RAPORT PËRFUNDIMTAR AUDITIMI

MBI AUDITIMIN E "SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT" NË

"INSTITUTIN E SIGURIMEVE SHOQËRORE"

Tiranë, Maj, 2023

PËRMBAJTJA

LISTA E SHKURTIMEVE

Shkurtimi	Emërtimi i Plotë
KLSH	Kontrolli i Lartë i Shtetit
RSH	Republika e Shqipërisë
ISSH	Instituti i Sigurimeve Shoqërore
AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit
AKCESK	Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
BCP	Business Continuity Plan
CMIS	Contribution Management Information System
DMAIS	Document management and Archiving Information System
PCAMS	Pension Calculation and Assignement Management System
NJTIK	Njësia e Teknologjisë së informacionit e të komunikimit
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
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 Funksionimin e Kontrollit të Lartë të Shtetit", datë 27.11.2014, zhvilloi një Auditim të Teknologjisë së Informacionit në Institutin e Sigurimeve Shoqërore, nga data 13.01.2022 deri më datë 15.03.2022.

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 Institutin e Sigurimeve Shoqërore, është pjesë e Planit Vjetor 2023 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 Instituti i Sigurimeve Shoqërore disponon, për të garantuar disponibilitet dhe integritet të të dhënave. Mbështetur në punën në terren, evidencat e marra kanë qenë të mjaftueshme dhe të besueshme për punën audituese. Rezultatet kryesore të punës audituese përfshihen në këtë përmbledhje ekzekutive të Raportit Përfundimtar. Nga ana e ISSH nuk ka patur observacione lidhur me Projektraportin e auditimit Auditimi i sistemeve të Informacionit është i rëndësishëm për institucionet, 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.	ISSH nuk ka një strategji institucionale, përfshirë atë për Teknologjinë e Informacionit, duke mos pasqyruar qartë objektivat lidhur me infrastrukturën, burimet e nevojshme, si dhe instrumentat e nevojshme për matjen e objektivave. Mungesa e një plani strategjik mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së ISSH.	Faqe 11-16	E Lartë	Instituti i Sigurimeve Shoqërore të marrë masat e nevojshme për hartimin dhe miratimin e Planit Strategjik Institucional, përfshirë planifikimin strategjik mbi teknologjinë e informacionit ku të adresohen qartë objektivat e institucionit duke reflektuar ndryshimet institucionale, strukturore dhe ndryshimet në teknologjinë e informacionit dhe komunikimit (TIK), të ndodhura ndër vite në ISSH.
2.	Nga verifikimi në terren në Drejtorinë rajonale të ISSH Vlorë, grupi i auditimit konstatoi se Infrastruktura Network e pajisjeve ndihmëse që nevojiten për shërbimet e komunikimit dhe ruajtjes së të dhënave është në kushtet jo minimale dhe optimale, ku shërbimet e ngritura mbi këto rrjete nuk janë të sigurta dhe nuk mbështesin vazhdimësinë e punës. Nga auditimi u konstatua se në Drejtoritë Rajonale (Vlorë, Lezhë) nuk ka një linjë back up interneti në rast të shkëputjes së linjës, duke sjellë kështu mosfunksionim të sistemit dhe ndërprerje të ofrimit të shërbimeve. Kompjuterat në drejtoritë rajonale (Vlorë, Lezhë) nuk janë të pajisur me antivirus për mbrojtje ndaj sulmeve. -Nuk ka një server qëndror të pajisur me Active Directory Domain Controller për menaxhimin e përdoruesve dhe vendosjen e politikave të sigurisë.	faqe 16-22	E Lartë	ISSH të marrë masa për pajisjen dhe standardizimin e infrastrukturës IT në Drejtoritë Rajonale si dhe të marrë masa për hartimin dhe miratimin e një procedure standarde për komunikimin dhe zgjidhjen e problematikave që lindin me Drejtoritë Vendore në lidhje me sistemet IT, me qëllim sigurimin e kushteve optimale për ofrimin e shërbimit dhe mbarëvajtjen e punës pa ndërprerje.

	-Nuk kanë një pajisje firewall për mbrojtjen e rrjetit nga sulmet e jashtme.			
3.	Nga auditimi u konstatua se ISSH nuk disponon një infrastrukturë BCC (Business Continuity Center), si dhe nuk ka një plan mbi vazhdimësinë e punës dhe rimëkëmbjet nga katastrofat 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. Backup-et e sistemeve PCAMS, CMIS dhe DMAIS janë të ruajtura në Tape library, të cilat pasi mbushen ruhen në të njëjtën godinë me sistemet PCAMS, CMIS dhe DMAIS. -Kopjet (backup) e të dhënave nuk testohen rregullisht	faqe 16-22	E Lartë	-Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, bazuar në rëndësinë që ka ofrimi i shërbimit pas një fatkeqësie, të ndërmarrin hapat e nevojshëm për ndërtimin e një qendre *Business Continuity.* -Drejtoria e Burimeve të Informacionit të marrë masa për kryerjen dhe testimin periodik të backup-it të të dhënave të sistemeve duke e dokumentuar procesin.
4.	Nga auditimi u konstatua se në databazën e PCAMS në tablespace Audit_Aux nuk ka hapësira të nevojshme të alokuara në memorie (HDD); kjo mungesë e hapësirës (në tablespace) ka sjellë ulje të performancës dhe gabime në databazë. -Nga auditimi i sistemit DMAIS në lidhje me performancën e veprimeve, duke u bazuar në treguesit si: Koha e përgjigjes, koha e përpunimit, përdorimi i burimeve të sistemit, u konstatua se DMAIS i përgjigjet me vonesë kërkesave të përdoruesve.	faqe 24-31	E Lartë	Instituti i Sigurimeve Shoqërore të marrë masa që në vijim të kryejë sistemimet e nevoshme në databazën e sistemeve duke u bazuar në problematikat e shfaqura vazhdimisht nga njoftimet për gabime të ndodhura në sistem.
5.	Nga auditimi u konstatua se infrastruktura e përdorur për operimin e sistemeve (PCAMS, CMIS, DMAIS) si: (Red Hat Enterprise Linux (RHEL) 5, Windows server 8, Databaza në Oracle 11g, Cisco asa5520-bun), është në statusin end of life (ka arritur fundin e jetës), që do të thotë se prodhuesi i këtyrë pajisjeve dhe softeve nuk ofron më asistencë teknike, përditësime të sigurisë ose rregullim të gabimeve për këto	faqe 24-31	E Lartë	Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, të marrin masa për përditësimin dhe standardizimin e infrastrukturës IT, si dhe të monitorojnë sistemet që nuk përditësohen më për çdo tregues të mundshëm të shkeljeve të sigurisë ose dështimeve të sistemit.

	versione, duke ndikuar në plotësimin e nevojave aktuale si dhe rritjen e kapaciteteve në të ardhmen.			
6.	Nga auditimi i përdoruesve të sistemeve PCAMS (Sistemi elektronik i kalkulimit dhe pagesës së përfitimeve), CMIS (Sistemi elektronik për menaxhimin e kontributeve) DMAIS (Sistemi elektronik për digjitalizimin e dokumenteve të Arkivit Qendror) u konstatua se nuk ka të dhëna se cilat janë personat e autorizuar që ushtrojnë rolin e adiministratorit të sistemeve (CMIS, ADMIN, DMAIS, DATALOD PCAMS). Fjalëkalimi në sistemet (PCAMS, CMIS, DMAIS) nuk është i parametrizuar për nga kompleksiteti dhe gjatësia e tij. Për kriteret e fjalëkalimit të përdoruesve fundor nuk janë hartuar apo implementuar standarde me qëllim forcimin e tij.	faqe 24-31	E Lartë	Instituti i Sigurimeve Shoqërore të marrë masa për hartimin dhe miratimin e rregullores për krijimin dhe administrimin e përdoruesve të brendshëm, ku të jenë të pasqyruara saktë të drejtat dhe detyrimet për të gjithë përdoruesit Gjithashtu, ISSH të marrë masa për hartimin dhe miratimin e politikave mbi fjalëkalimin e përdoruesve në sistemet (PCAMS, CMIS, DMAIS) ku të përcaktohet kompleksiteti minimal në gjatësi, karaktere speciale apo numra si dhe periodiciteti për ndryshimin e tij.

1.3 Konkluzioni i përgjithshëm dhe Opinioni i Auditimit:

Grupi i auditimit mbështetur në Standardet ndërkombëtare të Auditimit përkatësisht në ISSAI 100, ISSAI 5300, ISSAI 5310 si dhe nenet 3 dhe 14 të ligjit nr.154 datë 27.11.2014 "*Për Organizimin dhe Funksionimin e KLSH"* ushtroi auditimin në Institutin e Sigurimeve Shoqërore mbi Sistemet e Teknologjisë së Informacionit për periudhën ushtrimore 01.01.2021-31.12.2022 në të cilat përfshihet Qeverisja IT, Siguria e Informacionit, Marrëveshjet e Nivel Shërbimit dhe të dhënat e Sistemeve CMIS, PCAMS, DMAIS.

Konstatohet se investimet në sistemet e informacionit nuk kanë zgjidhur problemet e sigurisë së informacionit, si dhe sigurimin e vazhdueshmërisë së biznesit. Zhvillimi i shërbimeve dhe infrastrukturës nuk është mbështetur në praktikat më të mira.

Pajisjet fizike, programet softuerike të cilat ndërveprojnë në mënyrë që sistemet të operojnë, janë të pa përditësuara (në fund të jetës) e nuk ofrohet suport nga prodhuesi. Nga auditimi i sistemeve kryesore, duke u bazuar në performancën e veprimeve me tregues si: koha e përgjigjes, koha e përpunimit, përdorimi i burimeve të sistemit, komentet e përdoruesve, rezulton se sistemet i përgjigjen me vonesë kërkesave të përdoruesve.

Në gjykimin tonë, identifikimi dhe administrimi i elementëve kritikë në ofrimin e shërbimeve dhe garantimin e sigurisë së të dhënave, si dhe të vazhdimësisë në ofrimin e shërbimit nëpërmjet Teknologjisë së Informacionit është i pamjaftueshëm.

ISSH nuk ka marrë masa për kalimin e strukturave përgjegjëse TIK tek AKSHI, si dhe dorëzimin e Sistemeve dhe Infrastrukturës TIK ekzistuese nën administrimin dhe inventarin e AKSHI-t, së bashku me të drejtat dhe detyrimet juridiko-civile sipas përcaktimeve dhe afateve të vendosura në VKM Nr. 673, datë 22.11.2017, "*Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit"*, i ndryshuar.

II. HYRJE

Mbështetur në Ligjin 154/2014, datë 27.11.2014 "*Për Organizimin dhe Funksionimin e KLSH*", në zbatim të Programit të Auditimit nr. 1188/1, datë 13.01.2023 të miratuar nga Kryetari i KLSH, me afat auditimi 13.01.2023 deri në 15.03.2023, në Institutin e Sigurimeve Shoqërore (më poshtë ISSH), ku periudha e audituar është 01.01.2021 deri në 31.12.2022, u krye auditimi me objekt "*Auditimi i Sistemeve të Teknologjisë së Informacionit*", nga audituesit:

1. R. A., përgjegjës grupi
2. D. B., anëtar
3. A. A., anëtar

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 Institutin e Sigurimeve Shoqërore, 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 opinioni, 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 efiçente. 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.1188/1, datë 13.01.2023:

1. Auditimi i funksionimit të Qeverisjes TIK

a) Verifikimi i politikave, standardeve dhe burimeve njerëzore në TIK.

2. Auditimi i Sigurisë së Informacionit

a) Siguria e të dhënave, verifikimi i sigurisë fizike dhe vazhdimësia e ofrimit të shërbimit.

3. Auditmi i zhvillimit dhe i blerjes në Teknologjinë e Informacionit

4. Auditimi i sistemeve

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

b) Përdoruesit e sistemeve, të drejtat dhe gjurmët e veprimeve në sistem.

5.Të ndryshme të dala gjatë auditimit

II.4 Përgjegjësitë e strukturave drejtuese të subjektit të audituar

Veprimtaria e ISSH bazohet në ligjin nr. 7703, datë 11.05.1993, "Për sigurimet shoqërore në Republikën e Shqipërisë", i ndryshuar.". Detyrat dhe kompetencat e Institutit të Sigurimeve Shoqërore fokusohen kryesisht në:

Në përmirësimin e skemave aktuale nëpërmjet reformimit të shtyllës publike të pensioneve e forcimit të një lidhjeje më të drejtpërdrejtë midis kontributeve të paguara dhe përfitimeve të ardhshme, futjes graduale të skemave të përfitimeve suplementare të menaxhuara nga subjekte jopublike, krijimit të llogarive personale të çdo kontribuesi dhe përfituesi, arritjen e transparencës maksimale, duke krijuar akses personal tek klientët.

