KONTROLLI I LARTË I SHTETIT

KRYETARI

Adresa: Bulevardi "Dëshmorët e Kombit", Tiranë,Tel-Fax:042 232491

V E N D I M

Nr. 166 Datë 28/12/2016

PËR

EVADIMIN E MATERIALEVE TË AUDITIMIT TË TEKNOLOGJISË SË INFORMACIONIT TË USHTRUAR NË DREJTORINË E PËRGJITHSHME TË THESARIT DHE DREJTORINË E SHËRBIMEVE DHE TEKNOLOGJISË SË INFORMACIONIT NË MINISTRINË E FINANCAVE

Pasi u njoha me Raportin Përfundimtar të Auditimit dhe projektvendimin e paraqitur nga Grupi i Auditimit të Departamentit të Auditimit të Buxhetit Qendror, Administratës së Lartë Publike, Menaxhimit Financiar dhe Auditimit të Brendshëm, pasi u njoha me shpjegimet e dhëna nga subjekti i audituar, mendimin për cilësinë e auditimit nga Drejtori i Drejtorisë Juridike, Sigurimit të Cilësisë dhe Zbatimit të Standardeve, vlerësimin mbi objektivitetin dhe cilësinë e auditimit nga Drejtori i Departamentit të Auditimit të mësipërm, në mbështetje të nenit 10, 14 dhe 15 të ligjit nr.154/2014, datë 27.11.2014 *"Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit"*, duke vlerësuar përpjekjet dhe arritjet e Ministrisë së Financave për përdorimin e Teknologjisë së Informacionit si mjet për arritjen e stabilitetit ekonomik nëpërmjet drejtimit me eficiencë, efektivitet dhe transparencë të financave publike;

V E N D O S A:

I. Të miratoj Raportin Përfundimtar të Auditimit të Teknologjisë së Informacionit për periudhën 01.01.2015 - 31.12.2015 të ushtruar në Ministrinë e Financave, Drejtorinë e Përgjithshme të Thesarit dhe Drejtorinë e Shërbimeve dhe Teknologjisë së Informacionit.

II. Të miratoj rekomandimet e përcaktuara dhe të kërkoj marrjen e masave, për sa vijon:

OPINION I AUDITIMIT

Grupi i auditimit arrin në konkluzionin se Ministria e Financave megjithë përpjekjet e bëra nuk ka marrë masa të mjaftueshme rregullatore dhe organizative për garantimin e sistemeve të informacionit. Në gjykimin tonë, menaxhimi i elementëve kritikë në sistemet e informacionit, është i pa pamjaftueshëm dhe i pa përshtatshëm.
Investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht sigurimin e Vazhdueshmërisë së Biznesit dhe nuk kanë siguruar Rimëkëmbjen nga Katastrofat.

A. MASA ORGANIZATIVE

1. Nga auditimi i qeverisjes së IT u konstatua se MF nuk ka strategji për Teknologjinë e Informacionit, duke mos pasqyruar qartë objektiva lidhur me infrastrukturën, burimet e nevojshme si dhe indikatorë për matjen e objektivave. Mungesa e Planit Strategjik, mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së MF (*Sa më sipër trajtuar më hollësisht në faqet nr.4 të Raportit të Auditimit).*
Rekomandoj:

Strukturat drejtuese të MF, duke marrë në konsideratë kohën, burimet e nevojshme të marrin masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

2. Nga auditimi i politikave dhe procedurave IT në MF, u konstatua se Manuali IT i vitit 2015 është i pa miratuar. Drejtoria e Shërbimeve dhe Teknologjisë së Informacionit nuk disponon dokumentacion mbi: Regjistrat/loget e administratorit të rrjetit dhe rezultatet e analizave të logeve; Listën e informacionit të kategorizuar; Politikat dhe procedura referuar çështjeve të konfigurimit në fushën e operacioneve; Planin e sigurisë së ndërtesave ku shtrihet Sistemi Informatik Financiar i Qeverisë; Listën/matricën e aksesit; Listën e artikujve të cilësuar si prioritare për proceset emergjente; Procedurat për Planin e Vazhdueshmërisë së Biznesit dhe Rimëkëmbjes nga Katastrofat dhe procedurat e Testimit; Listën e testeve të kryera për vitin 2015 dhe rezultatet veprimet e ndërmarra. Mungesa e dokumentacioneve të mësipërme bën që institucioni të mos ketë të identifikuar risqet me efekt negativ në IT dhe veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura (*Sa më sipër trajtuar më hollësisht në faqet nr12 të Raportit të Auditimit).*
Rekomandoj:

Strukturat drejtuese në bashkëpunim me Drejtorinë e Shërbimeve dhe Teknologjisë së Informacionit të marrin masat për hartimin e dokumentacionit të nevojshëm për zbatimit të politikave e procedurave IT në MF.
Institucioni të identifikoje risqet me efekt negativ në IT dhe veprimet si reagim ndaj kërcënimeve duke i zgjidhur incidentet e ndodhura.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

3. Nga auditimi mbi menaxhimin e burimeve njerëzore në DPTH për vitin 2015 rezulton se ka pasur luhatje të vazhdueshme në Burimet njerëzore, shoqëruar me vende vakante të strukturës në disa prej pozicioneve të rëndësishme në Drejtori, mbart riskun e përmbushjes së misionit dhe

funksioneve kryesore si sigurimi dhe realizimin e shërbimeve operacionale, garantimi i parasë së gatshme për kryerjen e transaksioneve dhe pagesave.
Nga auditimi konstatohet se DPTH pa marrë në konsideratë natyrën specifike nuk ka hartuar politika të veçanta për rekrutimin e stafit. Përpjekjet për zhvillimin e kapaciteteve të stafit nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit gjatë vitit 2015 kanë qenë të pa mjaftueshme.
Nga auditimi i menaxhimit të burimeve njerëzore në DSTI për vitin 2015 rezulton se ka pasur luhatje të vazhdueshme në Burimet njerëzore me krijimin e vendeve vakant në disa prej pozicioneve të rëndësishme, zhvillimi i kapaciteteve të stafit nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit gjatë vitit 2015 kanë qenë të pa mjaftueshme.
Ndarja e detyrave në nivel sektorial është e njëjtë duke treguar formalizëm në hartimin e tyre. Mos menaxhimi i burimeve njerëzore përbën një risk në plotësimin e misionit të DSTI për sigurimin dhe realizimin e shërbimeve IT për qeverisjen e përgjithshme (*Sa më sipër trajtuar më hollësisht në faqet nr. 4 të Raportit të Auditimit).*
Rekomandoj:

Ministria e Financave të marrë masa për menaxhimin e burimeve njerëzore duke plotësuar vendet vakante dhe hartojë politika për zhvillimin e tyre nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

4. Nga auditimi i marrëveshjeve të nivelit të shërbimit për vitin 2015 rezulton se në DSTI dhe DPTH nuk ka patur suport mirëmbajtje e zhvillimi për disa nga sistemet, MF nuk ka ndërmarrë asnjë masë ndaj këtij risku. Në regjistrin e risqeve është caktuar si masë për minimizimin e këtij risku, zhvillimi i trajnimeve mbi TI. Por pavarësisht se është caktuar kjo masë, Grupi i auditimit konstaton se DSTI dhe DPTH për vitin 2015 kanë dobësi të theksuara në identifikimin, planifikimin dhe zhvillimin e trajnimeve, duke rritur vështirësinë e mirëmbajtjes së sistemeve (*Sa më sipër trajtuar më hollësisht në faqet nr.16, 34 të Raportit të Auditimit).*
Rekomandoj:

Ministria e Financave të marrë masa për kryerjen e analizave kosto-përfitim për suportet e nevojshme të sistemeve të Teknologjisë së Informacionit. Të hartojë politika për sigurimin e suporteve të nevojshme si dhe të zhvillojë burimet e brendshme nëpërmjet trajnimeve në lidhje e sistemeve, sigurinë dhe teknologjinë e informacionit.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

5. Nga auditimi i aplikacionit "Sistemi Informatik Financiar të Qeverisë" (SIFQ) të implementuar në Ministrinë e Financave gjatë vitit 2015 rezulton se Drejtoria e Përgjithshme e Tatimeve (Institucion Varësie) ka filluar zbatimin në kushtet reale të punës të sistemit të ri informatik tatimor. Pjesë e këtij procesi është edhe integrimi i këtij sistemi me SIFQ. Gjatë vitit 2015 nga SIFQ është dërguar informacion ditor mbi transaksionet e arkëtimeve të ardhurave tatimore për tu pasqyruar në Sistemin Informatik Tatimor.

