



KONTROLLI I LARTË I SHTETIT
RAPORT PËRFUNDIMTAR PËR AUDITIMIN E USHTRUAR NË AGJENCINË
E PROKURIMIT PUBLIK

RAPORT PËRFUNDIMTAR AUDITIMI



MBI AUDITIMIN E “SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT” NË “AGJENCINË E PROKURIMIT PUBLIK”

Tiranë, Qershor, 2022

PËRMBAJTJA

Nr.	EMËRTIMI	Faqe
I.	PËRMBLEDHJE EKZEKUTIVE	4
1	Përshkrim i shkurtër i Projektit të Auditimit	4
2	Përshkrim i gjetjeve kryesore dhe rekomandimeve	5
3	Konkluzioni i përgjithshëm dhe Opinioni i Auditimit	7
II.	HYRJE	7
1	Objekti i auditimit	7
2	Qëllimi i auditimit	7
3	Identifikimi i çështjes	8
4	Përgjegjësitë e strukturave drejtuese të subjektit të audituar	8
5	Përgjegjësitë e audituesve	8
6	Kriteret e vlerësimit	9
7	Standardet e auditimit	9
8	Metoda e auditimit	10
9	Dokumentimi i auditimit	10
III.	PËRSHKRIMI I AUDITIMIT	10
1	Informacioni i përgjithshëm mbi subjektin nën auditim	10
2	Përshkrimi i rezultateve sipas drejtimeve të auditimit	10
2.1	Auditimi i funksionimit të Qeverisjes TIK	10-23
a.	<i>Verifikimi i Strategjisë, politikave dhe burimeve njerëzore në TIK.</i>	
b.	<i>Identifikimi dhe menaxhimi i risqeve në TIK dhe në ofrimin e shërbimit.</i>	
2.2	Auditimi i sigurisë së informacionit	23-38
a.	<i>Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit</i> <i>Kontrolli i shkallës së sigurisë së aplikacioneve, të drejtat e përdoruesve dhe menaxhimi i tyre.</i>	
2.3	Auditimi i zhvillimit dhe blerjes në teknologjinë e informacionit	38-44
a.	<i>Marrëveshjet e Nivelit të Shërbimit (Service Level Agreement)</i>	
2.4	Auditimi i sistemeve	44-46
a.	<i>Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output</i>	
IV.	GJETJET DHE REKOMANDIMET	48-53

LISTA E SHKURTIMEVE

Shkurtimi	Emërtimi i Plotë
KLSH	Kontrolli i Lartë i Shtetit
RSH	Republika e Shqipërisë
APP	Agjencia e Prokurimit Publik
SPE	Sistemi i Prokurimit Publik
AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit
AKCESK	Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
BCP	Business Continuity Plan
ALCIRT	Agjencia Kombëtare për Sigurinë Kibernetike
BCC	Business Continuity Center
MNSH	Marrëveshjeve Nivel Shërbimi
AK	Autoriteti Kontraktues
OE	Operator Ekonomik
TI(IT)	Teknologjia e Informacionit
TIK	Teknologjia e Informacionit dhe Komunikimi
VKM	Vendim i Këshillit të Ministrave
KM	Këshilli i Ministrave
PBB	Produkti i Brendshëm Bruto
COBIT	Objektivat e Kontrollit për Informacionin dhe Teknologjinë përkatëse
INTOSAI	Organizata Ndërkombëtare e Institucioneve Supreme të Auditimit
ISSAI	Standardet Ndërkombëtare të Institucioneve Supreme të Auditimit
BE	Bashkimi Evropian
SSL	Secure Sockets Layer
VPN	Virtual Private Network
LAN	Local area network
IP	Internet Protocol

1.PËRMBLEDHJE EKZEKUTIVE

Kontrolli i Lartë i Shtetit (KLSH) mbështetur në nenet 3 dhe 14 të ligjit 154 “Për Organizimin dhe Funksonimin e Kontrollit të Lartë të Shtetit”, datë 27.11.2014, zhvilloi një Auditim të Teknologjisë së Informacionit në Agjencinë e Prokurimit Publik, nga data 12.01.2022 deri më datë 08.04.2022.

Grupi i auditimit mblodhi informacione, zhvilloi pyetësorë e intervista për caktimin e zonave me risk të lartë dhe mbështetur në to hartoi matricat e auditimit.

Kërkesat për informacion për fushat përkatëse u hartuan në përputhje me manualin e Auditimit të Teknologjisë së Informacionit.

I.1. Përshkrim i shkurtër i Projektit të Auditimit

Projekti i auditimit, për auditimin e Sistemeve të Teknologjisë së Informacionit, në Agjencinë e Prokurimit Publik, është pjesë e Planit Vjetor 2022 të auditimit të KLSH-së, miratuar nga Kryetari i KLSH. Projektimi i këtij auditimi, është bërë bazuar në një analizë risku, si gjatë hartimit të planit vjetor, po ashtu edhe gjatë hartimit të Programit të Projektit të Auditimit, ku KLSH, ka vlerësuar si të rëndësishëm auditimin e sistemeve të teknologjisë që Agjencia e Prokurimit Publik disponon, për të garantuar disponibilitet dhe integritet të të dhënave. Nga ana e subjekteve (APP dhe AKSHI) janë përcjellë në KLSH dy kopje të Projektraportit të auditimit të shoqëruar me deklaratën e nënshkruar nga titullari i institucionit. Nga grupi i auditimit janë shqyrtuar observacionet e dërguara mbi akt konstatimet dhe projektraportin e auditimit. Në konsideratë janë marrë ato kundërshti për të cilat janë paraqitur dokumentacion shtesë, ndërsa për rastet e tjera të cilat nuk gjejnë argumentim, mangësitë gjejnë pasqyrim në këtë Raport Përfundimtar Auditimi. Mbështetur në punën audituese në terren, evidencat e marra kanë qenë të mjaftueshme dhe të besueshme për punën audituese, mbështetur në Projektraportin e auditimit, komentet e subjektit të audituar, qëndrimin e grupit të auditimit ndaj komenteve të subjektit, rezultatet kryesore të punës audituese përfshihen në këtë përmbledhje ekzekutive të Raportit Përfundimtar. Auditimi i sistemeve të Informacionit është e rëndësishme për institucionet, kjo si pasojë e rritjes së kompleksitetit të kontrollit të aksesit dhe ruajtjes së konfidencialitetit, integritetit dhe gatishmërisë së të dhënave nga marrëdhëniet e rrjeteve publike me ato private dhe nga bashkë përdorimi i burimeve të informacionit. Siguria e Informacionit përcaktohet si mundësia e një sistemi për të mbrojtur informacionin dhe burimet e sistemeve në përputhje me termat e konfidencialitetit, integritetit dhe gatishmërisë. Sistemet e informacionit janë bashkime komplekse të teknologjisë, proceseve dhe njerëzve që funksionojnë së bashku për të rregulluar përpunimin, ruajtjen, dhe transferimin e informacionit për të mbështetur misionin e institucionit dhe funksionet e tij. Lidhur nga sa më sipër, çdo institucion shtetëror që ofron shërbime ndaj qytetarëve e ka si detyrim ndërtimin e programit të sigurisë së informacionit me elementët kyç të cilët janë: “Mjedisi i sigurisë së informacionit, Vlerësimi i riskut, Politikat e sigurisë, Organizimi i sigurisë së TIK, Menaxhimi i aseteve, Siguria e burimeve njerëzore, Siguria fizike dhe mjedisore, Kontrolli i aksesit, Menaxhimi i incidenteve të sigurisë së TIK, Menaxhimi i vazhdueshmërisë së biznesit, Përputhshmëria”.

I.2. Përshkrim i gjetjeve kryesore dhe rekomandimeve:

Gjetje nr.	Përmbledhje e Gjetjes	Referenca me Raportin Përfundimtar	Rëndësia	Rekomandimi
1.	<p>Nga auditimi u konstatua se :</p> <p>-Sektori i TI atashuar në APP është në mungesë të përgjegjësit dhe 1 (një) specialisti. AKSHI me shkresën nr.785 Prot., datë 04.02.2020 ka caktuar vetëm një specialist TI në APP, strukturë kjo e cila vazhdon ende të funksionojë si e tillë, duke sjell risk në mos përmbushje të objektivave institucionale.</p> <p>Rregullorja e Brendshme nuk është përshtatur (<i>amenduar</i>) duke mos reflektuar ndryshimet institucionale të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “<i>Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit</i>”, i ndryshuar, si dhe ri-organizimin e strukturës në Agjencinë e Prokurimit Publik</p>	faqe 10-23	E Lartë	<p>-Agjencia Kombëtare e Shoqërisë së Informacionit të marrë masa të menjëhershme për plotësimin e vendeve vakante të sektorit IT atashuar në APP.</p> <p>-Struktura drejtuese të Agjencisë Kombëtare të Shoqërisë së Informacionit të marrin masa për miratimin e akteve rregullative në përputhje me përcaktimet ligjore dhe nënligjore me qëllim reflektimin e ndryshimeve institucionale, strukturore dhe kompjuterike të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “<i>Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit</i>”, i ndryshuar.</p>
2.	<p>APP nuk disponon një infrastrukturë BCC, për garantimin e vazhdimësisë së ofrimit të shërbimit, si dhe nuk kanë kryer azhurnimin e planit mbi vazhdimësinë e punës dhe rimëkëmbjet nga katastrofat</p>	faqe 23-38	E Lartë	<p>AKSHI bazuar në VKM Nr.673 datë 22.11.2017 pika 6k për rëndësinë që ka ofrimi i shërbimit pas një fatkeqësie, të ndërmarrin hapat e nevojshëm për ndërtimin e qendre <i>Business Continuity</i> si dhe të azhurnojnë dhe të testojnë planin e rekuperimit nga katastrofa (disaster recovery plan) me qëllim dhënien e sigurisë së arsyeshme se do të funksionojë në të gjitha situatat hipotetike dhe se burimet njerëzore janë të mirënjohura me zbatimin e hapave që duhen ndjekur</p>

<p>3.</p>	<p>Nga auditimi u konstatua se fjalëkalimi i administratorit të databazës është i ndarë në dy pjesë sipas përcaktimeve të Urdhrit nr. 4104 Prot., datë 21.06.2021 të Drejtorit të Përgjithshëm të APP-së. Gjithashtu sipas përcaktimeve të këtij urdhri bëhen ndryshimet dhe për ndryshimin e username dhe fjalëkalimit për: <i>Username dhe password i router; Username dhe password i switch; Akses i Server Management Storage; Akses i storage të DB (EVA, EVA2); Akses i storage EVA; Akses i C7000.</i></p> <p>Urdhri i sipërcituar i cili përcakton se një pjesë e fjalëkalimeve administrohet nga përfaqësuesi i APP dhe një pjesë e fjalëkalimeve administrohet nga specialisti i TI-s së AKSHI-t atashuar pranë APP, është hartuar dhe miratuar në mënyrë të njëanshme vetëm nga Titullari i APP dhe nuk ka marrë edhe miratimin e strukturave drejtuese të AKSHI-t, si palë administruese në proces.</p>	<p>faqe 23-38</p>	<p>E Lartë</p>	<p>Agjencia e Prokurimit Publik në bashkëpunim me AKSHI-n të marrin masa për hartimin dhe miratimin e një akti rregullativ të përbashkët për caktimin e administrimit të bazës së të dhënave të Sistemit të Prokurimit Elektronik, ku të përcaktohen qartë përgjegjësitë mbi administrimin e Sistemit të Prokurimit Elektronik në përputhje me dispozitat ligjore në fuqi.</p>
<p>4.</p>	<p>Nga auditimi u konstatua se, APP nuk ka një akt rregullativ të brendshëm, me qëllim organizimin dhe funksionimin e brendshëm të bazës së të dhënave, në përputhje me kërkesat e ligjit nr.10325, datë 23.09.2010, për “Bazat e të dhënave shtetërore”, neni 5, ku citohet se: “Rregulloret për organizimin dhe funksionimin e brendshëm të bazës së të dhënave shtetërore përcaktohen nga institucioni administrues dhe miratohen nga titullari i tij, në përputhje me standardet, rregullat dhe procedurat e përcaktuara sipas nenit 10 të këtij ligji”.</p>	<p>faqe 23-38</p>		<p>Agjencia e Prokurimit Publik si institucion administrues i bazës së të dhënave shtetërore që gjenerohen nëpërmjet Sistemit të Prokurimit Elektronik, të marri masa për përmbushjen e përcaktimeve ligjore mbi rregulloren për organizimin dhe funksionimin e brendshëm të bazës së të dhënave shtetërore.</p>

5.	Nga auditimi u konstatua se, nuk disponohet një akt rregullator për menaxhimin e logeve dixhitale në administratën publike, në kundërshtim me pikën 4 shkronja a) të “Rregullores për menaxhimin e log-eve digjitale në Administratën Publike”, miratuar me Urdhrin nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike.	faqe 23-38	E Lartë	Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit të marrin masa për hartimin e një rregulloreje për menaxhimin e gjurmës elektronike të auditimit, me qëllim uljen e riskut mbi sigurinë e të dhënave me pasojë humbjen dhe tjetërsimin e tyre. Gjithashtu në këtë dokument duhet të specifikohet qartë vendi ku ruhen gjurmët, për cilat veprime të përdoruesit ruhen këto gjurmë, koha, struktura përgjegjëse për monitorimin dhe analizimin e tyre, detyrat dhe përgjegjësitë, e çdo element që i shërben sigurisë së të dhënave dhe parandalimit në tjetërsimin e tyre.
6.	:Nga auditimi i të dhënave të sistemit për vitin 2021 konstatohet se: Sistemi i prokurimit Elektronik nuk ka kontrollet e nevojshëm të validimit për të mos lejuar lidhjen e kontratave pa pasur fondin limit të nevojshëm, ka raste në të cilat fondi i prokuruar është më i madh se vlera e fondi limit.	faqe 44-46	E Lartë	APP të marri masat teknike të nevojshme për implementimin e mekanizmave të kontrollit të inputit në bazën e të dhënave të Sistemit të Prokurimit Publik për të garantuar integritetin dhe plotësinë e të dhënave që ruhen në të.

I.3. Konkluzioni i përgjithshëm dhe Opinioni i Auditimit:

Kemi audituar Sistemet e Teknologjisë së Informacionit për periudhën ushtrimore 01.01.2020-31.12.2021 në të cilat përfshihet Qeverisja IT, Siguria e Informacionit, Marrëveshjet e Nivel Shërbimit dhe të dhënat e Sistemit Elektronik për Prokurimet Publike .

- Grupi i auditimit është mbështetur në Standardet ndërkombëtare të Auditimit përkatësisht në ISSAI 100, ISSAI 5300, ISSAI 5310 si dhe nenet 3 dhe 14 të ligjit 154 “Për Organizimin dhe Funksionimin e KLSH” datë 27.11.2014

- Sipas opinionit tonë, pas shqyrtimit të evidencave të marra, identifikimi dhe administrimi i elementëve kritikë në ofrimin shërbimeve dhe garantimin e sigurisë së të dhënave si dhe vazhdimësisë në ofrimin e shërbimit nëpërmjet Teknologjisë së Informacionit është i pa pamjaftueshëm. Në Administrimin e Sistemit të Prokurimit Elektronik ka mbivendosje të detyrave dhe përgjegjësive, midis Agjencisë së Prokurimit publik dhe Agjencisë Kombëtare të Shoqërisë së Informacionit.

Shërbimet e ofruara nga AKSHI në APP nuk monitorohen sipas përcaktimeve të marrëveshjes së Nivel Shërbimit. Struktura e TI së AKSHIT në APP ka mungesa të burimeve njerëzore.

II. HYRJE

Mbështetur në Ligjin 154/2014, datë 27.11.2014 “Për Organizimin dhe Funksionimin e KLSH”, në zbatim të Programit të Auditimit nr. 15/1, datë 03.02.2022 të miratuar nga Kryetari i KLSH, me afat auditimi 12.01.2022 deri në 08.04.2022, në Agjencinë e Prokurimit Publik (më poshtë APP) ,ku periudha e audituar është 01.01.2020 deri në 31.12.2021, u krye auditimi me objekt “*Auditimi i Sistemeve të Teknologjisë së Informacionit*”, nga audituesit:

1. R.A, përgjegjës grupi
2. K.S, anëtare
3. A.K, anëtare

II.1. Objekti i auditimit

Objekti i Auditimit TIK është përcaktimi nëse objektivat e subjektit arrihen në mënyrën e duhur duke përdorur burimet IT, duke përfshirë pajtueshmërinë me kërkesat ligjore dhe rregullative, konfidencialitetin, integritetin si dhe disponueshmërinë e sistemeve të informacionit dhe të dhënave që gjenden në të.

II.2. Qëllimi i auditimit

Qëllimi i Auditimit TIK ushtruar në Agjencinë e Prokurimit Publik, është dhënia e opinionit apo vlerësimit nëse ekzistojnë kontrollet dhe mekanizmat e duhur me qëllim krijimin, mirëmbajtjen e burimeve IT dhe funksioneve për të cilat këto burime shërbejnë. Për të arritur në dhënien e një opinionit, janë mbledhur informacione, të dhëna dhe prova, për të përcaktuar nëse nëpërmjet teknologjisë së informacionit mbrohen asetet, ruhet integriteti i të dhënave, si dhe synimet e subjektit që auditohet arrihen në mënyrë efektive duke përdorur burimet në mënyrë eficiente. Kërkesat për informacion sipas drejtimeve të programit të auditimit, u hartuan në përputhje me Manualin e Auditimit të Teknologjisë së Informacionit.

II.3 Identifikimi i çështjeve:

Drejtimet e këtij auditimi janë bazuar në programin e auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit të protokolluar me nr.15/1, datë 03.02.2022:

1. Auditimi i funksionimit të Qeverisjes TIK

- a. Verifikim i strategjisë, politikave dhe procedurave dhe vlerësimi i burimeve njerëzore në TIK
- b. Identifikimi dhe menaxhimi i risqeve në TIK dhe në ofrimin e shërbimit

2. Auditimi i sigurisë së informacionit

- a. Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit
- b. Të drejtat e përdoruesve dhe menaxhimi i tyre.

3. Auditimi i zhvillimit dhe blerjes në teknologjinë e informacionit

- a. Procedurat e investimeve në fushën e TIK dhe Marrëveshjet e Nivelit të Shërbimit (Service Level Agreement).

4. Auditimi i sistemeve

- a. Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output

II.4 Përgjegjësitë e strukturave drejtuese të subjektit të audituar

Veprimtaria e APP bazohet në Ligjin Nr. 162/2020 “Për Prokurimin Publik”. Detyrat dhe kompetencat e Agjencisë së Prokurimit Publik fokusohen kryesisht në:

- Përgatitjen e projekt-propozimeve për rregullat e prokurimit publik dhe aktet ligjore e nënligjorë në fushën e prokurimit publik;
- Verifikimin e zbatimit të procedurave të prokurimit publik;
- Monitorimin e mbarëvajtjes së sistemit të prokurimit publik, si dhe zbatimin e masave dhe aktiviteteve në mënyrë që të arrijë dhe të ruajë një sistem plotësisht transparent dhe efikas ;
- Hartimin dhe nxjerrjen e Buletinit të Njoftimeve Publike;

- Përrjashtimin e operatorëve ekonomikë nga pjesëmarrja në prokurimet publike për një periudhë nga 3 muaj deri në 3 vjet;

Nxitjen dhe organizimin e kualifikimit të punonjësve të qeverisjes qendrore dhe vendore, të përfshirë në veprimtaritë e prokurimit publik";

II.5 Përgjegjësitë e audituesve

Kontrolli i Lartë i Shtetit auditoi Agjencinë e Prokurimit Publik, mbi periudhën e veprimtarisë nga 01.01.2020 deri në 31.12.2021, duke i kushtuar vëmendje çështjeve që lidhen me zbatimin e ligjshmërisë dhe rregullshmërisë si dhe standardeve ndërkombëtare të teknologjisë dhe auditimit TIK.

Nga grupi i auditimit, me përgjegjësi të plotë, janë analizuar të gjitha çështjet që përmban Programi i Auditimit nr. 15/1, datë 03.02.2022 miratuar nga Kryetari i KLSH. Në realizimin e këtij Projekt Auditimi, grupi i auditimit është mbështetur në bazën ligjore mbi të cilën funksionon KLSH, standardet e auditimit, legjislacionin e fushës në të cilën operon APP. Gjithashtu, gjatë veprimtarisë audituese, është siguruar një evidencë e përshtatshme, e mjaftueshme dhe e besueshme auditimi, në të cilën jemi mbështetur në dhënien e konkluzioneve dhe rekomandimeve.

II.6 Kriteret e vlerësimit

Kriteret e vlerësimit janë bazuar në ligjet, rregulloret në fuqi, standardet ndërkombëtare COBIT dhe ISSAI 5300 për auditimin e Teknologjisë së Informacionit si dhe Manualin e Teknologjisë së Informacionit. Opinioni i auditimit mbështetet në praktikat më të mira, Standardet Kombëtare dhe Ndërkombëtare të Auditimit. Në këtë projekt raport krahas gjetjeve që janë konstatuar, grupi i auditimit ka rekomanduar disa masa organizative, për përmirësimin e situatës.

Aktet ligjore dhe rregullative mbi të cilat është mbështetur vlerësimi janë si më poshtë:

- Ligji Nr. 9643, datë 20.11.2006, (ndryshuar)
- Ligji Nr. 162 datë 23.12.2020 “Për Prokurimin Publik”.
- Kushtetuta e Republikës së Shqipërisë (nenet 162-165)
- Ligji Nr. 154/2014 “Mbi Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit”;
- Ligji Nr. 10296, datë 08.07.2010 “ Për Menaxhimin Financiar dhe Kontrollin”, i ndryshuar dhe aktet ligjore të zbatimit të tij.
- Legjislacioni mbi krimin Kibernetik.
- Ligji Nr. 9918, datë 19.05.2008 “Për komunikimet Elektronike në Republikën e Shqipërisë”.
- Ligji Nr. 10325, datë 23.09.2010, Për Bazat e të Dhënave Shtetërore”.
- Ligji Nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012 “ Për Mbrojtjen e të Dhënave Personale”.
- Vendim Nr. 285, Datë 19.5.2021 Për Miratimin e Rregullave Të Prokurimit Publik (Ndryshuar Me Vendimin Nr. 710, Datë 24.11.2021)
- VKM 673, datë 22.11.2017 “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar;
- Vendimi nr. 914, datë 29.12.2014, i Këshillit të Ministrave, “Për miratimin e rregullave të prokurimit publik”,
- VKM nr. 710, datë 21.08.2013 “Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit”, i ndryshuar;
- VKM nr. 945, datë 02.11.2012 “Për miratimin e rregullores administrimi i sistemit të bazave të të Dhënave Shtetërore”.
- Rregullore e Brendshme e Agjencisë së Prokurimit Publik.

- Standardet TIK;
- Udhëzimi nr. 30, datë 27.12.2011 “Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik”, i ndryshuar;
- Udhëzimi nr. 1159, datë 17.03.2014 “Për hartimin e Marrëveshjes të Nivelit të Shërbimit”, i ndryshuar;
- Rregulloret përkatëse të Agjencisë Kombëtare të Shoqërisë së Informacionit;
- Udhëzim nr. 2 datë 2.9.2013 i Ministrit për ITIK “Për standardizimin e hartimit të Termave të Referencës për projektet TIK në administratën publike

II.7 Standardet e auditimit

Auditimi është kryer, në përputhje me Kodin Etik, Standardet, dhe teknikat e auditimit të teknologjisë së informacionit, duke përfshirë pyetësorë, intervista, testim dhe procedura, të cilat u gjykuan se ishin të nevojshme, për të dhënë një vlerësim sa më objektiv, profesional e të pavarur, të saktë, të plotë e të qartë, duke u fokusuar veçanërisht në standardet e fushës së auditimit të TIK, si: COBIT 4.1, Manuali i Auditimit IT, ISSAI 5310, etj

II.8 Metodat e auditimit

Metodat mbi auditimin e sistemeve të Teknologjisë së Informacionit që grupi i auditimit ka ndjekur në APP, janë si më poshtë:

- Intervista zhvilluar në subjekt me personat përgjegjës;
- Verifikime të sistemit si auditues;
- Shqyrtimi i dokumentacionit rregullativ të institucionit;
- Analizimi i të dhënave të eksportuara nga sistemi;

II.9 Dokumentimi i auditimit

Dokumentimi i auditimit është bazuar në rregulloren e brendshme të KLSH si dhe në manualin aktiv të auditimit të Teknologjisë së Informacionit në të cilin janë përfshirë:

- Planifikimi, qëllimi dhe objektivat e auditimit;
- Programi i auditimit;
- Evidencat e grumbulluara në lidhje me të dhënat e sistemit, raporte të ndryshme me të dhëna nxjerrë nga sistemi;
- Letrat e punës mbajtur nga audituesit sipas detyrave të përcaktuara gjatë fazës së auditimit në terren.