Shërbimet që ofron ISSH:

- Pension pleqërie

- Pension invaliditeti
- Pension familjar
- Pensioni social
- Përfitim për barrëlindje
- Përfitim për paaftësi të përkohshme në punë
- Përfitim në rast aksidenti në punë dhe sëmundje profesionale
- Sigurim vullnetar
- Sigurim shtetëror suplementar
- Sigurim suplementar për ushtarakët
- Sigurim për të vetpunësuarit në bujqësi
- Pagesa për lindje/vdekje

II.5 Përgjegjësitë e audituesve

Kontrolli i Lartë i Shtetit auditoi Institutin e Sigurimeve Shoqërore, mbi periudhën e veprimtarisë nga 01.01.2021 deri në 31.12.2022, 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. 1188/1, datë 13.01.2023 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 ISSH. 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:

- Standardet Ndërkombëtare të Auditimit (ISSA1) të INTOSAI-t.
- Udhëzues dhe Manuale të Auditimit të Teknologjisë së Informacionit si: ISSAI 5300, Manuali Aktiv i Auditimit IT si dhe Standardet e COBIT.
- Kushtetuta e Republikës së Shqipërisë (nenet 162-165);
- Ligji nr.154/2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit";
- Ligji Nr. 162 Date 23.12.2020 Për Prokurimin Publik.
- Ligji nr. 7703, datë 11.05.1993 "Për sigurimet shoqërore në RSH", të ndryshuar.
- Ligji nr. 10296, datë 08.07.2010 "Për menaxhimin financiar dhe kontrollin", i ndryshuar dhe aktet ligjore në zbatim të tij;
- Ligji nr. 114/2015 "Për auditimin e brendshëm në sektorin publik";
- 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";
- Ligji nr. 119/2014 "Për të drejtën e informimit";
- VKMnr.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 673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit", i ndryshuar;

- 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;
- 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, testime 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 ISSH, janë si më poshtë:

- Intervista zhvilluar në subjekt me personat përgjegjës;
- Verifikime të sistemit si audites;
- 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

1. Informacioni i përgjithshëm mbi subjektin nën auditim

Instituti i Sigurimeve Shoqërore (ISSH) është administrues i sigurimeve shoqërore dhe i politikave të pensioneve në veçanti, vendosja e personave të siguruar dhe përmirësimi i shërbimit ndaj tyre në qendër të veprimtarisë së këtij institucioni, mbulimi i popullsisë me elemente të sigurimeve shoqërore në çdo vend dhe kohë kur lind kjo e drejtë, rritja e numrit të kontribuesve dhe grumbullimi i të ardhurave nga kontributet e fermerëve dhe të siguruarit vullnetar, përmirësimi i efiçiencës në menaxhimin e fondeve të sigurimeve shoqërore, i fondeve përkohësisht të lira dhe fondit rezervë.

Misioni i sistemit të sigurimeve shoqërore është mbulimi i të gjithë popullsisë me element të sigurimeve shoqërore dhe akordimi i përfitimeve për pension, paaftësi të përkohëshme në punë, barrëlindje, aksidente në punë dhe sëmundje profesionale e përfitime suplementare në momentin e lindjes të së drejtës dhe nevoja për to.

Vizioni i sistemit të sigurimeve shoqërore është fokusuar në përmirësimin e skemave aktuale nëpërmjet reformimit të shtyllës publike të pensioneve e forcimit të një lidhjeje më të drejtpërdrejtë midis kontributeve të paguara dhe përfitimeve të ardhshme, futjes graduale të

skemave të përfitimeve suplementare të menaxhuara nga subjekte jopublike, krijimit të llogarive personale të çdo kontribuesi dhe përfituesi, arritjen e transparencës maksimale, duke krijuar akses personal tek klientët.
Shërbimet që ofron ISSH:
- Pension pleqërie
- Pension invaliditeti
- Pension familjar
- Pensioni social
- Përfitim për barrëlindje
- Përfitim për paaftësi të përkohshme në punë
- Përfitim në rast aksidenti në punë dhe sëmundje profesionale
- Sigurim vullnetar
- Sigurim shtetëror suplementar
- Sigurim suplementar për ushtarakët
- Sigurim për të vetpunësuarit në bujqësi
- Pagesa për lindje/vdekje

2.Përshkrimi i rezultateve të auditimit

2.1Auditimi i Funksionimit të Qeverisjes TIK

. Verifikimi i procedurave dhe burimeve njerëzore në TIK

Instituti i Sigurimeve Shoqërore (ISSH) është institucion publik i pavarur, organizimi dhe funksionimi i të cilit rregullohet me ligjin nr. 7703, datë 11.05.1993, "Për sigurimet shoqërore në Republikën e Shqipërisë", i ndryshuar. Instituti i Sigurimeve Shoqërore drejtohet nga:
- Këshilli Administrativ
- Drejtori i Përgjithshëm

Këshilli Administrativ i Institutit të Sigurimeve Shoqërore është organi më i lartë ekzekutiv. Ai përbëhet nga 12 anëtarë, nga të cilët:
- 6 anëtarë, përfaqësues të Qeverisë
- 6 anëtarë, përfaqësues të Sindikatave dhe Punëdhënësve

Drejtori i Përgjithshëm i ISSH-së zgjidhet nga Këshilli Administrativ i Institutit të Sigurimeve Shoqërore.

Organizimi i përgjithshëm
Struktura e Përgjithshme Organizative e Institutit të Sigurimeve Shoqërore është si më poshtë:
- Drejtoria e Përgjithshme e ISSH (DPISSH)
- Drejtoria e Arkivës Qendrore e Institutit të Sigurimeve Shoqërore
- Drejtoria Rajonale e Sigurimeve Shoqërore Tiranë
- 11 Drejtori Rajonale të Sigurimeve Shoqërore
- Degë Rajonale të Sigurimeve Shoqërore në Tropojë dhe Sarandë (për shkak të largësisë).
- Agjenci Lokale të Sigurimeve Shoqërore, të kategorisë së parë dhe të dytë.

Sa i përket Drejtorisë së Përgjithshme, njësia e cila është përgjegjëse për zhvillimin e funksioneve të IT në linjë me kërkesat e biznesit të ISSH është Drejtoria e Burimeve të Informacionit (DBI).

- **Verifikimi i strategjisë, politikave dhe burimeve njerëzore në TIK**

Strategjia TIK

Strategjia e TI përfaqëson lidhjen e përbashkët midis objektivave të Strategjisë së TI dhe atyre të strategjisë së institucionit. Objektivat e strategjisë së TI duhet të marrin parasysh nevojat e

tashme dhe të ardhshme të biznesit, kapacitetin aktual të TI për të ofruar shërbime dhe kërkesat e burimeve. Strategjia duhet të marrë në konsideratë ekzistencën e infrastrukturës dhe arkitekturës së TI, investimeve, modelit të ofrimit, burimet duke përfshirë stafin, si dhe paraqitjen e strategjisë që integron këto elementë në një qasje të përbashkët për të mbështetur objektivat e institucionit.

Nga auditimi u konstatua se:

ISSH nuk ka një strategji institucionale, përfshirë, këtu, edhe strategjinë për Teknologjinë e Informacionit, duke mos pasqyruar qartë objektivat lidhur me infrastrukturën, burimet e nevojshme, si dhe instrumentat e nevojshme për matjen e objektivave. Mungesa e një plani strategjik mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së ISSH. DBI funksionon me një rregullore për Sigurinë e Informacionit, e cila është miratuar në datë 17.01.2022 nga Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI). Kjo rregullore përcakton parimet dhe rregullat e përgjithshme të Sigurisë së Informacionit në drejtoritë e AKSHI-t të atashuara pranë institucioneve qendrore, si dhe përgjegjësitë që lidhen me sigurinë me qëllim ruajtjen e integritetit, disponueshmërisë dhe konfidencialitetit të aseteve të informacionit. Pra, kjo rregullore është e kufizuar vetëm në aspektin e sigurisë së informacionit dhe nuk përfshin elemente të tjera të TI, duke mos bërë planifikime strategjike mbi infrastrukturën IT, si dhe duke mos pasqyruar qartë objektivat lidhur me burimet dhe instrumentet e nevojshme për matjen e objektivave, në kundërshtim me Ligjin nr.10296, datë 08.07.2010 "Për menaxhimin financiar dhe kontrollin" kreu i "Përgjegjshmëria menaxheriale", neni 8, "Përgjegjshmëria menaxheriale e titullarit" ku citohet: "Titullarët e njësive publike në fushën e menaxhimit financiar dhe kontrollit kanë këto kompetenca kryesore:

a) hartimin e politikave, miratimin dhe monitorimin e objektivave të njësive publike që ata drejtojnë, të planeve strategjike e vjetore, përfshirë strategjinë e menaxhimit të riskut dhe të plan-veprimeve për arritjen e objektivave;

b) ngritjen e grupit të menaxhimit strategjik të njësisë publike në përputhje me kërkesat e nenit 27 të këtij ligji."

Verifikimi i politikave dhe burimet njerëzore në TIK

Struktura e Drejtorisë së përgjithshme është ndryshuar me miratim të VKA nr.2, datë 18.03.2022 "Për një shtesë në numrin e përgjithshëm të punonjësve të Institutit të Sigurimeve Shoqërore dhe ndryshime në strukturën organizative të ISSH-së", mbështetur ne nenin 74, shkronja b/1 të ligjit nr.7703 datë 11.05.1993 "Për Sigurimet Shoqërore në Republikën e Shqipërisë". Ndryshimet e fundit në Strukturën e ISSH-së janë miratuar me Urdhër të Drejtorit të Përgjithshëm nr.6714 prot., datë 07.10.2022. Me VKA nr.15, datë 02.11.2022 "Për disa ndryshime në rregulloren nr. 3/2 datë 26.02.2008 "Për personelin e ISSH" autorizohet Drejtori i Përgjithshëm që të bëjë ndryshime në organizimin e brendshëm të ISSH-së brenda numrit të përgjithshëm të punonjësve të miratuar në funksion të ndryshimeve ligjore si institucion shërbimofrues.

Aktualisht struktura e DBI në DPISSH paraqitet si më poshtë:

Tab nr.1

	DREJTORIA E BURIMEVE TË INFORMACIONIT	10
1	**Drejtor Drejtorie**	**1**
	Sektori i Administrimit të Rrjetit dhe Teknologjisë	**3**
1	Përgjegjës Sektori	1
2	Specialist	1
3	Specialist	1
	Sektori i Programimit të Software-it	**3**
1	Përgjegjës Sektori	1

2	Specialiste	1
3	Specialist	1
	Sektori i Administrimit të Bazës së të dhënave	**3**
1	Përgjegjës Sektori	1
2	Specialiste	1
3	Operator	1

– Burimi: ISSH

Nga auditimi konstatohet se burimet njerëzore të Drejtorisë së Burimeve të Informacionit pranë DPISSH janë të qëndrueshme dhe të plota sipas strukturës organike të Drejtorisë së Burimeve të Informacionit.

- ***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.

Nga auditimi u konstatua se:
Në kundërshtim me pikën 23 të VKM-së nr. 673, datë 22.11.2017, në të cilën citohet se: "*Strukturat përgjegjëse TIK 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 dhe do të trajtohen në bazë të përcaktimeve të legjislacionit në fuqi për nëpunësit civilë, 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",* ISSH nuk është bërë pjesë ende e burimeve njerëzore në AKSHI.

Aktualisht, struktura e IT në Drejtorinë e Përgjithshme dhe Drejtoritë Rajonale të Sigurimeve Shoqërorë paraqitet me 60 vende pune. Nga këto, rezulton se 3 vende janë vakante, përkatësisht si në tabelën vijuese:

Tab Nr.2 / Burimi: ISSH

VENDET VAKANTE NË STRUKTURËN E DBI		
1	Specialist IT DRSSH Fier	1
2	Kryetari i Degës IT DRSSH Kukës	1
3	Specialist operator pranë Sektorit të numerizimit të të dhënave të dokumentave arkivore në Drejtorinë e Arkivit Qendror	1

Nga auditimi u konstatua se:
Këto vakanca kanë ardhur si pasojë e largimit të punonjësve IT. Nga këto:
- pozicioni i specialistit IT të DRSSH Fier ka 3 muaj që ka mbetur vakant dhe ISSH ka hapur konkursin për këtë vend pune;
- pozicioni i Kryetarit të Degës It të Kukësit ka 4 vite që ka mbetur vakant dhe aktualisht nuk ka një konkurs të hapur;
- pozicioni i Specialistit Operator në Drejtorinë e Arkivit Qendror ka 18 muaj i mbetur vakant dhe aktualisht nuk ka një konkurs të hapur.

