REPUBLIKA E SHQIPËRISË
KONTROLLI I LARTË I SHTETIT
Departamentit i Auditimit të Teknologjisë së Informacionit dhe Investimeve të Huaja
Adresa: Blv"Dëshmorët e Kombit", nr.3, Tiranë; E-mail: klsh.org.al; web-site:www.klsh.org.al

Nr.886/7 Prot. Tiranë, më 29.12.2017

V E N D I M

Nr.199, Datë 28.12.2017

PËR
AUDITIMIN E USHTRUAR NË INSTITUTIN E STATISTIKAVE,

MBI "AUDITIMIN E TEKNOLOGJISË SË INFORMACIONIT".

(Për periudhën nga data 01.01.2016 - 31.12.2016)

Pasi u njoha me Raportin Përfundimtar të Auditimit dhe Projektvendimin e paraqitur nga Grupi i Auditimit të Departamentit të Auditimit të Teknologjisë së Informacionit dhe Investimeve të Huaja, shpjegimet e dhëna nga subjekti i audituar, si dhe vlerësimet mbi objektivitetin dhe cilësinë e auditimit nga Drejtori i Departamentit të mësipërm, Drejtori i Departamentit Juridik dhe Kontrollit të Zbatimit të Standardeve të Auditimit dhe Etikës si dhe Drejtori i Përgjithshëm, duke vlerësuar rëndësinë e teknologjisë së informacionit në përmbushjen e misionit të INSTAT-it në prodhimin e statistikave asnjanëse, transparente dhe të përditësuara, si dhe rëndësinë e tyre në proceset e zhvillimit e transformimit të fushave ekonomiko sociale të vendit, 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 të Teknologjisë së Informacionit me objekt: vlerësimin e funksionimit të Qeverisjes TI dhe Sigurisë së Informacionit të ushtruar në Institutin e Statistikave, Drejtoria e Teknologjisë së Informacionit, sipas programit të auditimit nr. 866/1, datë 10.10.2017 për veprimtarinë nga data 01.01.2016. deri më datën 31.12.2016.

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

A. OPINIONI I AUDITIMIT:

Grupi i auditimit duke pasur parasysh rolin e teknologjisë se informacionit në përmbushjen e misionit të INSTAT-it në prodhimin e statistikave asnjanëse, transparente dhe të përditësuara, si dhe rëndësinë e tyre në proceset e zhvillimit e transformimit të fushave ekonomiko sociale mbështetur në Standardet Kombëtare dhe Ndërkombëtare të Auditimit, si më poshtë:ISSAI 1 Neni 22, Ligjin e KLSH Nr.154/2014 Neni 3 dhe 14, Manualin e Auditimit të Teknologjisë së Informacionit (WGITA), COBIT 4.1, ISSAI 5300.6, 8 dhe 12.2, 16.19, 21.1, 23, ISSAI 100.36,48, ISSAI 5310, pas shqyrtimit të të dhënave dhe dokumentacionit TI të vënë në dispozicion nga INSTAT, arriti në konkluzionin se:
Zhvillimi i Teknologjisë se Informacionit në mungesë të një Strategjie në INSTAT ka sjellë mos pasqyrimin qartë të objektivave të institucionit lidhur me infrastrukturën TI dhe burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen e saj.
Mungesa e Planit Strategjik mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së INSTAT nga Teknologjia e Informacionit
Me gjithë përpjekjet e bëra, INSTAT nuk ka marrë masa të mjaftueshme rregullatore dhe organizative për garantimin e sistemeve të informacionit.
Në gjykimin tonë, menaxhimi i elementëve kritikë në sistemet e informacionit, është i pa pamjaftueshëm dhe i papërshtatshëm, Investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht sigurimin e Vazhdueshmërisë së Biznesit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat.

B. MASA ORGANIZATIVE:

1. Gjetje nga auditimi: Nga auditimi i Strategjisë, politikave dhe procedurave në TI) rezultoi se INSTAT nuk ka Strategji të veçantë për Teknologjinë e Informacionit, mungesa e të cilës ka sjellë mos pasqyrimin e qartë të objektivave TI lidhur me infrastrukturën, burimet e nevojshme, si dhe instrumenteve të nevojshëm për realizimin e objektivave. Mungesa e Planit Strategjik të TI, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së INSTAT. (*Sa më sipër trajtuar më hollësisht në faqet nr. 4,10 të Raportit të Auditimit)*

Rekomandimi: Drejtoria e Teknologjisë së Informacionit dhe strukturat drejtuese të INSTAT-it të adresojnë qartë objektivat në fushën e Teknologjisë së Informacionit dhe duke marrë në konsideratë kohën, burimet e nevojshme të marrin masa për hartimin e miratimin e Planit Strategjik të Teknologjisë së Informacionit.