III. PËRSHKRIMI I AUDITIMIT

III.1 Informacioni i përgjithshëm mbi subjektin nën auditim

Agjencia e Prokurimit Publik është organ qendror, person juridik publik në varësi të Kryeministrit, që financohet nga Buxheti i Shtetit. Veprimtaria e saj bazohet në Ligjin Nr. 162/2020 “Për Prokurimin Publik”. Detyrat dhe kompetencat e Agjencisë së Prokurimit Publik fokusohen kryesisht në:

- Përgatitjen e projekt-propozimeve për rregullat e prokurimit publik dhe aktet ligjore e nënligjore në fushën e prokurimit publik;
- Verifikimin e zbatimit të procedurave të prokurimit publik;
- Monitorimin e mbarëvajtjes së sistemit të prokurimit publik, si dhe zbatimin e masave dhe aktiviteteve në mënyrë që të arrijë dhe të ruajë një sistem plotësisht transparent dhe efikas ;
- Hartimin dhe nxjerrjen e Buletinit të Njoftimeve Publike;
- Përfundimin e operatorëve ekonomikë nga pjesëmarrja në prokurimet publike për një periudhë nga 3 muaj deri në 3 vjet;

Nxitjen dhe organizimin e kualifikimit të punonjësve të qeverisjes qendrore dhe vendore, të përfshirë në veprimtaritë e prokurimit publik;

III.2. Përshkrimi i rezultateve të auditimit

III.2.1 Auditimi i Funkcionimit të Qeverisjes Tik

a. Verifikimi i strategjisë, politikave dhe burimeve njerëzore në TIK

➤ *Strategjia TIK*

Agjencia e Prokurimit Publik është pjesë e Strategjisë gjithëpërfshirëse Kombëtare të Prokurimit Publik e miratuar me VKM nr. 850, datë 04.11.2020 “Për miratimin e strategjisë kombëtare për prokurimin publik 2020 – 2023 dhe të planit të veprimit për zbatimin e saj”, e cila u realizua nga një grup ndërinstitucional pune, i përbërë nga të gjitha institucionet që veprojnë në fushën e prokurimit, bazuar në urdhrin e Kryeministrit nr. 102, datë 03.07.2019, “Për ngritjen e grupit ndërinstitucional të punës për bashkërendimin, hartimin, zbatimin dhe monitorimin e Strategjisë Kombëtare për Prokurimin publik dhe planit të veprimit”. Këto institucione janë përgjegjëse për ndjekjen e zbatimit e aktiviteteve të përcaktuara në Strategjinë dhe Planin e Veprimit. Sikurse paraqitet edhe në objektivat specifike dhe aktivitetet kryesore të propozuara në këtë Strategji dhe Planin e Veprimit, Agjencia e Prokurimit Publik është institucioni kryesor për koordinimin dhe monitorimin e objektivave dhe aktiviteteve të parashikuara.

Qëllimi i politikave dhe objektivat specifike të strategjisë janë si më poshtë:

Qëllimi i politikës 1 – Prokurim publik eficient dhe i qëndrueshëm;

Objektivi specifik 1 – Përmirësimi i legjislacionit të prokurimit dhe përafrimi me acquis të BE-së;

Objektivi specifik 2 – Fuqizimi i rolit dhe kapaciteteve të Agjencisë së Prokurimit Publik;

Objektivi specifik 3 – Organizimi dhe profesionalizimi i funksionit të prokurimit;

Objektivi specifik 4 – Rritja e eficiencës në prokurimin publik;

Objektivi specifik 5 – Zgjerimi i politikave dhe i metodave për prokurimin e qëndrueshëm;

Objektivi specifik 6 – Forcimi i integritetit në prokurimin publik;

Objektivi specifik 7 – Përmirësimi i sistemit elektronik të prokurimit;

Qëllimi i politikës 2 – Përmirësimi i kuadrit ligjor dhe institucional për koncesionet dhe partneritetin publik-privat;

Objektivi specifik 1 – Reforma rregullatore;

Objektivi specifik 2 – Kuadri institucional;

Qëllimi i politikës 3 – Riorganizimi i prokurimeve në fushën e mbrojtjes dhe të sigurisë;

Objektivi specifik 1 – Përmirësimi i kuadrit rregullator të prokurimeve në fushën e mbrojtjes dhe sigurisë;

Objektivi specifik 2 – Përmirësimi i kuadrit institucional për prokurimet në fushën e mbrojtjes dhe sigurisë;

Qëllimi i Politikës 4 – Blerja e përqendruar;

Objektivi specifik 1 – Veprimtaria e Agjencisë së Blerjeve të Përqendruara;

Objektivi specifik 2 – Blerja e përqendruar në fushën e shëndetësisë;

Qëllimi i politikës 5 – Përmirësimi i sistemit të shqyrtimit të ankesave.

Sikurse paraqitet edhe në objektivat specifike dhe aktivitetet kryesore të propozuara në këtë Strategji, Agjencia e Prokurimit Publik është institucioni kryesor për koordinimin dhe monitorimin e objektivave dhe aktiviteteve të parashikuara. Objektivi është fuqizimi i rolit të APP-së si institucion politikë bërës nëpërmjet parashikimit të qartë të kompetencave në dispozitat ligjore, si edhe ngritjes së vazhdueshme të kapaciteteve të punonjësve të APP-së. Ky objektivi është parashikuar të arrihet nëpërmjet një sërë masash të rëndësishme, si:

Masa 1.2.1: Rritja e kompetencave të APP-së në të gjitha fazat e procesit në vijim të miratimit të ligjit të ri të prokurimit publik.

Masa 1.2.2: Trajnimi i vazhdueshëm i punonjësve të APP-së sipas fushave. (Afati kohor 2020–2022)

Treguesit e performancës:

1. Përcaktimi i saktë i kompetencave në nenet e ligjit të ri të PP-së;
2. Plani i trajnimit i hartuar;
3. Trajnimi i 40 punonjësve të APP-së sipas fushave;
4. Vizita studimore/trajnime në vendet e tjera.

Për sa më sipër grupi i auditimit ka administruar dokumentet strategjik, të miratuar si më poshtë:

- Axfenda Dixhitale e Shqipërisë 2015-2020 (Strategjia nder sektorialë)
- Indikatorët e Strategjisë Axfenda Dixhitale 2015-2020
- Plani i veprimit i strategjisë Axfenda Dixhitale e Shqipërisë 2015-2020

Verifikim i politikave dhe burimet njerëzore në TIK

Grupi i auditimit, me qëllim auditimin e nivelit të dokumentimit të politikave dhe procedurave në lidhje me teknologjinë e informacionit në APP, verifikoi Rregulloren e Brendshme të institucionit si dhe udhëzime të tjera të brendshme. Auditimi për këtë çështje, pati në konsideratë risqet që vijnë nga mungesa e politikave dhe procedurave të shkruara si dhe nga praktikatat me të cilat institucioni zhvillon aktivitetin e tij.

- ❖ Aktualisht, APP e ushtron aktivitetin e tij mbështetur në rregulloren e miratuar me Vendim nr. 14, datë 13.09.2018 të Drejtorit të Përgjithshëm *“Për miratimin e Rregullores së Brendshme të Institucionit të Agjencisë së Prokurimit Publik”*, i ndryshuar me Vendim nr. 3, datë 30.04.2019 *“Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik”*.

Nga auditimi u konstatua se, Rregullorja e Brendshme nuk është përshtatur (*amenduar*) duke mos reflektuar ndryshimet institucionale të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 *“Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”*, i ndryshuar, si dhe ri-organizimin e strukturës në Agjencinë e Prokurimit Publik, konkretisht:

- në rregulloren e brendshme të APP detyrat dhe përgjegjësitë janë të njëjta me rregulloren e miratuar me Vendim nr. 14, datë 13.09.2018, në të cilën struktura ishte ende e pandryshuar.
- Gjithashtu në Drejtorinë e Administrimit të të Dhënave dhe Publikimit ka mbivendosje me detyrat e Strukturës Përgjegjëse të AKSHI-t atashuar në APP, për shembull:

Në rregulloren e brendshme neni 14 pika 2, 8 dhe 11 citohet si në vijim:

“2. Harton dhe implementon në kohë dhe me cilësi planin për krijimin e një rubrike të re në website, me qëllim kryerjen e procedurave me vlerë të vogël në sistemin elektronik”;

“5. Harton në kohë dhe me cilësi specifikimet teknike për kontratat që APP-ja do të lidh me të tretët, me qëllim rritjen e sigurisë së sistemit elektronik dhe arshivës elektronike”;

“8. Bashkëpunon në kohë dhe me cilësi për procesin Upgrade të sistemit të Prokurimit Elektronik me qëllim testimin e serverave, evidentimin e problemeve dhe ndjekjen e tyre deri në zgjidhje”;

“11. Monitoron procesin e kontrollit fizik të sistemit me qëllim identifikimin e problemeve dhe delegimin e tyre te personat përgjegjës për përmirësim”; etj.

Ku sipas Rregullores së Brendshme *“Mbi detyrat dhe funksionimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”* miratuar me nr. 1990 prot., datë 16.04.2020 janë detyra të cilat realizohen nga Sektori i IT në Agjencinë e Prokurimit Publik konkretisht, tek detyrat e përgjegjësit të sektorit pika 6 citohet: *“Administron, editon, sipas kërkesave website-in zyrtar të institucionit”*, pika 11, *“Monitoron funksionimin e sistemeve të institucionit dhe propozon tek AKSHI, institucionit nevojat e këtyre sistemeve për përmirësim/mirëmbajtje duke bashkëpunuar me drejtorinë e cila i përdor këto sisteme”*, pika 11 te detyrat e specialistit të sektorit *“ Identifikimi i problemeve dhe analizim për zgjidhjen e tyre”*, etj.

❖ Gjatë fazës së auditimit në terren grupi i auditimit administroi një sërë rregulloresh dhe manualesh, që APP disponon nga ku u konstatua se institucioni administron dhe ka në përdorim një bazë rregullative, konkretisht:

- Plani i Sigurisë i Rishikuar versioni 4;
- Rregullore e Brendshme për Administrimin e Bazës së të Dhënave;
- Manual për administratorin e sistemit të prokurimit elektronik për menaxhimin e përdoruesve;
- Plan Rikuperimi nga Katastrofa.

Nga auditimi u konstatua se, këto dokumente nuk janë rishikuar dhe update-uar duke mos reflektuar ndryshimet institucionale të ndodhura me hyrjen në fuqi të VKM-së nr. 673, datë 22.11.2017 “Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar, në Agjencinë e Prokurimit Publik. Ato i janë paraqitur grupit të auditimit si përgjigje ndaj pyetësorit dhe përdoren si bazë rregullatore nga APP.

Gjatë fazës së auditimit në terren nga Sektori i IT nga AKSHI atashuar pranë APP grupit të auditimit i ‘u vendosën në dispozicion rregullore dhe manualesh, që disponon, nga ku u konstatua se institucioni administron dhe ka në përdorim një bazë rregullative, konkretisht:

- Procedurat e menaxhimit të aksesit;
- Politika e menaxhimit të ndryshimeve;
- Politika e brendshme e auditimit të IT;
- Procedura e menaxhimit të incidentit të sigurisë ISMS;
- Politikat e menaxhimit të Logeve;
- Procedura për matjen e efektivitetit të kontrolleve të sigurisë;
- Procesi i vlerësimit të rrezikut;

Nga auditimi u konstatua se, këto dokumente nuk janë të miratuara nga organet drejtuese të AKSHI-t. Ato i janë paraqitur grupit të auditimit si përgjigje ndaj pyetësorit dhe përdoren si bazë rregullatore nga Sektori IT i AKSHI-t atashuar pranë APP. Gjithashtu u konstatua se këto rregullore përveçse janë draft-e janë në formë shpjeguese duke mos përmbushur kështu qëllimin e vet politikave dhe procedurave që udhëzojnë mjedisin e përgjithshëm të IT të institucionit me qëllim sigurimin e kontrolleve respektive dhe mekanizmat e zbatimit. *Politikat vendosin strukturën për operacionet e përditshme në mënyrë që të arrihen qëllimet e vendosura nga organet qeverisëse. Politikat mbështeten nga procedurat dhe proceset, të cilët përcaktojnë sesi do të realizohet dhe kontrollohet puna.*

➤ **Burimet njerëzore në TIK**

Bazuar në VKM nr. 673, datë 22.11.2017, strukturat përgjegjëse TIK të institucioneve dhe organeve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, bëhen pjesë e strukturës së AKSHI-t. Punonjësit aktualë të njësive të teknologjisë së informacionit e të komunikimit (NJTIK), në përbërje të strukturave të institucioneve dhe organeve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, kalojnë tek AKSHI, brenda datës 31.12.2017.

- Në kundërshtim me pikën 23 të VKM-së nr. 673, datë 22.11.2017, në të cilën citohet se: “*Strukturat përgjegjëse TIK bëhen pjesë të strukturës së AKSHI-t. Punonjësit aktualë të njësive të teknologjisë së informacionit e të komunikimit (NJTIK), në përbërje të strukturave të institucioneve dhe organeve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, kalojnë tek AKSHI, brenda datës 31.12.2017 dhe do të trajtohen në bazë të përcaktimeve të legjislacionit në fuqi për nëpunësit civil, në rastin e mbylljes dhe ristrukturimit të institucionit, apo Kodit të Punës. AKSHI vendos në dispozicion të institucioneve të përmendura në shkronjën “i”, të pikës 6, personelin e mjaftueshëm dhe të certifikuar sipas*

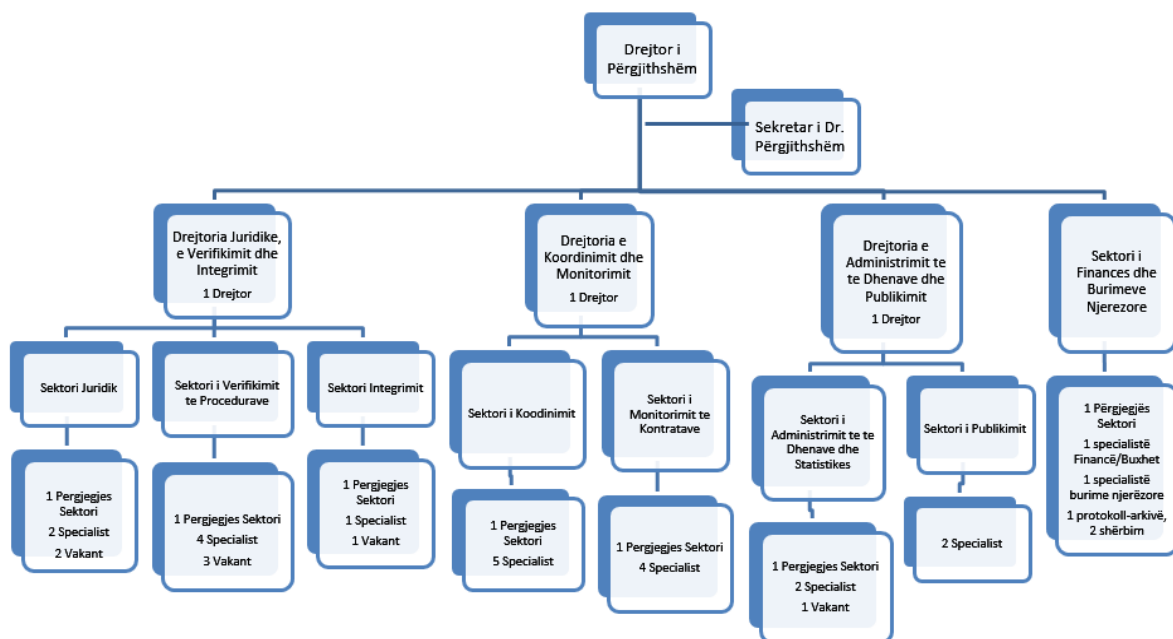
legjislacionit në fuqi, për të mbajtur në funksion optimal sistemet të cilat nuk preken nga fusha e veprimit të këtij vendimi”, **Agjencia e Prokurimit Publik nuk ka bërë kalimin e burimeve njerëzore në AKSHI.**

Me anë të Urdhrit të Brendshëm të Titullarit të Agjencisë së Prokurimit Publik Nr. 51, datë 10.04.2018 dhe Urdhrit të Brendshëm Nr. 112, datë 26.11.2018 funksionet e IT janë kryer nga stafi i Sektorit të Administrimit të të Dhënave duke qenë se AKSHI nuk kishte alokuar ende pranë APP strukturën IT. AKSHI me anë të urdhrin Nr. 15, datë 04.02.2020 ka atashuar një specialist në sektorin e IT pranë APP për të kryer detyrat sipas Rregullores së Brendshme të AKSHI-t nr. 1900, datë 16.04.2020 “*Mbi detyrat dhe funksionimi i Agjencisë Kombëtare të Shoqërisë së Informacionit*”.

Nga auditimi u konstatua se, sipas Rregullores së Brendshme të AKSHI-t të sipërcituar struktura IT pranë APP është e përbërë nga 1 (një) Përgjegjës Sektori dhe 2 (dy) Specialist, kjo strukturë është në mungesë të përgjegjësit dhe 1 (një) specialisti e cila sjell risk në mos përmbushje të objektivave të përcaktuara.

Me anë të Urdhrit të Kryeministrit Nr. 54, datë 15.03.2019 është miratuar struktura dhe organika e Agjencisë së Prokurimit Publik, duke përfshirë të gjithë punonjësit sipas kategorisë, hierarkisë, pozicionit të punës, sipas drejtorive përkatëse.

Figura nr.1: Struktura e APP

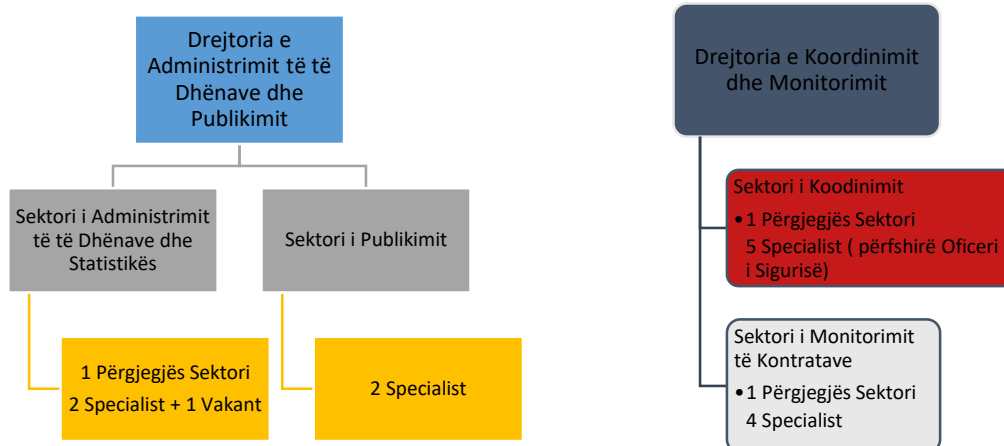


Burimi: APP

Kjo strukturë dhe organikë është ndryshuar me anë të Urdhrit të Kryeministrit nr. 149, datë 28.12.2021 ku Drejtoria e Administrimit të të Dhënave dhe Publikimit emërtohet si Drejtoria e Menaxhimit të Bazës së të Dhënave dhe Publikimit, me dy sektorë në varësi përkatësisht: Sektori Menaxhimit të Bazës së të Dhënave me 1 (një) përgjegjës sektori dhe 2 (dy) specialist dhe Sektor i Publikimit me 3 (tre) specialistë.

Për periudhën objekt auditimi *Drejtorja e Administrimit të Dhënave dhe Publikimit* është në varësi të drejtpërdrejtë të Drejtorit të Përgjithshëm të APP. Struktura aktuale është e përbërë nga 7 (shtatë) punonjës dhe ka në varësi: 1. Sektorin e Administrimit të dhënave dhe Statistikës me përbërje 1 (një) Përgjegjës Sektori dhe 3 (tre) Specialist me 1 (një) pozicion vakant dhe 2. Sektorin e Publikimit me 2 (dy) Specialist.

Figura nr.2: Struktura e Drejtorisë së Administrimit të Dhënave dhe Publikimit dhe Drejtorisë së Koordinimit dhe Monitorimit.



Burimi: Përpunuar nga grupi i auditimit

- Në rregulloren e miratuar me Vendim nr. 03, datë 30.04.2019 të Drejtorit të Përgjithshëm “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik”, neni 18 përcaktohen detyrat e Oficerit të Sigurisë, ku sipas këtij neni Oficeri i Sigurisë i ushtron këto detyra në varësinë e Drejtorisë së Administrimit të të Dhënave dhe Publikimit. Me anë të Urdhrit “Për ushtrimin e detyrave” nr. 9168/11 prot., datë 24.05.2019, ngarkohet në ushtrimin e detyrave të rolit të Oficerit të Sigurisë/CSIRT nëpunësi z L.K. Ndërkohë Oficeri i Sigurisë sipas Strukturës së APP miratuar me anë të Urdhrit të Kryeministrit Nr. 54, datë 15.03.2019, konstatohet se është specialist në Sektorin e Koordinimit nën varësinë e Drejtorisë së Koordinimit dhe Monitorimit. Gjithashtu edhe sipas të dhënave nga struktura plan-fakt për vitin 2020-2021 ky punonjës rezulton se ka qenë nën varësinë e po kësaj drejtorie.

Nga auditimi u konstatua se, raportimi i Oficer të Sigurisë nuk kryhet në nivelin më të lartë drejtues të APP, bazuar në standardet ndërkombëtare dhe praktikat më të mira, pasi vetëm në këtë mënyrë mund të garantohet pavarësia e tij dhe mund të shmangen konfliktet e interesit që lindin, për arsye të ushtrimit të kompetencave të tij.

Nga auditimi u konstatua se, sipas përshkrimeve të punës punonjësi i caktuar në rolin e Oficerit të Sigurisë kryen detyrat e specialistit në Sektorin e Koordinimit deri në mars të 2022 me ndryshimin e strukturës së re. Konstatohet se detyrat në rolin e Oficerit të Sigurisë bazuar dhe në rregulloren e brendshme datë 30.04.2021 të APP-së, nuk janë realizuar sipas pozicionit të ngarkuar me urdhër nr. 9168 prot., datë 24.05.2019.

Nisur nga shtrirja e teknologjisë së informacionit si dhe nga rëndësia e të dhënave që ruhen dhe përpunohen nga Sektori i IT-s së AKSHI-t dhe Drejtorisë së Administrimit të Dhënave dhe Publikimit me anë të Sistemit të Prokurimit Elektronik, grupi i auditimit konstatoi se pozicionimi i këtij pozicioni nuk i përgjigjet shtrirjes së teknologjisë së informacionit në Agjencinë e Prokurimit Publik. Raportimi i pozicionit Oficer Sigurie, duhet jetë në nivelin më të lartë drejtues të APP bazuar në përgjegjësinë që i jep ligji për administrimin dhe mbrojtjen e të dhënave të prokurimit publik si dhe standardet ndërkombëtare.

Tabela nr. 1: Struktura Drejtorisë së Administrimit të Dhënave dhe Publikimit Plan/Fakt

Nr.	Emërtimi	Niveli arsimor	Numër v.2020	
			Plan	Fakt
1	Drejtor	Shkenca Inxhinierike	1	1
Spektori i Administrimit të të Dhënave dhe Statistikës				
2	Përgjegjës Sektori	Shkenca Inxhinierike, Shkenca Kompjuterike	1	1
3	Specialist	Shkenca Kompjuterike	1	1

4	Specialist	Shkenca Inxhinierike	1	1
5	Specialist	Shkenca Ekonomike	1	1
Sektori i Publikimit				
6	Specialist Sektori i Publikimit	Shkenca Inxhinierike	1	1
7	Specialist Sektori i Publikimit	Shkenca Shoqërore, Inxhinierike, Kompjuterike	1	1

Burimi: APP, Përpunuar nga grupi i auditimit

Tabela nr. 2: Struktura Drejtorisë së Administrimit të Dhënave dhe Publikimit Plan/Fakt

Nr.	Emërtimi	Niveli arsimor	Numër v.2021	
			Plan	Fakt
1	Drejtor	Shkenca Inxhinierike	1	1
Sektori i Administrimit të Dhënave dhe Statistikës				
2	Përgjegjës Sektori	Shkenca Kompjuterike	1	1
3	Specialist	Vakant	-	-
4	Specialist	Shkenca Inxhinierike	1	1
5	Specialist	Shkenca Ekonomike	1	1
Sektori i Publikimit				
6	Specialist Sektori i Publikimit	Shkenca Shoqërore	1	1
7	Specialist Sektori i Publikimit	Shkenca Shoqërore, Inxhinierike, Kompjuterike	1	1

Burimi: APP, Përpunuar nga grupi i auditimit

Në rregulloren e brendshme të Agjencisë së Prokurimit Publik miratuar me Vendim nr. 03, datë 30.04.2019 “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik”, të Drejtorit të Përgjithshëm, përcaktohen detyrat dhe përgjegjësitë e Drejtorisë së Administrimit të Dhënave dhe Publikimit sipas pozicioneve: Drejtor, Përgjegjës Sektori dhe Specialist.