Për 2 pozicionet e fundit, ISSH ka hapur konkurset përkatëse për këto vende të lira gjatë periudhës nën auditim, por nuk ka pa patur asnjë fitues.

- ***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 Institutit të Sigurimeve Shoqërore duhet të jetë i vetëdijshëm për rregullat dhe standardet e sigurisë dhe të jetë i aftë t'i zbatojë dhe ndjekë 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:
ISSH nuk ka patur plan trajnimi vjetor për vitin 2021 dhe 2022 për burimet njerëzore të DBI në lidhje me Teknologjinë e Informacionit. Gjatë vitit 2022, janë zhvilluar 4 trajnime në lidhje me problematikat e dala gjatë funksionimit të aplikimeve online dhe të sistemeve PCAMS, DMAIS dhe CMIS.
- Nga auditimi nuk u administruan dokumentacione mbi propozimet përkatëse nga niveli menaxherial i ISSH 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. ISSH nuk ka zhvilluar trajnime të mjaftueshme për zhvillimin profesional të punonjësve. Në lidhje me këtë çështje, nga Drejtoria e Burimeve të Informacionit janë kërkuar zhvillimi i 4 temave si më poshtë:

1. Problematika të dala gjatë funksionimit të Aplikimit online
2. Problematika të dala gjatë funksionimit të sistemit PCAMS
3. Probleme me dhënien e vërtetimeve nga sistemi DMAIS
4. Problematika të dala gjatë funksionimit të sistemit CMIS

Këto tema janë problematika të sistemeve dhe i ka zhvilluar në programin e trajnimit miratuar nga Drejtori i Përgjithshëm me nr. 4004 prot, datë 08.06.2022, tema të cilat janë pasqyruar dhe në kurikulat e program-trajnimit të IT ku kanë marrë pjesë 18 punonjës. Megjithatë, stafi i DBI nuk ka kryer asnjë ditë trajnim për sigurinë e informacionit.

Nga auditimi u konstatua se:
ISSH dhe DBI nuk kanë kryer një analizë të nevojave për trajnim të stafit të DBI, si dhe nuk kanë një plan trajnimesh për vitin 2023.

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 ISSH.

Nga administrimi i dokumentacionit u konstatua se Instituti i Sigurimeve Shoqërore identifikon dhe menaxhon risqet institucionale duke disponuar regjistrin e riskut të përgjithshëm institucional. Strategjia e Menaxhimit të Riskut në Sistemin e Sigurimeve Shoqërore është miratuar nga Drejtori i Përgjithshëm me shkresën nr. 8245/2, datë 28.02.2020 dhe përmban parimet e përgjithshme të menaxhimit të riskut në sistemin e sigurimeve shoqërore i cili

menaxhohet nga ISSH dhe strukturat rajonale e lokale në varësit të tij. Përpos kësaj, për vitin 2022, DBI ka përgatitur dhe një hartë risku për të identifikuar dhe menaxhuar risqet e teknologjisë së informacionit.

Megjithatë, ***nga auditimi u konstatua se:***
Për vitin 2021, ISSH nuk ka disponuar një regjistër risku të teknologjisë së informacionit në mospërputhje me me nenin 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, Udhëzimin nr. 21, datë 25.10.2016 "Për nëpunësit zbatues të të gjitha niveleve", UMF nr. 16, datë 20.07.2016 "Për përgjegjësitë dhe detyrat e koordinatorit të menaxhimit financiar dhe kontrollit dhe koordinatorit të riskut në njësitë publike", si dhe Rregulloren IT "*Mbi parimet dhe rregullat e përgjithshme të sigurisë së informacionit*", pika 4.4 "*Analiza e riskut dhe ndryshimit të dokumenteve*": "Drejtoria e Burimeve të Informacionit do të kryejë analiza të riskut për asetet e informacionit të ISSH".

Për sa më sipër, për vitin 2021, ISSH:
a. Nuk ka kryer identifikime dhe vlerësime të risqeve IT, duke mos identifikuar dhe prioritarizuar të dhënat kritike, programet aplikative, operacionet dhe burimet.
b. Nuk ka patur një mekanizëm efektiv dhe të mirëdokumentuar të identifikimit dhe vlerësimit të riskut të sigurisë së informacionit.

1. Titulli i gjetjes: Mungesa e një strategjie institucionale, përfshirë strategjinë për Teknologjinë e Informacionit
Situata: Nga auditimi u konstatua se:
ISSH nuk ka një strategji institucionale, përfshirë atë për Teknologjinë e Informacionit, duke mos pasqyruar qartë objektivat lidhur me infrastrukturën, burimet e nevojshme, si dhe instrumentat e nevojshme për matjen e objektivave. Mungesa e një plani strategjik mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së ISSH.
Kriteri: Ligji nr.10296, datë 08.07.2010 "Për menaxhimin financiar dhe kontrollin" i ndryshuar, standardet ndërkombëtare të TI dhe praktikat më të mira të fushës.
Ndikimi/efekti: Mospasqyrim i qartë i objektivave lidhur me infrastrukturën, burimet e instrumentat nevojshme për matjen e objektivave, si dhe risk i keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së ISSH.
Shkaku: Mosmenaxhimi dhe mosmiratimi në bazën ligjore, nënligjore dhe aktet rregullative, si dhe moszbatimi i praktikave më të mira në zhvillimin dhe menaxhimin institucional.
Rëndësia: E lartë
Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masat e nevojshme për hartimin dhe miratimin e Planit Strategjik Institucional, përfshirë planifikimin strategjik mbi teknologjinë e informacionit ku të adresohen qartë objektivat e institucionit duke reflektuar ndryshimet institucionale, strukturore dhe ndryshimet në teknologjinë e informacionit dhe komunikimit (TIK), të ndodhura ndër vite në ISSH.

2. Titulli i gjetjes: Mosplotësim i strukturës së burimeve njerëzore
Situata: Nga auditimi u konstatua se:
Në strukturën e IT në Drejtorinë e Përgjithshme dhe Drejtoritë Rajonale të Sigurimeve Shoqërore (DRSSH) ka 60 vende pune, nga të cilat rezulton se ka 3 vende vakante të cilat nuk janë plotësuar ende. Këto vakanca kanë ardhur si pasojë e largimit të punonjësve IT.
Kriteri: Ligji nr.10296, datë 08.07.2010 "Për menaxhimin financiar dhe kontrollin" i ndryshuar.
Ndikimi/efekti: Risk i lartë për mosidentifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit në ISSH.
Shkaku: Mosmarrja e masave të nevojshme për plotësimin e vendeve vakante.
Rëndësia: E lartë

Rekomandimi: Strukturat drejtuese në ISSH, në bashkëpunim me Drejtorinë e Burimeve Njerëzore, të marrin të gjitha masat e nevojshme për plotësimin e vendeve vakante sipas strukturës organike të tyre.

3. Titulli i gjetjes: Trajnim dhe zhvillim profesional i pamjaftueshëm i burimeve njerëzore
Situata: Nga auditimi u konstatua se:
Nga auditimi u konstatua se ISSH nuk ka patur plan trajnimi vjetor për burimet njerëzore të Drejtorisë së Burimeve të Informacionit, në lidhje me Teknologjinë e Informacionit. Gjatë vitit 2022, janë zhvilluar 4 trajnime në lidhje me problematikat e dala gjatë funksionimit të aplikimeve online dhe të sistemeve PCAMS, DAMIS dhe CMIS, por nuk ka patur propozime nga niveli menaxherial i ISSH për zhvillimin e trajnimeve mbi sistemet, sigurinë dhe teknologjinë e informacionit. ISSH nuk ka zhvilluar trajnime të mjaftueshme për zhvillimin profesional të punonjësve.
Kriteri: Ligji nr.10296, datë 08.07.2010 "Për menaxhimin financiar dhe kontrollin" i ndryshuar.
Ndikimi/efekti: Risk i lartë për mosidentifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit në ISSH.
Shkaku: Mosmarrja e masave të nevojshme për trajnimin dhe zhvillimin profesional të punonjësve të TI.
Rëndësia: E lartë
Rekomandimi: Strukturat drejtuese në ISSH të marrin masa për identifikimin e nevojave për trajnimin e stafit IT dhe të çdo përdoruesi të sistemeve TIK në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit, si dhe të hartojnë e miratojnë plane vjetore trajnimi.

2.2. Auditimi i Sigurisë së Informacionit

a)Siguria e të dhënave, verifikimi i sigurisë fizike dhe vazhdimësia e ofrimit të shërbimit.

Në zbatim të pikës 3"*Auditimi i Sigurisë së Informacionit* ", në Institutin e Sigurimeve Shoqërore u shqyrtua dokumentacioni i mëposhtëm:

Në zbatim të *auditimit të Sigurisë së Informacionit*, u shqyrtua dokumentacioni i mëposhtëm:
- Verifikime onsite të dhomës së serverave dhe infrastrukturës network të ISSH.
- Skema e komunikimit të network-ut;
- Verifikimi i Politikave mbi Sigurinë e Informacionit;
- Verifikimi i Procedurave për backup-in e të dhënave;
- Verifikimi i dokumenteve të planeve për vazhdueshmërinë e biznesit dhe rimëkëmbjes nga katastrofat;

Auditimi i Sigurisë së Informacionit

Auditi i Sigurisë së Informacionit është një proces i vlerësimit të sigurisë së informacionit në Institucion për të identifikuar dhe adresuar rreziqet dhe incidentet e mundshme. Ky proces ndihmon Insitucionet të sigurojnë që të dhënat dhe informacioni të jenë të mbrojtur dhe të sigurtë, të përmbushin kërkesat e ligjeve dhe standardeve të sigurisë së informacionit, dhe të rrisin ndërgjegjësimin e punonjësve të Institucioneve rreth sigurisë së informacionit dhe rreziqeve të mundshme. Auditimi i sigurisë së informacionit identifikon sfidat dhe rreziqet e mundshme në nivelin e sigurisë së informacionit dhe ndihmon në zhvillimin e strategjive për t'i përballuar ato. Në të njëjtën kohë, ai identifikon politikat dhe procedurat e sigurisë së informacionit dhe vlerëson se a janë ato të përshtatshme dhe të ndjekura me përpikëri nga punonjësit e Institucionit.
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".

Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet

Verifikimi i shkallës së sigurisë së dhomës së serverave me qëllim parandalimin e humbjes ose të dëmtimit të pajisjeve kompjuterike, aksesit të paautorizuar, kopjimit ose shikimit të informacionit sensitiv. Auditimi mbi shkallën e sigurisë së dhomës së serverave u krye në bazë të manualit të auditimit IT, ISSAI 5310 dhe ISO 27001 si dhe rregullores për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK për administratën publike. Dukë qenë se dhoma e serverave është një pikë delikate e një sistemi informatik dhe përqendrimi i pajisjeve kompjuterike, mekanike, elektrike dhe elektronike është më i lartë se në ambientet e tjera të punës, dëmet eventuale të shkaktuara në këtë ambient do të sillnin probleme serioze në funksionimin e të gjithë sistemit. Për këtë qëllim, grupi i auditimit, të shoqëruar nga personat përgjegjës të ISSH-së vizitoi onsite pajisjet fizike të ISSH.

Ambienti fizik i dhomës së serverave

Meqenëse për periudhën nën auditim (01.01.2021-31.12.2022) sipas përcaktimeve të VKM 673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtarë 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. 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 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.

Foto nr.1 *Dhoma e serverëve në ISSH*

Për funksionimin e Sistemeve të Teknologjisë së Informacionit në ISSH është në funksionim një dhomë serverash, nga auditimi i saj u konstatua se Dhoma e serverave e ristrukturuar rezultoi se plotëson parametrat TIK të përcaktuara nga AKSHI për ndërtimin e dhomës së Serverave.
-Nga verifikimi i dhomës së serverëve në ISSH rezultoi se një Rack(raft) me pajisje kompjuterike) nuk i përkiste ISSH . Nga intervista me përfaqsuesit e ISSH, grupit iu informua se këto pajisje i përkisnin AKSHI-t por nuk kishte dokumentacion mbi dakordësinë dhe arsyen e vendosjes së pajisjeve brenda dhomës së serverëve të ISSH, kjo mund të sjelli kompromentimin e të dhënave duke qenë një institucion i rëndësisë së veçantë, ku në mjediset e tij mban sisteme dhe pajisje kompjuterike të cilat ruajnë dhe përpunojnë të dhëna sensitive.
Nga auditimi mbi pajisjet firewall, dhe infrastruktura e networkut konstatohet se infrastruktura e serverave të ISSH është end of life dhe e amortizuar. Kjo infrastrukturë nuk i plotëson kërkesat aktuale dhe ato të rritjes së kapacitetit në të ardhmen.

