MBI AUDITIMIN E USHTRUAR NË AGJENCINË E KONTROLLIT TË BARNAVE DHE PAJISJEVE MJEKËSORE (AKBPM) "MBI VLERËSIMIN E SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT, PËR PERIUDHËN 01.01.2014 - 31.12.2014

Ky auditim është produkt i pjesëmarrjes së Grupit të Auditimit në programin e IDI-t (Iniciativa për zhvillim e INTOSAI-t) për zhvillimin e Auditimit IT në Institucionet Supreme të Auditimit, dhe mbështetet në Manualin e Auditimit të IT dhe ISSAI 5310 "Metodologjia e Rishikimit të Sigurisë së Sistemeve të Informacionit".

Auditimi është kryer në bazë të programit të auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit nr. 1039/3, datë 19.01.2015.

Raporti Përfundimtar i Auditimit të ushtruar në Agjencinë e Kontrollit të Barnave dhe Pajisjeve Mjekësore (AKBPM), me objekt "Vlerësimin e Sistemeve të Teknologjisë së Informacionit, për periudhën për periudhën 01.01.2014 - 31.12.2014, si dhe masat për përmirësimin e gjendjes, janë miratuar me Vendim të Kryetarit të KLSH-së Nr. 82, datë 20.06.2015. Bazuar në nenet 15, 25, 30 dhe 32 të ligjit nr. 154/2014, datë 27.11.2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit", për përmirësimin e gjendjes, me shkresën nr. 1039/25, datë 20.06.2015, Raporti Përfundimtar i Auditimit dhe rekomandimet përkatëse i janë dërguar znj. Ornela Ymeraj, Drejtor i Agjencisë së Kontrollit të Barnave dhe Pajisjeve Mjekësore, ku janë rekomanduar dhe kërkuar zbatimi i masave të mëposhtme:

1. Gjatë auditimit u konstatua se ka planifikime të dobëta strategjike, mungesë e planeve të shkruara mbi implementimin e teknologjisë në agjenci, implementimi i shërbimit për faqen web, nuk është dokumentuar si duhet nga agjencia edhe nga operatori. Nga auditimi i faqes së internetit regjistruar me domain-in *akbpm.gov.al* kryer sipas procedurave të urdhrit të prokurimit nr. 18. dt 12.09.2014 konstatohet se ka probleme në Aksesimin e faqes dhe probleme me lidhje të shkëputura. Këto problematika, kanë ardhur si pasojë e mungesës së planifikimit strategjik në drejtim të fushës së teknologjisë së informacionit. Si pasojë e kësaj, konstatohet edhe mosplanifikimi i vazhdueshmërisë së këtij shërbimi, duke e lënë faqen e internetit në kushtet e mosfunksionimit total (*trajtuar më hollësisht në faqet 11-12, të Raportit Përfundimtar të Auditimit*).

Për sa më sipër është rekomanduar:

Referuar rëndësisë dhe kostove për prokurimet e kryera në fushën e teknologjisë së informacionit, rekomandojmë që AKBPM të marrë masa për hartimin e planit strategjik IT, të zbatojë në përputhje me të implementimin e investimeve në fushën e IT, si dhe të specifikojë procedura të monitorimit, për të shmangur risqet e lidhura me vazhdueshmërinë së infrastrukturës teknologjike.

Brenda vitit 2015

2. Nga auditimi i qeverisjes së teknologjisë së informacionit u konstatua se:

a. Nuk ekziston një strukturë qeverisëse, strategjike, e cila do të kompletonte praktikat menaxhuese aktuale dhe do të ndihmonte në arritjen e objektivave të veprimtarisë së subjektit,
b. Nuk janë marrë masa për ngritjen e Grupit të Menaxhimit Strategjik, i cili në bazë të Ligjit të Menaxhimit Financiar dhe Kontrollit, do të kishte në përbërje të tij, një specialist të fushës së teknologjisë së informacionit në institucion, i cili do të ishte pjesë e vendimmarrjes qoftë e institucionit, qoftë edhe e aspekteve që lidhen me IT.
Mungesa e një Strategjie të teknologjisë së informacionit në AKBPM, sjell një risk të lartë për asetet që ajo posedon, për informacionin që përpunon, për të dhënat që ruhen në të, për të cilat nuk garantohet vazhdueshmëria në rast të ndodhjes së aktiviteteve me karakter negativ. Përshkrimet e punës nuk i nënshtrohen verifikimeve apo rishikimeve periodike të kryera nga eprorët e linjës, si dhe nuk është bërë vlerësimi vjetor i punës për çdo punonjës.