Nga auditimi u konstatua se, përshkrimet e punës mbas ristrukturimit të strukturës me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit, i ndryshuar, nuk kanë ndryshuar nga detyrat e mëparshme që po të njëjtët specialist kryenin.

Nga auditimi u konstatua se: Nga auditimi u konstatua se përshkrimet e punës për stafin e Drejtorisë së Administrimit të Dhënave dhe Publikimit mbi mënyrën e organizimit, funksionimit dhe ndarjes së përgjegjësive specifike të roleve, punëve dhe veprimeve operacionale brenda drejtorisë janë të pa update-uara, ku konstatohen mos përputhje të detyrave të punonjësve në përshkrimet e punës së secilit prej tyre me rregulloren e brendshme të APP, si dhe detyra të cilat nuk janë më kompetencë e punonjësve të kësaj drejtorie me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit, i ndryshuar. Gjithashtu mungon përshkrimi punës për përgjegjësia aktual të Sektorit të Administrimit të Dhënave dhe Statistikës, sipas përshkrimit të punës në dosjen personale kryen detyrat e specialistit.

➤ **Trajnimet**

Trajnimi është një nga shtyllat e rëndësishme për menaxhimin e kapaciteteve. Personeli që ka akses në asetet dhe sistemet e teknologjisë së informacionit të Agjencisë së Prokurimit Publik të jetë i vetëdijshëm për rregullat dhe standardet e sigurisë dhe të jenë të aftë t'i zbatojnë dhe ndjekin ato gjatë punës së tyre.

- Është e nevojshme që procesi të mbështetet në një identifikim dhe analizë të nevojave për trajnim të stafit, me qëllim që të sigurohet parashikimi, programimi dhe implementimi i suksesshëm i veprimtarive trajnuese.

- Për periudhën objekt auditimi u konstatua se Agjencia e Prokurimit Publik, nuk ka plan trajnimi vjetor për vitin 2020 dhe 2021 për burimet njerëzore të drejtorisë së Administrimit të të Dhënave në lidhje me Teknologjinë e Informacionit. Gjatë vitit 2021 kanë zhvilluar trajnime në lidhje me Menaxhimin Strategjik, Statistikë, mbi Prokurimin Publik etj, por në asnjë rast mbi teknologjinë e informacionit.

- Gjithashtu, konstatohet se stafi i Sektorit IT atashuar në Agjencinë e Prokurimit Publik nuk ka zhvilluar trajnime mbi sistemet, sigurinë dhe teknologjinë e informacionit. Sipas rregullores vlerësimin për nevojat e stafit për trajnime dhe kualifikime si dhe sigurimin se stafi ka marrë pjesë në të gjitha trajnimet e zhvilluara e kryen përgjegjësi i sektorit të Sektorit të IT në APP, i cili është pozicion vakant. Në kundërshtim me Rregulloren e Brendshme nr. 1900, datë 16.04.2020 “*Mbi detyrat dhe funksionimi i Agjencisë Kombëtare të Shoqërisë së Informacionit*” sektori i IT atashuar pranë APP nuk ka zhvilluar trajnime për periudhën objekt auditimi mbi sistemet, sigurinë dhe teknologjinë e informacionit.

- Nga auditimi nuk u administruan dokumentacione mbi propozimet përkatëse nga niveli menaxherial i APP (ku përfshihet dhe drejtoria e burimeve njerëzore) për zhvillimin e trajnimeve. Nuk dokumentohet procesi i kërkesave, nevojave dhe analizimi i tyre për trajnim. Duke mos plotësuar kështu nevojat për trajnim mbi sistemet, sigurinë dhe teknologjinë e informacionit.

b. Identifikimi dhe menaxhimi i risqeve në TIK dhe në ofrimin e shërbimit

Regjistri i Riskut, përfaqëson një dokument të projektuar në formën e matricës monitoruese, në të cilin evidentohet informacion mbi riskun e identifikuar, riskun e qenësishëm (para kontrolleve) dhe riskun pas kontrolleve duke evidentuar gjithashtu nevojën për kontrolle të mëtejshme.

Menaxhimi i riskut IT është aplikimi i metodave të menaxhimit të riskut në teknologjinë e informacionit për të menaxhuar riskun e TI-së, pra: Rreziku i institucionit që lidhet me përdorimin, pronësinë, operimin, përfshirjen, ndikimin dhe adoptimin e IT në APP.

APP me anë të Vendimit nr. 12 datë 29.09.2021 “*Për miratimin e Gjurmëve të Auditit*”, ka miratuar gjurmën e auditimit në zbatim të ligjit Nr. 10296/2010 “*Për menaxhimin financiar dhe kontrollin*”, i ndryshuar.

Grupit të auditimit ju vendos në dispozicion raportimi nga Drejtoria e Administrimit të të Dhënave dhe Publikimit mbi “*Analizën e riskut mbi realizimin e objektivave për Drejtorinë e Administrimit të të dhënave dhe Publikimit në periudhën Janar – Dhjetor 2020*” dhe për vitin 2021

- Në lidhje me këtë çështje grupi i auditimit administroi dokumentin “*Procesi i vlerësimit të rrezikut*”, dokument draft i pa miratuar, i cili është hartuar nga AKSHI version 2021. Ky dokument trajton hapat që duhet të ndërmerret institucioni për përcaktimin e risqeve mbi sigurinë e informacionit. Në përfundim nuk është gjeneruar asnjë dokument lidhur me përcaktimin e këtyre risqeve.

Nga auditimi i regjistrat të riskut për vitin 2020 dhe vitin 2021 të Agjencisë së Prokurimit Publik konstatohet se në të dy regjistrat nuk rezulton që gjatë kësaj periudhe të ketë patur përditësime me risqe të reja të identifikuar konkretisht:

-Nuk janë identifikuar risqet në burimet njerëzore, të cilat duhen adresuar për të siguruar mirëfunksionimin dhe administrimin e Sistemit të Prokurimit Elektronik;

-Nuk janë analizuar dhe identifikuar mbivendosjet e kompetencave dhe detyrave në lidhje me administrimin e Sistemit të Prokurimit Elektronik, si dhe hapat që do të ndërmerren për

minimizimin e problemeve që mund të ndodhin në Sistemin e Prokurimit Elektronik si dhe përgjegjësitë ndërmjet AKSHI-t dhe APP-s.

-Ndarja ose transferimi i risqeve së bashku me asetet tek AKSHI duke qenë se transferimi i aktiveve është bërë gjatë vitit 2020, periudhë për të cilën APP nuk ka marrë masa për rishikimin dhe update-im e regjistrit të riskut për këtë periudhë;

-Nuk janë identifikuar risqe në lidhje me: sigurinë, disponibilitetin dhe integritetin e sistemit dhe të dhënave që gjenerohen nëpërmjet Sistemit të Prokurimit Elektronik; edhe risqet që lidhen me teknologjinë e informacionit.

1.Titulli i gjetjes: Identifikimi dhe vlerësimi i problematikave mbi burimet njerëzore.

Situata: Nga auditimi u konstatua se:

- Sektori i TI atashuar në APP është në mungesë të përgjegjësive dhe 1 (një) specialisti. AKSHI me shkresën nr.785 Prot., datë 04.02.2020 ka caktuar vetëm një specialist TI në APP, strukturë kjo e cila vazhdon ende të funksionojë si e tillë, duke sjell risk në mos përmbushje të objektivave institucionale.

-Sektorin e IT të AKSHI-t atashuar pranë APP përdor një bazë rregullatore të cilat nuk janë të miratuara nga organet drejtuese të AKSHI-t. Gjithashtu këto akte rregullore janë draft- akte te papërfunduara.

-Rregullorja e Brendshme e Agjencisë së Prokurimit Publik nuk është përshtatur (*amenduar*) duke mos reflektuar ndryshimet institucionale të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “*Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*”, i ndryshuar, Ligjit nr. 162/2020 “*Për Prokurimin Publik*” si dhe ri-organizimin e strukturës në Agjencinë e Prokurimit Publik. Konkretisht Drejtoria e Administrimit të të Dhënave dhe Publikimit në APP ka mbivendosje të detyrave funksionale me Rregulloren e Brendshme të AKSHI-it “*Mbi detyrat dhe funksionimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*”, duke bërë që detyrat funksionale që duhet të kryheshin nga sektori i TI të AKSHI-t atashuar pranë APP realizohen nga Drejtoria e Administrimit të të Dhënave dhe Publikimit në APP. Si dhe përshkrimet e punës për stafin e Drejtorisë së Administrimit të të Dhënave dhe Publikimit janë të pa përditësuara.

Kriteri: Rregullore e Brendshme nr. 03, datë 30.04.2019 “*Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik*”. Rregullore e Brendshme “*Mbi detyrat dhe funksionimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*” nr. 1990 prot., datë 16.04.2020 si dhe VKM nr. 673, datë 22.11.2017 “*Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*”, i ndryshuar.

Ndikimi/Efekt: Mos arritje e objektivave institucionale si pasojë e keq adresimit të përcaktimit të detyrave, kompetencave dhe përgjegjësi.

Shkaku: Mos menaxhim si dhe mos miratim në bazën ligjore, nënligjore dhe aktet rregullative.

Rëndësia: E Lartë.

1.1.Rekomandimi: Agjencia Kombëtare e Shoqërisë së Informacionit të marrë masa të menjëhershme për plotësimin e vendeve vakante të sektorit IT atashuar në APP.

1.2.Rekomandimi: Struktura drejtuese të Agjencisë Kombëtare të Shoqërisë së Informacionit të marrin masa për miratimin e akteve rregullative në përputhje me përcaktimet ligjore dhe nënligjore me qëllim reflektimin e ndryshimeve institucionale, strukturore dhe kompjuterike të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “*Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*”, i ndryshuar.

1.3.Rekomandimi: Agjencia e Prokurimit Publik me plotësimin e strukturës IT si organikë e AKSHI-t pranë saj të marrë masa për përditësimin e rregullores së brendshme institucionale në të cilën të pasqyrohen dhe reflektohen qartë detyrat operacionale në lidhje me ndryshimet institucionale, strukturore dhe kompjuterike të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “*Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*”, i

ndryshuar. Gjithashtu Agjencia e Prokurimit Publik të marrë masa dhe për përditësimin e përshkrimeve të punës në koherencë me rregulloren e brendshme.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia e Prokurimit Publik dhe me shkresë nr. 15/7 datë 06.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit APP:

..... APP ka qenë në komunikim të vazhdueshëm me AKSHI-n lidhur me stafin e IT. APP do të vijojë komunikimin me AKSHI-n, për të marrë një konfirmim final se kush do të jetë struktura përfundimtare IT që do ti kalojnë të gjitha detyrat përkatëse në lidhje me SPE.

Për sa i përket gjetjes së grupit të auditimit se në rregulloren e APP-së nuk janë reflektuar parashikimet e rregullores së brendshme të AKSHI-t, nuk arrihet të kuptohet se mbi çfarë baze ligjore grupi i auditimit, kërkon ndryshimin e rregullores së një institucioni, për shkak të ndryshimit të rregullores së brendshme të një institucioni tjetër! Për më tepër, nuk kuptohet nëse grupi i auditimit ka administruar ndonjë komunikim të AKSHI-t drejtuar APP-së ku ti bëjë me dije ndryshimet e veta që impaktojnë rregulloret tona të brendshme, pasi në APP nuk ka të administruar zyrtarisht një komunikim të tillë.

Gjetja i referohet mos miratimit të akteve nënligjore nga ana e AKSHI-t. Sic kemi theksuar edhe në pikat më sipër, përgjegjësitë dhe detyrat e APP janë përcaktuar në dispozitat e ligjit 162/2020. APP nuk ka kompetencë dhe autorizim ligjor të miratojë akte ligjore dhe nënligjore të zbatim të VKM nr. 673, datë 22.11.2017 “Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar, por është përgjegjëse vetëm për hartimin e propozimeve ligjore dhe nënligjore në fushën e prokurimeve publike. Në lidhje me këtë gjetje, kërkojmë që rekomandimi të mos adresohet për APP.

Pretendimi i subjektit AKSHI:

Agjencia Kombëtare e Shoqërisë së Informacionit shpreh gadishmërinë për dhënien e kontributit të nevojshëm dhe mirëpret çdo kërkesë për bashkëpunim nga Agjencia e Prokurimit Publik.

Qëndrimi i Grupit të Auditimit:

Grupi i auditimit ka cilësuar dhe përshkruar situatën faktike të ndodhur në APP që me hyrjen në fuqi të VKM nr.673, datë 22.11.2017 “Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar, si dhe nënshkrimit të MNSH ndërmjet AKSHI-t dhe APP-s, nënshkruar ndërmjet palëve. Prandaj është e nevojshme marrja e masave për përditësimin dhe reflektimin e ndryshimeve institucionale të ndodhura në rregulloren e brendshme të funksionimit të veprimtarisë së APP-së. Nga administrimi i dokumentacionit të vendosur në dispozicion ka konstatuar se APP ka në përdorim një bazë rregullative të cilat nuk janë rishikuar dhe update-uar duke mos reflektuar ndryshimet institucionale të ndodhura me hyrjen në fuqi të VKM-së nr. 673, datë 22.11.2017 “Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar, në Agjencinë e Prokurimit Publik, të cilat na janë vendosur në dispozicion si dokumenta të cilat shërbejnë si bazë rregullatore funksionale nga ana juaj. Gjithashtu të gjitha dokumentat janë cituar dhe trajtuar në raport, për rrjedhojë konstatimi i grupit të auditimit nuk ndryshon.

2.Titulli i gjetjes: Mungesa e parashikimit dhe zhvillimit të trajnimeve.

Situata: Nga auditimi u konstatua se:

- Agjencia e Prokurimit Publik, nuk ka plan trajnimi vjetor për vitet 2020 - 2021 për burimet njerëzore të drejtorisë së Administrimit të të Dhënave. Gjatë vitit 2021 kanë zhvilluar trajnime në lidhje me Menaxhimin Strategjik, Statistikë, mbi Prokurimin Publik etj, por në asnjë rast mbi administrimin e sistemit SPE. Gjithashtu, APP nuk disponon dokumentacione mbi propozimet përkatëse nga niveli menaxherial i APP (ku përfshihet dhe drejtoria e burimeve njerëzore) për zhvillimin e trajnimeve. Nuk dokumentohet procesi i kërkesave, nevojave dhe analizimi i tyre për trajnim, duke mos plotësuar kështu nevojat për trajnim mbi sistemet, sigurinë dhe teknologjinë e informacionit.

- Stafi i Sektorit IT atashuar në Agjencinë e Prokurimit Publik nuk ka zhvilluar trajnime mbi sistemet, sigurinë dhe teknologjinë e informacionit, në kundërshtim me rregulloren e brendshme të AKSHI-t nr. 1900, datë 16.04.2020 “Mbi detyrat dhe funksionimi i Agjencisë Kombëtare të Shoqërisë së Informacionit”.

Kriteri: Standardet ndërkombëtare të TIK për rritjen e kapaciteteve, si dhe Rregullorja e Brendshme miratuar me Vendim nr. 03, datë 30.04.2019 “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik”, Rregullore e Brendshme e AKSHI-t nr. 1900, datë 16.04.2020 “Mbi detyrat dhe funksionimi i Agjencisë Kombëtare të Shoqërisë së Informacionit”.

Ndikimi/Efekti: Risk në mos përmbushje të objektivave të përcaktuara. Mungesa e aftësive për zbatimin e rregullave dhe standardeve të sigurisë së informacionit gjatë përdorimit të aseteve.

Shkaku: Mos identifikimi i problematikave mbi burimet njerëzore dhe mungesë planifikimi për zhvillimin e trajnime për burimet njerëzore.

Rëndësia: E Lartë.

2.1. Rekomandimi: Agjencia e Prokurimit Publik të marrë masa për identifikimin e nevojave për trajnimin e stafit të drejtorisë së Administrimit të të Dhënave i cili merret me administrimin e bazës së të dhënave dhe të çdo përdoruesi të sistemit, si dhe të hartojë e miratojë plane për zhvillimin e trajnimeve në lidhje me sistemin e SPE.

2.2. Rekomandimi: Agjencia Kombëtare e Shoqërisë së Informacionit të marrë masa për identifikimin e nevojave dhe zhvillimin e trajnimeve për stafin aktual të sektorit IT atashuar në APP dhe në vijimësi me plotësimin e plotë të këtij sektori.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia e Prokurimit Publik dhe me shkresë nr. 15/7 datë 06.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit APP:

.... lidhur me detyrimin për trajnimin e stafit IT, institucioni jonë nuk ka staf IT që të trajnojnë mbi teknologjinë e informacionit.

Pretendimi i subjektit AKSHI:

Fusha e teknologjisë dhe informacionit zhvillohet dhe përmirësohet vazhdimisht dhe trajnimet e stafit janë në vëmendjen e AKSHI-t dhe kryhen me prioritet. Z. B L me detyrë Specialist i Sektorit i IT në APP, Drejtoria e Marrëdhënieve E-Gov me Institucionet, ka qënë prezent në trajnimin e kryer nga Drejtoria e Monitorimit dhe Mbrojtës Kibernetike të Sistemeve dhe Infstrukturave e-Gov e AKSHI-t, me fokus sigurine kibernetike. Trajnimi konsistonte në sigurinë e sistemeve, infstrukturave dhe nivelin end-user (përdorues) (04/03/2022). AKSHI, në përmbushje të fushës së veprimtarisë dhe detyrave funksionale mirëpret çdo sugjerim apo propozim të APP-së, në kuadër të bashkëpunimit të ndërsjelltë ndërinstytucional.

Qëndrimi i Grupit të Auditimit:

Argumentet e parashtuara nga subjekti i audituar janë përgjithësisht shpjeguese pa fakte të reja. Përsa i përket faktit që APP nuk ka staf IT që të trajtojnë mbi teknologjinë e informacionit, ndoshta APP nuk ka strukture IT, por ka staf IT i cili merret me administrimin e SPE për të cilën nuk ka të kryer asnjë ditë trajnimit.

Argumentet e paraqitura nga AKSHI janë përgjithësisht shpjeguese nuk prekin si dhe nuk hedhin posht konstatimet e auditimit për pasojë konstatimet e grupit të auditimit nuk ndryshojnë, njëkohësisht shpreh dakordësimin në kuadër të bashkëpunimit të ndërsjelltë ndër-institucional.

3. Titulli i gjetjes: Detyrat dhe raportimi i Oficerit të Sigurisë në Agjencinë e Prokurimit Publik.

Situata: Nga auditimi u konstatua se:

- Oficeri i Sigurisë i përcaktuar me Urdhrin e titullarit të APP me nr. 9168/11 prot., datë 24.05.2019 “Për ushtrimin e detyrave”, nuk ka realizuar detyrat e përcaktuara në kundërshtim me Nenin 18 të Rregullores së Brendshme “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik” miratuar me Vendim nr. 03 datë 30.04.2019 të Drejtorit të Përgjithshëm të APP. Gjithashtu raportimi i tij sipas rregullores së brendshme të APP nuk kryhet në nivelin më të lartë drejtues të APP, në mospërputhje me standardet ndërkombëtare dhe praktikat më të mira, pasi vetëm në këtë mënyrë mund të garantohet pavarësia e tij dhe mund të shmangen konfliktet e interesit që lindin, për arsye të ushtrimit të kompetencave të tij.

Kriteri: Neni 18 i Rregullores së Brendshme miratuar me Vendim nr. 03 datë 30.04.2019 të Drejtorit të Përgjithshëm “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik”, si dhe Urdhrit “Për ushtrimin e detyrave” nr. 9168/11 Prot., datë 24.05.2019.

Ndikimi/Efekti: Mos kryerja e detyrave të përcaktuara sipas Rregullores së Brendshme “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik”.

Shkaku: Pozicionimi i Oficerit të Sigurisë nuk i përgjigjet shtrirjes së teknologjisë së informacionit në Agjencinë e Prokurimit Publik.

Rëndësia: E Lartë.

3.1. Rekomandimi: Agjencia e Prokurimit Publik të marrë masa që të kryhen detyrat nga Oficeri i Sigurisë të përcaktuara në Rregulloren e Brendshme të APP si dhe për rregullimin e linjës së varësisë në nivelet menaxheriale, ku raportimi i tij të jetë në nivelin më të lartë drejtues duke kryeje vetëm detyrat e Oficerit të Sigurisë dhe jo funksione të tjera, me qëllim garantimin e pavarësisë dhe shmangien e konfliktit të interesit, në ushtrimin e kompetencave të tij.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 “Mbi Projekt Raportin e Auditimit” nga Agjencia e Prokurimit Publik ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit:

... APP në mënyrë të vazhdueshme (edhe përpara rekomandimit të KLSH në vitin 2018, ka pasur komunikim dhe me DAP për mënyrën se si të përmbushej ky detyrim në përputhje me legjislacionin përkatës. Në kushtet që nuk u krijua mundësia e një pozicioni specifik, në strukturën e APP-së si dhe në zbatim të rekomandimeve të KLSH, oficeri i sigurisë është caktuar me urdher të brendshëm nr. 9168 prot., datë 24.05.2019 nga titullari i institucionit.

Sa i përket konstatimit tuaj që në këtë urdher nuk është përcaktuar linja e raportimit sikurse kërkon legjislacioni përkatës, sjellim në vëmendjen tuaj që urdhri duhet të lexohet në mënyrë sistematike dhe në tërësinë e vet, jo vetëm në përmbajtjen e dispozitivit, por duke nisur nga

baza ligjore, mbi të cilin ka dalë. Konkretisht ky urdhër ka dalë ndër të tjera edhe në bazë të nenit 18 të Rregullores së Brendshme të APP-së, nr. 14, datë 13.09.2018. Në këtë nen janë të përcaktuara detyrat e Oficerit të Sigurisë si dhe linja e raportimit të tij që nuk është sikurse citohet nga ju te sektori i koordinimit, por te administratori përgjegjës i sigurisë mbi gjëndjen e sigurisë. Lutem referojuni n.18 të Rregullores së APP-së.

Nga na tjetër, në momentin që është nënshkruar marrëveshja me AKSHI-n ky funksion për sistemin e prokurimit elektronik, që është dhe objekt i këtij auditimi, nuk kryhet me nga APP, por nga AKSHI.

Qëndrimi i Grupit të Auditimit:

Roli i Oficerit të Sigurisë është caktuar me urdhër të brendshëm nr.1968 prot., datë 24.04.2019 nga titullari i APP, si dhe i janë caktuar detyrat në rregulloren e Brendshme miratuar me Vendim nr.3, datë 30.04.2019 akte këto të hartuara dhe miratuara të mëvonshëm kronologjikisht se nënshkrimi i MNSH ndërmjet AKSHI-t dhe APP-s, nënshruar ndërmjet palëve me shkresën nr.1836 prot., datë 08.04.2018 protokolluar në AKSHI dhe me nr.2982 prot., datë 08.04.2019 protokolluar në APP. Rrjedhimisht grupi i auditimit nuk e shikon të arsyeshme argumentin tuaj në lidhje me konstatimin së detyrat në rolin e Oficerit të Sigurisë, nuk janë realizuar sipas pozicionit të ngarkuar me udhër nr. 916 prot., datë 24.05.2019.

Përsa i përket observimit se: “... në momentin që është nënshkruar marrëveshja me AKSHI-n ky funksion për sistemin e prokurimit elektronik, që është dhe objekt i këtij auditimi, nuk kryhet më nga APP, por nga AKSHI.” Në asnjë pikë të MNSH nuk është shkruar se ky rol duhet të kryhet nga AKSHI dhe nëse do të kryhej nga AKSHI atëherë përse roli i Oficerit të Sigurisë është caktuar se do të kryhet nga vet punonjësit e APP? Kjo dal me Urdhër të brendshëm, gjithashtu ka të përcaktuar detyrat edhe në rregulloren e brendshme siç edhe ju e keni cituar kjo miratuar mbas nënshkrimit të MNSH. Përsa më sipër grupi i auditimit mban të njëjtin qëndrim.

4. Titulli i gjetjes: Identifikimi i risqeve në Sistemin e Prokurimit Elektronik.

Situata: Nga auditimi u konstatua se, regjistri i riskut i APP përgjatë viteve 2020 - 2021 nuk rezulton të ketë patur përditësime mbi risqet e reja të identifikuar, konkretisht:

-Nuk janë identifikuar risqet në burimet njerëzore, të cilat duhen adresuar për të siguruar mirëfunksionimin dhe administrimin e Sistemit të Prokurimit Elektronik;

-Nuk janë analizuar dhe identifikuar mbivendosjet e kompetencave dhe detyrave në lidhje me administrimin e Sistemit të Prokurimit Elektronik, si dhe hapat që do të ndërmerren për minimizimin e problemeve që mund të ndodhin në Sistemin e Prokurimit Elektronik si dhe përgjegjësitë ndërmjet AKSHI-t dhe APP-s.