Verifikimi në terren i Drejtorive rajonale të ISSH

Në përmbushje të objektivave të përcaktuara në Programin e Auditimit nr. 1188/1, datë 23.01.2023 grupi auditimit kreu disa verifikime në terren në Drejtoritë Rajonale të ISSH Vlorë dhe Lezhë.

Foto nr.2 dhe 3: *Foto nga Infrastruktura Network në Drejtorinë Rajonale ISSH Vlorë*

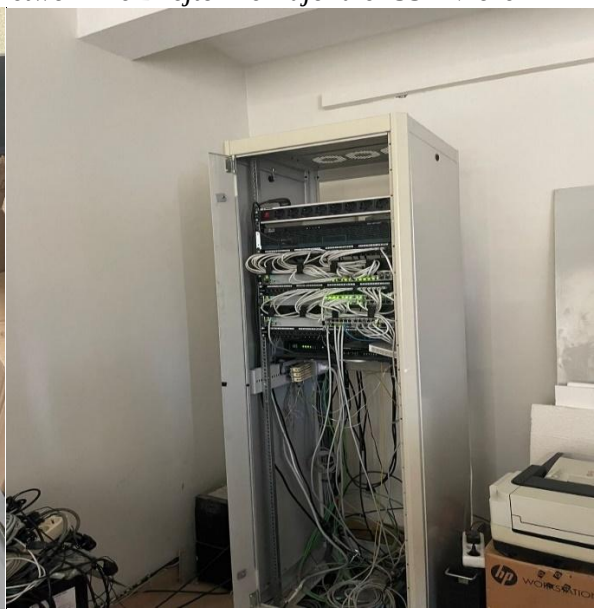



Foto nr4 dhe 5: *Foto nga Infrastruktura Network në Drejtorinë Rajonale ISSH Lezhë*


-Nga verifikimi në terren në Drejtorinë rajonale të ISSH Vlorë grupi i auditimit konstatoi se Infrastruktura Network e pajisjeve ndihmëse që nevojiten për shërbimet e komunikimit dhe ruajtjes së të dhënave është në kushtet jo minimale dhe optimale, ku shërbimet e ngritura mbi këto rrjete nuk janë të sigurta dhe nuk mbështesin vazhdimësinë e punës.
-Nga auditimi u konstatua se në drejtoritë rajonale (Vlorë, Lezhë) nuk ka një linjë back up interneti në rast të shkëputjes së linjës, duke sjellë kështu mosfunksionim të sistemit dhe ndërprerje të ofrimit të shërbimeve.
- Kompjuterat në drejtoritë rajonale (Vlorë, Lezhë) nuk janë të pajisur me antivirus për mbrojtje ndaj sulmeve.
-Nuk ka një server qëndror të pajisur me Active Directory Domain Controller për menaxhimin e përdoruesve dhe vendosjen e politikave të sigurisë.
-Nuk kanë një pajisje firewall për mbrojtjen e rrjetit nga sulmet e jashtme.

Procedura e backup-it
Qëllimi i procedurës së kryerjes së backup-it të sistemeve në përdorim është që të sigurojë metoda dhe procedura të standardizuara mbi këto procese, duke siguruar kështu ruajtjen e të dhënave të serverave dhe mundësimin e rikthimit të këtyre të dhënave në raste të defekteve kritike ose rasteve të tjera të humbjes së të dhënave.
Nga auditimi u konstatua se:
-Backup-et e sistemeve PCAMS, CMIS dhe DMAIS janë të ruajtura në Tape library, të cilat pasi mbushen ruhen në të njëjtën godinë me sistemet PCAMS, CMIS dhe DMAIS.
-Kopjet (backup) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Backup- i Bazës së të Dhënave.

Mbi verifikimin e dokumentimit të planeve për vazhdueshmërinë e biznesit dhe rimëkëmbjes nga katastrofat
Qëllimi i menaxhimit të vazhdimësisë është të mirëmbahen kërkesat e vazhdimësisë së institucionit. Menaxhimi i vazhdimësisë përfshin rishikimin periodik dhe azhornimin e afatit të rimëkëmbjes për të siguruar që ato janë në përputhje me Planet e Vazhdimësisë së Biznesit. Vazhdueshmëria a biznesit (BCP) është procesi që një institucion ndjek për të planifikuar dhe testuar rimëkëmbjen e operimit të saj pas një ndërprerjeje.
Auditimi mbi ofrimin e Vazhdimësisë së ofrimit të shërbimeve u bazua mbi 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, risqeve të identifikuara dhe praktikave më të mira. Referuar kësaj VKM-je: "Çdo institucion i cili ka ose do të zhvillojë sisteme në fushën e teknologjisë së informacionit, që ofron shërbime për qytetarët, për biznesin dhe për ndërveprim e shkëmbimit të informacionit për administratën publike nëpërmjet sistemeve elektronike, duhet të parashikojë dhe të realizojë investime për krijimin e sistemit të vazhdueshmërisë së punës (Business Continuity) dhe sistemit të ruajtjes së informacionit (Backup), me qëllim mundësimin e ofrimit të shërbimit pa ndërprerje dhe parandalimin e humbjes ose të shkatërrimit aksidental të të dhënave". Në këtë VKM cilësohet gjithashtu edhe dokumentimi i politikave mbi planin e vazhdueshmërisë së punës dhe rikuperimit nga katastrofat, si dhe të bëhet i mundur evidentimi i sistemeve të cilat janë kritike për ofrimin e shërbimit 24/7.
Nga auditimi u konstatua se ISSH:
-nuk disponon 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", pika 1.
-nuk ka bërë të mundur evidentimin e sistemeve kritike për ofrimin e shërbimit 24 orë në 7 ditë të javës.
-nuk disponon dokument të politikave të vazhdueshmërisë së punës (BCP) dhe një plan të rikuperimit nga katastrofa (disaster recovery) me qëllim garantimin e vazhdueshmërisë së ofrimit

të shërbimeve në raste të jashtëzakonshme emergjencash në kundërshtim me pikën 1 shkronja c) dhe ç), të 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.
Këto dokumente përcaktojnë masat, procedurat dhe objektivat të mirë dokumentuara për rivendosjen në funksionim të sistemit në rastet e emergjencave dhe që sigurojnë vazhdueshmërinë e punës së sistemeve si dhe përcaktimin e RTO (Objektivat e Kohës së Rimëkëmbjes) dhe RPOs (Objektivat e Punës së Ripërtëritjes) për çdo proces kritik.

Faqja web e ISSH https://www.issh.gov.al

Në faqen web të ***ISSH*** janë publikuar informacione të ndryshme mbi shërbimet që ofron institucioni. Rubrikat kryesore të faqes janë: Lajme, Kontribues, Përfitues, Baza Ligjore, Statistika, Programi i Transparencës, Kontakt.
Nga auditimi rezultoi se
-Faqja Web e ISSH nuk përdor një lidhje të sigurtë (*connection security*) HTTPS (*HyperText Transfer Protocol Secure*) që do të thotë se serveri i faqes së internetit përdor një certifikatë sigurie për të vërtetuar identitetin e internetit në shfletues.

Ne bazë të Ligjit 119/2014 datë18.09.2014. "Për të drejtën e informimit" në faqen web të ISSH është i miratuar Programi i Transparencës po disa nga kategoritë e tij janë të paplotësuara.

Për sa është trajtuar në këtë pikë të Projekt Raportit të Auditimit është mbajtur Aktkonstatimi nr. 2, datë 15.03.2023, protokolluar në Institutin e Sigurimeve Shoqërore me nr. 2158 datë 15.03.2023, mbi të cilin nuk janë paraqitur observacioneme .

1.Titulli i Gjetjes: Vendosje e pajisjeve që nuk i përkasin institucionit në ambientin e dhomës së serverëve pa hartuar një dokumentacion përkatës.
Situata: Nga verifikimi i dhomës së serverëve në ISSH u konstatua se një Rack (raft me paisje kompjuterike) nuk ishte pronë e ISSH por pronë e AKSHIT i cili ruhej në dhomën e serverëve të ISSH. Për këto pajisje nga ISSH nuk disponohej asnjë dokumentacion justifikues për transferimin si dhe qëllimin e vendosjes së tyre në ambientet e dhomës së serverëve të ISSH.
Kriteri: Infrastruktura TIK sipas praktikave më të mira.
Ndikimi/Efekti: Risk në thyerjen e sigurisë së Informacionit.
Shkaku: Mungesa e dokumentacionit të duhur.
1.Rekomandimi: Instituti i Sigurimeve Shoqërore të marri masa të menjëhershme për hartimin e dokumentacionit përkatës, ku të sqarohet arsyeja e vendosjes së pajisjeve kompjuterike (jo të institucionit) në dhomën e serverëve dhe personat e autorizuar që mund të kenë akses tek to.

2.Titulli i Gjetjes: Problematika e Infrastrukturës TIK dhe Sigurisë së Informacionit në në Drejtoritë Rajonale të ISSH Vlorë dhe Lezhë.
Situata 1: Nga verifikimi në terren në Drejtorinë rajonale të ISSH Vlorë, grupi i auditimit konstatoi se Infrastruktura Network e pajisjeve ndihmëse që nevojiten për shërbimet e komunikimit dhe ruajtjes së të dhënave është në kushtet jo minimale dhe optimale, ku shërbimet e ngritura mbi këto rrjete nuk janë të sigurta dhe nuk mbështesin vazhdimësinë e punës.
Situata 2: Nga auditimi u konstatua se në Drejtoritë Rajonale (Vlorë, Lezhë) nuk ka një linjë back up interneti në rast të shkëputjes së linjës, duke sjellë kështu mosfunksionim të sistemit dhe ndërprerje të ofrimit të shërbimeve.

Situata 3: Kompjuterat në drejtoritë rajonale (Vlorë, Lezhë) nuk janë të pajisur me antivirus për mbrojtje ndaj sulmeve.
-Nuk ka një server qëndror të pajisur me Active Directory Domain Controller për menaxhimin e përdoruesve dhe vendosjen e politikave të sigurisë.
-Nuk kanë një pajisje firewall për mbrojtjen e rrjetit nga sulmet e jashtme.
Kriteri: Standardet ndërkombëtare dhe praktikat më të mira të fushës.
Ndikimi/Efekti: Risk në mos përmbushje të objektivave të përcaktuara.
Shkaku: Mos zbatim i standardeve më të mira të fushës.
2. Rekomandimi: ISSH të marrë masa për pajisjen dhe standardizimin e infrastrukturës IT në Drejtoritë Rajonale si dhe të marrë masa për hartimin dhe miratimin e një procedure standarde për komunikimin dhe zgjidhjen e problematikave që lindin me Drejtoritë Vendore në lidhje me sistemet IT, me qëllim sigurimin e kushteve optimale për ofrimin e shërbimit dhe mbarëvajtjen e punës pa ndërprerje.

3.Titulli i gjetjes: ISSH nuk disponon një infrastrukturë BCC, për garantimin e vazhdimësisë së ofrimit të shërbimit.dhe Backup-et e sistemeve nuk testohen vazhdimisht.
Situata 1: Nga auditimi u konstatua se ISSH nuk disponon një infrastrukturë BCC (Business Continuity Center), si dhe nuk ka një plan mbi vazhdimësinë e punës dhe rimëkëmbjet nga katastrofat 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.
Situata 2: Backup-et e sistemeve PCAMS, CMIS dhe DMAIS janë të ruajtura në Tape library, të cilat pasi mbushen ruhen në të njëjtën godinë me sistemet PCAMS, CMIS dhe DMAIS.
-Kopjet (backup) e të dhënave nuk testohen rregullisht .
Kriteri: 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., i ndryshuar.
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.
3.1.Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, bazuar në rëndësinë që ka ofrimi i shërbimit pas një fatkeqësie, të ndërmarrin hapat e nevojshëm për ndërtimin e një qendre *Business Continuity.*
3.2.Rekomandimi: Drejtoria e Burimeve të Informacionit të marri masa për kryerjen dhe testimin periodik të backup-it të të dhënave të sistemeve duke e dokumentuar procesin.