Nga Drejtoria e Përgjithshme e Tatimeve, në drejtim të Drejtorisë së Thesarit, janë dërguar informacione të të dhënave të sistemit C@ST në formë të pjesshme, jo në afat dhe manualisht. Përpjekjet e Ministrisë së Financave si Institucion Qendror administrues i SIFQ për zgjidhjen e problematikave të shfaqura nuk kanë gjetur bashkëpunimin e duhur nga ana e Drejtorisë së Përgjithshme të Tatimeve duke shkaktuar një impakt konstant negativ në procesin e rakordimit dhe raportimit të treguesve fiskale të Qeverisë për vitin 2015 (*Sa më sipër trajtuar më hollësisht në faqet nr4,18 të Raportit të Auditimit.*
Rekomandoj:

Ministria e Financave si Institucion administrues i SIFQ të marri masa për koordinimit të veprimeve mes palëve të interesuara dhe dhënëse të informacionit nëpërmjet implementimit të politikave dhe procedurave për menaxhimin e ndryshimeve në sistemet dhe aplikacionet kryesore të IT.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

6. Nga auditimi i shkallës së sigurisë së aplikacionit konstaton se Sektori i Sigurisë së Sistemit të Informacionit të Drejtorisë së Shërbimeve dhe e Teknologjisë së Informacionit, nuk kryen procesin e monitorimit logimeve për ngjarjet e sigurisë së informacionit në sistemin SIFQ dhe infrastrukturën e tij (databaza Oracle dhe platforma Solaris UNIX), si edhe tek pajisjet e rrjetit (firewall, routers, switches etj). Pa loget dhe rishikimin periodik të logeve të sigurisë, aktivitetet e dyshimta që ndodhin në sistemin SIFQ ose në nivelin e rrjetit mund të kalojnë pa u vënë re (*Sa më sipër trajtuar më hollësisht në faqet nr.9, 10, 20 të Raportit të Auditimit).*
Rekomandoj:

Të merren masa për kryerjen procesit te monitorimit log-ve për ngjarjet e sigurisë së informacionit në sistemin SIFQ dhe infrastrukturën e tij (databaza Oracle dhe platforma Solaris UNIX), si edhe tek pajisjet e rrjetit (firewall, routers, switches, etj).

Brenda 3 mujorit të parë të vitit 2017 dhe në vijimësi

7. Nga auditimi i shkallës së aksesit të përdoruesve të jashtëm dhe të brendshëm në aplikacion "Sistemit Informatik Financiar të Qeverisë (SIFQ), sigurisë së tij dhe rëndësinë e informacionit që rrjedh prej tij grupi i auditimit konstaton se nuk ka një plan për ndryshimin e fjalëkalimeve të përdorueseve me të drejta të plota. Mungesa e ndryshimit të kriterit ose standardeve të fjalëkalimeve, rrit riskun e zbulimit të fjalëkalimeve dhe vjedhjen e tyre nga individë të pa autorizuar, duke përfituar akses në sistemet e informacionit (*Sa më sipër trajtuar më hollësisht në faqet nr.9, 21, 22 të Raportit të Auditimit).*
Rekomandoj:

Drejtoria e Shërbimeve dhe Teknologjisë së Informacionit (Sektori i Sigurisë së Sistemit të Informacionit) të përgatisë dhe paraqesë për miratim në Strukturat drejtuese një manual me politika të qarta mbi sigurinë e informacionit mbi ndryshimin e fjalëkalimeve të përdorueseve me të drejta të plota. Procesi i ndërimit të fjalëkalimeve të monitorohet në vazhdimësi.

Brenda 3 mujorit të parë të vitit 2017 dhe në vijimësi

8. Nga auditimi i **Planeve për Vazhdueshmërinë e Biznesit dhe Rimëkëmbjes nga Katastrofat** rezultoi se Ministria e Financave nuk ka të ndërtuar një strategji të rimëkëmbjes nga katastrofat si dhe nuk ka plane që përcaktojnë vazhdimësinë e proceseve në rastet e dështimit të qendrës së të dhënave primare (data center) që suportojnë sistemin SIFQ. Momentalisht Ministria e Financave nuk ka qendër të rimëkëmbjen nga katastrofat (DRC) për data centerin primar ku hostohen serverat e sistemit SIFQ dhe infrastrukturën e rrjetit. MF nuk disponon dokumentacione në lidhje me Planet e vazhdueshmërisë së punës (BCP) dhe rimëkëmbjes nga katastrofat (DRC), Procedurat e testimit dhe rezultatet e tyre sidhe veprimet e rekomandimet e ndërmarra. MF nuk ka listë të artikujve të vlerësuar prioritare për proceset emergjente (*Sa më sipër trajtuar më hollësisht në faqet nr.5,22 të Raportit të Auditimit).*
Rekomandoj:

Të merren masa për ndërtimin dhe hartimin e Planeve të Vazhdimësisë së Biznesit Rimëkëmbjen nga Katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat. Gjithashtu, të merren masa për hartimin e planit të sigurisë së informacionit dhe implementimi e tij duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në IT. Planifikimi dhe testimi i sistemeve IT të kryhet në përputhje me kërkesat për të cilat këto sisteme ndërtohen.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

9. Nga auditimi u konstatua se Procedura e backup për Sistemet e Informacionit në MF nuk janë në përputhje me VKM nr. 710, dt. 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", backup tek AKSHI kryhen manualisht vetëm në raste të veçanta.