-Ndarja ose transferimi i risqeve së bashku me asetet tek AKSHI duke qenë se transferimi i aktiveve është bërë gjatë vitit 2020, periudhë për të cilën APP nuk ka marrë masa për rishikimin dhe update-im e regjistrit të riskut për këtë periudhë;

-Nuk janë identifikuar risqe në lidhje me: sigurinë, disponibilitetin dhe integritetin e sistemit dhe të dhënave që gjenerohen nëpërmjet Sistemit të Prokurimit Elektronik.

Kriteri: Neni 11, pika 2, neni 12 pika 3/d dhe nenet 19-21 të ligjit 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”, i ndryshuar.

Ndikimi/Efekti: Mos identifikim, mos adresim i problematikave që mund të shfaqen në Sistemin e Prokurimit Elektronik, shkelje e sigurisë.

Shkaku: Mos update-im i regjistrit të riskut për Sistemin e Prokurimit Elektronik.

Rëndësia: E Lartë.

4.1.Rekomandimi: Agjencia e Prokurimit Publik të marr masa për përditësimin e regjistrit të riskut institucionale, si dhe në bashkëpunim me AKSHI-n të marrin masa për identifikimin dhe analizimin e risqeve për Sistemin e Prokurimit Elektronik me qëllim analizimin dhe vlerësimin e risqeve, për të mos riskuar përmbushjen e objektivave të institucionit. Gjithashtu të marrin

masa për hartimin dhe dokumentimin e një plani veprimi për minimizimin / parandalimin e risqeve të identifikuar, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia e Prokurimit Publik dhe me shkresë nr. 15/7 datë 06.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit APP:

Sa i përket këtij Rekomandimi, APP konstaton se nuk ndahen dhe adresohen qartë detyrimet që ka APP dhe detyrimet që ka AKSHI bazuar në parashikimet ligjore përkatëse në fuqi. Sikurse citohet dhe nga vet grupi i auditimit APP ka hartuar dhe vënë në dispozicion të grupit të kontrollit regjistrat e riskut për vitin 2020 dhe vitin 2021. Sa i përket konstatimit se këto risqe nuk janë updatuar, vlerësojnë se ky konstatim nuk është i bazuar në asnjë akt. APP vlerësojnë të ndryshojë risqet e mundshme vetëm në rast se kjo gje vlerësohet nga analiza e të gjitha të dhënave, mbi të cilin e zhvillon aktivitetin e saj.

Pretendimi i subjektit AKSHI:

Sikurse theksuam edhe në rekomandimet e sipërcituara, AKSHI është i hapur dhe i gatshëm për bashkëpunim në përmbushje të rekomandimeve të lëna nga KLSH-ja.

Qëndrimi i Grupit të Auditimit:

Qëllimi është përmirësimi i mëtejshëm dhe i sigurt në përdorimin e teknologjisë së informacionit. Për sa i përket observimit se nuk ndahen dhe adresohen qartë detyrimet që ka APP dhe detyrimet që ka AKSHI ju në bashkëpunim me AKSHI-n duhet të analizoni dhe të konsideroni risqet që lidhen me Teknologjinë duke bërë një ndarje sa më reale midis atyre që do të administroni vetë dhe atyre që për shkaqe teknike i delegohen AKSHI-t.

Për sa më sipër grupi i auditimit mban të njëjtin qëndrim.

2.2. Auditimi i Sigurisë së Informacionit

Siguria e informacionit është bërë gjithnjë e më shumë e rëndësishme për institucionet, kjo vjen si pasojë e rritjes së kompleksitetit të kontrollit të aksesit dhe ruajtjes së konfidencialitetit, integritetit dhe gatishmërisë së të dhënave nga marrëdhëniet e rrjeteve publike me ato private dhe nga bashkë përdorimi i burimeve të informacionit. Siguria e Informacionit mund të përcaktohet si metoda e një sistemi për të mbrojtur informacionin dhe burimet e sistemeve në përputhje me kushtet e konfidencialitetit, integritetit dhe gatishmërisë.

Lidhur nga sa më sipër, çdo institucion publik shtetëror që ofron shërbime ndaj qytetarëve e ka si detyrim ndërtimin e programit të sigurisë së informacionit me elementët kyç të cilët janë: *“Mjedisi i sigurisë së informacionit, Vlerësimi i riskut, Politikat e sigurisë, Organizimi i sigurisë së TI, Menaxhimi i komunikimeve dhe operacioneve, Menaxhimi i aseteve, Siguria e burimeve njerëzore, Siguria fizike dhe mjedisore, Kontrolli i aksesit, Menaxhimi i incidenteve të sigurisë së TI”*.

a. Auditimi i Sigurisë së të dhënave dhe vazhdimësia e ofrimit të shërbimit”

Objektivi. Identifikimi i elementëve të sigurisë, për të dhënat që kërkojnë monitorim të vazhdueshëm, mbrojtjen e tyre, sigurimi i ofrimit të shërbimit pa ndërprerje si dhe administrimi i përdoruesve mbi këto të dhëna.

kemi shqyrtuar:

- Aktet ligjore/nënligjore/rregullative mbi sigurinë;
- Analizimin e gjurmës audituese të dokumentuar në letër si dhe elektronike (Audit Logs);
- Politikat e vazhdimësisë së shërbimit;

- Listën e përdoruesve të sistemit;
- Procedurat e miratuara për BCC, DRC, Backup;

Konstatohet se :

- APP dhe AKSHI janë institucione me rëndësi të lartë që posedojnë data baza shtetërore informacioni, që ruajnë, përpunojnë dhe gjenerojnë të dhëna me rëndësi , nuk disponojnë një infrastrukturë BCC (Business Continuity Center), në kundërshtim me VKM nr.710, datë 21.08.2013 “Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit”, i ndryshuar.
- Plani i rikuperimit nga katastrofat, plan i cili përdoret për të rikthyer sistemin në gjendje pune në raste katastrofash, i formuluar nga kontraktuesi i SPE, nuk është përditësuar që prej vitit 2017.
- APP, e cilësuar si Operator i infrastrukturave kritike dhe të rëndësishme të informacionit nuk ka të caktuar nga AKSHI pikën e kontaktit për Sistemin e Prokurimit Publik, person përgjegjës për infrastrukturën kritike dhe të rëndësishme të informacionit dhe t’ia komunikojnë Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike sipas Vendimit Nr. 553, datë 15.7.2020.

1.Titulli i gjetjes: APP nuk disponon një infrastrukturë BCC (Business Continuity,center) për garantimin e vazhdimësisë së ofrimit të shërbimit, si dhe nuk është kryer azhurnimi i planit mbi vazhdimësinë e punës dhe rimëkëmbjet nga katastrofat.

Situata 1: Agjencia e Prokurimit Publik, si institucion që posedon sistem informacioni që ruan të dhëna me rëndësi për realizimin e procedurave të Prokurimit, nuk disponon një infrastrukturë BCC (Business Continuity Center), në kundërshtim me *VKM Nr.673 datë 22.11.2017 pika 6k.*

Situata 2: APP disponon politika të shkruara mbi rimëkëmbjet nga katastrofat (disaster recovery plan). Plani i fundit i rikuperimit nga katastrofa i vënë në dispozicion të grupit të auditimit është i vitit 2017 . APP nuk disponon dokumentacion për ngritjen e grupit të punës apo të testeve zhvilluara për funksionimin e këtyre politikave të rëndësishme për Sistemin e Prokurimit Publik . Këto teste nuk kryhen në mënyrë periodike me qëllim dhënien e sigurisë së arsyeshme se sistemi do të funksionojë në të gjitha situatat hipotetike.

Kriteri: *VKM Nr.673 datë 22.11.2017 pika 6k*

Ndikimi/efekti: Risk në humbjen e të dhënave në rast fatkeqësie natyrore.

Shkaku: Nuk janë marrë masat e nevojshme.

Rëndësia: E lartë.

1.1.Rekomandimi: AKSHI bazuar në *VKM Nr.673 datë 22.11.2017 pika 6k* për rëndësinë që ka ofrimi i shërbimit pas një fatkeqësie, të ndërmarrin hapat e nevojshëm për ndërtimin e qendre *Business Continuity* si dhe të azhurnojnë dhe të testojnë planin e rekuperimit nga katastrofa (disaster recovery plan) me qëllim dhënien e sigurisë së arsyeshme se do të funksionojë në të gjitha situatat hipotetike dhe se burimet njerëzore janë të mirënjohura me zbatimin e hapave që duhen ndjekur..

Pretendimi i AKSHI-t: Sqarojmë se Disaster Recovery (Qendra e Vazhdimësisë së Biznesit) është në fazë implementimi aktualisht dhe ky projekt do të adresojë këto problematika, ndërsa dokumentacioni përkatës mbi planin e rekuperimit është pjesë integrale e ISO 27001

Qëndrimi i Grupit të auditimit : Grupi auditimit mban të njëjtin qëndrim për ndërtimin e një qendre BCC.

2.Titulli i gjetjes: Nga auditimi u konstatua se AKSHI nuk kanë marrë masat e nevojshme për rritjen e sigurisë së informacionit në “Sistemin e Prokurimit Publik” dhe nuk ka përcaktuar, pikën e kontaktit si person përgjegjës në AKCESK.

Situata: Në listën e infrastrukturës kritike të informacionit në sektorin qeveritar është përfshirë operatori administrues Agjencia e Prokurimit Publik me sistemin kritik “Sistemi prokurimit Publik” i cili nuk ka përcaktuar, pikën e kontaktit, person përgjegjës për infrastrukturën kritike dhe të rëndësishme të informacionit, dhe t’ia komunikojnë Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

Sa konstatuar më lart është në kundërshtim me VKM nr. 553, datë 15.07.2020 “Për miratimin e listës së infrastrukturës kritike të informacionit dhe listës së infrastrukturave të rëndësishme të informacionit”.

Kriteri: VKM nr. 553, datë 15.07.2020 “Për miratimin e listës së infrastrukturës kritike të informacionit dhe listës së infrastrukturave të rëndësishme të informacionit”

Ndikimi/Efekti: Mos marrja e masave të sigurisë cenon sigurinë e informacionit në sistemet e informacionit dhe disponueshmërinë e besueshmërinë e shërbimeve në sistemin kritik “Sistemi prokurimit Publik”.

Shkaku: Mos kryerja e detyrave funksionale sipas përcaktimeve ligjore përkatëse

Rëndësia: E lartë

2.1.Rekomandim: AKSHI të marri masat e nevojshme për përcaktimin e personit përgjegjës për infrastrukturën kritike “Sistemi i Prokurimit Publik” dhe vendimmarrjen t’ia komunikojë Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

Pretendimi i AKSHI-t Ju bëjmë me dije se personi kontakti në Agjencinë e Prokurimit Publik për Sistemin e Prokurimit publik ka qenë A H dhe më datë 11.03.2022 është përcjellë drejt AKCESK dokumenti me personin e kontaktit të përditësuar i cili është z.B L

Qëndrimi i grupit të auditimit: Në lidhje me pretendimin e paraqitur në observacion nuk është bashkëlidhur dokument justifikues. Për sa më sipër grupi i qëndron konstatimit të tij.

b. Kontrolli i shkallës së sigurisë së aplikacioneve, të drejtat e përdoruesve dhe menaxhimi i tyre

Grupi i auditimit shqyrtoi dokumentacionet e mëposhtme:

- Plani i Sigurisë i Rishikuar versioni 4, Janar 2019;
- Rregullore e Brendshme për Administrimin e Bazës së të Dhënave;
- Aneksi 1. Udhëzim për përdorimin dhe mirëmbajtjen e pajisjeve të teknologjisë së informacionit;
- Aneksi 2. Procedurat e Backup-it dhe Recovery;
- Aneksi 3. Udhëzim për përdorimin dhe pajisjen me llogari përdoruesi në sistemin e prokurimit publik për punonjësit e Agjencisë së Prokurimit Publik;
- Manual për administratorin e sistemit të prokurimit elektronik për menaxhimin e përdoruesve;
- Plan Rikuperimi nga Katastrofa.

Konstatohet se, këto dokumente të vëna në dispozicion grupit të auditimit, janë të pa miratuara si dhe të pa up-dateuara me hyrjen në fuqi të VKM nr. 673, datë 27.11.2017. Gjithashtu, konstatohet se Aneksi 2., si dhe Plani i Rikuperimit nga Katastrofa kanë përmbajtje identikisht të njëjtë si Rregullorja e Brendshme për Administrimin e Bazës së të Dhënave.

Rregullorja e brendshme për administrimin e bazës së të dhënave që i është vendosur në dispozicion grupit të auditimit përshkruan vetëm politikat e backup-it të të dhënave.

- Me anë të Urdhrit nr. 4104 Prot., datë 21.06.2021, të ngritur nga Drejtoresha e Përgjithshme e APP-së Urdhërohet të realizohet ndryshimi i username dhe fjalëkalimit si më poshtë:

Username dhe password i DB;

Username dhe password i router;

Username dhe password i switch;

Akses i Server Management Storage;

Akses i storage të DB (EVA, EVA2);
Akses i storage EVA;
Akses i C7000.

Në pikën 2 (dy) të po këtij urdhri caktohet që një pjesë e fjalëkalimit të administrohet nga përfaqësuesi i APP, znj. XH.L dhe një pjesë e fjalëkalimit nga specialisti i IT së Agjencisë Kombëtare të Shqipërisë së Informacionit i alokuar pranë Agjencisë së Prokurimit Publik z. B L.

Konstatohet se, nuk janë caktuar me anë të një Urdhri të posaçëm nga titullarët respektiv të personave të sipërcituar për caktimin, ndarjen e detyrave dhe përgjegjësi në lidhje me administrimin e bazës së të dhënave. Ky Urdhër ndër të tjera është bazuar në Njoftimin nr. 785 Prot., datë 04.02.2020 të AKSHI i cili cakton z. B L si strukturë përgjegjëse TIK pranë APP në pozicionin e Specialistit.

Nga auditimi konstatohet se, Urdhri nr. 4104 Prot., datë 21.06.2021, nuk është nënshkruar nga të dyja palët (AKSHI-APP) por vetëm nga APP si dhe nuk ka një Urdhër nga organet drejtuese të AKSHI-t për caktimin e Administrimit të një pjese të fjalëkalimit nga Specialisti i Sektorit të IT të AKSHI në APP. Një veprim i tillë nuk citohet në asnjë pikë të marrëveshjes në nivel shërbimi ndërmjet dy institucioneve protokolluar me nr. 1836 prot., (AKSHI) dhe nr. 2982 prot., (APP), ku t'i jepet e drejtë titullarit të një institucioni të ngrejë urdhra me punonjës/specialist të një ins titucioni tjetër.

Me anë të Proces-Verbal nr. 4169 Prot., datë 23.06.2021 është realizuar ndryshimi i fjalëkalimit të passwordit si më poshtë:

Username dhe password i DB;
Username dhe password i router;
Username dhe password i switch;
Akses i Server Management Storage;
Akses i storage të DB (EVA, EVA2);
Akses i storage EVA;
Akses i C7000.

Ku një pjesë e fjalëkalimit administrohet nga përfaqësuesi i APP dhe një pjesë nga përfaqësuesi i AKSHI.

U konstatua se, sipas komunikimeve me personat përgjegjës, para kësaj periudhe administratorë kanë qenë 2 (dy) punonjës nga APP të cilat kanë vazhduar të kenë të drejtë si administrator edhe mbas hyrjes në fuqi të VKM-s nr. 673 datë 27.11.2017. Grupit të auditimit nuk iu vendos në dispozicion asnjë shkresë zyrtare nga organet drejtuese të APP-së për emërimin zyrtarisht të këtyre 2 (dy) punonjës si Administrator.

Edhe pasi është emëruar specialisti i AKSHI në APP më datë 04.02.2020 kanë vazhduar të jenë po punonjëset e APP administrator sistemi.

Gjithashtu konstatohet se, nuk rezulton të jetë miratuar ndonjë akt rregullativ i brendshëm i APP, me qëllim organizimin dhe funksionimin e brendshëm të bazës së të dhënave, në përputhje me kërkesat e ligjit nr.10325, datë 23.09.2010, për “Bazat e të dhënave shtetërore”, neni 5, ku citohet se: “Rregulloret për organizimin dhe funksionimin e brendshëm të bazës së të dhënave shtetërore përcaktohen nga institucioni administrues dhe miratohen nga titullari i tij, në përputhje me standardet, rregullat dhe procedurat e përcaktuara sipas nenit 10 të këtij ligji”.

- “Manuali për administratorin e sistemit të prokurimit elektronik për menaxhimin e përdoruesve” është Versioni 1, i vitit 2018 dhe i pa miratuar.

Ky manual ka për qëllim përcaktimin e rregullave të shkruara në lidhje me veprimet e administratorit në sistem përsa i përket menaxhimit të llogarive të përdoruesve, si dhe kontrolleve dhe procedurave të sigurisë së informacionit që aplikohen në sistem në lidhje me llogaritë e përdoruesve dhe fjalëkalimet e tyre. Konstatohet se ky manual është i pa updatuar

në lidhje me menaxhimin e llogarisë së administratorit i cili ka për qëllim menaxhimin e llogarive të përdoruesve si miratimi i operatorëve ekonomikë të huaj, krijimi i llogarive të administratorit për autoritetin kontraktor, për operatorët ekonomike dhe për punonjësit e APP, bllokimin apo ndryshimin i fjalëkalimeve të tyre. Bazuar në këtë manual Personi i autorizuar për përdorimin e llogarisë së Administratorit i vihet në dispozicion vetëm një punonjësi të APP me anë të një Memo informuese, ku është i përcaktuar llogaria e përdoruesi dhe fjalëkalimi fillestar.

Nga auditimi u konstatua se, për periudhën objekt auditimi, APP nuk disponon një akt rregullativ për administrimin e përdoruesve të Sistemit të Prokurimit Elektronik në të cilin të përcaktohen qartë procedurat që do të ndiqen për administrimin dhe monitorimin e përdoruesve. Respektivisht aktet të cilat i janë vënë në dispozicion grupit të auditimit:

- *Procedura e Manaxhimit të Aksesit*, e cila është e pa miratuar;
- *Plani i Sigurisë i Rishikuar*, versioni 4 Janar 2019, e cila është e pa update-uar;

➤ **Të drejtat e përdoruesve**

- a. *Të drejtat e përdoruesve dhe menaxhimi i tyre*

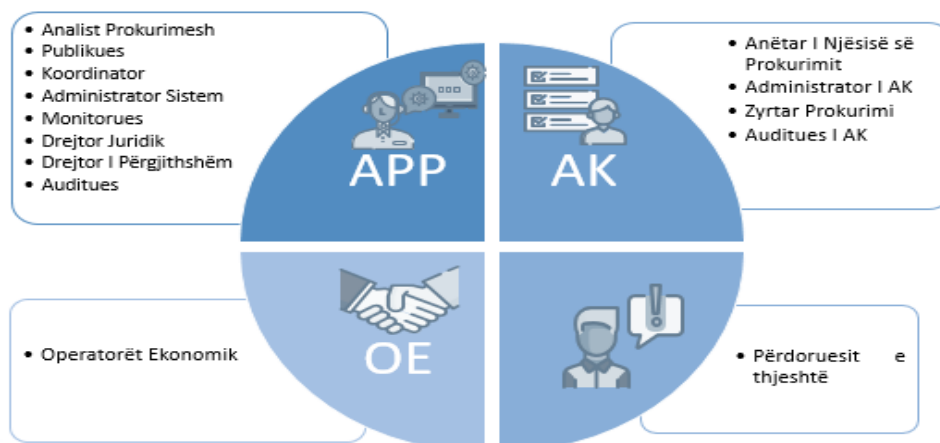
Në platformën e Sistemit të Prokurimit Elektronik është bërë ndarja e përdoruesve në tre grupe kryesore përdoruesish të cilët duan të komunikojnë me sistemin, konkretisht:

- Përdoruesit e Portalit;
- Përdoruesit Mobile;
- Përdoruesit e Sistemit Elektronik të Prokurimit.

Përdoruesit e Sistemit të Prokurimit Elektronik janë të gjithë përdoruesit e identifikueshëm nga sistemi i prokurimit, të cilët aksesojnë funksionalitetet e sistemit me anë të një llogarie përdoruesi dhe fjalëkalim të vlefshëm, që të kryejnë funksione të avancuara si krijime njoftimesh për tendera, pjesëmarrje në tendera, vlerësime etj. Ky grup përbëhet nga tre nëngrupe të mëdha përdoruesish që janë:

- **Operatorët Ekonomik** janë përdoruesit të cilët marrin pjesë në procedurat e prokurimit të shpallur nga autoritetet kontraktore në sistem, duke ngarkuar dokumentacionin përkatës si dhe ofertën financiare;
- **Autoritetet Kontraktore** është grupi i përdoruesve, të cilët merren me krijimin e regjistrimit të elementëve të njoftimeve për tender, përfitues, për lidhje kontrate si dhe kryen vlerësime të ofertave dhe dokumentacioneve, si dhe institucionet e tjera të lidhura me prokurimin publik;
- **Agjencia e Prokurimit Publik**, publikon elementet e regjistrave të parashikimeve publike, njoftimet si njoftim kontrate, njoftim fituesit, njoftim të lidhjes së kontratës dhe njoftim anulimi për procedurat e shpallura nga autoritetet kontraktore, koordinon veprimet me personat përgjegjës, etj.

Fig nr.1 Përdoruesit e Sistemit të Prokurimit Elektronik



Burimi: APP përpunuar nga grupi i auditimit

➤ **Llogaritë e përdoruesit në rolet:**

a) Për Autoritet Kontraktore (AK) janë krijuar disa role si:

- **Administrator i Sistemit për AK (CAAdmin)**, ky rol ka të drejtë të krijojë llogari përdoruesi për llogaritë e përdoruesit pranë AK, anëtarët e njësisë së prokurimit, të komisionit të hapjes dhe vlerësimit të ofertave, auditues. Të bëjë ndryshim të fjalëkalimeve për llogaritë e përdoruesve pranë AK, të cilët e humbasin atë. Të bëjë bllokimin / mbylljen e llogarisë së përdoruesit i cili largohet nga AK, duke zgjedhur opsionin “I Gabuar” tek fusha “Është Miratuar” por nuk ka të drejtë ta fshijë llogarinë. Kryen pezullimin e një procedure në sistem bazuar në dispozitat ligjore, dërgon për miratim elementet (zërat) e regjistrimit në sistem, shënon si të realizuar elementët blerje nën 100.000 (njëqind mijë) lekë, amendamentet etj

-**Njësia e Prokurimit(AdminOfficer)** është anëtari i njësisë së prokurimit dhe ka të drejtë të krijojë dhe të ndjekë mbarëvajtjen hap pas hapi të procedurave të prokurimit publik në SPE në zbatim të LPP, etj.

-**Komisioni i Vlerësimit të Ofertave (Procurement Officer)** është anëtari i Komisionit të Hapjes dhe Vlerësimit të Ofertave ka të drejtë të hapë procedurën e prokurimit publik në datën dhe orën e përcaktuar në sistem, shkarkon dokumentacionin e dorëzuar në zbatim të LPP, etj.