4.Titulli i gjetjes: Mungesë e Informacionit të faqes së internetit të ISSH përgjatë navigimit.
Situata: Në kuadrin e transparencës bazuar në Ligjin 119/2014 datë18.09.2014. "Për të drejtën e informimit, ISSH ka të afishuar në faqen e saj web (issh.gov.al), kontribues, përfitues, programin e transparencës, etj. Nga auditimi i faqes web konstatua se:
Tek menuja "Programi Transparencës":
Seksioni "Regjistri i Kërkesave dhe Përgjigjeve" nuk është publikuar viti 2022;
Seksioni "Sistemi i mbajtjes së dokumentiacionit, llojet dhe format e dokumenteve" nuk përmban asnjë informacion;
Seksioni "Mekanizmat kontrollues dhe monitorues " nuk përmban asnjë informacion.
Kriteri: *Ligjit 119/2014 datë18.09.2014. "Për të drejtën e informimit*
Ndikimi/efekti: Mungesë transparence në veprimtarinë e ISSH
Shkaku: Mos përditësimi i faqes web me marrë masat e nevojshme.
Rëndësia: E mesme

4.Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa për përditësimin dhe përmirësimin e faqes web (me informacione, rregullore,a kte, etj) si dhe reflektimin e mangësive të dala nga auditimi, me qëllim rritjen e transparencës dhe ndihmesën ndaj qytetarëve.

3.2Auditimi i zhvillimit dhe blerjes në teknologjinë e informacionit

Në Institutin e Sigurimeve Shoqërore, u shqyrtua dokumentacioni si më poshtë:

1. Lista e prokurimeve TIK të periudhës 01.01.2021 – 31.12.2022;
2. Procedura "Ndjekje e marrëveshjes së shërbimit për sistemet informatike të DMAIS për menaxhimin dhe arkivimin e dokumentave, PCAMS për llogaritjen dhe caktimin e pensioneve, FMS për menaxhimin financiar, CMIS për menaxhimin e deklarimit online të kontribuesve, rrjetit informatik dhe pajisje të caktuara të dhomës së serverave, pajisje IT për ISSH dhe komunikim ISSH-Arkiva (ISSH-Drejtori në varësi)" për Institutin e Sigurimeve Shoqërore, viti 2021.
3. Procedura "Mirëmbajtja e faqes zyrtare të ISSH-së – Mirëmbajtja e software-ve të teknologjisë së informacionit", viti 2022[1].

Bazuar në Regjistrin e Realizimeve të ISSH vënë në dispozicion të grupit të auditimit, procedurat e vetme në fushën e teknologjisë së informacionit që ka zhvilluar ISSH, të paaudituara më parë nga KLSH, janë ato të mësipërmet dhe grupi i auditimit i shqyrtoi të dyja.

Mbi procedurën "Ndjekje e marrëveshjes së shërbimit për sistemet informatike të DMAIS për menaxhimin dhe arkivimin e dokumentave, PCAMS për llogaritjen dhe caktimin e pensioneve, FMS për menaxhimin financiar, CMIS për menaxhimin e deklarimit online të kontribuesve, rrjetit informatik dhe pajisje të caktuara të dhomës së serverave, pajisje IT për ISSH dhe komunikim ISSH-Arkiva (ISSH-Drejtori në varësi)":

Kontrata me objekt "Marrëveshje shërbimi për sistemet informatike të DMAIS për menaxhimin dhe arkivimin e dokumentave, PCAMS për llogaritjen dhe caktimin e pensioneve, FMS për menaxhimin financiar, CMIS për menaxhimin e deklarimit online të kontribuesve, rrjetit informatik dhe pajisje të caktuara të dhomës së serverave, pajisje IT për ISSH dhe komunikim ISSH-Arkiva (ISSH-Drejtori në varësi)" për Institutin e Sigurimeve Shoqërore" është lidhur ndërmjet AKSHI-t dhe bashkimit të operatorëve "I.S." Sh.p.k. dhe "I." Sh.p.k. me vlerë totale 201,355,200 (dyqind e një milion e treqind e pesëdhjetë e pesë mijë e dyqind) lekë me TVSH. Kontrata është lidhur në datën 21.04.2021 me një kohëzgjatje prej 24 muajsh mirëmbajtje.

Procedura e prokurimit të kësaj marrëveshjeje shërbimi është hartuar nga AKSHI dhe ISSH ka patur si detyrë vetëm ndjekjen e saj. Për çdo muaj, kontraktuesi ka dorëzuar pranë ISSH "Raportin mujor të shërbimeve të Sistemeve Informative të ndërtuara në ambientet e ISSH". Ky raport tregon të detajuara shërbimet e kryera nga Kontraktuesi në infrastrukturën Hardware, Software dhe Networking të Institutit të Sigurimeve Shoqërore gjatë një periudhe 1-mujore. ISSH ka kryer pagesat në bankë në bazë të faturave tatimore për ofrimin e shërbimit.

[1] Sa i përket procedurës "Mirëmbajtja e faqes zyrtare të ISSH-së – Mirëmbajtja e software-ve të teknologjisë së informacionit", viti 2021, ajo është audituar më parë nga KLSH.

Nga auditimi i kësaj procedure zbatimi u konstatua se:

Sistemet që ka në përdorim ISSH (PCAMS, FMS, DMAIS, CMIS) janë të papërditësuara dhe nuk ka patur asnjë kërkesë nga ana e ISSH për përditësimin e tyre, mundësi kjo e parashikuar edhe nga pika 10.5 e Kushteve të veçanta të kontratës midis AK dhe Kontraktuesit.

Në këtë nen të Kontratës citohet:
"*Në rast se nga ana e AK apo Përfituesit do të ketë kërkesa për përshtatje apo azhornime të sistemit informatik të DMAIS, PCAMS, FMS, CMIS, implementime apo integrime të reja të HW, të cilat pas analizimit reflektojnë ndërhyrje, shërbime, furnizime, apo transferime të infrastrukturës fizike ku janë hostuar sistemet që nuk janë parashikuar në specifikimet teknike, atëherë realizimi i kërkesave do të përpunohet sipas rendit të mëposhtëm të kërkesës për ndryshim: Komunikim me shkrim i kërkesës, analizë dhe vlerësim i ndikimit të realizimit të kërkesës, estimim teknik dhe financiar, aprovim, implementim, testim dhe pranim, instalim dokumentim. Puna e kryer dhe ndryshimet potenciale do të pasqyrohen si pjesë e raportit mujor i periudhës përkatëse. Këto kërkesa për ndryshim do të realizohen vetëm pas aprovimit nga të dyja palët.*"
Përditësimet e sistemeve kanë qenë të nevojshme për mirëfunksionimin e tyre dhe ISSH nuk i ka dërguar asnjë kërkesë Kontraktuesit bazuar në pikën e mësipërme të Kontratës.

Mbi realizimin e procedurës së prokurimit me vlerë të vogël "Mirëmbajtja e faqes zyrtare të ISSH-së":

Nga shqyrtimi i dokumentacionit të vënë në dispozicion, grupi i auditimit konstaton se me Kërkesën nr. 1788 prot., dt. 08.03.2022, ISSH ka argumentuar arsyet për kryerjen e këtij shpenzimi dhe domosdoshmërinë e këtij prokurimi.
- Në bazë të urdhrit nr. 1788/1, datë 10.03.2022 "Për krijimin e komisionit mbi hartimin e termave të referencës dhe kriteret për kualifikim për procedurën me objekt prokurimi "Mirëmbajtja e faqes zyrtare të ISSH-së", në të njëjtën datë janë hartuar specifikimet teknike dhe fondi limit.
- Më datë 11.03.2022 u ngrit Urdhri "Për prokurimin me vlerë të vogël" nr. 1788/2 me anë të të cilit ka filluar procedura e prokurimit me objekt "Mirëmbajtja e faqes zyrtare të ISSH-së" me fond limit në vlerën 260,000 lekë pa TVSH.
- Komisioni ka paraqitur në sistemin e prokurimit elektronik ftesën për ofertë me të dhënat e objektit të prokurimit. Më datë 16.03.2022 është bërë klasifikimi përfundimtar ku rezulton se kanë marrë pjesë 7 operatorë ekonomik (OE), nga të cilët është kualifikuar 1 OE, ndërsa 6 të tjerë janë skualifikuar pasi kanë dhënë vlerë ofertë më tepër se fondi limit i procedurës ose kanë ofertuar me një ofertë më të ulët se 50% të fondit të parashikuar.
- Komisioni ka mbajtur procesverbalin më datë 21.03.2022, duke përcaktuar si ofertë fituese operatorin ekonomik "K.", me vlerë oferte 254,000 lekë pa TVSH, i cili ka konfirmuar nëpërmjet sistemit për realizimin e shërbimit të kërkuar. Me nr. 1788/3prot, datë 23.03.2022, është hartuar dhe lidhur kontrata e shërbimit ndërmjet titullarit të AK dhe OE fitues.
- Më datë 28.03.2022, me anë të Urdhrit të Drejtorit të Përgjithshëm nr. 1788/4, është ngritur komisioni për ndjekjen dhe realizimin e shërbimit ku 2 nga 3 anëtarët e komisionit kanë qenë specalistë të fushës.
1. Me urdhër transfertën bankare është likuiduar fatura tatimore nr. 149/2022, datë 25.03.2022, për mirëmbajtjen e faqes zyrtare të ISSH, ndaj operatorit "K.", në vlerën 81,000 lekë me TVSH.
2. Me urdhër transfertën bankare është likuiduar fatura tatimore nr. 312/2022, datë 28.07.2022, për mirëmbajtjen e faqes zyrtare të ISSH, ndaj operatorit "K.", në vlerën 76,200 lekë me TVSH.

3. Me urdhër transfertën bankare është likuiduar fatura tatimore nr. 624/2022, datë 29.12.2022, për mirëmbajtjen e faqes zyrtare të ISSH, ndaj operatorit "K.", në vlerën 152,400 lekë me TVSH. Dosja e kësaj procedure prokurimi është e plotë.

Për sa është trajtuar në këtë pikë të Raportit Përfundimtar të Auditimit është mbajtur Aktkonstatimi nr.3, datë 15.03.2023, protokolluar në Institutin e Sigurimeve Shoqërore me nr. 2159 datë 15.03.2023, mbi të cilin nuk janë paraqitur observacioneme .

1. Titulli i gjetjes: Mungesë kërkesash për përditësimin e Sistemeve
Situata: Nga auditimi u konstatua se:
Nga auditimi i kontratës së zbatimit me objekt "Marrëveshje shërbimi për sistemet informatike të DMAIS për menaxhimin dhe arkivimin e dokumentave, PCAMS për llogaritjen dhe caktimin e pensioneve, FMS për menaxhimin financiar, CMIS për menaxhimin e deklarimit online të kontribuesve, rrjetit informatik dhe pajisje të caktuara të dhomës së serverave, pajisje IT për ISSH dhe komunikim ISSH-Arkiva (ISSH-Drejtori në varësi)" u konstatua se:
Sistemet që ka në përdorim ISSH (PCAMS, FMS, DMAIS, CMIS) janë të papërditësuara dhe nuk ka patur asnjë kërkesë nga ana e ISSH për përditësimin e tyre, mundësi kjo e parashikuar nga pika 10.5 e Kushteve të veçanta të kontratës midis AK dhe Kontraktuesit. Përditësimet e sistemeve kanë qenë të nevojshme për mirëfunksionimin e tyre dhe ISSH nuk i ka dërguar asnjë kërkesë Kontraktuesit bazuar në pikën e mësipërme të Kontratës.
Kriteri: Pika 10.5 e Kushteve të veçanta të Kontratës midis Autoritetit Kontraktor dhe Kontraktuesit, praktikat e mira në fushën e TI.
Ndikimi/efekti: Problematika, ngadalësime dhe mungesë komunikimi midis të dhënave në sistem.
Shkaku: Moszbatimi i kushteve të veçanta të kontratës.
Rëndësia: E lartë
1.1 Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, të marrin masa që në kontratat e mirëmbajtjes së sistemeve të ISSH që do të lidhen në vazhdimësi të sanksionohet që Kontraktuesi duhet të kryejë rregullisht përditësim të këtyre sistemeve.
1.2 Rekomandimi: Instituti i Sigurimeve Shoqërore të verifikojë rregullisht nëse sistemet PCAMS, DMAIS, FMS, CMIS kanë nevojë për përditësime, ndërhyrje apo korrigjime duke i bërë kërkesën përkatëse Kontraktuesit.