Nuk u gjetën procedura të testimit të backup. Në Drejtorinë e Përgjithshme të Thesarit mbahen në PC e përdoruesve pa backup parashikime, analiza dhe të dhëna të tjera të rëndësishme në Excel dhe Word. Ky informacion mbart vlerë të shtuar dhe humbja e modifikimi i tyre mbart riskun e gabimeve dhe humbja e të dhënave për menaxhimin e aktivitetit të cash-it (*Sa më sipër trajtuar më hollësisht në faqet nr.24 të Raportit të Auditimit).*
Rekomandoj:

Të merren masa për kryerjen dhe testimin periodik të backup-it për sistemet, pajisjet kompjuterike dhe të dhënat.

Të merren masa për klasifikimin e të dhënave të rëndësishme që ndodhen jashtë sistemit, kalimin e tyre në server, mbulimin e tyre me backup.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

10. Nga Auditimi i **menaxhimit të risqeve në IT** u konstatua se nuk ka marrë masa të mjaftueshme për identifikimin dhe minimizimin e risqeve për:

a. Qendrën BCC si mekanizëm për vazhdimësinë dhe rikuperimin e Sistemit të Thesarit në raste sulmesh të jashtme apo fatkeqësish natyrore,
b. Vendndodhja e "datacenterit" në godinën e vjetër të ministrisë dhe ndërprerja e shpeshtë e energjisë elektrike;
c. Teknologjia e vjetërsuar e serverave ekzistues dhe ulja e performancës së tyre.
d. Memoria fizike e serverave është e ulët për shkak se janë pajisje të vjetra dhe me parametra të ulët me një jetëgjatësi 7 vjet .
e. Mos përshtatshmëria e sistemeve ekzistuese për shkak të vjetërsimit të tyre.
f. Kompleksiteti dhe vështirësia e mirëmbajtjes së sistemeve të reja që implementohen;
g. Dokumentim i papërshtatshëm i procedurave të TI dhe sistemeve ekzistuese dhe të reja;
h. Drejtoria e Shërbimeve dhe e Teknologjisë së Informacionit nuk ka një plan se si menaxhohen risqet e lidhura me projektet e investuara ku të përcaktohej, lista e risqeve, detyrat dhe përgjegjësitë për menaxhimin e risqeve.
i. Ministria e Financave nuk ka marrë masa për minimizimin përditësimi e regjistrit të risqeve (*Sa më sipër trajtuar më hollësisht në faqet nr.9,26 të Raportit të Auditimit).*
Rekomandoj:

MF të bëjë përditësimin dhe dokumentimin e regjistrit të risqeve IT dhe të marrë masa për hartimin dhe dokumentimin e një plani veprimi për minimizimin/ parandalimin e risqeve të identifikuara, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave nga Drejtoria TI.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

11. Nga Auditimi u konstatua se në MF nuk ekziston një procedurë e dokumentuar e identifikimit, trajtimit dhe raportimit të incidenteve. Mungesa e një procedure të menaxhimit të incidenteve sjell paqartësi dhe mangësi në trajtimin e tyre, njohjen e nivelit të riskut që kërcënime të përcaktuara mbartin për MF-në, nivelit të impaktit në veprimtarinë e MF-së, dokumentimin dhe zgjidhjen e tyre, e cila redukton kohën e zgjidhjes, në rast përsëritje të të njëjtit incident, etj (*Sa më sipër trajtuar më hollësisht në faqet nr.27 të Raportit të Auditimit).*
Rekomandoj:

MF të marrë masa për hartimin e një plani veprimi për identifikimin, raportimin, trajtimin, dokumentimin dhe monitorimin e incidenteve.

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

12. Nga Auditimi u konstatua se ambienti fizik i dhomës së rrjetit nuk është në përputhje me standarted e përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI (*Sa më sipër trajtuar më hollësisht në faqet nr. 5 të Raportit të Auditimit).*

Rekomandoj:

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

Brenda 6 mujorit të parë të vitit 2017 dhe në vijimësi

13. Nga auditimi i kërkesave dhe procesit të aprovimit të tyre si dhe hartimit të regjistrit të prokurimeve rezulton se analiza "kosto përfitim" për mbajtjen e shërbimeve nëpërmjet zhvillimit të burimeve të brendshme apo kalimit të tyre me MNSH ("outsourcing") nuk është zhvilluar. Nga audidimi u konstatua se në mospërputhje me VKM nr.710, datë 21.8.2013 mbi "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit" për vitin 2015 Drejtoria e IT-së nuk ka patur suport për disa nga sistemet në MF duke i krijuar vështirësi në mirëmbajtjen e sistemeve.