-**Auditues i AK (CAAuditor)** (ka të drejta vetëm read-only) i cili gjeneron raportin informues për procedurën e prokurimit, lexon procedurën në sistem, etj.

b)Roli për Operatorët ekonomike (Economic Operator) është roli i Operatorëve ekonomike, të cilët mund të logohen në SPE me anë të NIPT-it të tyre. Kanë të drejtë të krijojnë ofertë ekonomike në një procedurë deri në afatin e fundit të pritjes së ofertave të përcaktuar në sistem, të bëjnë kërkesa për sqarim në sistem, të dërgojnë apo të marrin mesazhe nga AK, etj.

c)Roli i Audituesit në sistem monitoron procedurat e krijuara nga autoritet kontraktore pas përfundimit të afatit ankimor për vlerësimin e ofertave pranë autoritetit kontraktor, për çdo fazë të mbyllur të procedurës. Gjeneron raport, për procedurat e prokurimit të cilat janë para hapjes dhe vlerësimit në sistem, etj.

d)Roli i Publikuesit në sistem është zyrtari pranë APP-së i cili bën publikimin ose pezullimin e njoftimeve të procedurave, njoftim fituesit dhe njoftimeve të kontratave të nënshkruara që të hidhen në sistem nga anëtarët e njësisë së prokurimit pranë çdo autoriteti kontraktor, etj.

e)Roli i Administratorit. Me anë të Administratorit mund të:

- Krijohen llogaritë e përdoruesit për Administratorin e Sistemit të Autoritet Kontraktor;
- Krijohen llogaritë e përdoruesit për Operatorët Ekonomikë;
- Miratohen llogaritë e përdoruesve Operatorët Ekonomikë të Huaj, që kanë aplikuar në portal;
- Krijohen llogaritë e përdoruesit për anëtarët e Komisionit të Prokurimit Publik;
- Krijohen llogaritë e përdoruesit për Prokurorinë e Përgjithshme;
- Bëhet ndryshim i fjalëkalimeve për llogaritë e mësipërme, në rast se humbasin fjalëkalimin;
- Bëhet bllokimi i llogarive për Administratorin e Sistemit të Autoritet Kontraktor, në rast se autoriteti kontraktor pushon së ekzistuari;
- Bëhet bllokimi i llogarive për Operatorin Ekonomik, në rast se operatori ekonomik përjashtohet me Vendim të APP nga Procedurat e Prokurimit Publik, nga Procedurat Konkurruese Koncesionare/Partneritetin Publik Privat si dhe procedurat e Ankandit Publik;
- Bëhet bllokimi i llogarive për anëtarët e Komisionit të Prokurimit Publik, në rast se anëtarët largohen nga pozicioni i tyre në KPP;
- Krijon llogaritë e përdoruesit për Agjencinë e Prokurimit Publik në rolet:
 - Analist Prokurimesh (Llogari përdoruesi për specialistët e Sektorit të Informacionit

- dhe Statistikave);
- Nëpunës i Publikimit (Llogari përdoruesi për specialistët e Sektorit të Publikimit);
- Koordinator (Llogari përdoruesi për Drejtoria e Kordinimit dhe Monitorimit të Kontratave);
- Monitorues;
- Auditues PP (Llogari përdoruesi për specialistët e Drejtorisë Drejtoria Juridike dhe e Integritimit);
- Administratori
- KVO
- Njësi Prokurimi
- Amin (AK)
- Director
- JuridicalDirector

- Sipas Planit të Sigurisë i rishikuar viti 2019 i pa update-uar por ende si bazë rregullore nga punonjësit e APP, **pika 4.2 Punonjësit e APP** në të cilën citohet se: *“Punonjësit e APP pajisen me llogari përdoruesi sipas përshkrimit të punës dhe në zbatim të detyrave të përcaktuara ...”* po ashtu edhe në **pikën 8.1** të po kësaj rregulloreje citohet se: *“Aksesi për përdoruesit e brendshëm në sistemet e APP duhet të jetë i bazuar në detyrat që ata kanë. Detyrat do të jenë të përcaktuara qartë, dhe për të minimizuar rrezikun e aktiviteteve mashtruese ose keqdashëse, ndarja e tyre do të jetë e detyrueshme.”*

Nga auditimi u konstatua se, nuk ka një rregullore apo dokument tjetër shkresor ku të përcaktohet qartë lidhja përdorues-punonjësi i APP duke sjell risk potencial të akordimit subjektiv të të drejtave mbi përdorimin e sistemit, si dhe akumulimin e privilegjeve.

Konkretisht për rolet:

- *Analist Prokurimesh;*
- *Nëpunës i publikimit;*
- *Koordinator;*
- *Monitorues.*

Bazuar në manualin për administratorin e sistemit të prokurimit elektronik për menaxhimin e përdoruesve i cili është i pa update-uar, (Version 1, 2018) jo vetëm nga ndryshimet strukturore që kanë ndodhur ndër vite në APP por edhe me hyrjen në fuqi të VKM nr. 673, datë 23.11.2017, konstatohet se llogaria e Analist Prokurimesh përdoret nga specialistët e Sektorit të Informacionit dhe Statistikave nuk përdoret vetëm nga specialistët e këtij sektori por edhe nga specialist i sektorit të koordinimit konkretisht useri “lk”;

- Nëpunës i Publikimit (Llogari përdoruesi për specialistët e Sektorit të Publikimit);
- Koordinator (Llogari përdoruesi për Drejtoria e Kordinimit dhe Monitorimit të Kontratave);
- Monitorues
- Auditues PP (Llogari përdoruesi për specialistët e Drejtorisë Drejtoria Juridike dhe e Integritimit

- Çdo Autoritet Kontraktor ka në dispozicion një llogari administratori me anë të së cilës krijon, mbyll llogari me rolin përkatës sipas nevojave të institucionit për të aksesuar në sistemin e APP.

Nga auditimi u konstatua se, hapja e këtyre përdoruesve mbetet pothuajse e pamonitoruar, pasi vetë APP nuk kryen monitorime që lidhen me këtë veprim, duke rritur riskun e krijimit të përdoruesve të paautorizuar, e për pasojë humbjen e konfidencialitetit të të dhënave apo keqpërdorimin e tyre.

- Me anë të Urdhrit nr. 10761/1 Prot., datë 21.12.2018, punonjësi z.D B autorizohet për përdorimin e llogarisë së përdoruesit në rolin e Administratorit të Sistemit të Prokurimit Publik, pozicionuar sipas strukturës Specialist i Sektorit të Administrimit të të Dhënave. Me nënshkrimin e MNSH-së ndërmjet AKSHI-t dhe APP-s, nënshkruar ndërmjet palëve me shkresën nr. 1836 prot., datë 08.04.2019 protokolluar në AKSHI dhe me nr. 2982 prot., datë 08.04.2019 protokolluar në APP nuk është përcaktuar se cili do të jetë administratori i sistemit në funksion të përcaktimit të procedurave organizative dhe teknike dhe masave për miratimin, krijimin, bllokimin apo ndryshimin e fjalëkalimeve të llogarive të përdoruesve nga Administratori i Sistemit të Prokurimit Elektronik.

Nga auditimi u konstatua se, APP nuk disponon akte rregullator për menaxhimin e log-eve digjitale në administratën publike, në kundërshtim me pikën 4 shkronja a) të “Rregullores për menaxhimin e log-eve digjitale në Administratën Publike”, miratuar me urdhrin nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT) Institucioni duhet të përcaktojë një rregullore të shkruar për menaxhimin e log-eve sipas kërkesave të institucionit. Kjo rregullore duhet të specifikojë qartë të gjitha kërkesat për ruajtjen e log-eve përkatëse për çdo sistem/pajisje të institucionit, procedurat e administrimit dhe përgjegjësitë në përputhje me këtë rregullore dhe legjislacionin në fuqi.

Përdoruesit e Sistemit të Prokurimit Elektronik (SPE)

APP disponon 324 310 përdorues të sistemit SPE nga të cilët 314 288 përdorues aktiv, 9993 përdorues të bllokuar dhe 29 përdorues të përjashtuar, përkatësisht të ndarë sipas roleve përkatëse në sistem:

- CAAdmin 2136 përdorues aktiv dhe 322 përdorues të bllokuar;
- KPP 18 përdorues aktiv;
- KVO 31 353 përdorues aktiv dhe 4869 përdorues të bllokuar;
- Njësi Prokurimi 26 747 përdorues aktiv dhe 4035 përdorues të bllokuar;
- Operatori Ekonomik 250 310 përdorues aktiv dhe 66 përdorues të bllokuar;
- Auditor 3724 përdorues aktiv dhe 701 përdorues të bllokuar;
- Operator Ekonomik 29 përdorues të përjashtuar;

Nga auditimi mbi përdoruesit e Sistemit të Prokurimit Publik u konstatua se:

- Administratori i sistemit i cili bën menaxhimin e llogarive të përdoruesve mbështetet në Manualin për Administratorin e Sistemit të Prokurimit Elektronik për Menaxhimin e Përdoruesve i cili është i pa update-uar, (Version 1, 2018).

- nuk janë aplikuar në sistem kritere të detyrueshme për rritjen e vështirësisë së fjalëkalimit për përdoruesit, si periodiciteti për ndryshimin e tij, me qëllim rritjen e sigurisë në identifikimin e përdoruesit etj, bazuar në pikën 4 “Kërkesat e Sigurisë” pika a. të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuar nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

- Nuk janë dokumentuar dhe implementuara politika për fjalëkalimet e sistemeve qendrore dhe administrimit bazuar në pikën 4 “Kërkesat e Sigurisë” pika b. Të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuara nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

Krijimi i përdoruesve në sistem nga ana e administratorit të sistemit

Për të krijuar përdorues me role të caktuara në sistem, Administratori i sistemit duhet të klikojë tek dosja “Përdoruesit”. Në këtë seksion duhet të klikohet butoni “Krijo përdorues të ri” (Create New user).

Në dritaren që do shfaqet fusha e emërtuar “Login” duhet të plotësohet si më poshtë:

- “emër_mbiemër” në rast se do krijohet një anëtar i njësisë së prokurimit

- “emër.mbiemër” në rast se do krijohet një anëtar i komisionit të hapjes dhe vlerësimit të ofertave
- “emërmbiemër” në rast se do krijohet një anëtar i komisionit të shqyrtimit të ankesave ose audit

Nga verifikimi i detajuar mbi përdoruesit e Sistemit të Prokurimit Elektronik konstatohet se:

- Administratori i sistemit i cili bën menaxhimin e llogarive të përdoruesve mbështetet në Manualin për Administratorin e Sistemit të Prokurimit Elektronik për Menaxhimin e Përdoruesve i cili është i pa update-uar, (Version 1, 2018).

- Nuk janë aplikuar në sistem kritere të detyrueshme për rritjen e vështirësisë së fjalëkalimit për përdoruesit, si periodiciteti për ndryshimin e tij, me qëllim rritjen e sigurisë në identifikimin e përdoruesit etj, bazuar në pikën 4 “Kërkesat e Sigurisë” pika a. të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuar nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

- Nuk janë dokumentuar e implementuar politikat për fjalëkalimet e sistemeve qendrore dhe administrimit bazuar në pikën 4 “Kërkesat e Sigurisë” pika b. Të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuara nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

- Administratori i sistemit i cili në sistem ka rolin System Admin është krijuar me “Data e Krijimit” 11/01/2018 si dhe nuk i ka të plotësuara të gjitha fushat në sistem. Kjo situatë sjell risk për humbjen e gjurmës audituese, risk për kryerjen apo moskryerjen e veprimeve të autorizuar në sistem;

-Ka përdorues për të cilët fushën “Hyr” që është username me të cilin përdoruesi logohet dhe fushën “Emri i Plote” janë si përdorues aktiv në sistem me kredenciale të përgjithshme të cilët nuk janë përcaktuar se nga cili punonjës posedohen dhe përdoren. Ky fakt mbart një risk të lartë për ndërhyrje të paautorizuara në sistem duke mos lënë gjurmë mbi aktivitetin që kanë kryer;

- Për user-at në rolin e KVO fusha “Hyr” që është username me të cilin përdoruesi logohet nuk është sipas “Manualit të përdorimit të Sistemit të Prokurimit Elektronik për Administratorin e Autoritetit kontraktor”, formati i të cilit është “emër.mbiemër”. konstatohen raste që ky format është: emër_mbiemër, emër_mbiemërnumër, emër, emërnumër, emër.mbiemërnumër, etj.,

- Për user-at në rolin e Njesisë së Prokurimit fusha “Hyr” që është username me të cilin përdoruesi logohet nuk është sipas “Manualit të përdorimit të Sistemit të Prokurimit Elektronik për Administratorin e Autoritetit kontraktor”, formati i të cilit është “emër_mbiemër”, konstatohen raste që ky format është: emër.mbiemër, emër*mbiemër, emër_numëmbiemër, emër_mbiemërnumër, emër.mbiemërnumër, gërma e parë e emrit.mbiemër, emër, emërmbiemër@gmail.com, etj.,

- Administratori i Autoritetit Kontraktor në këtë rast Agjencia e Prokurimit Publik është me rolin “Amin. Ak”;

- Ekziston aktiv përdoruesi me fushën “Hyr” = xh që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me Data e Krijimi 08/02/2016 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si përgjegjëse sektori duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh, për të cilën mungon edhe përshkrimi i punës;

- Ekziston aktiv përdoruesi me fushën “Hyr” = gj që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me “Data e Krijimi” 05/09/2007 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si Drejtor i Drejtorisë së Administrimit të të Dhënave dhe Publikimit duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh;

- Ekziston aktiv përdoruesi me fushën “Hyr” = LK që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me Data e Krijimi 03/20/2010 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si specialist në Sektorin e

Koordinimit duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh;

- Mbajnë statusin “aktiv” përdorues në rolin “auditor”, konkretisht auditues të KLSH-së, të cilët kanë përfunduar detyrat e tyre gjatë auditimit në terren dhe përdoruesit në sistem rezultojnë të jenë akoma aktiv;
- Rezulton se ka përdorues për të cilët fusha “Email” është NULL (i paplotësuar);
- Ekzistojnë përdorues për të cilët fusha “Email” është mm/dd/vv;
- Ekzistojnë përdorues për të cilët data e krijimit është ‘Po’ ose ‘Jo’.

3.Titulli i gjetjes: Janë ngritur urdhra të pabazuara juridikisht dhe në kundërshtim me Ligjin nr.10296, datë 08.07.2010 “*Për menaxhimin financiar dhe kontrollin*”.

Situata: Nga auditimi u konstatua se fjalëkalimi i administratorit të databazës është i ndarë në dy pjesë sipas përcaktimeve të Urdhrit nr. 4104 Prot., datë 21.06.2021 të Drejtorit të Përgjithshëm të APP-së. Gjithashtu sipas përcaktimeve të këtij urdhri bëhen ndryshimet dhe për ndryshimin e username dhe fjalëkalimit për: *Username dhe password i router; Username dhe password i switch; Akses i Server Management Storage; Akses i storage të DB (EVA, EVA2); Akses i storage EVA; Akses i C7000.*

Urdhri i sipërcituar i cili përcakton se një pjesë e fjalëkalimeve administrohet nga përfaqësuesi i APP dhe një pjesë e fjalëkalimeve administrohet nga specialisti i TI-s së AKSHI-t atashuar pranë APP, është hartuar dhe miratuar në mënyrë të njëanshme vetëm nga Titullari i APP dhe nuk ka marrë edhe miratimin e strukturave drejtuese të AKSHI-t, si palë administruese në proces.

Kriteri: Kreu II, neni 8, pika 7 e Ligjit nr.10296, datë 08.07.2010 “*Për menaxhimin financiar dhe kontrollin*”.

Ndikimi/Efekt: Risk i lartë për keq adresim të shpërndarjes së punës mbi sistemin e SPE në APP.

Shkaku: Mos zbatim i akteve ligjore dhe nënligjore të marrëdhënieve ndërmjet APP dhe AKSHI-t.

Rëndësia: E Lartë.

3.1.Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me AKSHI-n të marrin masa për hartimin dhe miratimin e një akti rregullativ të përbashkët për caktimin e administrimit të bazës së të dhënave të Sistemit të Prokurimit Elektronik, ku të përcaktohen qartë përgjegjësitë mbi administrimin e Sistemit të Prokurimit Elektronik në përputhje me dispozitat ligjore në fuqi.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia e Prokurimit Publik dhe me shkresë nr. 15/7 datë 06.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit APP:

Sa i përket gjetjes së sipërcituar, sikurse është prapësuar më sipër ky urdhër është pjesë e një procesi që ka filluar që në vitin 2020 me atashimin e specialistit të IT së AKSHI, të alokuar pranë APP, ju vu në dispozicion një pjesë e fjalëkalimeve, si dhe u vu në dijeni AKSHI me anë të shkrësës për ndarjen e kredencialeve dhe menyrën e organizimit të punës. Ky proces është dakordësuar me të gjitha palët dhe APP është kujdesur gjithmone të verë në dijeni AKSHI-n për çdo veprim që kryen. Urdhri i dal nga titullari është në vazhdimësi të këtij procesi përderisa ka pasur miratimin paraprak të AKSHI për ndarjen e kredencialeve.

Pretendimi i subjektit AKSHI:

Përcaktimi i personave përgjegjës (ndjekësve të kontratës), realizohet me ngritjen e urdhrave nga titullarët e secilit institucion. Gjithashtu në Rregulloren Nr. 1, datë 17.01.2022 “Për sigurinë e Informacionit” të AKSHI-t përcaktohen në mënyrë shteruese të gjitha të drejtat

administrative, masat teknike si dhe posedimi e zotërimi i fjalëkalimeve të sistemeve e databazës.

Qëndrimi i Grupit të Auditimit:

Argumentat e parashikuara nga APP janë përgjithësisht shpjeguese pa fakte të tjera të dokumentuara.

Proçesi i dakordësimit nuk është dokumentuar dhe nënshkruar nga të dyja palët. Dokumentat që vërtetojnë se urdhëri i dal nga titullari ka pas miratimin paraprak të AKSHI për ndarjen e kredencialeve nuk i është vendos në dispozicion grupit të auditimit.

Observimi i AKSHI-t mbi Rregulloren nuk ka lidhje me konstatimin e grupit të auditimit pasi lidhet me caktimin e administratorit në urdhra të pabazuara juridikisht dhe në kundërshtim me Ligjin nr.10296, datë 08.07.2010.

Për sa më sipër grupi i auditimit nuk ndryshon qëndrim.

4. Titulli i gjetjes: Mungesa e akteve rregullative për organizimin, funksionimin e brendshëm dhe mirë administrimin e bazës së të dhënave shtetërore për Sistemin e Prokurimit Elektronik.

Situata: Nga auditimi u konstatua se, APP nuk ka një akt rregullativ të brendshëm, me qëllim organizimin dhe funksionimin e brendshëm të bazës së të dhënave, në përputhje me kërkesat e ligjit nr.10325, datë 23.09.2010, për *“Bazat e të dhënave shtetërore”*, neni 5, ku citohet se: *“Rregulloret për organizimin dhe funksionimin e brendshëm të bazës së të dhënave shtetërore përcaktohen nga institucioni administrues dhe miratohen nga titullari i tij, në përputhje me standardet, rregullat dhe procedurat e përcaktuara sipas nenit 10 të këtij ligji”*.

Kriteri: Neni 5 i Ligjit nr.10325, datë 23.09.2010, për *“Bazat e të dhënave shtetërore”*.

Shkaku: Mos zbatim i ligjit nr.10325, datë 23.9.2010, për *“Bazat e të dhënave shtetërore”*.

Rëndësia: E Lartë.

4.1. Rekomandimi: Agjencia e Prokurimit Publik si institucion administrues i bazës së të dhënave shtetërore që gjenerohen nëpërmjet Sistemit të Prokurimit Elektronik, të marri masa për përmbushjen e përcaktimeve ligjore mbi rregulloren për organizimin dhe funksionimin e brendshëm të bazës së të dhënave shtetërore.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 “Mbi Projekt Raportin e Auditimit” nga Agjencia e Prokurimit Publik ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit:

Në lidhje me gjetjen e mësipërme, APP ju ka vendosur në dispozicion të gjitha rregulloret e brendshme, udhezimet dhe manualet mbi të cilat është organizuar dhe përdoret databaza e të dhënave. Gjithashtu, Plani i Sigurisë versioni 2019 i rishikuar i cili ju është vendosur në dispozicion vepron në mbështetje të nenit 100 të Kushtetutës dhe në mbështetje të Ligjit Nr. 10325, datë 23.09.2010 “Për Bazat e të Dhënave Shtetërore”, të ligjit LIGJ Nr. 2/2017 “PËR SIGURINË KIBERNETIKE”, Vendimin e Këshillit të Ministriave Nr. 659, datë 03.10.2007 “Për rregullat e kryerjes se procedurave të prokurimit publik me mjete elektronike”.

Qëndrimi i Grupit të Auditimit:

Plani i Sigurisë versioni 2019 i rishikuar siç është konstatuar edhe nga grupi i auditimit është i pa miratuara si dhe i pa update-uar që me hyrjen në fuqi të VKM nr. 673, datë 27.11.2017. Për pasojë konstatimi i grupit të auditimit nuk ndryshon.

5. Titulli i gjetjes: Mungesë në përcaktimin e lidhjes punonjës-përdorues.

Situata: Nga auditimi u konstatua se, nuk ka një akt rregullativ ku të përcaktohet lidhja ndërmjet pozicionit të punës të specialistit dhe të drejtave që ky pozicion duhet të ketë në sistem.

Konkretisht për rolet:

- *Analist Prokurimesh*
- *Nëpunës i publikimit;*
- *Koordinator;*
- *Monitorues.*

Kriteri: Plani i Sigurisë i rishikuar viti 2019 i cili përdoret si bazë rregullatore nga punonjësit e APP.

Ndikimi/Efekti: Risk potencial të akordimit subjektiv të të drejtave mbi përdorimin e sistemit, si dhe akumulim të privilegjeve të userave në sistem.

Shkaku: Akumulim të privilegjeve për përdoruesit e sistemit.

Rëndësia: E mesme.

6.1.Rekomandimi: APP 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 përdorues i sistemit me qëllim uljen e riskut të dhënies së të të drejtave mbi përdorimin e sistemit, si dhe mbivendosjes sëtributeve.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 “Mbi Projekt Raportin e Auditimit” nga Agjencia e Prokurimit Publik ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit:

Në përshkrimet e punës së gjithësecilit ashtu edhe në Aneks 3. Udhëzim për përdorimin dhe pajisjen me llogari përdoruesi në sistemin e prokurimit publik për punonjësit e agjencisë së prokurimit publik të cilat janë vendosur në dispozicion secili përdorues e ka të specifikuar dhe identifikohet qarte se kujt i perket llogaria e përdoruesit në fjale.

Referuar Aneks 3. Udhëzim Për Përdorimin dhe pajisjen Me Llogari Përdoruesi Në Sistemin E Prokurimit Publik Për Punonjësit e Agjencisë së Prokurimit Publik,

...

Specialistët të cilët do jenë pjesë e Sektorit të Informacionit duhet të pajisjen me këtë llogari përdoruesi në zbatim të detyrave të përcaktuara tek përshkrimi i punës.

Qëndrimi i Grupit të Auditimit:

Situata e konstatuar mbështetet në administrimin e dokumentacionit të vendosur në dispozicion, konkretisht: Plani i Sigurisë i Rishikuar Aneksi 3 e cila përdoret si bazë rregullatore nga punonjësit tuaj. Sipas këtij Plani përcaktohet se aneksi për përdoruesit e brendshëm në sistemet e APP bazohet në detyrat që ata kanë sipas përshkrimit të punës dhe në zbatim të detyrave të përcaktuara, ku nga konstatimet e grupit të auditimit përshkrimet e punës si dhe plani i sigurisë janë të pa update-uar me ndryshimet institucionale të ndodhura me hyrjen në fuqi të VKM-së nr.673, datë 22.11.2017 “Për Riorganizimin e Agjencië Kombëtare të Shoqërisë së Informacionit”, i ndryshuar. Për sa më sipër qëndrimi i grupit të auditimit nuk ndryshon.

6. Titulli i gjetjes: Administrimi i përdoruesve të Sistemit të Prokurimit Elektronik.

Situata: Nga auditimi u konstatua se në Marrëveshjen e Nivelit të Shërbimit të nëshkruar ndërmjet AKSHI-t dhe APP-s, nuk është përcaktuar se cili do të jetë administratori i sistemit në funksion të përcaktimit të procedurave organizative dhe teknike dhe masave për miratimin, krijimin, bllokimin apo ndryshimin e fjalëkalimeve të llogarive të përdoruesve nga Administratori i Sistemit të Prokurimit Elektronik në kundërshtim me VKM nr. 673, datë 22.11.2017 “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar.

Kriteri: Pika 7 e “Rregullores së Sigurisë së Informacionit”, miratuar me Urdhër nr. 30, datë 17.01.2022 nga AKSHI, VKM Nr. 673, datë 22.11.2017, “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, Marrëveshje Nivel Shërbimi (SLA) nënshkruar ndërmjet AKSHI-t dhe APP-s.

Ndikimi/Efekti: Keq administrim i përdoruesve të Sistemit të Prokurimit Elektronik krijon kushte për shkelje të sigurisë.

Shkaku: Mos marrja e masave në lidhje mbi përcaktimin e administrimit të përdoruesve të Sistemit të Prokurimit Elektronik.

Rëndësia: E Lartë.

6.1. Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit të marrin masat për përcaktimin e administratorit të sistemit në funksion të procedurave organizative ,teknike dhe marrjen e masave për krijimin, bllokimin apo ndryshimin e fjalëkalimeve të llogarive të përdoruesve të Sistemit të Prokurimit Elektronik në përputhje me dispozitat ligjore në fuqi.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit AKSHI:

Në pikën 1, të Aneksit 2, “Procedurat e thjeshtuara të menaxhimit të aksesit dhe proceseve të punës”, të Rregullores Nr.1, datë 17.01.2022 “Për sigurinë e Informacionitë, përcaktohet shprehimisht se: “Administratori i sistemit dhe i databazës duhet të sigurojë që fjalëkalimi të jetë në përputhje me qëllimin për të cilin është lëshuar.