2.4 Auditmi i Sistemeve

Në zbatim të pikës 4"*Auditimi i sistemeve*", në Institutin e Sigurimeve Shoqërore u shqyrtua dokumentacioni i mëposhtëm:

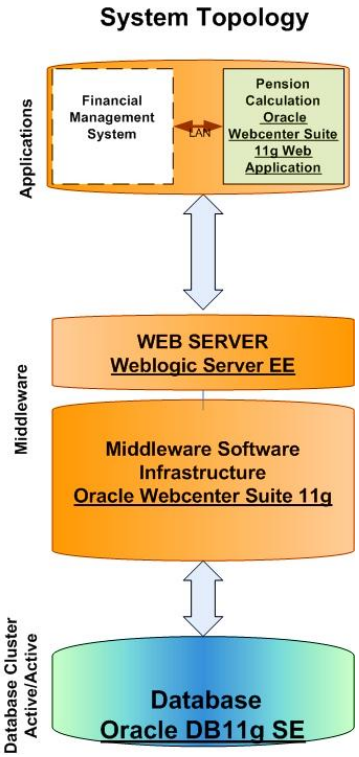
- Aktet rregullative të ISSH që lidhen me sistemet dhe veprimet operacionale brenda dhe jashtë sistemit;
- Manualet e përdorimit të sistemeve;
- Intervista të drejtpërdrejta me punonjës që administrojnë sisteme informatike apo shërbime të caktuara;
- Të dhënat për përdoruesit të sistemit;
- Vizita ne terren dhe verifikimi në sistem;

ISSH disponon 3 sisteme kryesore, me baza të dhënash të regjistruara si kombëtare në zbatim të ligjit nr.10325, datë 23.9.2010, "*Për bazat e të dhënave shtetërore*":

Drejtoria e Burimit të Informacionit në ISSH është drejtoria qe është ngarkuar me menaxhimin e të gjitha sistemeve informatike.

PCAMS –Pension Calculation and Assignement Management System

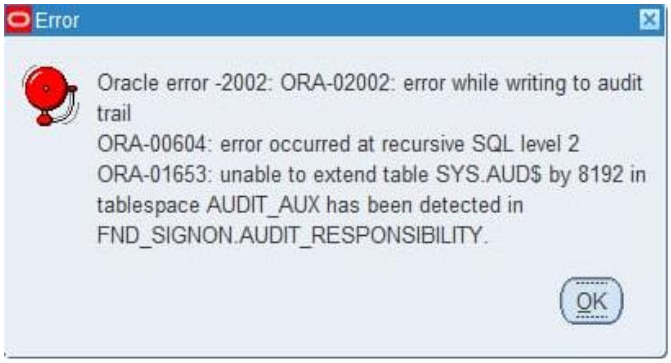
Sistemi i menaxhimit të llogaritjes dhe pagesave të përfitimeve.



Shërbimet që ofron ky sistem janë:

- **Pritja e kërkesave:** Aplikimet për të gjitha shërbimet e ISSH bëhen nëpërmjet portalit qeveritar e-Albania.
- **Llogaritja online e përfitimit:** Inspektoret shikojnë listën e kërkesave për aplikim bashkë me gjitha dokumentet përkatëse (që vijnë me postë) dhe vazhdojnë me hedhjen dhe llogaritjen elektronike të përfitimeve. Edhe në këtë moment verifikimi behet përsëri me anë të NID (Numrit te Identifikimit) në regjistrin e gjendjes civile online. Theksojmë se kërkimi dhe verifikimi në regjistrin e gjendjes civile online bëhet vetëm nëpërmjet NID-it, pra, jo me emër, mbiemër apo gjeneralitete të tjera. Gjate kontrollit të NID-it, janë hasur shumë probleme të qytetarëve me të dhënat e tyre në zyrat e gjendjeve civile. Pasi një përfitim mbaron së llogarituri dhe merr miratimet përkatëse në sistem, ai gjenerohet në mënyrë elektronike për në zyrat e pagesave të postës shqiptare.
- **Pagesat elektronike të përfitimeve.** Aktualisht, posta shqiptare i kryen pagesat në mënyrë elektronike me anë të një web servisi. Një qytetar nuk mund të paguhet n.q.s. ka disa përfitime në pika të ndryshme paguese. Një qytetar, nëse ka më shumë se sa një periudhe pa tërhequr, nuk mund të tërheqë vetëm disa periudha, ose të gjitha ose asnjë prej tyre. Agjentët pagues të postës shqiptare nuk mund të anulojnë një veprim ditën tjetër, anulimi i pagesave bëhet vetëm brenda ditës. Kjo mënyrë pagese është më transparente dhe qytetarët shërbehen në kohë reale. Vetëm pikat paguese në zonat rurale nuk e kanë këtë shërbim.
- **Dhënia e vërtetimeve për të ardhurat mujore të përfitimit:** Të interesuarit dorëzojnë aplikimet pranë zyrave të ISSH-së. Ky vërtetim lëshohet për efekt dokumentacioni për jashtë shtetit dhe jepet vetëm në zyrat e ISSH-së.
- Përsa i takon dosjeve që kishin qenë të lidhura para vënies në punë të programit, janë hedhur në sistem dhe gjatë hedhjes së tyre janë kapur edhe ndryshimet në datëlindje, apo personat që në mënyrë të padrejtë kishin dy përfitime.

Fig nr 1.Error në database



- *-Nga auditimi u konstatua se në databasen e PCAMS në tablespace Audit_Aux nuk ka hapësira të nevojshme të alokuara në memorie (HDD); kjo mungesë e hapësirës (në tablespace) sjell degradim të performancës dhe gabime në databazë.*

DMAIS- Document management and Archiving Information System
Sistemi elektronik i digjitalizimit dhe arkivimit të dokumenteve të Arkivit Qendror.

- Ky sistem është ngritur për të digjitalizuar dhe arkivuar të gjithë dokumentacionin e vjetërsisë në pune i cili përfshin: regjistrat e ish-Kooperativave Bujqësore para vitit 1994, regjistrat e ish Ndërmarrjeve Shtetërore para vitit 1994 dhe listë pagesat pas vitit 1994.
- Në këtë sistem digjitalizohet gjithçka, duke filluar që nga:
- Regjistrimi i regjistrave dhe listë pagesave.
- Vendndodhja e tyre fizike në arkiv.
- Certifikimi për çdo faqe nga specialistet përkatës.
- Skanimi i çdo faqeje te regjistrave dhe liste pagesave.
- Digjitalizimi i të dhënave të faqeve.
- Hyrjet/Daljet e regjistrave nga Arkiva. Ne këtë pikë theksojmë se kur një regjistër skanohet ai kthehet menjëherë ne arkivë dhe digjitalizimi i faqeve bëhet nëpërmjet imazheve të skanuara.
- Dhënia e vërtetimeve për vjetërsi në pune.
- Ky sistem nuk ka lidhje me regjistrin e gjendjes civile sepse informacioni i faqeve është i paket përsa i përket gjeneraliteteve, jo shume mire i lexueshëm ose i dëmtuar në disa raste, meqenëse janë regjistra të viteve para 1994.

-Nga auditimi i sistemit DMAIS në lidhje me performancën e veprimeve duke u bazuar në treguesit si: Koha e përgjigjes, koha e përpunimit, Përdorimi i burimeve të sistemit, komentet e përdoruesve, u konstatua se DMAIS i përgjigjet me vonesë kërkesave të përdoruesve.

-Nga auditimi u konstatua se për sistemet CMIS dhe DMAIS nuk ka një ambient test për menaxhimin e ndryshimeve që siguron që çdo ndryshim i bërë në sistemin të mos ndikojë negativisht në performancën e përgjithshme të sistemit. Mungesa e një testi ambient gjithashtu do të thotë që nuk ka mënyra për të verifikuar nëse ndryshimet e bëra në sistemin funksionojnë siç duhet ose jo.

-Nga auditimi u konstatua se për operimin e sistemeve përdoren: Red Hat Enterprise Linux (RHEL) 5. Windows server 8, Databasa në Oracle 11g, Cisco asa5520-bun. Gjithë infrastruktura ka arritur fundin e jetës, që do të thotë se prodhuesi nuk ofron më asistencë teknike, përditësime të sigurisë ose ndreqje të gabimeve për këto versione.

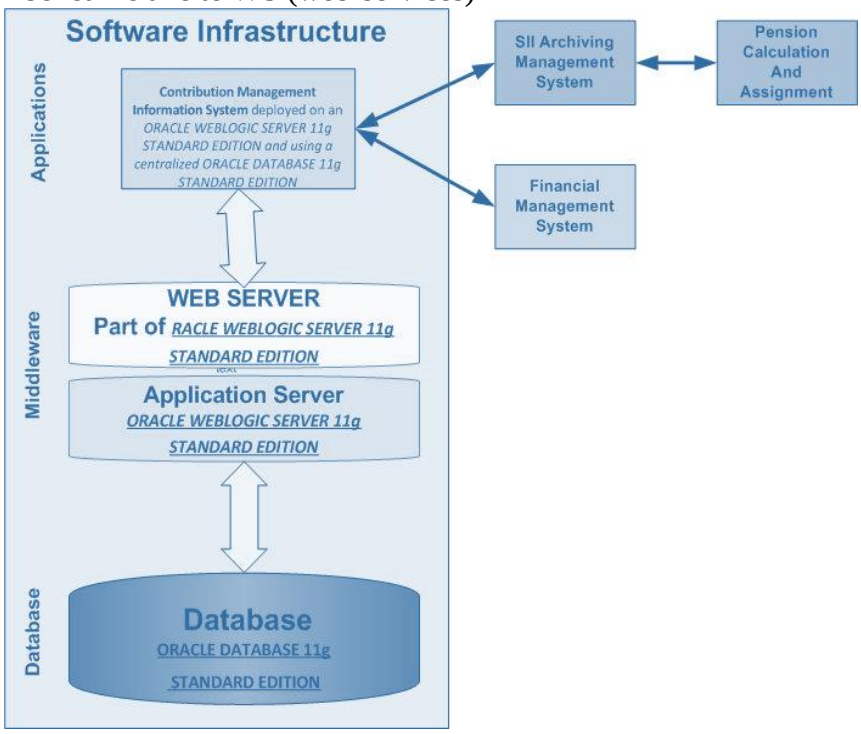
Gjatë auditimit të TI-së, u konstatua se sistemet (CMIS , DMAIS, PCAMS) kanë mungesa të ndërveprimit me njëri-tjetrin. Kjo mungesë e integrimit ndërmjet sistemeve rezulton në çështje të shumta, duke përfshirë:

- Mospërputhja e të dhënave: Meqenëse të dhënat u futën në sisteme të ndryshme veçmas, ekzistonte një rrezik i lartë i të dhënave të paqëndrueshme nëpër sisteme, duke çuar në raportim, vendimmarrje dhe analizë të pasaktë.

- Proceset që konsumojnë kohë: Mungesa e integrimit ndërmjet sistemeve rezultoi në futje të tepërta të të dhënave, rritje të përpjekjeve manuale dhe flukse pune komplekse. Kjo rrit kohën e nevojshme për detyrat dhe uli efikasitetin e përgjithshëm.
- Rreziqet e sigurisë: Çdo sistem menaxhohej veçmas, duke çuar në rreziqe të mundshme sigurie për shkak të kontrolleve të ndryshme të aksesit, mekanizmave të vërtetimit dhe dobësive në secilin sistem. Pamundësia për të ndarë të dhënat ndërmjet sistemeve nënkupton që subjekti humb mundësitë për të fituar njohuri mbi operacionet e tyre, për të optimizuar proceset dhe për të marrë vendime të bazuara në të dhëna.

CMIS – Contribution Management Information System
Sistemi elektronik I menaxhimit te kontributeve.

