjes Së Nivelit Të Shërbimit i cili citon*: "Institucionet, të cilat janë duke zhvilluar sisteme të reja në fushën e TIK-ut, detyrimisht, të parashikojnë MNSH-në, si pjesë të procedurës së realizimit të investimit për këto sisteme. Kohëzgjatja e kësaj marrëveshjeje duhet të jetë jo më e shkurtër se 4 (katër) vjet."*

c)U konstatua se në të gjitha MNSH nuk përfshihen: *koha e raportimit; koha e përgjigjes; prioriteti; përshkallëzimi*
Kjo në kundërshtim me pikën 7 të Udhëzimit Nr. 1159, datë 17.3.2014 për Hartimin E Marrëveshjes së Nivelit të Shërbimit e cila citon:
Të drejtat dhe detyrimet e ofruesit të shërbimit Ky seksion duhet të përcaktojë të drejtat dhe detyrimet që ofruesi i shërbimit ka ndaj institucionit, në lidhje me ofrimin e shërbimit. Për sa u përket detyrimeve, duhet të përcaktohen metodologjitë dhe specifikat e suportit të ofruesit të shërbimit të MNSH-së; për sa i përket ndërmarrjes së të gjitha veprimeve në kohën e duhur. Në lidhje me shërbimet që do të përcaktohen në marrëveshje, ofruesi i shërbimeve duhet t'u përgjigjet dhe të zgjidhë kërkesat ose incidentet e paraqitura nga institucioni. Gjithashtu, ofruesi i shërbimit duhet të ofrojë dokumentacionin e plotë për komponentët e shërbimit; të garantojë personel të kualifikuar dhe në numër të mjaftueshëm për realizimin e shërbimit; të ofrojë sigurimin e pjesëve të këmbimit (kur është e aplikueshme) dhe në sasinë që do të duhen për t'u ndërruar brenda harqeve kohore të përcaktuara.
Më hollësisht trajtuar në pikën VI.2, faqet nr. 14-17. të raportit të Auditimit.
12.1 Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan në të ardhmen për të shmangur mangësi në praktikat e zbatimit të kontratave duhet të marrin masa për zbatimin e kontrates në përputhje me legjislacionin në fuqi.

Menjëherë dhe në vijimësi

13. Gjetje nga Auditimi: Siguria e aplikacioneve si rezultat i mos dokumentimit të procesit të hapjes dhe mbylljes së kredencialeve të përdoruesve në aplikacionet është e kompromentuar.

Më hollësisht trajtuar në pikën VI.3, faqen nr. 22. të raportit të Auditimit.

13.1 Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan në bashkëpunim me Sektorin e Inovacionit IT dhe mbrojtjes Kibernetike duhet të marrin masa për dokumentimin e procesit të hapjes dhe mbylljes së kredencialeve të përdoruesve në aplikacione.

Menjëherë dhe në vijimësi

14. Gjetje nga Auditimi: Bashkia Elbasan nuk ka infrastrukturën e nevojshme për të siguruar aplikacionet e zhvilluara, ambienti fizik komprometon sigurinë e aplikacioneve. Bashkia Elbasan nuk ka ambient të veçantë për testime përpara kalimit të ndryshimeve në sistemin Live për aplikacionet mungesa e të cilit komprometon sigurinë e sistemit, të dhënave si dhe vazhdimësinë e ofrimit të shërbimeve.

(Më hollësisht trajtuar në pikën VI.3, faqet nr. 22-23. të raportit të Auditimit.)

14.1 Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan në bashkëpunim me Sektorin e Inovacionit IT dhe mbrojtjes Kibernetike, të marrin masa për një riorganizim të hapësirave fizike dhe logjike në pajisjet server lidhur me shërbimet që ofron aktualisht, me qëllim:

- Garantimin e vazhdimësisë së shërbimeve të ofruara.
- Përfitimin e një performance më të mirë të aplikacioneve.
- Krijim hapësire për një kopje të sistemit në funksion të testimeve apo trajnimeve të ndryshme sipas rastit.

Brenda Vitit 2019 dhe në vijimësi

15. Gjetje nga Auditimi: Sistemi i Administrimit të Taksave (TAIS) nuk ndërvepron me sistemin QKB për të marrë automatikisht të dhënat e bizneseve me impakt mos informimin në kohë për bizneset e reja të regjistruara.
(Më hollësisht trajtuar në pikën VI.3, faqen nr.23 të raportit të Auditimit.)

15.1 Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan, në bashkëpunim me Sektorin IT dhe Drejtorinë e Taksave Vendore të marrin masa për hartimin e një plan veprimi për të siguruar ndërveprimin e bazës së të dhënave të QKB me atë TAIS.

Brenda Vitit 2019 dhe në vijimësi

16. Gjetje nga Auditimi: Sistemi i Administrimit të Taksave (TAIS) nuk disponon sisteme kontrolli për parandalimin e inputeve të pa sakta në bazën e të dhënave, duke lejuar parregullsi në fushat e rëndësishme të bazës së të dhënave si "NIPT", "Adresa" "Emërtimi i Biznesit"
(Më hollësisht trajtuar në pikën VI.3, faqen nr.23 të raportit të Auditimit.)

16.1 Rekomandimi: Sektori i Inovacionit IT dhe mbrojtjes Kibernetike në bashkëpunim me Drejtorinë e Taksave Vendore si dhe zhvilluesin e sistemit TAIS, të marrë masa për të përcaktuar kriteret e nevojshme dhe detyrueshme të formatit për çdo fushë të bazës së të dhënave në TAIS si dhe të vendosi sisteme kontrolli për parandalimin e inputeve të gabuara.

Menjëherë dhe në vijimësi

17. Gjetje nga Auditimi: Siguria e vazhdimësisë së punës së aplikacioneve është e cenuar nga:
a. Mungesa e testeve të Back-up dhe Restore

b. Mos përcaktimin në rregullore të frekuencës së kryerjes së Back-up dhe testimit te tij

c. Mos përcaktimi i afatit të ruajtjes së informacionit në Backup

d. Ruajtjes të Back-up në të njëjtin ambient me bazën e të dhënave primare (dhoma e serverëve).

Më hollësisht trajtuar në pikën VI.3, faqen nr.24 të raportit të Auditimit.

17.1 Rekomandimi: Strukturat Drejtuese në Bashkinë Elbasan në bashkëpunim me Sektorin e Inovacionit IT dhe mbrojtjes Kibernetike, të marrin masa për përcaktimin e kryerjes së testeve të Back-Up dhe Restore, frekuencën e kryerjes së këtyre testeve, afatin e ruajtjes së informacionit në Back-Up si dhe ruajtja e Back Up në një ambient të ndryshëm nga ai i dhomës së serverëve.

Brenda vitit 2020 dhe në vijimësi

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

Bujar LESKAJ

K R Y E T A R