Në regjistrin e risqeve është caktuar si masë për minimizimin e këtij risku, zhvillimi i trajnimeve mbi TI. Por pavarësisht se është caktuar kjo masë për minimizimin e riskut, nuk janë zhvilluar trajnime. Nga maj 2014 deri më shtator 2015 nuk ka patur suport funksional. Shërbimi është kërkuar nga DPTH dhe është buxhetuar por procesi i tenderimit ka dështuar.

Gjatë kësaj periudhe ka patur problematika serioze në sistem edhe për vetë faktin e gjendjes së rënduar të makinerive të sistemit (HW). Kontrata Nr. 4330/16 datë 30.09.2015 me objekt "Shërbim Suporti AMOFTS (Oracle)" me kompaninë "Conaltus sh.p.k." ka paraqitur probleme në zbatimin e saj. Nga shtatori 2015 e në vazhdim SIFQ është pa suport funksional

Nga auditimi i procedurës së prokurimit "Krijimi i Sistemit të Informatizuar të Menaxhimit të Dëmshpërblimeve të Ish të Përndjekurve Politikë" për krijimin e Sistemit të Informatizuar të Menaxhimit të Dëmshpërblimit të ish të Përndjekurve Politik dhe MNSH për 4 (katër) vite rezultoi kontrata është hartuar në përputhje me udhëzimin 1119 datë17.3.2014, të Ministrit të Shtetit për Inovacionin dhe Administratën Publike pa marrë në konsideratë ndryshimin që i bën këtij Udhëzimi Nr. 4099, datë 3.11.2014 Pikës 5 të udhëzimit nr. 1159, "pika 5. "5.MNSH-ja për pajisjet hardware, aplikacionet, licencat ose kombinimet e tyre duhet të fillojë me njëherë nga momenti i marrjes në dorëzim nga porositësi të pajisjes hardware, të aplikacionit, licencës apo kombinimit të tyre. Garancia për pajisjet hardware është me kohë zgjatje minimale 1-vjeçare." Për rrjedhojë AK ka filluar mirëmbajtjen pasi ka përfunduar garancia e cila ka shërbyer edhe si suport. Konstatohet mosrakordim në kohë i MF me Agjencinë Kombëtare Shoqërisë së Informacionit për kalimin online të shërbimit.

Konstatohet një bashkëpunim i pa mjaftueshëm midis Drejtorisë së Pagesave dhe Dëmshpërblimeve dhe Drejtorisë së Shërbimeve dhe Teknologjisë së Informacionit për shfrytëzim i gjithë kapaciteteve që ofron programi në drejtim të gjenerimit të raporteve dhe statistikave (*Sa më sipër trajtuar më hollësisht në faqet nr. 32 të Raportit të Auditimit).*

Rekomandoj:

MF në cilësinë e Autoritetit Kontraktor, kryejë analizën "kosto përfitim" për përcaktimin e shërbimeve që do mbahen nga burimet e brendshme dhe atyre që do kalojnë me MNSH ("outsourcing").

Të kihet parasysh që në të ardhmen në hartimin dhe zbatimin e projekteve të teknologjisë së informacionit të kryejë azhornimin e nevojshëm të dokumentacionit të prokurimit në përputhje me ndryshimet ligjore në fuqi.

MF të marri masa për rritjen e bashkëveprimit ndërinstitucional në përputhje me politikat dhe strategjitë për parashikimin dhe koordinimit e investimet në fushën e IT, si dhe kalimin online të shërbimit të Sistemit të Informatizuar të Menaxhimit të Dëmshpërblimeve të Ish të Përndjekurve Politikë.

Marrjen e masave për shfrytëzim i gjithë kapaciteteve që ofrojnë investimet e kryera.

Brenda 3 mujorit të parë të vitit 2017 dhe në vijimësi

Me ndjekjen dhe kontrollin e zbatimit të detyrave dhe masave të përcaktuara në këtë vendim ngarkohet Departamenti i Auditimit të Buxhetit Qendror, Administratës së Lartë Publike, Menaxhimit Financiar dhe Auditimit të Brendshëm.

Bujar LESKAJ

K R Y E T A R