Prania e strukturës së IT, larg vendimmarrjes si dhe e pa plotësuar me personel lë hapësira për risk të paidentifikuar, të pamatur, pasojat e të cilit nuk mund të evidentohen. Gjithashtu u konstatua se, për ruajtjen dhe zhvillimin e kompetencave profesionale të punonjësve gjatë vitit 2014, në agjenci nuk janë organizuar trajnime për rritjen e kapaciteteve profesionale të punonjësve në fushën e IT, në kundërshtim kjo me Manualin për Menaxhimin Financiar dhe Kontrollin, Kap. II, pika 2.5.1.

Në aktet e auditimit nuk vërehen elemente të auditimit të Teknologjisë së Informacionit. Misioni i auditimit vëren se nuk janë hartuar gjurmët e auditimit të detajuara për procedurat kryesore, bazuar në gjurmët standarde të emetuara nga Ministria e Financave. Nuk janë identifikuar me emërtimin "Lista e proceseve të punës", nuk ka miratim dhe arkivim të kësaj gjurme, veprime këto në mospërmbushje të kërkesave të nenit 16, pika 2 dhe 3 të ligjit nr. 10296 datë 8.7.2010 "Për menaxhimin financiar dhe kontrollin" dhe të detyrimeve të kapitullit III të "Manualit për Menaxhimin Financiar dhe Kontrollin", miratuar nga Ministri i Financave me Urdhrin nr. 54, datë 15.07.2010.
Menaxherët e njësisë nuk zotërojnë informacion të mjaftueshëm për qëllimet dhe rëndësinë e menaxhimit financiar dhe të kontrollit, nuk është respektuar nga të gjithë hallkat e njësisë dhe se, institucioni nuk ka kryer trajnime për kuptimin dhe zbatimin e ligjit.
Njësia nuk ka hartuar një procedurë për mbledhjen dhe dokumentimin e gabimeve dhe analizën e tyre. Nuk ekziston një protokoll i brendshëm për korrespondencat midis strukturave lart-poshtë e paralel, apo raportimet e kryera në nivelin e lartë të strukturave. Mos kryerja e këtyre veprimeve përbëjnë risk në këtë institucion pasi nuk lihen gjurmë për auditimin e veprimtarisë të nëpunësve të këtij Institucioni (*trajtuar më hollësisht në faqet14-16, të Raportit Përfundimtar të Auditimit*).

Për sa më sipër është rekomanduar:

Institucioni të marrë masa për implementimin e ligjit të Menaxhimit Financiar dhe Kontrollit në drejtim të misionit të fushës së teknologjisë së informacionit dhe ndërlidhjes së kësaj fushe me objektivat e veprimtarisë së AKBPM-së; identifikimit të risqeve; parashikimit të veprimeve të përshtatshme të kontrollit sistemet e IT; hartimit të gjurmëve të auditimit; hartimit të planeve të trajnimit për rritjen e kapaciteteve profesionale në fushën e IT, identifikimit të "Listës së proceseve të punës"; vendosja e një strukture IT në institucion e shoqëruar nga përshkrimet e punës si dhe ndarjet e detyrave si dhe ngritja e Grupit të Menaxhimit Strategjik, në përbërje të të cilit të jetë një specialist i IT, në përputhje me Ligjin për menaxhimin Financiar dhe Kontrollin. Zbatimi i Ligjit të Menaxhimit Financiar dhe Kontrollit në fushën e teknologjisë së informacionit, sjell më pranë vendimmarrjes sektorin e IT-së.

Menjëherë

3. Nga auditimi në agjenci, u konstatua mungesë e praktikave dokumentare lidhur me sistemin e regjistrimit dhe ruajtjes së të dhënave të barnave, mungesë e marrëveshjeve ose kontratave të lidhura për përfitimin e këtij aplikacioni. Gjithashtu, u konstatua se kompjuterat që kryejnë regjistrimin e të drejta administratori në sistemin operativ. Nisur nga kjo, punonjësit me akses të pakontrolluar në kompjuter, mund të shkarkojnë programe të ndryshme nga interneti, duke dëmtuar së pari memorien e kompjuterit (duke e zënë hapësirën me regjistrat për programet e shkarkuara), më tej duke zënë kohën dhe fuqinë e procesorit të kompjuterit, si dhe së fundmi duke i dhënë mundësinë programeve me ndikim negativ (malware) të depërtojnë në kompjuter, dhe të modifikojnë ose të shkatërrojnë të dhënat e ruajtura aty, si dhe në rastin më të keq duke ndërhyrë në disponibilitetin dhe integritetin e të dhënave të ruajtura në program. Në agjenci nuk ka ndarje formale detyrash dhe përgjegjësish lidhur me sistemin e regjistrimit, duke lënë hapësirë procedurale për mbingarkesë funksionesh dhe kryerje detyrash të pacaktuara (*trajtuar më hollësisht në faqet16-21, të Raportit Përfundimtar të Auditimit*).