Brenda 3 mujorit të parë të vitit 2018 dhe në vijimësi

2. Gjetje nga auditimi: Drejtoria e Teknologjisë së Informacionit në aktivitetin e saj për vitin 2016 ka vepruar me bazë rregullatore për Teknologjinë e Informacionit të pa miratuar nga strukturat drejtuese. (*Sa më sipër trajtuar më hollësisht në faqet nr.4,11 të Raportit të Auditimit).*

Rekomandimi: Strukturat drejtuese të INSTAT-i të marrë masa në të ardhmen që për standardet, politikat dhe rregulloret e reja dhe ndryshimet e tyre të aprovohen nga organet përkatëse përpara përdorimit. Drejtoria e Teknologjisë së Informacionit duhet të marri masa për menaxhimin e ndryshimit nëpërmjet komunikimit, trajnimit e testimit në të gjitha nivelet e organizatës në intervale sistematike kohore të ndryshimeve në rregulloret dhe procedurat korresponduese.

Në vijimësi

3. Gjetje nga auditimi: Grupi i auditimit konstaton dhe vlerëson kryerjen nga INSTAT-ti i një auditimi të brendshëm për TI gjatë vitit 2016, por shikon se plani i veprimit për zbatimin e të metave të konstatuara është formal si rezultat i mungesës së vlerësimit real të impaktit që mbartin risqet e të metat e konstatuara. Përpjekjet për vlerësimin dhe menaxhimin e risqeve janë të pa mjaftueshme. (*Sa më sipër trajtuar më hollësisht në faqet nr.4,11 të Raportit të Auditimit).*

Rekomandimi: Strukturat drejtuese të INSTAT, duke marrë në konsideratë kohën dhe burimet e nevojshme, të marrin masa për hartimin e politikave dhe planeve të menaxhimit të riskut, si dhe të përcaktojë burimet e mjaftueshme për të menaxhuar risqet.

Brenda 3 mujorit të parë të vitit 2018 dhe në vijimësi

4. Gjetje nga auditimi: Nga auditimi i burimeve njerëzore në strukturën e TI u konstatua se ka një strukturë të plotë, me ndarje detyrash e përshkime pune, e cila ka zhvilluar dhe ka marre trajnime sipas një plani të miratuar gjatë vitit 2016, por krahas kësaj grupi i auditimit konstaton se INSTAT-i gjatë vitit 2016 ka pasur:

a. Lëvizje të shpeshta të burimeve njerëzore në Drejtorinë e Teknologjisë së Informacionit.

b. Mungesa në organikën e Drejtorisë së TI në pozicionet kritike gjatë vitit 2016 (*Sa më sipër trajtuar më hollësisht në faqet nr.4,13 të Raportit të Auditimit).*

Rekomandimi: INSTAT të marrë masa për plotësimin e burimeve njerëzore në Drejtorinë e Teknologjisë së Informacionit duke plotësuar vendet vakante si dhe hartimit të politikave për menaxhimin e ndryshimeve të tyre për pozicionet kritike.

Brenda 3 mujorit të parë të vitit 2018 dhe në vijimësi

5. Gjetje nga auditimi: Nga auditimi i procedurave të dhënies, ndryshimit apo heqjes së aksesit të përdoruesve të jashtëm dhe të brendshëm në infrastrukturën e IT të INSTAT-it, konstatohet se për vitin 2016 ka pasur një sasi të konsiderueshme shtimi heqje apo ndryshimi të përdoruesve në sistemet TI. Grupi i auditimit konstaton se kryerja pa formular i hapjes, mbylljes dhe ndryshimit të përdoruesve nuk siguron menaxhimin e sigurtë të procesit dhe krijon precedent që përdorues që kanë ndryshuar statusin të kenë të drejtë aksesi në sistemet e INSTATIT-t (*Sa më sipër trajtuar më hollësisht në faqet nr.4,13,15 të Raportit të Auditimit).*

Rekomandimi: Drejtoria e Teknologjisë së Informacionit INSTATIT të hartojnë, miratojnë e zbatojnë rregulla për hapjen dhe mbylljen e përdoruesve në sistemet e teknologjisë së informacionit, gjurmët e procesit procesit të dokumentohen.

Menjëherë dhe në vijimësi

6. Gjetje nga auditimi: Nga auditimi u konstatua se INSTAT-ti në mospërputhje me VKM nr. 710, dt. 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", si dhe praktikave më të mira të fushës nuk ka:

a. strategji të rimëkëmbjes nga katastrofat;

b. plane që përcaktojnë vazhdimësinë e proceseve, në rastet e dështimit të qendrës së të dhënave që suportojnë sistemet;

c. listë të testeve të BACKUP të kryera për vitin 2016.

d. listë të artikujve të vlerësuar prioritare për proceset emergjente

(*Sa më sipër trajtuar më hollësisht në faqet nr.14,15,16 të Raportit të Auditimit).*

Rekomandimi: INSTAT, të marrë masa të për të:

a. ndërtuar një strategji të rimëkëmbjes nga katastrofat;

b. kryerjen e vlerësimin e aseteve të Teknologjisë së Informacionit dhe hartimin e listës të artikujve prioritare për proceset emergjente;

c. të parashikojë dhe të realizojë investime me qëllim mundësimin e ofrimit të shërbimit pa ndërprerje dhe parandalimin e humbjes ose të shkatërrimit aksidental të të dhënave;

d. të hartojë Planin e Vazhdueshmërisë së Biznesit;

e. Të marri masa për krijim e ambienteve të testimit të BACKUP dhe kryeje testimet dhe dokumentimin e procesit.