Në veçanti, fjalëkalimi duhet:

- të jetë në çdo rast i ndarë minimalishi midis dy personave përgjegjës për sistemin dhe bazën e të dhënave;
- të jetë me një gjatësi minimale prej 14 karakteresh (ose ekuivalent me numrin maksimal të përcaktuar të karaktereve nëse ekzistojnë kufizime më të rrepta për sisteme ose aplikacione specifike);
- të përfshijë karaktere alfabetike (shkronjat e mëdha dhe të vogla), numerike dhe karaktere speciale (!, \$, &, etj.), me rregullat përkatëse që do të specifikohen më poshtë;
- të mos përfshijë informacione që mund të gjurmohen te përdoruesit (p.sh. emri, mbiemri, data e lindjes);
- të ndryshohet çdo 90 ditë, të paktën, nëse nuk përdoret një faktor i dytë i vërtetimit;
- të ndalojë ri-përdorimin e katër e fjalëkalimeve të mëparshëm në rastin e zëvendësimit të fjalëkalimit.”

Qëndrimi i Grupit të Auditimit:

Konstatimi i grupit të auditimit lidhet me nevojën për përmirësim dhe adresimin e saktë që ka kjo problematikë, pa anashkaluar punën dhe hapat që janë ndërmarrë nga ana juaj, për pasojë konstatimet e grupit të auditimit nuk ndryshojnë.

7. Titulli i gjetjes: Mungesa e menaxhimit të logeve.

Situata: Nga auditimi u konstatua se, nuk disponohet një akt rregullator për menaxhimin e logeve dixhitale në administratën publike, në kundërshtim me pikën 4 shkronja a) të “Rregullores për menaxhimin e log-eve digjitale në Administratën Publike”, miratuar me Urdhër nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike.

Kriteri: Urdhri nr. 109 datë 10.06.2016 i “Rregullores për menaxhimin e log-eve digjitale në Administratën Publike”, miratuar me të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT).

Ndikimi/Efekti: Pamundësi për të identifikuar ndërhyrjet në sistem nga përdoruesit e sistemit duke qenë se Regjistrat e të dhënave janë nën administrim të APP

Shkaku: Mos zbatim i rregullores miratuar nga AKCESK.

Rëndësia: E Lartë.

7.1. Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit t’i japin rëndësi sigurisë dhe mbrojtjes së të dhënave duke filluar së pari me hartimin e një procedure apo rregullore për menaxhimin e gjurmës elektronike të auditimit, me qëllim uljen e riskut mbi sigurinë e të dhënave me pasojë humbjen dhe tjetërsimin e tyre. Gjithashtu në këtë dokument duhet të specifikohet qartë vendi ku ruhen gjurmët, për cilat veprime të përdoruesit ruhen këto gjurmë, koha, struktura përgjegjëse për monitorimin dhe analizimin e tyre, detyrat dhe përgjegjësitë, e çdo element që i shërben sigurisë së të dhënave dhe parandalimit në tjetërsimin e tyre.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia e Prokurimit Publik dhe me shkresë nr. 15/7 datë 06.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit APP:

Sistemi i Prokurimit Publik ka pasur menyren e ruajtjes se logeve ne server me Agjent. Agjenti ka qene instaluar te hosti dhe ai bënte filtrimin dhe agregimin e log-eve. Më pas i dërgon ato në server. Agjenti AuditVault startohej nga ana jone dhe me pas eshte ribere konfigurimi qe ky agjent te startohej automatikisht ne momentin qe dilte Unreachable. Administrimi i logeve behet nga AKSHI pas kalimit te infrastruktures tek AKSHI.

Sa më sipër kërkojmë rivlerësimin e rekomandimit dhe ri adresimin e tij, ku AKSHI të ketë rolin kryesor, për shkak të kompetencave që i jep legjislacioni përkatës.

Pretendimi i subjektit AKSHI:

Dokumentat të cilat hartojnë procedurat e ndryshme mbi të gjithë elementet (gurmë elektronike, vlerësimi i riskut dhe siguria kibernetike) janë të miratuara dhe konform standarteve ndërkombëtare ISO 27001 më të cilat AKSHI është i certifikuar.

Qëndrimi i Grupit të Auditimit:

Ju sqarojmë se, si administrator të sistemit AKSHI ofron kushte teknike që gjurma elektronike e auditimit të ruhet, ndërsa se çfarë do të ruhet e përcakton institucioni administrues i bazës së të dhënave që është APP në bashkëpunim me AKSHI-n.

Në lidhje me observimin nga ana e AKSHI-t grupit të auditimit nuk i është vendos në dispozicion asnjë dokumentacion shoqërues.

Përsa më sipër grupi i auditimit mban të njëjtin qëndrim.

8. Titulli i gjetjes: Keq menaxhim dhe keq administrim i përdoruesve të Sistemit të Prokurimit Elektronik, duke krijuar kushte për shkelje të sigurisë.

Situata: Nga auditimi mbi përdoruesit e Sistemit të Prokurimit Elektronik u konstatua se:

- Administratori i sistemit i cili bën menaxhimin e llogarive të përdoruesve mbështetet në Manualin për Administratorin e Sistemit të Prokurimit Elektronik për Menaxhimin e Përdoruesve i cili është i pa update-uar, (Version 1, 2018).

- Nuk janë aplikuar në sistem kriteret të detyrueshme për rritjen e vështirësisë së fjalëkalimit për përdoruesit, si periodiciteti për ndryshimin e tij, me qëllim rritjen e sigurisë në identifikimin e përdoruesit etj, bazuar në pikën 4 “Kërkesat e Sigurisë” pika a. të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuar nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

- Nuk janë dokumentuar e implementuar politikat për fjalëkalimet e sistemeve qendrore dhe administrimit bazuar në pikën 4 “Kërkesat e Sigurisë” pika b. Të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuara nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

- Administratori i sistemit i cili në sistem ka rolin System Admin është krijuar me “Data e Krijimit” 11/01/2018 si dhe nuk i ka të plotësuara të gjitha fushat në sistem. Kjo situatë sjell risk për humbjen e gjurmës audituese, risk për kryerjen apo moskryerjen e veprimeve të autorizuar në sistem;

-Ka përdorues për të cilët fushën “Hyr” që është username me të cilin përdoruesi logohet dhe fushën “Emri i Plote” janë si përdorues aktiv në sistem me kredenciale të përgjithshme të cilët nuk janë përcaktuar se nga cili punonjës posedohen dhe përdoren. Ky fakt mbart një risk të lartë për ndërhyrje të paautorizuara në sistem duke mos lënë gjurmë mbi aktivitetin që kanë kryer;

- Për user-at në rolin e KVO fusha “Hyr” që është username me të cilin përdoruesi logohet nuk është sipas “Manualit të përdorimit të Sistemit të Prokurimit Elektronik për Administratorin e Autoritetit kontraktor”, formati i të cilit është “emër.mbiemër”. konstatohen raste që ky format është: emër_mbiemër, emër_mbiemërnumër, emër, emërnumër, emër.mbiemërnumër, etj..

- Për user-at në rolin e Njësisë së Prokurimit fusha “Hyr” që është username me të cilin përdoruesi logohet nuk është sipas “Manualit të përdorimit të Sistemit të Prokurimit Elektronik për Administratorin e Autoritetit kontraktor”, formati i të cilit është “emër_mbiemër”, konstatohen raste që ky format është: emër.mbiemër, emër*mbiemër, emër_numërmbiemër, emër_mbiemërnumër, emër.mbiemërnumër, gërma e parë e emrit.mbiemër, emër, emërmbiemër@gmail.com, etj..

- Administratori i Autoritetit Kontraktor në këtë rast Agjencia e Prokurimit Publik është me rolin “Amin. Ak”;

- Ekziston aktiv përdoruesi me fushën “Hyr” = Xh që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me Data e Krijimi 08/02/2016 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si përgjegjëse sektori duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh, për të cilën mungon edhe përshkrimi i punës;

- Ekziston aktiv përdoruesi me fushën “Hyr” = gj që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me “Data e Krijimi” 05/09/2007 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si Drejtor i Drejtorisë së Administrimit të të Dhënave dhe Publikimit duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh;

- Ekziston aktiv përdoruesi me fushën “Hyr” = l k që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me Data e Krijimi 03/20/2010 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si specialist në Sektorin e Koordinimit duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh;

- Mbajnë statusin “aktiv” përdorues në rolin “auditor”, konkretisht auditues të KLSH-së, të cilët kanë përfunduar detyrat e tyre gjatë auditimit në terren dhe përdoruesit në sistem rezultojnë të jenë akoma aktiv;

- Rezulton se ka përdorues për të cilët fusha “Email” është NULL (i paplotësuar);

- Ekzistojnë përdorues për të cilët fusha “Email” është mm/dd/vv;

- Ekzistojnë përdorues për të cilët data e krijimit është ‘Po’ ose ‘Jo’.

Gjithashtu nga auditimi u konstatua se, hapja e këtyre përdoruesve mbetet pothuajse e pamonitoruar, pasi vetë APP nuk kryen monitorime që lidhen me këtë veprim, duke rritur riskun e krijimit të përdoruesve të paautorizuar, e për pasojë humbjen e konfidencialitetit të të dhënave apo keqpërdorimin e tyre.

Kriteri: Ligji nr. 2/2017, datë 26.01.2017 “Për Sigurinë Kibernetike”; neni 27 i ligjit nr. 9887, “Për mbrojtjen e të dhënave personale”, i ndryshuar, ISO/IEC 27001 “Information security management”.

Ndikimi/Efekti:

- Risk për kryerjen e veprimeve në sistem nga persona të paautorizuar;
- Risk për komprometimin e të dhënave dhe humbjes së gjurmës audituese;
- Risk për mos-evidentimin dhe mos-parandalimin e problematikave që lidhen me sigurinë e të dhënave.

Shkaku: Mos hartimi dhe miratimi i akteve rregullative, mos monitorim i përdoruesve duke krijuar kushte për shkelje të sigurisë.

Rëndësia: E Lartë.

8.1. Rekomandimi: Agjencia e Prokurimit Publik të marrë masa për unifikimin e të dhënave për përdoruesit e Sistemit të Prokurimit Elektronik të të njëjtës kategori sipas manualeve përkatëse, të plotësojë të dhënat që mungojnë për çdo përdorues, të ndërtojë kontrolle për mbylljen e përdoruesve në kohën e duhur, të mbyllë përdoruesit të cilët kanë përfunduar objektin e krijimit, me qëllim ruajtjen e sistemit nga ndërhyrjet e paautorizuara, të marrë masa për rritjen e sigurisë së identifikimit të përdoruesit si periodiciteti për ndryshimin e tij. Gjithashtu të marrë masa për analizimin e situatës aktuale të evidentuara nga auditimi në lidhje me integritetin dhe plotësinë e të dhënave mbi përdoruesit e Sistemit të Prokurimit Elektronik.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 “Mbi Projekt Raportin e Auditimit” nga Agjencia e Prokurimit Publik ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit:

Keto llogari janë krijuar që në momentin e krijimit të sistemit dhe janë aktive dhe administrohen nga përdoruesit e APP sipas detyrave funksionale të tyre. Megjithatë APP do marr masat për perditesimin e username....

Gjithashtu, ë asnje rast nuk ekzitojne 2 emra perdoruesi të njëjte në sistem (username), pasi sistemi nuk te lejon që në databaze te figurojne 2 emra perdoruesi (username) te njejte. Emri i perdoruesit eshte unik ashtu si eshte NIPT i autoritetit kontraktor apo NIPT-i i operatorit ekonomik. Mund te ekzistojne perdorues me emra te njejte (emer mbiemer) pasi mund te kene llogari si anetar i njesise se prokurimit, anetar i KVO apo auditues apo te kene qene pjese e nje institucioni tjeter, por ne asnje rast nuk mund te ekzistojne emer perdoruesi i njejte (username).

Qëndrimi i Grupit të Auditimit:

Grupi i auditimit për këto konstatime është bazuar në dokumentacionin e vënë në dispozicion nga ana juaj.

Praktika për njoftimin e përfundimit të aksesit nuk gjendet e dokumenatuar si dhe nuk është detyrim i përdoruesit të njoftojë mbylljen e llogarive. Kjo do të thotë se, nuk qëndron argumenti juaj, por mbetet risku potencial për ndërhyrje të paautorizuar, për të cilën grupi i auditimit mban të njëjtin qëndrim.

Përsa i përket observacioneve të sipërcituara më lartë nga ju, referuar edhe manualeve të përdoruesit Udhëzimi nr.7 dt. 30.07.2021, në këtë manual përcaktohet formati edhe në rastet kur mund të ketë përsëritje (“Emri i përdoruesit ekziston”) gjë për të cilën grupi i auditimit e ka konstatuar që në asnjë rast nuk është ndjekur ky format për usera që i posedon i njëjti person. Përsa më sipër konstatimi i grupit të auditimit nuk ndryshon.

2.3.Auditimi i zhvillimit dhe i blerjes në Teknologjinë e Informacionit

a. Marrëveshjet e Nivelit të Shërbimit (Service Level Agreement).

Grupi i auditimit ka marrë në konsideratë dhe në shqyrtim marrëveshjen e bashkëpunimit ndërmjet AKSHI-t dhe APP-s, nënshkruar ndërmjet palëve me shkresën nr. 1836 prot., datë 08.04.2019 protokolluar në AKSHI dhe me nr. 2982 prot., datë 08.04.2019 protokolluar në APP, me qëllim përcaktimin e nivelit të shërbimit që AKSHI duhet ti ofrojë Agjencisë së Prokuimit Publik sipas përcaktimeve të Aneksit 1 bashkëlidhur kësaj marrëveshjeje. Synimi i marrëveshjes është ofrimi i shërbimeve me qëllim rritjen e efektivitetit, kufizimin e risqeve teknike, ruajtjen e integritetit dhe vazhdueshmërinë e punës, etj. Kjo marrëveshje bazohet në VKM nr. 673, datë 22.11.2017 “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar. Në këtë marrëveshje thuhet se cili është objekti i marrëveshjes, të drejtat dhe detyrimet e ofruesit të shërbimit.

Një nga pikat e kësaj marrëveshjeje është administrimi i incidenteve, problemeve dhe disponueshmërisë. Ofruesi i shërbimit (AKSHI) duhet të zotërojë një bazë të dhënash të gabimeve të njohura dhe historikun e incidenteve të mëparshme. Me anë të procedurës së administrimit të problemeve ofruesi i shërbimit (AKSHI) duhet të kryej analizën e prirjes së informacionit për të identifikuar rrënjët e incidenteve dhe mundësitë për të parandaluar ndodhjen e tyre. Ofruesi i shërbimit (AKSHI) duhet të jetë i disponueshëm për të ofruar shërbim në institucionin përfitues të këtij shërbimi që është APP.

Për plotësimin e këtyre kërkesa thelbësore grupi i auditimit nuk administroi asnjë dokument që të vërtetonte zbatimin e këtyre pikave. APP si dhe Sektori TIK i AKSHI-t atashuar pranë APP menaxhojnë risqet mbi bazë ngjarjesh. Suporti, mbështetje teknike dhe logjike për operacionet IT kryhen nëpërmjet shkëmbimeve verbale dhe nuk dokumentohen duke mos bërë të mundur monitorimin e shërbimit të ofruar.

Gjithashtu, në marrëveshjen e nivelit të shërbimit evidentojmë disa elementë të tjerë të rëndësishëm:

- *Objekti i marrëveshjes*: Kjo marrëveshje synon në ofrimin e shërbimeve me qëllim rritjen e efektivitetit, kohëzgjatjes, kufizimin e risqeve teknike, pra ruajtjen e integritetit, konfidencialitetit dhe vazhdueshmërinë e punës objekt i kësaj marrëveshjeje.

- *Ofruesi i shërbimit (AKSHI)* do të ofrojë shërbimet e veta nga një staf teknologjik profesional dhe i specializuar.

- *Ofruesi i shërbimit* duhet të krijojë/diskutojë me përfituesin e shërbimit një axhendë periodike kontrollesh si më poshtë:

a. Javore

- Kontroll i logeve të serverave
- Kontroll i statistikave
- Kontroll i statistikave për programe
- Kontroll i disqeve për problem në rast nevojë
- Të kryejë mirëmbajtje proaktive

b. Mujore

- Testim/kontroll i kompletuar i pjesëve më kritike të infrastrukturës së klientit
- Kontroll i detajuar i gjithë log-eve hardware/software
- Rishikim i të dhënave mbi performancën e serverave
- Rekomandime për upgrade të mundshme hardware
- Në aneksin nr. 1 të marrëveshjes paraqitet një katalog me 43 shërbime (*secili shërbim ka nën shërbime*), për të cilat AKSHI zotohet se i kryen. Këto shërbime ndahen në 2 nivele suporti. Sipas këtij aneksi, institucioni bën kërkesën pranë punonjësve të AKSHI-t të atashuar në këtë institucion (NJTIK), me specialistë të fushës së teknologjisë së informacionit, për dhënien e suportit për sistemet, infrastrukturën TIK dhe suportin help desk, i cili konsiderohet si niveli 1. Me marrjen e kërkesës, niveli 1 nëse është në gjendje të zbatojë kërkesën, ofron zgjidhje dhe njofton institucionin që kërkesa është zbatuar dhe raporton pranë AKSHI-t, i cili konsiderohet si niveli 2 i suportit i cili teorikisht ka specializim më të lartë lidhur me fushën e teknologjisë

së informacionit. Nëse niveli 1 e ka të pamundur të ofrojë zgjidhjen, atëherë menjëherë njofton për asistencë nivelin 2, i cili ofron zgjidhjen dhe njofton institucionin që kërkesa është zbatuar. Gjithashtu në Listën nr. 1 në katalogun e shërbimeve bashkëlidhur Vendimit nr. 673, datë 22.11.2017, përcaktohen shërbime të përqendruara që ofrohen nga AKSHI nëpërmjet teknologjisë së informacionit e komunikimit (TIK) për qeverisjen elektronike, për administratën shtetërore, qytetarët, bizneset. *Për këto shërbime nuk janë përcaktuar tregues të matshëm për efektivitetin e shërbimeve që AKSHI ofron ndaj APP.*

Sipas VKM Nr. 673, datë 22.11.2017 “Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”, i ndryshuar, pikat 5/gj, 6/i/k, 11/a/b, dhe 23, AKSHI zotohet se ka aftësitë e nevojshme për shërbimet e ofruara në këtë kontratë.

Nga auditimi u konstatua se: sipas marrëveshjes së nënshkruar ndërmjet AKSHI-t dhe APP-s nuk administrohet dokumentacion apo gjurmë dokumentare për monitorimin e këtyre treguesve të sipërcituar. Shërbimet e përcaktuara në këtë Marrëveshje Nivel Shërbimi, janë pak ose aspak të matshme, duke mos patur mundësinë e monitorimit rigoroz të zbatimit të tyre.

Mbi ndërvëprimin institucional dhe organizativ APP - AKSHI

Meqenëse për periudhën nën auditim (01.01.2020-31.12.2021) sipas përcaktimeve të VKM 673, datë 22.11.2017 “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar, AKSHI është institucioni përgjegjës për sistemet, infrastrukturën hardware dhe software, koordinimin e bazës së të dhënave, menaxhimin e strukturës TIK etj, të subjektit nën auditim (APP), për përmbushjen e projektit të auditimit është përfshirë si subjekt nën auditim edhe struktura e IT pranë APP.

Referuar VKM Nr. 673, datë 22.11.2017 “Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”, i ndryshuar, në ndarjen IV, “Dispozita kalimtare dhe të fundit”, në pikat e mëposhtme citohet se:

18. *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.***

19. *Për sistemet dhe infrastrukturat TIK të cilat kalojnë në administrim dhe inventar të AKSHI-t dhe që zhvillohen ose mirëmbahen nëpërmjet marrëveshjeve ose kontratave të nënshkruara nga institucionet me palë të treta, të reflektohen ndryshimet përkatëse në këto akte.*

20. *Harton planin e transferimit nën administrimin e AKSHI-t të aseteve që preken nga fusha e veprimit të këtij vendimi.*

23. *Strukturat përgjegjëse TIK bëhen pjesë të strukturës së AKSHI-t. Punonjësit aktualë të njësisve të teknologjisë së informacionit e të komunikimit (NJTIK), në përbërje të strukturave të institucioneve dhe organeve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, kalojnë tek AKSHI, brenda datës **31.12.2017** dhe do të trajtohen në bazë të përcaktimeve të legjislacionit në fuqi për nëpunësit civil, në rastin e mbylljes dhe ristrukturimit të institucionit, apo Kodit të Punës. AKSHI vendos në dispozicion të institucioneve të përmendura në shkronjën “i”, të pikës 6, personelin e mjaftueshëm dhe të certifikuar sipas legjislacionit në fuqi, për të mbajtur në funksion optimal sistemet të cilat nuk preken nga fusha e veprimit të këtij vendimi.*

Në zbatim të pikave të sipërcituara më lartë nga Drejtori i Përgjithshëm i APP dhe AKSHI janë nxjerrë urdhra për ngritjen e grupeve të punës, ku pjesë përbërëse e grupit janë punonjës të APP-s dhe AKSHI-t, si në vijim:

1. Urdhër i përbashkët Nr. 5059/3 Prot., datë, 04.07.2018 nga APP dhe Nr. 3118 Prot., datë, 02.07.2018 nga AKSHI. Me anë të këtij urdhëri janë ngritur grupet e punës me qëllim përcaktimin e listës së aktiveve për infrastrukturën hardware dhe sistemet IT, objekt kalimi

kapital, si dhe identifikimin dhe propozimin e të drejtave dhe detyrimeve të institucioneve në lidhje me shërbimet utilitare.

Në zbatim të këtij urdhri u konstatua se dorëzimi i Aktiveve për infrastrukturën hardware dhe sistemeve të IT që APP kishte në regjistrin e aktiveve të saj, janë bërë pjesë e inventarit të AKSHI-t me anë të akt-dorëzimit Nr. 1570/4 Prot., datë 21.07.2020 nga APP dhe Nr. 3461 Prot., datë 21.07.2020 nga AKSHI. Konstatohet se ky proces ka përfunduar rreth 2 (dy) vite jashtë afatit të vendosur në VKM Nr. 673, datë 22.11.2017, “Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit”, i ndryshuar.

2. Urdhër i përbashkët Nr. 7097/1 Prot., datë, 16.12.2020 nga APP dhe Nr. 6710 Prot., datë, 10.12.2020 nga AKSHI. Urdhri i përbashkët me qëllim kalimin kapital nga APP të pajisjeve të sistemit “Sistemi i Prokurimit Elektronik”, me objekt “Blerje pajisje elektronike për Sistemin e prokurimit Publik” i kontratës Nr. Prot 5596, datë 26.10.2020. Në zbatim të këtij urdhri u konstatua se është bërë dorëzimi i Aktiveve për infrastrukturën hardware dhe sistemeve të IT që APP kishte në regjistrin e aktiveve të saj, janë bërë pjesë e inventarit të AKSHI-t me anë të akt-dorëzimit Nr. 7097/3 Prot., datë 22.12.2020 nga APP dhe Nr. 6954 Prot., datë 22.12.2020 nga AKSHI.

Janë dorëzuar nga APP në aktivet e infrastrukturës hardware të AKSHI-t Aktivet si më poshtë:

Nr.	Emërtimi i aktivitetit	Periudha e blerjes	Sasia
1	Enclosure (shasi) për storage ekzistues HPE 3PAR 8000SFF(2.5in) Field Integrated Drive Enclosure	28.10.2020	2
2	HDD 1.8TB SAS 10K SFF (2.5in)HPE 3 PAR 8000 1.8TB+SW 10KSFF HDD	28.10.2020	12
3	Instalim, Konfigurim dhe integrim	19.11.2020	1

APP ka realizuar investim në “Blerje pajisje elektronike për Sistemin e Prokurimit Elektronik” në periudhën Tetor 2020 veprim ky në kundërshtim me pikat e VKM Nr. 673, datë 22.11.2017, “Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit”, i ndryshuar konkretisht në:

Kreu II “Kompetencat, detyrat dhe përgjegjësitë e AKSHI-t”

- pika 6, shkronja i) citohet: “Përgjigjet për ngritjen, mirëmbajtjen dhe administrimin e sistemeve dhe aplikacioneve të teknologjisë së informacionit dhe komunikimit, për infrastrukturën e qendëruar dhe infrastrukturën TIK, për institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave. Ai organizon prokurimin e përqendruar për pajisjet TIK, me vlerë mbi kufirin monetar të prokurimeve me vlera të vogla, dhe për institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, të cilat, jo më vonë se data 30 qershor, i dërgojnë kërkesë me shkrim AKSHI-t për nevojat e tyre për projektet dhe pajisjet TIK për vitin pasardhës.”

Kreu IV. Dispozita kalimtare dhe të fundit.