Për sa më sipër është rekomanduar:

-AKBPM të marrë masa për dokumentimin e programeve kompjuterik që shërbejnë për zhvillimin e proceseve të ndryshme të punës së institucionit;

- Specifikimi i personave përgjegjës për përdorimin e programit, monitorimin e tij, specifikimi i të drejtave të përdoruesve të programit si dhe të sistemit operativ në kompjuterat ku është instaluar program aplikativ.

Në vijimësi

4. Nga auditimi i inputeve dhe outputeve të programit aplikativ mbi regjistrimin e barnave, u konstatua se: Agjencia nuk ka të hartuara politika për personat e autorizuar për të hyrë në program, kohëzgjatjen e aksesimit të programit, politika për anulimin e llogarive në program. Ekzistojnë ende 2 llogari të hapura për dy ish-punonjës të agjencisë, të cilët kanë kohë që kanë shkëputur marrëdhëniet e punës me agjencinë.

Për këtë program, agjencia nuk disponon një përshkrim formal të të dhënave që regjistrohen dhe të të dhënave që përpunohen, nuk ekzistojnë mekanizma të kontrollit të inputeve që hyjnë në program, mungojnë kontrolle të evidentimit të rekordeve të duplikuara.

Përsa i përket output-eve që gjenerohen nga ky aplikacion, ato përmbajnë dokumente administrative në funksion të institucionit, të tilla si autorizime importi, autorizim zhdoganimi, autorizim përdorimi të barnave. Ky proces i gjenerimit të output-IT, së pari nis me nxjerrjen e dokumenteve, të cilat më tej ekstraktohen me memorie të jashtme, dhe printohen në tjetër vendndodhje, kjo për shkak të mungesës së lidhjes midis terminaleve ku ruhet programi, dhe printerëve. Ky veprim lë hapësirë për tjetërsimin e informacionit të gjeneruar nga programi.

Duhet theksuar se agjencia nuk përmban politika ose procedura të shkruara se cilat janë output-et e gjeneruara nga programi, dhe se cilët janë personat përgjegjës për marrjen dhe posedimin e këtyre dokumenteve. Mungesa e politikave dhe procedurave të shkruara lidhur me programin, sjell edhe mungesën e verifikimit të vlefshmërisë së raporteve të gjeneruara (dokumenteve zyrtare), duke dhënë mundësinë e gjenerimit të autorizimeve me të dhëna jo të sakta.

Nga auditimi i output-eve të programit, u konstatua se agjencia nuk disponon politika të shkruara të trajtimit të dokumenteve jo të sakta, duke mos lënë hapësirë për auditimin dhe kontrollin e këtyre output-eve, për të verifikuar eficencën dhe efektivitetin e gjenerimit të autorizimeve (*trajtuar më hollësisht në faqet 16-18, të Raportit Përfundimtar të Auditimit*).

Për sa më sipër është rekomanduar:

Të merren masa për hartimin e politikave dhe procedurave standarde për specifikimin e kritereve për të gjitha inputet dhe outputet që gjenerohen nga programet të cilat funksionojnë aktualisht dhe në të ardhmen në AKBPM; llojin e të dhënave që futen në program; të merren masa të përcaktohen personat përgjegjës për futjen e të dhënave, marrjen në dorëzim të output-eve, si dhe të hartohen procedura të shkruara për trajtimin e problemeve dhe pengesave të hasura gjatë futjes së të dhënave ose gjenerimit të outputit.

Menjëherë

5. Nga auditimi i sigurisë logjike, u konstatua se agjencia nuk disponon procedura rishikimi të sigurisë së aplikacionit, logfilet regjistrohen në Server, dhe këto logfile nuk janë hapur asnjëherë, sepse nuk ka qenë e nevojshme; nuk janë hasur asnjëherë shkelje të sigurisë, konstatim i cili nuk mund të verifikohet, pasi agjencia nuk mban procesverbale të rregullta, mujore ose periudhe tjetër, me anë të të cilave do të konkludohej mbi statistikat dhe eficencën e sigurisë.