- Ky sistem është ngritur për të menaxhuar në mënyrë elektronike kontributet. Shërbimet e këtij sistemi janë:
- **Të vetëpunësuar në bujqësi.** Çdo qytetar qe paraqitet pranë zyrave të ISSH-së për të derdhur kontributet si i vetëpunësuar në bujqësi regjistrohet në këtë sistem me anë të NID-it të tij personal, i cili verifikohet në kohe reale në regjistrin e gjendjes civile online. Llogaritja e kontributit behet në mënyrë elektronike dhe urdhër veprimi printohet menjëherë nga sistemi.
- **Marrëveshja e vullnetarit.** Çdo qytetar që paraqitet pranë zyrave te ISSH-se për të lidhur marrëveshje për të derdhur kontribute vullnetare regjistrohet në ketë sistem njësoj si të vetë punësuarit në bujqësi.
- **Listëpagesat.** Ne ketë shërbim, punonjësit e drejtorisë se kontributeve te ISSH-se mund te kontrollojnë ne mënyrë elektronike listë pagesat që vijnë nga drejtoria e Tatimeve. Kjo pjese e sistemit i merr të dhënat nga sistemi informatik i tatimeve dhe transmetimi i tyre në sistem behet me ane te WS (web-services)



Drejtoria e IT importon në këtë aplikacion të dhënat që DPT dërgon në ISSH për listë pagesat, që prej vitit 2013 kur u bë një deklarim i detyrueshëm elektronik për të punësuarit në sektorin privat dhe shtetëror, caktuar me anë të ligjit nr. 9136, datë 11.09.2003 i ndryshuar "Për mbledhjen e kontributeve të detyrueshme të sigurimeve shoqërore dhe shëndetësore në republikën e Shqipërisë". Për transferimin e këtyre të dhënave, dy institucionet janë bazuar në

marrëveshjen e vitin 2011, si dhe në protokollin e komunikimit, për hapat që do të ndiqen për transferimin e tyre.

Nga auditimi u kryen verifikime intervista dhe pyetësorë në lidhje me të dhënat e input/output në aplikacionin CMIS , janë konstatuar disa problematika lidhur me të dhënat e importuara nga DPT në ISSH, të cilat po i përmendim si më poshtë:

- Rastet e evidentimit të vendosjes gabim të Numrit Personal NID kanë sjellë një problem në sistemin CMIS nuk shfaqen akoma listëpagesat e periudhave të personave gjyqfitues.
- Në sistemin CMIS nuk shfaqen muaj të veçantë, për subjekte të ndryshme dhe individë të ndryshëm, në vite të ndryshme, periudha të cilat ndërkohë shfaqen në sistemin tatimor.
- Në rastet kur subjektet kryejnë pagesa pjesore dhe për punëmarrës të vecantë, të dhënat e kontributeve të paguara nuk shfaqen në sistemin CMIS.
- Në rastet kur subjektet kryejnë korigjimin e deklaratës tatimore listëpagesat ESIG-25, krijon probleme të mundshme sidomos lidhur me kushtet e përfitimeve afat shkurtëra, pasi subjektet "luajnë" me deklarimet e punonjësve. (psh një punonjës merr përfitimin nga ISSH më pas bëhet rivlerësim i listëpagesës duke ndryshuar pagën ose duke e hequr fare punonjësin nga listëpagesa).
- Janë evidentuar raste të sjelljes në listëpagesa të personave që kanë ndëruar jetë.
- Në shumë raste, sidomos tek pagat minimale njëra nga pagat, vlera e pagës bruto (gross_salary) ose pagës kontributive (gross_salary_contib) vijnë me vlerën "0" (zero lekë).Në disa listëpagesa vlera e pagës bruto (gross_salary) ose pagës kontributive (gross_salary_contib) vijnë nën pagën minimale edhe pse numri i ditëve të punuara është 22 ose 26.
- - Evidentohen raste të vendosjes gabim të Numrit Personal NID.

Përdoruesit e sistemeve, të drejtat dhe gjurmët e veprimeve në sistem.

Nga auditimi i përdoruesve të sistemeve (PCAMS,CMIS,DMAIS) u konstatua se për përdoruesit me të drejta të plota: CMIS, ADMIN, DMAIS,DATALOD PCAMS në rolin e administratorit, nuk ka të dhëna të punonjësit që posedojnë ketë llogari..
-Fjalëkalimi në sistemet (PCAMS,CMIS,DMAIS) nuk është i parametrizuar për nga kompleksiteti dhe gjatësia e tij. Për kriteret e fjalëkalimit të përdoruesve fundor nuk janë hartuar apo implementuar standarde me qëllim forcimin e tij.
Menaxhimi i log-eve ndihmon institucionin publik pasi nëpërmjet kësaj gjurme sigurohet informacioni mbi sigurinë që të ruhet me detaje dhe për një kohë të mjaftueshme. Analizat e log-eve mundësojnë identifikimin e incidenteve, aktiviteteve mashtruese, thyerjen e politikave, problemet operacionale pak pasi ato ndodhin. Ato gjithashtu ndihmojnë në hetimin e ngjarjeve të ndryshme, auditimin dhe ndihmojnë institucionin në problemet e brendshme.
Tabelat kryesore të databazës kane tabelat përkatëse të historikut ku ruhet informacioni si ka qenë dhe si është ndryshuar.
Nga auditimi u konstatua se ISSH nuk dispononte një akt rregullator për menaxhimin e logeve digjitale.

Për sa është trajtuar në këtë pikë të Raportit Përfundimtar të Auditimit është mbajtur Aktkonstatimi nr.4, datë 15.03.2023, protokolluar në Institutin e Sigurimeve Shoqërore me nr. 2160 datë 15.03.2023, mbi të cilin nuk janë paraqitur observacioneme .

1. Titulli i Gjetjes: Mungesë e hapësirave në databazë
Situata 1: Nga auditimi u konstatua se në databazën e PCAMS në tablespace Audit_Aux nuk ka hapësira të nevojshme të alokuara në memorie (HDD); kjo mungesë e hapësirës (në tablespace) ka sjell ulje të performancës dhe gabime në databazë.

Situata 2: Nga auditimi i sistemit DMAIS në lidhje me performancën e veprimeve, duke u bazuar në treguesit si: Koha e përgjigjes, koha e përpunimit, përdorimi i burimeve të sistemit, u konstatua se DMAIS i përgjigjet me vonesë kërkesave të përdoruesve.
Kriteri Standardet ndërkombëtare dhe praktikat më të mira të fushës..
Ndikimi/Efekti: Degradim të performancës dhe gabime në databazë
Shkaku: Mosmarrja e masave paraprake për parandalimin e problematikave që lidhen me performancën e funksionimit të sistemit.
1. Rekomandim: Instituti i Sigurimeve Shoqërore të marrë masa që në vijim të kryejë sistemimet e nevoshme në databazën e sistemeve duke u bazuar në problematikat e shfaqura vazhdimisht nga njoftimet për gabime të ndodhura në sistem

2.Titulli Gjetjes : Mungesë e ambienteve test për sistemet
Situata: Nga auditimi u konstatua se për sistemet CMIS dhe DMAIS nuk ka një ambient test për menaxhimin e ndryshimeve që të siguroj që çdo ndryshim i bërë në sistemin të mos ndikojë negativisht në performancën e përgjithshme të sistemit. Mungesa e një ambient testi do të thotë që nuk ka mënyra për të verifikuar nëse ndryshimet e bëra në sistem funksionojnë.
Kriteri: Praktikat më të mira
Ndikimi/Efekti: Mungesa e një ambient test do të thotë që nuk ka mënyra për të verifikuar nëse ndryshimet e bëra në sistemin funksionojnë.
2.1.Rekomandim: Instituti i Sigurimeve Shoqërore të marrë masa për zhvillimin e një ambienti test në servera për aplikimin e ndryshimeve përpara se ato të kalojnë në live si dhe hartimin e një akti rregullator për përcaktimin e hapave konkret për menaxhimin e ndryshimeve në sisteme. (kush i inicion, kush i autorizon, kush i zbaton, etj)

3.Titulli Gjetjes: Sistemet dhe pajisjet kompjuterike janë pa asistencën e prodhuesit
Situata: Nga auditimi u konstatua se infrastruktura e përdorur për operimin e sistemeve (PCAMS, CMIS, DMAIS) si: (Red Hat Enterprise Linux (RHEL) 5, Windows server 8, Databaza në Oracle 11g, Cisco asa5520-bun), është në statusin end of life (ka arritur fundin e jetës), që do të thotë se prodhuesi i këtyrë pajisjeve dhe softeve nuk ofron më asistencë teknike, përditësime të sigurisë ose rregullim të gabimeve për këto versione, duke ndikuar në plotësimin e nevojave aktuale si dhe rritjen e kapaciteteve në të ardhmen.
Kriteri: Praktikat më të mira të fushës.
Ndikimi/Efekti: Mosgarantim i vazhdimësisë së punës, risk për thyerje të sigurisë. Risk në mbarëvajtjen dhe ndërprerjen e punës duke ndikuar në performancën e sistemeve.
3.1 Rekomandim: Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, të marrin masa për përditësimin dhe standardizimin e infrastrukturës IT, si dhe të monitorojnë sistemet që nuk përditësohen më për çdo tregues të mundshëm të shkeljeve të sigurisë ose dështimeve të sistemit.

4.Titulli i gjetjes : Mungesë e ndërveprimit ndërmjet sistemeve
Situata: Nga auditimi u konstatua se sistemet (CMIS, DMAIS, PCAMS) nuk ndërveprojnë me njëri-tjetrin. Mungesa e ndërveprimit ndërmjet sistemeve rezulton në çështje të shumta, duke përfshirë: Mospërputhje e të dhënave, procese që konsumojnë kohë, rreziqe të sigurisë. Çdo sistem menaxhohet veçmas, duke çuar në rreziqe të mundshme sigurie për shkak të kontrolleve të ndryshme të aksesit, mekanizmave të vërtetimit dhe dobësive në secilin sistem. Pamundësia për të ndarë të dhënat ndërmjet sistemeve nënkupton që subjekti humb mundësitë për të fituar njohuri mbi operacionet e tyre, për të optimizuar proceset dhe për të marrë vendime të bazuara në të dhëna.
Kriteri: Praktikat më të mira të fushës
Ndikimi/Efekti: Mungesa e integrimit midis sistemeve sjell risk në inputin e të dhënave.
4.1 Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa për të vendosur në funksionim të plotë ndërveprimin ndërmjet sistemeve që ISSH disponon me qëllim rritjen e

efikastitetit për mirë menaxhimin e skemës së pensioneve si dhe për të llogaritur përfitimet, menaxhuar kontributet, digjitalizuar dokumentet dhe çdo aspekt tjetër që lidhet me veprimtarinë e institucionit.

5. Titulli i gjetjes Problematika lidhur me të dhënat e importuara nga DPT në ISSH.
Situata: Gjatë auditimit të Sistemit elektronik për menaxhimin e kontributeve (CMIS), sistem i cili komunikon nëpërmjet webservice-ve me Sistemin e Tatimeve, u konstatuan problematika si:

- Raste të vendosjes gabim të Numrit Personal NID, të cilat kanë sjellë një problem në sistemin CMIS nuk shfaqen akoma listëpagesat e periudhave të personave gjyqfitues.
- Në sistemin CMIS nuk shfaqen muaj të veçantë, për subjekte të ndryshme dhe individë të ndryshëm, në vite të ndryshme, periudha të cilat ndërkohë shfaqen në sistemin tatimor.
- Në rastet kur subjektet kryejnë pagesa pjesore dhe për punëmarrës të vecantë, të dhënat e kontributeve të paguara nuk shfaqen në sistemin CMIS.
- Në rastet kur subjektet kryejnë korigjimin e deklaratës tatimore listëpagesat ESIG-25, krijon probleme të mundshme sidomos lidhur me kushtet e përfitimeve afatshkurtra, pasi subjektet "luajnë" me deklarimet e punonjësve. (psh një punonjës merr përfitimin nga ISSH më pas bëhet rivlerësim i listëpagesës duke ndryshuar pagën ose duke e hequr fare punonjësin nga listëpagesa).
- Janë evidentuar raste të sjelljes në listë-pagesa të personave që kanë ndëruar jetë.
- Në shumë raste, sidomos tek pagat minimale njëra nga pagat, vlera e pagës bruto (gross_salary) ose pagës kontributive (gross_salary_contib) vijnë me vlerën "0" (zero lekë).Në disa listëpagesa vlera e pagës bruto (gross_salary) ose pagës kontributive (gross_salary_contib) vijnë nën pagën minimale edhe pse numri i ditëve të punuara është 22 ose 26.
- Evidentohen raste të vendosjes gabim të Numrit Personal NID.

Kriteri: Praktikat më të mira të fushës
Ndikimi/Efekti: Risk i lartë për mos identifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit.
5.1 Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me Drejtorinë e Përgjithshme të Tatimeve, të marrin masa të nevojshme që të optimizojnë sistemet elektronike që shfrytëzohen nga të dyja palët, me qëllim shkëmbimin e saktë të të dhënave midis tyre.