Brenda 3 mujorit të parë të vitit 2018 dhe në vijimësi

7. Gjetje nga auditimi: Masat e ndërmarra për Sigurinë Fizike dhe Mjedisore të janë të pamjaftueshme, në kundërshtim me Rregulloren e AKSH-it mbi "Ndërtimin e Dhomës së Serverave", si dhe rregullores së dhomës së serverave, të miratuar nga vetë INSTAT-i.

Më specifikisht:

a. Mbajtja e temperaturës së ambientit në 17 gradë celcius nuk është në përputhje me Rregulloren e AKSH-it, pika 4.4/b, në të cilën ndër të tjera specifikohet "sistemi ftohës i dhomës ....duhet të vendosen në 22 gradë celcius";

b. Tipi i kondicionerëve të përdorur dhe vendosja e tyre nuk siguron mbajtjen e parametrave optimale dhe nuk favorizon qarkullimin natyral të ajrit;

c. Konsiderojmë me risk mbajtjen e sistemit të kondicionimit të qendërzuar në dhomën e serverave pavarësish mos përdorimit;

d. Nga verifikimi i mureve të dhomës së serverave u konstatua se nuk ishin të pajisur me skermo kundër emetimeve të valëve elektromagnetike (Kafazi Faraday), në kundërshtim kjo me pikën 4.1/c të Rregullores së AKSHI-t;

e. Prania e dritares nuk plotëson kushtet e përcaktuara sipas Rregullores së AKSH-it mbi Ndërtimin e Dhomës së Serverave pika 4.1/e dhe cënon sigurinë fizike të dhomës;

f. Ambienti nuk ishte i pajisur me sensorë për detektimin e lëvizjeve në kundërshtim me Rregullore e AKSH-it pika 4.6/b, në të cilën specifikohet "Hyrja në dhomë duhet të jetë e siguruar me anë të një sistemit elektronik dhe natyrisht duhet të ketë sistem alarmi në rast thyerje të saj";

g. Në dhomën e serverave u identifikuan objekte që nuk kishin lidhje me funksionin e saj, të tilla si:

h. Panel i energjisë elektrike i godinës i cili cënon sigurinë e ambientit.

i. Pajisje të vjetra jashtë funksionit të cilat ruheshin për efekt të mungesës së magazinimit.

j. Ekzistenca e objekteve që nuk kanë lidhje të drejtpërdrejtë me funksionimin e dhomës së serverave, lë hapësirë për ngarkesë të panevojshme të ambientit dhe rrit riskun e cënimit të sigurisë fizike.

k. Në këtë ambient, u konstatua një situatë kaotike e kabllimit, e cila vështirëson dhe rrit në mënyrë të panevojshme kohën e riparimit në rast defekti.

l. Nuk ka kamera sigurie e cila do mundësonte indentitikimin e personave të cilët aksesojnë dhomën e serverëve;

m. Hyrja në dhomën e servera nuk bëhet nëpërmjet akses kontrollit dhe regjistri i përdorur për regjistrimin e hyrjeve nuk plotëson rregullat si: vendosjen e numrit te faqes dhe vendosjen e vulës së institucionit në faqe (miratimin);

n. Sistemet nuk janë të mbrojtura nga dëme që mund të shkaktohen nga zjarri. (*Sa më sipër trajtuar më hollësisht në faqet nr.17,18 të Raportit të Auditimit).*

Rekomandimi: INSTAT për të rritur sigurinë fizike dhe logjike të dhomës se serverave në drejtim të uljes së riskut të aksesit të paautorizuar,vendosjes vetëm të pajisjeve të përcaktuara në këto ambiente, ngritjes se sistemeve të përshtatshme kondicionimi, ndarjes së sistemeve elektrike, vendosjes së sistemeve të mbrojtjes e sinjalizimit të marrë masa të dokumentuara për përmirësimin e kushteve në dhomat e serverave, duke analizuar dobësitë të hartohet një plan veprimi bazuar në specifikimet e rregullores së AKSHI-t "për ndërtimin e dhomës së serverave".

Brenda 3 mujorit të parë të vitit 2018 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 dhe Investimeve të Huaja. Ky vendim përcillet në formë rekomandimi në subjektin e auditimit.

Bujar LESKAJ

K R Y E T A R