Gjithashtu, agjencia nuk disponon plane të trajtimit të katastrofave, duke rritur në këtë mënyrë riskun e humbjes ose tjetërsimit të të dhënave të ruajtura në program; nuk posedon marrëveshje në nivel shërbimi (SLA), ose kontrata të ndryshme lidhur me aplikimin, backup-i i të dhënave kryhet ne mungesë të planeve dhe procedurave të shkruara.

Ambienti në të cilin mbahet ky aplikim nuk plotëson standardet e përcaktuara nga AKSHI për ndërtimin e dhomës se serverëve (ambientet janë magazina pa nivele sigurie, pa ventilim e sinjalistikën e përcaktuar së bashku me barna e materiale të tjera pa lidhje funksionale me shërbimet e IT). Gjithsesi, mbajtja e të dhënave brenda institucionit, mbart riskun e humbjes së disponibilitetit dhe integritetit të të dhënave, në rast të ndodhjes së katastrofave ose shkatërrimeve të qëllimshme dhe jo të qëllimshme (aq më tepër që agjencia nuk ka një plan sigurie të shkruar të ndërtesës).

Agjencia nuk ofron trajnime ose programe ndërgjegjësimi për mbrojtjen e të dhënave si dhe reagimin në rast të katastrofave të mundshme, duke rritur riskun e mosdijes së veprimeve për tu kryer nga punonjësit. Testime të integritetit dhe të disponibilitetit të të dhënave janë kryer në mënyrë vullnetare, por nuk janë dokumentuar.

U konstatua mungesa e manualeve të përdorimit, të ndihmës online, të një qendre helpdesk-u. Nevojat për ndihmë, ose për rregullime të konfigurimeve të sistemit, bazohen në raste emergjente, të cilat nuk dokumentohen dhe nuk rishikohen. E drejta për kryerjen e veprimeve të mësipërme, në funksion të ndihmës, është e specialistit të IT (*trajtuar më hollësisht në faqet24-25, të Raportit Përfundimtar të Auditimit*).

Për sa më sipër është rekomanduar:

Institucioni të marrë masa për nxjerrjen e rregullores së sigurisë IT, të kryejë monitorimin e sigurisë dhe trajtimit të incidenteve dhe problemeve të konstatuara në aplikimin e barnave, të evidentojë procesin për zgjidhjen e problemeve të ngjashme në të ardhmen.

Në vijimësi

6. Nga auditimi i informacioneve rezultoi se Agjencia nuk ka Strategji të IT dhe nuk kuptohet sa duhet roli kritik i Sigurisë së Informacionit; nuk ka plan të sigurisë së IT, regjistër risqesh dhe nuk kryhet menaxhimi i riskut; agjencia nuk analizon rastet e incidenteve të sigurisë dhe ka shkallen e ulet të kuptimit e menaxhimit sigurisë ne institucion; kuk ka rregulla të brendshme,

referuar sigurisë së sistemeve të informacionit (*trajtuar më hollësisht në faqet 12-13,22-23, të Raportit Përfundimtar të Auditimit*).

Gjithashtu, mungesa në staf dhe mungesa e strukturës IT si njësi më vete paraqet risk potencial në kryrjen e detyrave të sigurisë; nuk ka gjurmë të analizimit të sigurisë në raportet, analizat apo auditimet e brendshme; nuk ka politika formale dhe të shkruara të sigurisë së informacionit dhe komunikimin, përdoruesit e rrjetit kompjuterik kanë të drejta të pa kufizuara dhe nuk përdoret menaxhimi i përqendruar i të drejtave.