- pika 22, citohet: “Për kompetencat, detyrat dhe përgjegjësitë, për të cilat nuk është lidhur kontrata për vitin 2017, si dhe për nevojat për projektet dhe pajisjet e teknologjisë së informacionit dhe komunikimit për vitin 2018, institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave të dërgojnë kërkesat e tyre pranë AKSHI-t, brenda 1 jave nga hyrja në fuqi e këtij vendimi.”

- pika 24, citohet: “Fondet buxhetore për shërbimet sipas shkronjës “i”, të pikës 6, të këtij vendimi, për institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit

të Ministrave, do të parashikohen në buxhetin vjetor të AKSHI-t. Për të gjitha institucionet jo buxhetorë, AKSHI do t'i ofrojë shërbimet kundrejt tarifave. Efektet financiare të kësaj pike fillojnë më 1 janar 2019.”

APP për investimin në *“Blerje pajisje elektronike për Sistemin e Prokurimit Elektronik”* ka dërguar kërkesë me shkrim në AKSHI për nevojat e tyre për projektet dhe pajisjet TIK për vitin 2020, sipas përcaktimeve të sipërcituara të VKM-së Nr. 673, datë 22.11.2017, *“Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”*, si dhe është bazuar në Aktin Normativ Nr. 28, datë 02.07.2020.

APP ka realizuar investim në *“Blerje pajisje elektronike për Sistemin e Prokurimit Elektronik”* në periudhën Tetor 2020 veprim ky në kundërshtim me pikat e VKM Nr. 673, datë 22.11.2017, *“Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”*, i ndryshuar konkretisht në: Kreu II *“Kompetencat, detyrat dhe përgjegjësitë e AKSHI-t”* pika 6, shkronja i) si dhe Kreu IV pika 22 dhe pika 24. APP për investimin në *“Blerje pajisje elektronike për Sistemin e Prokurimit Elektronik”* ka dërguar në AKSHI me shkresën Nr. 1986 Prot., datë 02.03.2020 *“Kërkesë për shtim kapacitetesh për sistemin e Arkivës të Sistemit të Prokurimit Elektronik”* ndërkohë APP ende nuk kishte dorëzuar aktivet për infrastrukturën hardware dhe sistemeve të IT që APP kishte në regjistrin e aktiveve të saj tek AKSHI, sipas Kreut IV, pika 18 e VKM Nr. 673, datë 22.11.2017 *“Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”*, i ndryshuar.

Nga auditimi mbi bazën ligjore dhe nënligjore të APP dhe AKSHI u konstatua se ka mbivendosje të kompetencave të detyrave dhe përgjegjësive mbi administrimin e sistemit të Prokurimit Elektronik, konkretisht: në nenin 4, pika 41 të ligjit nr. 162, datë 23.12.2020 *“Për Prokurimin Publik”*, citohet se: *“Sistemi i prokurimit elektronik” është një bazë të dhënash shtetërore, e krijuar sipas legjislacionit në fuqi e që përdoret për kryerjen e procedurave të prokurimit publik dhe administrohet nga Agjencia e Prokurimit Publik*, ndërkohë në pikën 9 të VKM nr. 673, datë 22.11.2017 *“Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”*, i ndryshuar, citohet: *“AKSHI është administrator i çdo sistemi TIK që ka si përdorues institucionet apo organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave”*. Në pikën 6 shkronja y) citohet se: *“Administron nga ana teknike sistemin informatikë të institucioneve të përmendura në shkronjën “i”, të pikës 6, në përputhje me parashikimet e këtij vendimi. Regjistrat e të dhënave të këtyre institucioneve që përbëhen nga bazat e të dhënave mbeten nën administrim të institucioneve respective.”*

U konstatua se, APP dhe AKSHI në MNSH-në e nënshkruar nga të dyja palët nuk ka marrë në konsideratë rëndësinë e institucionit, ngarkesën apo sasinë e informacionit që APP përpunon dhe përfshirjen e plotë të elementeve të MNSH sipas përcaktimeve ligjore dhe nënligjore në fuqi në caktimin e kushteve të veçanta duke ndërmarrë masa për të përcaktuar kompetencat e detyrave dhe përgjegjësive mbi administrimin e Sistemit të Prokurimit Elektronik.

Për sa është konstatuar më lart, mbi auditimin e funksionimit të qeverisjes TIK, mbajnë përgjegjësi Titullari i APP sipas detyrave dhe kompetencave të përcaktuara në rregulloren e brendshme institucionale miratuar me vendimin nr. 3, datë 30.04.2019 “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik”, si edhe Titullari i AKSHI-t sipas VKM nr. 673, datë 22.11.2017 “Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”, i ndryshuar.

1. Titulli i gjetjes: Nuk janë hartuar raportet e monitorimit të parashikuara në Marrëveshje Nivel Shërbimi ndërmjet APP dhe AKSHI-t.

Situata: Nga auditimi u konstatua se, nuk administrohet dokumentacion apo gjurmë dokumentare për monitorimin e treguesve të përcaktuar në Marrëveshje Nivel Shërbimi e nënshkruar ndërmjet APP dhe AKSHI-t. Shërbimet e përcaktuara në këtë Marrëveshje Nivel

Shërbimi, janë pak ose aspak të matshme, duke ndikuar në monitorimin e zbatimit të këtyre shërbimeve.

Kriteri: Marrëveshje Nivel Shërbimi (SLA) nënshkruar ndërmjet AKSHI-t dhe APP-s.

Ndikimi/Efekti: Pamundësi në monitorimin e zbatimit të MNSH ndërmjet APP dhe AKSHI.

Shkaku: Mos hartim i raporteve të parashikuara në marrëveshje.

Rëndësia: E Lartë.

1.1. Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit në vijimësi të kryejë analizimin, prioritarizimin dhe ofrimin e shërbimeve të përcaktuara në MNSH-në ndërmjet institucioneve (APP 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 të ofruar nga AKSHI.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia e Prokurimit Publik dhe me shkresë nr. 15/7 datë 06.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit APP:

Sjellim në vëmendje që APP, ka proceduar me AKSHI-n konform përcaktimeve të VKM Nr.673, date 22.11.2017 dhe konkretisht:

...

Nga ana tjetër Ministria e Financave dhe Ekonomisë vendosi që rialokimi i fondeve të bëhet në buxhetin e APP-së. Ky fond u miratua me Aktin Normativ Nr.28, date 02.07.2020, “Për disa ndryshime në Ligjin Nr. 88/2019, “Për buxhetin e vitit 2020”, të ndryshuar”.

Pretendimi i subjektit AKSHI:

... duke qenë se ky rekomandim është në kuadër të përmirësimit të detyrave dhe punës në tërësi, AKSHI mbetet i gatshëm të ofrojë të gjithë bashkëpunimin e nevojshëm dhe mirëpret sugjerime dhe kërkesat e APP-së për përmbushjen e tij.

Qëndrimi i Grupit të Auditimit:

Në lidhje me observacionin e sjell nga ana e APP nuk është e qartë lidhja midis gjetjes dhe observimit pasi grupi i auditimit sqaron se ky observim është reflektuar një herë në lidhje me gjetjen përkatëse në Projekt Raport.

AKSHI ndërkohë shpreh dakordësimin në kuadër të bashkëpunimit të ndërsjelltë ndërinstytucional. Përsa më sipër grupi i auditimit mban të njëjtin qëndrim.

2. Titulli i gjetjes: Mbivendosje e kompetencave mbi administrimin e Sistemit të Prokurimit Elektronik.

Situata: Nga auditimi mbi bazën ligjore dhe nënligjore të APP dhe AKSHI u konstatua se ka mbivendosje të kompetencave të detyrave dhe përgjegjësiave mbi administrimin e sistemit të Prokurimit Elektronik, konkretisht: në nenin 4, pika 41 të ligjit nr. 162, datë 23.12.2020 “Për Prokurimin Publik”, citohet se: “Sistem i prokurimit elektronik” është një bazë të dhënash shtetërore, e krijuar sipas legjislacionit në fuqi e që përdoret për kryerjen e procedurave të prokurimit publik dhe administrohet nga Agjencia e Prokurimit Publik”, ndërkohë në pikën 9 të VKM nr. 673, datë 22.11.2017 “Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”, i ndryshuar, citohet: “AKSHI është administrator i çdo sistemi TIK që ka si përdorues institucionet apo organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave”. Në pikën 6 shkronja y) citohet se: “Administron nga ana teknike sistemin informatikë të institucioneve të përmendura në shkronjën “i”, të pikës 6, në përputhje me parashikimet e këtij vendimi. Regjistrat e të dhënave të këtyre institucioneve që përbëhen nga bazat e të dhënave mbeten nën administrim të institucioneve respektive.”

Gjithashtu u konstatua se, APP dhe AKSHI në MNSH-në e nënshkruar nga të dyja palët nuk ka marrë në konsideratë rëndësinë e institucionit, ngarkesën apo sasinë e informacionit që APP përpunon dhe përfshirjen e plotë të elementeve të MNSH sipas përcaktimeve ligjore dhe nënligjore në fuqi në caktimin e kushteve të veçanta duke ndërmarrë masa për të përcaktuar kompetencat e detyrave dhe përgjegjësi mbi administrimin e Sistemit të Prokurimit Elektronik.

Kriteri: Neni 4, pika 41 i ligjit nr. 162, datë 23.12.2020 “Për Prokurimin Publik” dhe pika 9 e VKM nr. 673, datë 22.11.2017 “Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”, i ndryshuar.

Ndikimi/Efekt: Mbivendosje kompetencash e cila shkakton mos qartësim të të drejtave administruese të SPE.

Shkaku: Ligji 162/2020 në kundërshtim me VKM nr. 673 për administrimin e SPE.

Rëndësia: E Lartë.

2.1. Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit si administratorë të sistemit SPE mbështetur në aktet ligjore respektive të marrin masa për ngritjen e një grupi të përbashkët me qëllim identifikimin e mbivendosjeve ligjore si dhe propozimin e hartimin e ndryshimeve të nevojshme në bazën rregullatore për të drejtat Administruese të Sistemit e Prokurimit Elektronik.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022 nga Agjencia e Prokurimit Publik dhe me shkresë nr. 15/7 datë 06.06.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit “Mbi Projekt Raportin e Auditimit” ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit APP:

Sikurse kemi theksuar dhe më sipër, lidhur me sa është cilësuar duhet saktësuar se, neni 41 i ligjit 162/2020 parashikon procedurat e prokurimit dhe jo përkufizimin e sistemit të prokurimit elektronik. Ky përkufizim gjendet në pikën 4, të nenit 4 të ligjit 162/2020.

Së pari, VKM 673/2017 është një akt nënligjor, i cili në hierarkinë e akteve vjen pas ligjit, pra pas parashikimeve të ligjit 162/2020.

Së dyti, nuk vlerësojmë për mbivendosje të detyrave. Koncretisht, sipas parashikimeve të nenit 23, gërma “f” të ligjit 162/2020, *APP menaxhon bazën e të dhënave të procedurave të prokurimit në sistemin e prokurimit elektronik*, ndërkohë që AKSHI administron nga ana teknike sistemin informatik të institucioneve. Nga ana tjetër, sikurse edhe VKM 673/2017 parashikon, *regjistrat e të dhënave të institucioneve që përbëhen nga bazat e të dhënave mbeten nën administrim të institucioneve respektive*. Në cdo rast, në të dyja aktet bëhet fjalë për administrim/menaxhim i bazës së të dhënave.

Pretendimi i subjektit AKSHI:

Me hyrjen në fuqi të Ligjit nr. 34/2022 “Për përcaktimin e procedurës së veçantë për negocimin dhe zbatimin e kontratës me shoqërinë “Jones Group International” për forcimin e sigurisë kibernetike” kompania do të jetë kompetente në analizimin, vlerësimin e riskut dhe sigurinë kibernetike të infrastrukturave e sistemeve të institucioneve qeveritare në Republikën e Shqipërisë.

Qëndrimi i Grupit të Auditimit:

Përcaktimet ligjore mbi administrimin e sistemit të prokurimit elektronik nuk janë të qarta të drejtat administruese pasi grupi i auditimit ka konstatuar se ka mbivendosje në aktet rregullative të APP dhe detyrat funksionale në lidhje me administratorin e SPE që kalon përtej kompetencave të administrimit të regjistratit të të dhënave të SPE. Për këtë arsye ne kemi rekomanduar që të dy institucionet APP dhe AKSHI si administrator të këtij sistemi mbështetur në aktet ligjore respektive nevojitet të ndiqni hapat e nevojshëm në bazën

rregullatore për të drejtat Administruese të Sistemit Elektronik. Për këtë arsye grupi i auditimit mban të njëjtin qëndrim.

2.4 Auditimi i sistemeve

a. Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output

Objektivi: Vlerësimi i kontrolleve të aplikacioneve për të dhënat Input/Output ka si qëllim të verifikojë kontrollet e implementuara në aplikacionet që disponon dhe operon Agjencia e Prokurimit Publik si dhe hyrjen me saktësi të të dhënave dhe raportimin e tyre në funksion të arritjes së objektivave.

Verifikimi i kontrolleve të aplikacioneve për të dhënat Input/output të programit të auditimit kemi zhvilluar Pyetësorë e Intervista me punonjës dhe analizuar:

- Manualët e Sistemit;
- Ndjekjen e Proceseve të punës;
- Standardet e miratuara nga CESK;
- Raport fillestar i gjendjes së Sistemit SPE dhe Plani i zbatimit të Kontratës;
- Ekstrakti i procedurave të Prokurimit të vitit 2021 nga databaza;

Sistemi i Prokurimit Elektronik

Procedurat e prokurimit të kryera në Sistemin e Prokurimit Elektronik (SPE), përbëjnë një element thelbësor i cili i mundëson sektorit publik kryerjen e veprimeve të brendshme administrative, si shërbime bazë për publikun dhe bizneset, për të siguruar transparencë, dhe llogaridhënie për shpenzimet publike. Shpenzimet e prokurimeve publike përfaqësojnë një pjesë të konsiderueshme të PBB-së, fakt ky që i jep SPE-së një rol strategjik në nxitjen e një sërë objektivash politik të rëndësishëm për një zhvillim të qëndrueshëm, si dhe procedurave të prokurimit publik domosdoshmërinë e rritjes së efijencës dhe efikasitetit, si dhe sigurimin e mirë përdorimit të fondeve publike dhe të uljes shpenzimeve procedurale. Me qëllim vlerësimit e rrisqeve të lidhura me materialitetin në procedurat e prokurimeve publike të kryera për llogari të buxhetit të vitit 2021, grupi ka përdorur teknikat CAAT për analizimin dhe shpërndarjen e numrit dhe fondeve të tyre, të ndara sipas: tipit të kontratës, objektit, autoriteteve kontraktore, operatorëve ekonomikë, emërtimit, llojit të procedurës dhe llojit të prokurimit. Duke vlerësuar rolin e Regjistrin e Parashikimeve në SPE si një element të rëndësishëm në informimin e Operatorëve Ekonomikë mbi procedurat e parashikuara dhe luajtur një rol aktiv në rritjet e vlerës së përdorimit në kohë të parasë, konstaton se për vitin 2021 janë 865 autoritete kontraktore që kanë krijuar procedura prokurimi me vlerë të vogël në SPE dhe 415 AK kanë krijuar procedura prokurimi mbi kufirin monetar për prokurime me vlerë të vogël duke krijuar në Regjistrin e Parashikimeve në SPE 36926 elementë, nga të cilët 32851 elementë ose 88,97% e totalit kanë vijuar me procedurat, ndërsa 4075 elemente ose 11,03% e totalit janë me statusin të anuluar.

Në Platformën e Sistemit të Prokurimit Elektronik është bërë ndarja e përdoruesve në tre grupe kryesor përdoruesish të cilët duan të komunikojnë me sistemin :

- Përdoruesit e Portalit
- Përdoruesit Mobile
- Përdoruesit e Sistemit Elektronik të Prokurimit

Sistemi mundëson aksesin e operatorit ekonomik nëpërmjet pajisjeve mobile (cross-platform), tablet (cross-platform) dhe personal kompjuter (bazuar në browser). Çdo akses në sistem ka të përcaktuar rolet dhe në bazë të rolit, janë të përcaktuara dhe të drejtat e aksesimit të dhënave. Kërkesat ndaj sistemit balanohen ndërmjet makinave virtuale të cilat ofrojnë funksionalitetet e sistemit ndaj operatorëve ekonomikë dhe autoriteteve kontraktore.

Funksionaliteti për autoritetet kontraktues mundësohet vetëm nëpërmjet shfletueseve në

pajisje si personal kompjuter PC. Sistemi mbështetet nga një numër makinash virtuale të cilat ofrojnë funksionalitetin e cache dhe ruajtjes së sesionit të interaktivitetit të një përdoruesi. Ky sistem është i konfiguruar në cluster dhe “high available”. Konfigurimi i RDBMS është windows cluster me Always On Availability Groups. Sistemi i Prokurimit Elektronik ka një komunikim me Platformën Qeveritare të Ndërveprimit (e ashtuquajtura Government Gateway) për të bërë të mundur komunikimin me institucione të tjera dhe portalin e-Albania

Nga auditimi i të dhënave të sistemit rezulton se :

- Sistemi i prokurimit publik nuk ka kontrollet e nevojshëm të validimit e për mos lejuar lidhjen e kontratave pa pasur fondin limit të nevojshëm , ka raste në të cilat fondi i prokuruar është më i madh se vlera e fondi limit.
- Në sistemin e Prokurimit Elektronik, fusha e cila përdoret për plotësimin e të dhënave të urdhrat të prokurimit (numrin dhe datën), është fakultative, jo e detyrueshme për tu plotësuar, veprimi i cili sjell risk në faktorin e “mos plotësisë “ së të dhënave të sistemit.
- Nga analizimi i data bazës konstatohen fusha të pa plotësuar, çka tregon për mos vlerësimin e tyre si të detyrueshme për tu plotësuar. Rezultojnë raste procedurash të përfunduara dhe të arkivuara në të cilat nuk shfaqet vlera e kontratës dhe operatori ekonomik i shpallur fitues.
- Në prokurimet me vlerë të vogël nga auditimi i të dhënave u konstatua se në shumë raste është përdorur fondi limit me vlerë 0 (zero) ose 1 (një) duke shmangur gjurmët e procesit të prokurimit.

1.Titulli i Gjetjes: Sistemi i prokurimit publik nuk ka kontrollet e nevojshëm të validimit

Situata 1: Nga auditimi i të dhënave rezultuan lidhjeve të kontratave pa pasur fondin limit të nevojshëm,, në këto raste fondi i prokuruar është më i madh se fondi limit

Situata 2: Nga analizimi i data bazës të vitit 2021, konstatohen fusha të pa plotësuar, çka tregon për mos vlerësimin e tyre si të detyrueshme për tu plotësuar. Rezultojnë raste procedurash të përfunduara dhe të arkivuara në të cilat nuk shfaqet vlera e kontratës dhe operatori ekonomik i shpallur fitues.

Situata 3: Në prokurimet me vlerë të vogël nga auditimi i të dhënave u konstatua se në shumë raste është përdorur fondi limit me vlerë 0 (zero) ose 1 (një) duke shmangur gjurmët e procesit të prokurimit. Sipas udhëzimit Nr.3 datë 08.01.2018 “Mbi përdorimin e procedurës së prokurimit me vlerë të vogël dhe zhvillimin e saj me mjete elektronike” të ndryshuar, me të cilën parashikohet që mos shfaqet fondi limit. SPE nuk ka filtrat e nevojshëm për të shmangur këto vlera.

Situata 4: Në sistemin e Prokurimit Elektronik, fusha e cila përdoret për plotësimin e të dhënave të urdhrat të prokurimit (numrin dhe datën), është fakultative, jo e detyrueshme për tu plotësuar, veprimi i cili sjell risk në faktorin e “mos plotësisë “ së të dhënave të sistemit.

Kriteri: Ligjin Nr. 162/2020 “Për Prokurimin Publik”;

Udhëzim nr. 03, datë 08.01.2018 "mbi përdorimin e procedurës së prokurimit me vlerë të vogël dhe zhvillimin e saj me mjete elektronike" i ndryshuar;

Ndikimi/Efekti : Mungesë të gjurmëve në proceset e prokurimit elektronik

Shkaku: Mos vendosja e filtrave të nevojshëm në data bazën e Sistemit të Prokurimit Elektronik

Rëndësia: E Lartë.

1.1Rekomandim : APP të marri masat teknike të nevojshme për implementimin e mekanizmave të kontrollit të inputit në bazën e të dhënave të Sistemit të Prokurimit Elektronik për të garantuar integritetin dhe plotësinë e të dhënave që ruhen në të.

Për sa është trajtuar në këtë pjesë të Raportit Përfundimtar të Auditimit nga subjekti i audituar është paraqitur observacioni me shkresë nr. 15/8 datë 10.06.2022

Pretendimi i APP : Autoritetet kontraktore zhvillojnë procedurat e prokurimit mbështetur në parashikimet e legjislacionit të prokurimit publik në fuqi, dhe në këtë kuptim, referuar edhe parashikimeve të nenit 85/2 të VKM 285/2021 “Për miratimin e rregullave të prokurimit publik”, lidhja e kontratave do të bëhet vetëm pasi fondi do të jetë në dispozicion (në llogarinë përkatëse) të autoritetit/entit kontraktor. Pra, për efekt të procesit të prokurimit, (për të cilin është krijuar dhe funksionon SPE) nuk ndalohej shpallja dhe zhvillimi nëse fondet nuk janë ende në llogari të autoritetit. Kjo ndalesë është në një fazë tjetër, pasi është mbyllur procedura dhe kalohet në nënshkrimin e kontratës, pra nuk ka lidhje me sistemin e prokurimit.

Qëndrimi i grupit të auditimit: Në lidhje me pretendimin e paraqitur sqarojmë se fusha për plotësimin e urdhrat të Prokurimit duhet të plotësohet për garantimin e përputhshmërisë së rrjedhës logjike që ndjek një procedurë në sistem me rrjedhën logjike që dikton ligji i prokurimit Publik. Për sa më sipër grupi i qëndron opinionit të tij.

Pretendimi i APP :Procedurat e prokurimit me vlerë të vogël zhvillohen pa fond limit në SPE, pra fondi limit nuk u shfaqet operatorëve ekonomikë që ofrojnë, me qëllim që të rritet përgjegjshmëria e këtyre të fundit sa i takon ofertimit. Në këtë kuptim nuk vlen konstatimi se në prokurimet me vlerë të vogël në shumë raste është përdorur fondi limit me vlerë 0 ose 1 duke shmangur gjurmët e procesit të auditimit

Qëndrimi i grupit të auditimit: Në lidhje me pretendimin e paraqitur sqarojmë se fondi Limit nuk duhet të shfaqet nga sistemi, por vlera reale e fondit limit duhet të ruhet në sistem. Për sa më sipër grupi i qëndron opinionit të tij.

IV. GJETJET DHE REKOMANDIMET

A. MASA ORGANIZATIVE

1.Gjetje nga auditimi: Nga auditimi u konstatua se:

- Sektori i TI atashuar në APP është në mungesë të përgjegjësit dhe 1 (një) specialisti. AKSHI me shkresën nr.785 Prot., datë 04.02.2020 ka caktuar vetëm një specialist TI në APP, strukturë kjo e cila vazhdon ende të funksionojë si e tillë, duke sjell risk në mos përmbushje të objektivave institucionale.

-Sektorin e IT të AKSHI-t atashuar pranë APP përdor një bazë rregullatore të cilat nuk janë të miratuara nga organet drejtuese të AKSHI-t. Gjithashtu këto akte rregullore janë draft- akte te papërfunduara.

-Rregullorja e Brendshme e Agjencisë së Prokurimit Publik nuk është përshtatur (*amenduar*) duke mos reflektuar ndryshimet institucionale të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar, Ligjit nr. 162/2020 “Për Prokurimin Publik” si dhe ri-organizimin e strukturës në Agjencinë e Prokurimit Publik. Konkretisht Drejtoria e Administrimit të të Dhënave dhe Publikimit në APP ka mbivendosje të detyrave funksionale me Rregulloren e Brendshme të AKSHI-it “Mbi detyrat dhe funksionimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, duke bërë që detyrat funksionale që duhet të kryheshin nga sektori i TI të AKSHI-t atashuar pranë APP realizohen nga Drejtoria e Administrimit të të Dhënave dhe Publikimit në APP. Si dhe përshkrimet e punës për stafin e Drejtorisë së Administrimit të të Dhënave dhe Publikimit janë të pa përditësuara.

(Më hollësisht trajtuar në pikën (2.1) faqe (10-23) të Raportit Përfundimtar të Auditimit)

1.1.Rekomandimi: Agjencia Kombëtare e Shoqërisë së Informacionit të marrë masa të menjëhershme për plotësimin e vendeve vakante të sektorit IT atashuar në APP.