Përdorimi i postës private ne sistemit të agjencisë për qëllime pune; Rregullorja Brendshme ekzistuese është e vitit 2006, nuk ka analiza e raporte të incidenteve nga ndërhyrje nga jashtë e nga brenda, rrjeti kompjuterik është i organizuar pa infrastrukturën e konfigurimin e nevojshëm për të mundësuar monitorimin nuk mjete për monitorimin dhe analizimin e rrjetit; nuk kryhet analizim e raportim të bllokimeve sulmeve nga brenda e jashtë.
Kontrolli i statistikave të bllokimeve dhe sulmeve. Pajisjet e rrjetit shtrihet në ambiente që nuk kanë lidhje me funksionin e pajisjeve të vendosura aty; konstatojmë se AKBPM nuk ka zbatuar standardet e AKSHIT në ndërtimin e rrjetit kompjuterik dhomës së Serverëve dhe komunikimit i cili shtrihet në godinë në ambiente të pa përshtatshme e pa sigurinë e duhur në drejtim të sigurisë për të përmbushur objektivat e AKBPM; nuk ekzistojnë mjete dhe kontrolle mjedisorë (ndaluesi i zjarrit, alarmet, sistemet e energjisë.

Për sa më sipër është rekomanduar:

Institucioni të marrë masa për krijimin e strukturës së përshtatshme teknologjike dhe logjike në mënyrë që të garantohet integriteti, konfidencialiteti, plotësia dhe saktësia e të dhënave. Për këtë:

- Përmirësimi i Rregullores së Brendshme të AKBPM, duke shtuar edhe elementë për garantimin e sigurisë së Informacionit si dhe infrastrukturës teknologjike.
- Plotësimi i strukturës se IT me personelin e përcaktuar ne organike.
- Shtimi i funksioneve në përshkrimet e punës së personelit të IT, referuar sigurisë së informacionit
- Marrja e masave për njohjen dhe zbatimin e standardeve dhe specifikimeve teknike të Agjencisë Kombëtare të Shërbimit Informativ.

Në vijimësi

7. Nga auditimi i sistemit back-up, planit të vazhdueshmërisë në rast katastrofe dhe shërbimet e kontraktuara, u konstatua se Back up nuk përfshin të gjitha pajisjet, të dhënat dhe programet aplikativë kritikë; siguria dhe kushtet e këtyre ambienteve ku ruhet Back up nuk plotësojnë kushtet e përshtatshme të përcaktuara në Agjencinë Kombëtare të Shërbimit Informativ; auditimi nuk gjeti dokumentacion mbi testime të procedurave back up; agjencia nuk ka plane te rimëkëmbjes nga katastrofat; sistemi i furnizimit me energji i rrjetit kompjuterik i pa ndarë nga pajisjet e tjera të godinës komprometon dhe nuk garanton vazhdimësinë e punës në AKBPM.
Gjithashtu u konstatua se vendi i ruajtjes së backup së bashku me mallra e pajisje të tjera pa siguri fizike dhe rruajtje nga zjarri; auditimi e cilëson me risk me nivel te lartë mbajtjen në sheet-e Excel të llogarive e kontabilitetit të institucionit e mos përdorimi programit financiar të kontabilitetit; agjencia nuk te përcaktuar ne SLA për mirëmbajtjen e faqes se internetit dhe postes elektronike procedurat e backup te tyre, nuk u gjeten procedura te kryerjes se tyre dhe

testimeve përkatëse (*trajtuar më hollësisht në faqet24-25, të Raportit Përfundimtar të Auditimit*).

Për sa më sipër është rekomanduar:

Për garantimin e vazhdueshmërisë së infrastrukturës teknologjike e cila të përmbushë kërkesat e veprimtarisë së AKBPM-së, të merren masa për hartimin e planeve të backup-it dhe të rimëkëmbjes nga katastrofat. Gjithashtu procedurat e implementimit të këtyre planeve të përfshijnë pozicionimin e të dhënave të ruajtura në vendndodhje të sigurta, dhe larg institucionit.

Menjëherë

III. Në përfundim të vlerësimit të Raportit të Auditimit të IT në AKBPM nga IDI-n (Iniciativa për zhvillim e INTOSAI-t, gusht 2015) rekomandimet dhe ky raport do ti vihen në dispozicion Ministrisë të Shëndetësisë ose dhe Komisionit të Shëndetësisë në Kuvendin e Shqipërisë.

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.

Auditimi është kryer nga:

Shënim: Auditimi u krye përgjatë periudhës 20.01.2015 deri më 25.04.2015 nga audituesit Kozma Kondakçiu, përgjegjës grupi, Armanda Bega Lolita Baholli, Yrjada Jahja, më tej materiali u shqyrtua nga Kryeaudituesi z. Alush Zaçe, Drejtori i Drejtorisë Juridike dhe Zbatimit të Standardeve z. Ermal Yzeiraj, si dhe nga Drejtori i Departamentit zj. Manjola Naço.

KONTROLLI I LARTË I SHTETIT