1.2.Rekomandimi: Struktura drejtuese të Agjencisë Kombëtare të Shoqërisë së Informacionit të marrin masa për miratimin e akteve rregullative në përputhje me përcaktimet ligjore dhe nënligjore me qëllim reflektimin e ndryshimeve institucionale, strukturore dhe kompjuterike të

ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar.

1.3.Rekomandimi: Agjencia e Prokurimit Publik me plotësimin e strukturës IT si organikë e AKSHI-t pranë saj të marrë masa për përditësimin e rregullores së brendshme institucionale në të cilën të pasqyrohen dhe reflektohen qartë detyrat operacionale në lidhje me ndryshimet institucionale, strukturore dhe kompjuterike të ndodhura me hyrjen në fuqi të VKM nr. 673, datë 22.11.2017 “Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar. Gjithashtu Agjencia e Prokurimit Publik të marrë masa dhe për përditësimin e përshkrimeve të punës në koherencë me rregulloren e brendshme.

Menjëherë dhe në vijimësi

2. Gjetje nga auditimi: Nga auditimi u konstatua se:

- Agjencia e Prokurimit Publik, nuk ka plan trajnimi vjetor për vitet 2020 - 2021 për burimet njerëzore të drejtorisë së Administrimit të të Dhënave. Gjatë vitit 2021 kanë zhvilluar trajnime në lidhje me Menaxhimin Strategjik, Statistikë, mbi Prokurimin Publik etj, por në asnjë rast mbi administrimin e sistemit SPE. Gjithashtu, APP nuk disponon dokumentacione mbi propozimet përkatëse nga niveli menaxherial i APP (ku përfshihet dhe drejtoria e burimeve njerëzore) për zhvillimin e trajnimeve. Nuk dokumentohet procesi i kërkesave, nevojave dhe analizimi i tyre për trajnim, duke mos plotësuar kështu nevojat për trajnim mbi sistemet, sigurinë dhe teknologjinë e informacionit.

- Stafi i Sektorit IT atashuar në Agjencinë e Prokurimit Publik nuk ka zhvilluar trajnime mbi sistemet, sigurinë dhe teknologjinë e informacionit, në kundërshtim me rregulloren e brendshme të AKSHI-t nr. 1900, datë 16.04.2020 “Mbi detyrat dhe funksionimi i Agjencisë Kombëtare të Shoqërisë së Informacionit”.

(Më hollësisht trajtuar në pikën (2.1) faqe (10-23) të Raportit Përfundimtar të Auditimit)

2.1. Rekomandimi: Agjencia e Prokurimit Publik të marrë masa për identifikimin e nevojave për trajnimin e stafit të drejtorisë së Administrimit të të Dhënave i cili merret me administrimin e bazës së të dhënave dhe të çdo përdoruesi të sistemit, si dhe të hartojë e miratojë plane për zhvillimin e trajnimeve në lidhje me sistemin e SPE.

2.2. Rekomandimi: Agjencia Kombëtare e Shoqërisë së Informacionit të marrë masa për identifikimin e nevojave dhe zhvillimin e trajnimeve për stafin aktual të sektorit IT atashuar në APP dhe në vijimësi me plotësimin e plotë të këtij sektori.

Menjëherë dhe në vijimësi

3. Gjetje nga auditimi: Nga auditimi u konstatua se:

- Oficeri i Sigurisë i përcaktuar me Urdhrin e titullarit të APP me nr. 9168/11 prot., datë 24.05.2019 “Për ushtrimin e detyrave”, nuk ka realizuar detyrat e përcaktuara në kundërshtim me Nenin 18 të Rregullores së Brendshme “Për miratimin e disa shtesave dhe ndryshimeve në rregulloren e brendshme për organizimin e punës në Agjencinë e Prokurimit Publik “miratuar me Vendim nr. 03 datë 30.04.2019 të Drejtorit të Përgjithshëm të APP. Gjithashtu raportimi i tij sipas rregullores së brendshme të APP nuk kryhet në nivelin më të lartë drejtues të APP, në mospërputhje me standardet ndërkombëtare dhe praktikat më të mira, pasi vetëm në këtë mënyrë mund të garantohet pavarësia e tij dhe mund të shmangen konfliktet e interesit që lindin, për arsye të ushtrimit të kompetencave të tij.

(Më hollësisht trajtuar në pikën (2.1) faqe (10-23) të Raportit Përfundimtar të Auditimit)

3.1. Rekomandimi: Agjencia e Prokurimit Publik të marrë masa që të kryhen detyrat nga Oficeri i Sigurisë të përcaktuara në Rregulloren e Brendshme të APP si dhe për rregullimin e linjës së varësisë në nivelet menaxheriale, ku raportimi i tij të jetë në nivelin më të lartë drejtues duke kryeje vetëm detyrat e Oficerit të Sigurisë dhe jo funksione të tjera, me qëllim garantimin e pavarësisë dhe shmangien e konfliktit të interesit, në ushtrimin e kompetencave të tij.

Menjëherë dhe në vijimësi

4.Gjetje nga auditimi: Nga auditimi u konstatua se, regjistri i riskut i APP përgjatë viteve 2020 - 2021 nuk rezulton të ketë patur përditësime mbi risqet e reja të identifikuar, konkretisht:

-Nuk janë identifikuar risqet në burimet njerëzore, të cilat duhen adresuar për të siguruar mirëfunksionimin dhe administrimin e Sistemit të Prokurimit Elektronik;

-Nuk janë analizuar dhe identifikuar mbivendosjet e kompetencave dhe detyrave në lidhje me administrimin e Sistemit të Prokurimit Elektronik, si dhe hapat që do të ndërmerren për minimizimin e problemeve që mund të ndodhin në Sistemin e Prokurimit Elektronik si dhe përgjegjësitë ndërmjet AKSHI-t dhe APP-s.

-Ndarja ose transferimi i risqeve së bashku me asetet tek AKSHI duke qenë se transferimi i aktiveve është bërë gjatë vitit 2020, periudhë për të cilën APP nuk ka marrë masa për rishikimin dhe update-im e regjistrit të riskut për këtë periudhë;

-Nuk janë identifikuar risqe në lidhje me: sigurinë, disponibilitetin dhe integritetin e sistemit dhe të dhënave që gjenerohen nëpërmjet Sistemit të Prokurimit Elektronik.

(Më hollësisht trajtuar në pikën (2.1) faqe (10-23) të Raportit Përfundimtar të Auditimit)

4.1.Rekomandimi: Agjencia e Prokurimit Publik të marrë masa për përditësimin e regjistrit të riskut institucionale, si dhe në bashkëpunim me AKSHI-n të marrin masa për identifikimin dhe analizimin e risqeve për Sistemin e Prokurimit Elektronik me qëllim analizimin dhe vlerësimin e risqeve, për të mos riskuar përmbushjen e objektivave të institucionit. Gjithashtu të marrin masa për hartimin dhe dokumentimin e një plani veprimi për minimizimin / parandalimin e risqeve të identifikuar, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave.

Menjëherë dhe në vijimësi

5.Gjetje nga auditimi: APP nuk disponon një infrastrukturë BCC (Business Continuity,Center) për garantimin e vazhdimësisë së ofrimit të shërbimit, si dhe nuk është kryer azhurnimi i planit mbi vazhdimësinë e punës dhe rimëkëmbjet nga katastrofat.

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

5.1.Rekomandimi: AKSHI bazuar në VKM Nr.673 datë 22.11.2017 pika 6k për rëndësinë që ka ofrimi i shërbimit pas një fatkeqësie, të ndërmarrin hapat e nevojshëm për ndërtimin e qendre *Business Continuity* si dhe të azhurnojnë dhe të testojnë planin e rekuperimit nga katastrofa (disaster recovery plan) me qëllim dhënien e sigurisë së arsyeshme se do të funksionojë në të gjitha situatat hipotetike dhe se burimet njerëzore janë të mirënjohura me zbatimin e hapave që duhen ndjekur..

Menjëherë dhe në vijimësi

6.Gjetje nga auditimi: Nga auditimi u konstatua se AKSHI nuk kanë marrë masat e nevojshme për rritjen e sigurisë së informacionit në “Sistemin e Prokurimit Publik” dhe nuk ka përcaktuar, pikën e kontaktit si person përgjegjës në AKCESK në kundërshtim me përcaktimet e VKM nr. 553, datë 15.07.2020 “Për miratimin e listës së infrastrukturës kritike të informacionit dhe listës së infrastrukturave të rëndësishme të informacionit”.

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

6.1.Rekomandimi: AKSHI të marrin masat e nevojshme për përcaktimin e personit përgjegjës për infrastrukturën kritike “Sistemi i Prokurimit Publik” dhe vendimmarrjen t’ia komunikojë Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike”.

Menjëherë

7. Gjetje nga auditimi: Nga auditimi u konstatua se fjalëkalimi i administratorit të databazës është i ndarë në dy pjesë sipas përcaktimeve të Urdhrit nr. 4104 Prot., datë 21.06.2021 të Drejtorit të Përgjithshëm të APP-së. Gjithashtu sipas përcaktimeve të këtij urdhri bëhen ndryshimet dhe për ndryshimin e username dhe fjalëkalimit për: *Username dhe password i router; Username dhe password i switch; Akses i Server Management Storage; Akses i storage të DB (EVA, EVA2); Akses i storage EVA; Akses i C7000.*

Urdhri i sipërcituar i cili përcakton se një pjesë e fjalëkalimeve administrohet nga përfaqësuesi i APP dhe një pjesë e fjalëkalimeve administrohet nga specialisti i TI-s së AKSHI-t atashuar pranë APP, është hartuar dhe miratuar në mënyrë të njëanshme vetëm nga Titullari i APP dhe nuk ka marrë edhe miratimin e strukturave drejtuese të AKSHI-t, si palë administruese në proces.

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

7.1.Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me AKSHI-n të marrin masa për hartimin dhe miratimin e një akti rregullativ të përbashkët për caktimin e administrimit të bazës së të dhënave të Sistemit të Prokurimit Elektronik, ku të përcaktohen qartë përgjegjësitë mbi administrimin e Sistemit të Prokurimit Elektronik në përputhje me dispozitat ligjore në fuqi.

Menjëherë

8.Gjetje nga auditimi: Nga auditimi u konstatua se, APP nuk ka një akt rregullativ të brendshëm, me qëllim organizimin dhe funksionimin e brendshëm të bazës së të dhënave, në përputhje me kërkesat e ligjit nr.10325, datë 23.09.2010, për “Bazat e të dhënave shtetërore”, neni 5, ku citohet se: “Rregulloret për organizimin dhe funksionimin e brendshëm të bazës së të dhënave shtetërore përcaktohen nga institucioni administrues dhe miratohen nga titullari i tij, në përputhje me standardet, rregullat dhe procedurat e përcaktuara sipas nenit 10 të këtij ligji”.

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

8.1.Rekomandimi: Agjencia e Prokurimit Publik si institucion administrues i bazës së të dhënave shtetërore që gjenerohen nëpërmjet Sistemit të Prokurimit Elektronik, të marrin masa për përmbushjen e përcaktimeve ligjore mbi rregulloren për organizimin dhe funksionimin e brendshëm të bazës së të dhënave shtetërore.

Në vijimësi

9.Gjetje nga auditimi: Nga auditimi u konstatua se, nuk ka një akt rregullariv ku të përcaktohet lidhja ndërmjet pozicionit të punës të specialistit dhe të drejtave që ky pozicion duhet të ketë në sistem.

Konkretisht për rolet:

- *Analist Prokurimesh*
- *Nëpunës i publikimit;*
- *Koordinator;*
- *Monitorues.*

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

9.1.Rekomandimi: APP 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 përdorues i sistemit me qëllim uljen e riskut të dhënies së të drejtave mbi përdorimin e sistemit, si dhe mbivendosjes së attributeve.

Menjëherë dhe në vijimësi

10.Gjetje nga auditimi: Nga auditimi u konstatua se në Marrëveshjen e Nivelit të Shërbimit të nënshkruar ndërmjet AKSHI-t dhe APP-s, nuk është përcaktuar se cili do të jetë administratori i sistemit në funksion të përcaktimit të procedurave organizative dhe teknike dhe masave për miratimin, krijimin, bllokimin apo ndryshimin e fjalëkalimeve të llogarive të përdoruesve nga Administratori i Sistemit të Prokurimit Elektronik në kundërshtim me VKM nr. 673, datë 22.11.2017 “Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit”, i ndryshuar.

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

10.1. Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit të marrin masat për përcaktimin e administratorit të sistemit në

funkcion të procedurave organizative ,teknike dhe marrjen e masave për krijimin, bllokimin apo ndryshimin e fjalëkalimeve të llogarive të përdoruesve të Sistemit të Prokurimit Elektronik në përputhje me dispozitat ligjore në fuqi.

Menjëherë

11.Gjetje nga auditimi: Nga auditimi u konstatua se, nuk disponohet një akt rregullator për menaxhimin e logeve dixhitale në administratën publike, në kundërshtim me pikën 4 shkronja a) të “Rregullores për menaxhimin e log-eve digjitale në Administratën Publike”, miratuar me Urdhrin nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike.

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

11.1.Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit t’i japin rëndësi sigurisë dhe mbrojtjes së të dhënave duke filluar së pari me hartimin e një procedure apo rregullore për menaxhimin e gjurmës elektronike të auditimit, me qëllim uljen e riskut mbi sigurinë e të dhënave me pasojë humbjen dhe tjetërsimin e tyre. Gjithashtu në këtë dokument duhet të specifikohet qartë vendi ku ruhen gjurmët, për cilat veprime të përdoruesit ruhen këto gjurmë, koha, struktura përgjegjëse për monitorimin dhe analizimin e tyre, detyrat dhe përgjegjësitë, e çdo element që i shërben sigurisë së të dhënave dhe parandalimit në tjetërsimin e tyre.

Menjëherë dhe në vijimësi

12.Gjetje nga auditimi: Nga auditimi mbi përdoruesit e Sistemit të Prokurimit Elektronik u konstatua se:

- Administratori i sistemit i cili bën menaxhimin e llogarive të përdoruesve mbështetet në Manualin për Administratorin e Sistemit të Prokurimit Elektronik për Menaxhimin e Përdoruesve i cili është i pa update-uar, (Version 1, 2018).

- Nuk janë aplikuar në sistem kriteret të detyrueshme për rritjen e vështirësisë së fjalëkalimit për përdoruesit, si periodiciteti për ndryshimin e tij, me qëllim rritjen e sigurisë në identifikimin e përdoruesit etj, bazuar në pikën 4 “Kërkesat e Sigurisë” pika a. të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuar nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

- Nuk janë dokumentuar e implementuar politikat për fjalëkalimet e sistemeve qendrore dhe administrimit bazuar në pikën 4 “Kërkesat e Sigurisë” pika b. Të rregullores për “Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike” miratuara nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

- Administratori i sistemit i cili në sistem ka rolin System Admin është krijuar me “Data e Krijimit” 11/01/2018 si dhe nuk i ka të plotësuar të gjitha fushat në sistem. Kjo situatë sjell risk për humbjen e gjurmës audituese, risk për kryerjen apo moskryerjen e veprimeve të autorizuar në sistem;

-Ka përdorues për të cilët fushën “Hyr” që është username me të cilin përdoruesi logohet dhe fushën “Emri i Plote” janë si përdorues aktiv në sistem me kredenciale të përgjithshme të cilët nuk janë përcaktuar se nga cili punonjës posedohen dhe përdoren. Ky fakt mbart një risk të lartë për ndërhyrje të paautorizuara në sistem duke mos lënë gjurmë mbi aktivitetin që kanë kryer;

- Për user-at në rolin e KVO fusha “Hyr” që është username me të cilin përdoruesi logohet nuk është sipas “Manualit të përdorimit të Sistemit të Prokurimit Elektronik për Administratorin e Autoritetit kontraktor”, formati i të cilit është “emër.mbiemër”. konstatohen raste që ky format është: emër_mbiemër, emër_mbiemërnumër, emër, emërnumër, emër.mbiemërnumër, etj.,

- Për user-at në rolin e Njësisë së Prokurimit fusha “Hyr” që është username me të cilin përdoruesi logohet nuk është sipas “Manualit të përdorimit të Sistemit të Prokurimit Elektronik për Administratorin e Autoritetit kontraktor”, formati i të cilit është “emër_mbiemër”, konstatohen raste që ky format është: emër.mbiemër, emër*mbiemër, emër_numëmbiemër,

emër_mbiemërnumër, emër.mbiemërnumër, gërma e parë e emrit.mbiemër, emër, emërmbiemër@gmail.com, etj..

- Administratori i Autoritetit Kontraktor në këtë rast Agjencia e Prokurimit Publik është me rolin “Amin. Ak”;

- Ekziston aktiv përdoruesi me fushën “Hyr” = Xh që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me Data e Krijimi 08/02/2016 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si përgjegjëse sektori duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh, për të cilën mungon edhe përshkrimi i punës;

- Ekziston aktiv përdoruesi me fushën “Hyr” = gj që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me “Data e Krijimi” 05/09/2007 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si Drejtor i Drejtorisë së Administrimit të të Dhënave dhe Publikimit duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh;

- Ekziston aktiv përdoruesi me fushën “Hyr” = lk që është username me të cilin përdoruesi logohet në rolin “Analist Prokurimesh” i hapur me Data e Krijimi 03/20/2010 dhe vazhdon të jetë ende aktiv. Kjo bie në kundërshtim me pozicionin e punës si specialist në Sektorin e Koordinimit duke mos e patur si detyrë të përcaktuar në rregulloren e brendshme detyrat e analist prokurimesh;

- Mbajnë statusin “aktiv” përdorues në rolin “auditor”, konkretisht auditues të KLSH-së, të cilët kanë përfunduar detyrat e tyre gjatë auditimit në terren dhe përdoruesit në sistem rezultojnë të jenë akoma aktiv;

- Rezulton se ka përdorues për të cilët fusha “Email” është NULL (i paplotësuar);

- Ekzistojnë përdorues për të cilët fusha “Email” është mm/dd/vv;

- Ekzistojnë përdorues për të cilët data e krijimit është ‘Po’ ose ‘Jo’.

Gjithashtu nga auditimi u konstatua se, hapja e këtyre përdoruesve mbetet pothuajse e pamonitoruar, pasi vetë APP nuk kryen monitorime që lidhen me këtë veprim, duke rritur riskun e krijimit të përdoruesve të paautorizuar, e për pasojë humbjen e konfidencialitetit të të dhënave apo keqpërdorimin e tyre.

(Më hollësisht trajtuar në pikën (2.2) faqe (23-38) të Raportit Përfundimtar të Auditimit)

12.1.Rekomandimi: Agjencia e Prokurimit Publik të marrë masa për unifikimin e të dhënave për përdoruesit e Sistemit të Prokurimit Elektronik të të njëjtës kategori sipas manualeve përkatëse, të plotësojë të dhënat që mungojnë për çdo përdorues, të ndërtojë kontrolle për mbylljen e përdoruesve në kohën e duhur, të mbyllë përdoruesit të cilët kanë përfunduar objektin e krijimit, me qëllim ruajtjen e sistemit nga ndërhyrjet e paautorizuara, të marrë masa për rritjen e sigurisë së identifikimit të përdoruesit si periodiciteti për ndryshimin e tij. Gjithashtu të marrë masa për analizimin e situatës aktuale të evidentuara nga auditimi në lidhje me integritetin dhe plotësinë e të dhënave mbi përdoruesit e Sistemit të Prokurimit Elektronik.

Menjëherë dhe në vijimësi

13.Gjetje nga auditimi: Nga auditimi u konstatua se, nuk administrohet dokumentacion apo gjurmë dokumentare për monitorimin e treguesve të përcaktuar në Marrëveshje Nivel Shërbimi e nënshkruar ndërmjet APP dhe AKSHI-t. Shërbimet e përcaktuara në këtë Marrëveshje Nivel Shërbimi, janë pak ose aspak të matshme, duke ndikuar në monitorimin e zbatimit të këtyre shërbimeve.

(Më hollësisht trajtuar në pikën (2.3) faqe (38-44) të Raportit Përfundimtar të Auditimit)

13.1. Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit në vijimësi të kryejë analizimin, prioritarizimin dhe ofrimin e shërbimeve të përcaktuara në MNSH-në ndërmjet institucioneve (APP dhe AKSHI), hartimin e raporteve javore dhe mujore të shërbimeve të ofruara, me qëllim dhënien e sigurisë së arsyeshme për kryerjen me rigozitet të suportit të ofruar nga AKSHI.

Menjëherë dhe në vijimësi

14.Gjetje nga auditimi: Nga auditimi mbi bazën ligjore dhe nënligjore të APP dhe AKSHI u konstatua se ka mbivendosje të kompetencave të detyrave dhe përgjegjësive mbi administrimin e sistemit të Prokurimit Elektronik, konkretisht: në nenin 4, pika 41 të ligjit nr. 162, datë 23.12.2020 “Për Prokurimin Publik”, citohet se: “Sistemi i prokurimit elektronik” është një bazë të dhënash shtetërore, e krijuar sipas legjislacionit në fuqi e që përdoret për kryerjen e procedurave të prokurimit publik dhe administrohet nga Agjencia e Prokurimit Publik”, ndërkohë në pikën 9 të VKM nr. 673, datë 22.11.2017 “Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit”, i ndryshuar, citohet: “AKSHI është administrator i çdo sistemi TIK që ka si përdorues institucionet apo organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave”. Në pikën 6 shkronja y) citohet se: “Administron nga ana teknike sistemin informatikë të institucioneve të përmendura në shkronjën “i”, të pikës 6, në përputhje me parashikimet e këtij vendimi. Regjistrat e të dhënave të këtyre institucioneve që përbëhen nga bazat e të dhënave mbeten nën administrim të institucioneve respektive.” Gjithashtu u konstatua se, APP dhe AKSHI në MNSH-në e nënshkruar nga të dyja palët nuk ka marrë në konsideratë rëndësinë e institucionit, ngarkesën apo sasinë e informacionit që APP përpunon dhe përfshirjen e plotë të elementeve të MNSH sipas përcaktimeve ligjore dhe nënligjore në fuqi në caktimin e kushteve të veçanta duke ndërmarrë masa për të përcaktuar kompetencat e detyrave dhe përgjegjësive mbi administrimin e Sistemit të Prokurimit Elektronik.

(Më hollësisht trajtuar në pikën (2.3) faqe (38-44) të Raportit Përfundimtar të Auditimit)

14.1 Rekomandimi: Agjencia e Prokurimit Publik në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit si administratorë të sistemit SPE mbështetur në aktet ligjore respektive të marrin masa për ngritjen e një grupi të përbashkët me qëllim identifikimin e mbivendosjeve ligjore si dhe propozimin e hartimin e ndryshimeve të nevojshme në bazën rregullatore për të drejtat Administruese të Sistemit e Prokurimit Elektronik.

Brenda vitit 2022

15. Gjetje nga auditimi: Nga auditimi i të dhënave të sistemit të Prokurimit Elektronik për vitin 2021 u konstatua se:

- Sistemi i prokurimit publik nuk ka kontrollat e nevojshëm të validimit për të mos lejuar lidhjen e kontratave pa pasur fondin limit të nevojshëm, ka raste në të cilat fondi i prokuruar është më i madh se vlera e fondit limit.
- Konstatohen fusha të pa plotësuar, çka tregon për mos vlerësimin e tyre si të detyrueshme për tu plotësuar. Rezultojnë raste procedurash të përfunduara dhe të arkivuara në të cilat nuk shfaqet vlera e kontratës dhe operatori ekonomik i shpallur fitues.
- Në prokurimet me vlerë të vogël në shumë raste është përdorur fondi limit me vlerë 0 (zero) ose 1 (një) duke shmangur gjurmët e procesit të prokurimit. Sipas udhëzimit Nr.3 datë 08.01.2018 “Mbi përdorimin e procedurës së prokurimit me vlerë të vogël dhe zhvillimin e saj me mjete elektronike” të ndryshuar, me të cilën parashikohet që mos shfaqet fondi limit. SPE nuk ka filtrat e nevojshëm për të shmangur këto vlera.
- Në sistemin e Prokurimit Elektronik, fusha e cila përdoret për plotësimin e të dhënave të urdhrit të prokurimit (numrin dhe datën), është fakultative, jo e detyrueshme për tu plotësuar, veprimi i cili sjell risk në faktorin e “mos plotësisë” së të dhënave të sistemit.

(Më hollësisht trajtuar në pikën (2.4) faqe (44-46) të Raportit Përfundimtar të Auditimit)

15.1 Rekomandim : APP të marrin masat teknike të nevojshme për implementimin e mekanizmave të kontrollit të inputit në bazën e të dhënave të Sistemit të Prokurimit Elektronik për të garantuar integritetin dhe plotësinë e të dhënave që ruhen në të.

Menjëherë dhe në vijimësi

Për sa më sipër paraqitet ky Raport Përfundimtar Auditimi

KONTROLI I LARTË I SHTETIT