6.Titulli i Gjetjes: Mangësi teknike dhe rregullative për menaxhimin e përdoruesve
Situata 1: Nga auditimi i përdoruesve të sistemeve PCAMS (Sistemi elektronik i kalkulimit dhe pagesës së përfitimeve), CMIS (Sistemi elektronik për menaxhimin e kontributeve) DMAIS(Sistemi elektronik për digjitalizimin e dokumenteve të Arkivit Qendror) u konstatua se për përdoruesit me të drejta të plota (CMIS, ADMIN, DMAIS,DATALOD PCAMS) në rolin e administratorit, nuk ka të dhëna të punonjësit që posedojnë këtë llogari.
Situata 2: Fjalëkalimi në sistemet (PCAMS, CMIS, DMAIS) nuk është i parametrizuar për nga kompleksiteti dhe gjatësia e tij. Për kriteret e fjalëkalimit të përdoruesve fundor nuk janë hartuar apo implementuar standarde me qëllim forcimin e tij.
Kriteri: Ligji 2/2017 "Për Sigurinë Kibernetike", Standardet ndërkombëtare të TI (ISO 27000 Sistemi i menaxhimit të sigurisë së informacionit) dhe praktikat më të mira.
Ndikimi/Efekti: Cenim i sigurisë mbi të dhënat / hyrje e paautorizuar në sistem.
Shkaku: Mungesa e akteve rregullativë dhe politikave mbi fjalëkalimin e përdoruesve.
Rëndësia: E lartë
6.1 Rekomandim: Instituti i Sigurimeve Shoqërore të marrë masa për hartimin dhe miratimin e rregullores për krijimin dhe administrimin e përdoruesve të brendshëm, ku të jenë pasqyruar saktë të drejtat dhe detyrimet për të gjithë përdoruesit.
Gjithashtu, ISSH të marrë masa për hartimin dhe miratimin e politikave mbi fjalëkalimin e përdoruesve në sistemet (PCAMS, CMIS, DMAIS) ku të përcaktohet kompleksiteti minimal në gjatësi, karaktere speciale apo numra si dhe periodiciteti për ndryshimin e tij.

7. Titulli i gjetjes: Mungesa e menaxhimit të logeve.
Situata: Nga auditimi u konstatua se ISSH nuk ka hartuar akte rregullatore për menaxhimin e log-eve digjitale ku specifikohen kërkesat për ruajtjen e log-eve përkatëse për çdo sistem/pajisje të institucionit, procedurat e administrimit dhe përgjegjësitë.
Kriteri: Urdhri nr. 109 datë 10.06.2016 i *Rregullores për menaxhimin e log-eve digjitale*, miratuar me të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT).
Ndikimi/Efekti: Mospërcaktimi i logeve të duhura për tu ruajtur dhe personat e duhur pwr ti identifikuar dhe analizuar.
Shkaku: Moszbatim i rregullores miratuar nga AKCESK.
Rëndësia: E Lartë.
7.1. Rekomandimi: Instituti i Sigrimeve Shoqërore, në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit, të marrin masa për rritjen e sigurisë dhe mbrojtjes së të dhënave duke hartuar 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 tjetër që i shërben sigurisë së të dhënave dhe parandalimit në tjetërsimin e tyre.

IV. GJETJET DHE REKOMANDIMET

A. MASA ORGANIZATIVE:

1. Gjetje nga auditimi: Nga auditimi u konstatua se:
ISSH nuk ka një strategji institucionale, përfshirë atë për Teknologjinë e Informacionit, duke mos pasqyruar qartë objektivat lidhur me infrastrukturën, burimet e nevojshme, si dhe instrumentat e nevojshme për matjen e objektivave. Mungesa e një plani strategjik mbart riskun e keqadresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së ISSH.
(Më hollësisht trajtuar në pikën 2.1 faqet 11-16 të Raportit Përfundimtar të Auditimit)
1.1 Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masat e nevojshme për hartimin dhe miratimin e Planit Strategjik Institucional, përfshirë planifikimin strategjik mbi teknologjinë e informacionit ku të adresohen qartë objektivat e institucionit duke reflektuar ndryshimet institucionale, strukturore dhe ndryshimet në teknologjinë e informacionit dhe komunikimit (TIK), të ndodhura ndër vite në ISSH.

Menjëherë dhe në vijimësi

2. Gjetje nga auditimi: Nga auditimi u konstatua se në strukturën e IT në Drejtorinë e Përgjithshme dhe Drejtoritë Rajonale të Sigurimeve Shoqërore (DRSSH) ka 60 vende pune, nga të cilat rezulton se ka 3 vende vakante të cilat nuk janë plotësuar ende. Këto vakanca kanë ardhur si pasojë e largimit të punonjësve IT.
(Më hollësisht trajtuar në pikën 2.1 faqet 11-16 të Raportit Përfundimtar të Auditimit)
2.1 Rekomandimi: Strukturat drejtuese në ISSH, në bashkëpunim me Drejtorinë e Burimeve Njerëzore, të marrin të gjitha masat e nevojshme për plotësimin e vendeve vakante sipas strukturës organike të tyre.

Menjëherë dhe në vijimësi

3. Gjetje nga auditimi: Nga auditimi u konstatua se ISSH nuk ka patur plan trajnimi vjetor për burimet njerëzore të Drejtorisë së Burimeve të Informacionit, në lidhje me Teknologjinë e Informacionit. Gjatë vitit 2022, janë zhvilluar 4 trajnime në lidhje me problematikat e dala gjatë funksionimit të aplikimeve online dhe të sistemeve PCAMS, DAMIS dhe CMIS, por nuk ka patur propozime nga niveli menaxherial i ISSH për zhvillimin e trajnimeve mbi sistemet, sigurinë dhe teknologjinë e informacionit. ISSH nuk ka zhvilluar trajnime të mjaftueshme për zhvillimin profesional të punonjësve.

(Më hollësisht trajtuar në pikën 2.1 faqet 11-16 të Raportit Përfundimtar të Auditimit)

3.1 Rekomandimi: Strukturat drejtuese në ISSH të marrin masa për identifikimin e nevojave për trajnimin e stafit IT dhe të çdo përdoruesi të sistemeve TIK në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit, si dhe të hartojnë e miratojnë plane vjetore trajnimi.

Menjëherë dhe në vijimësi

4. Gjetje nga auditimi Nga verifikimi i dhomës së serverëve në ISSH u konstatua se një Rack (raft me pajisje kompjuterike) nuk ishte pronë e ISSH, por e AKSHIT i cili ruhej në dhomën e serverëve të ISSH. Për këto pajisje nga ISSH nuk disponohej asnjë dokumentacion justifikues për transferimin si dhe qëllimin e vendosjes së tyre në ambientet e dhomës së serverëve të ISSH. Vendosja e këtyre e pajisjeve kompjuterike mund të sjelli kompromet imin e të dhënave duke qenë një institucion i rëndësisë së veçantë, ku në mjediset e tij mban sisteme dhe pajisje kompjuterike të cilat ruajnë dhe përpunojnë të dhëna sensitive.

(Më hollësisht trajtuar në pikën 2.2 faqet 16-22 të Raportit Përfundimtar të Auditimit)

4.1 Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa të menjëhershme për hartimin e dokumentacionit përkatës, ku të argumentohet arsyeja e vendosjes së pajisjeve kompjuterike (jo të institucionit) në dhomën e serverëve dhe personat e autorizuar që kanë akses në to.

Menjëherë

5. Gjetje nga auditimi: Nga verifikimi në terren në Drejtorinë rajonale të ISSH Vlorë, grupi i auditimit konstatoi se:

-infrastruktura network e pajisjeve ndihmëse që nevojiten për shërbimet e komunikimit dhe ruajtjes së të dhënave është në kushtet jo optimale, ku shërbimet e ngritura mbi këto rrjete nuk janë të sigurta dhe nuk mbështesin vazhdimësinë e punës.

-Nuk ka një linjë back up interneti në rast të shkëputjes së linjës, duke sjellë kështu mosfunksionim të sistemit dhe ndërprerje të ofrimit të shërbimeve.

-Kompjuterat nuk janë të pajisur me antivirus për mbrojtje ndaj sulmeve.

-Nuk ka një server qëndror të pajisur me Active Directory Domain Controller për menaxhimin e përdoruesve dhe vendosjen e politikave të sigurisë.

-Nuk kanë një pajisje firewall për mbrojtjen e rrjetit nga sulmet e jashtme.

(Më hollësisht trajtuar në pikën 2.2 faqet 16-22 të Raportit Përfundimtar të Auditimit)

5.1 Rekomandimi: ISSH të marrë masa për pajisjen dhe standardizimin e infrastrukturës IT në Drejtoritë Rajonale si dhe të marrë masa për hartimin dhe miratimin e një procedure standarde për komunikimin dhe zgjidhjen e problematikave që lindin me Drejtoritë Vendore në lidhje me sistemet IT, me qëllim sigurimin e kushteve optimale për ofrimin e shërbimit dhe mbarëvajtjen e punës pa ndërprerje.

Në vijimësi

6. Gjetje nga auditimi: Nga auditimi u konstatua se ISSH nuk disponon një infrastrukturë BCC (Business Continuity Center), si dhe nuk ka një plan mbi vazhdimësinë e punës dhe rimëkëmbjet nga katastrofat 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.

Backup-et e sistemeve PCAMS, CMIS dhe DMAIS janë të ruajtura në Tape library, të cilat pasi mbushen ruhen në të njëjtën godinë me sistemet PCAMS, CMIS dhe DMAIS.

-Kopjet (backup) e të dhënave nuk testohen rregullisht.

(Më hollësisht trajtuar në pikën 2.2 faqet 16-22 të Raportit Përfundimtar të Auditimit)

6.1 Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, bazuar në rëndësinë që ka ofrimi i shërbimit pas një fatkeqësie, të ndërmarrin hapat e nevojshëm për ndërtimin e një qendre *Business Continuity.*

6.2 Rekomandimi: Drejtoria e Burimeve të Informacionit të marrë masa për kryerjen dhe testimin periodik të backup-it të të dhënave të sistemeve duke e dokumentuar procesin.

Menjëherë dhe në vijimësi

7.Gjetje nga auditimi: Nga auditimi i faqes web konstatua se:
Tek menuja "Programi Transparencës":
Seksioni "Regjistri i Kërkesave dhe Përgjigjeve" nuk është publikuar viti 2022;
Seksioni "Sistemi i mbajtjes së dokumentacionit, llojet dhe format e dokumenteve" nuk përmban asnjë informacion;
Seksioni "Mekanizmat kontrollues dhe monitorues " nuk përmban asnjë informacion.
(Më hollësisht trajtuar në pikën 2.2 faqet 16-22 të Raportit Përfundimtar të Auditimit)
7.1.Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa për përditësimin dhe përmirësimin e faqes web (me informacione, rregullore, akte, etj.), si dhe reflektimin e mangësive të dala nga auditimi, me qëllim rritjen e transparencës dhe ndihmesën ndaj qytetarëve.

Menjëherë dhe në vijimësi

8. Gjetje nga auditimi: Nga auditimi i kontratës së zbatimit me objekt "Marrëveshje shërbimi për sistemet informatike të DMAIS për menaxhimin dhe arkivimin e dokumentave, PCAMS për llogaritjen dhe caktimin e pensioneve, FMS për menaxhimin financiar, CMIS për menaxhimin e deklarimit online të kontribuesve, rrjetit informatik dhe pajisje të caktuara të dhomës së serverave, pajisje IT për ISSH dhe komunikim ISSH-Arkiva (ISSH-Drejtori në varësi)" u konstatua se:
Sistemet që ka në përdorim ISSH (PCAMS, FMS, DMAIS, CMIS) janë të papërditësuara dhe nuk ka patur asnjë kërkesë nga ana e ISSH për përditësimin e tyre, mundësi kjo e parashikuar nga pika 10.5 e Kushteve të veçanta të kontratës midis AK dhe Kontraktuesit. Përditësimet e sistemeve kanë qenë të nevojshme për mirëfunksionimin e tyre dhe ISSH nuk i ka dërguar asnjë kërkesë Kontraktuesit bazuar në pikën e mësipërme të Kontratës.
(Më hollësisht trajtuar në pikën 2.3 faqet 22-24 të Raportit Përfundimtar të Auditimit)
8.1 Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, të marrin masa që në kontratat e mirëmbajtjes së sistemeve të ISSH që do të lidhen në vazhdimësi të sanksionohet që Kontraktuesi duhet të kryejë rregullisht përditësim të këtyre sistemeve.
8.2 Rekomandimi: Instituti i Sigurimeve Shoqërore të verifikojë rregullisht nëse sistemet PCAMS, DMAIS, FMS, CMIS kanë nevojë për përditësime, ndërhyrje apo korrigjime duke i bërë kërkesën përkatëse Kontraktuesit.

Në vijimësi

9. Gjetje nga auditimi: Nga auditimi u konstatua se në databazën e PCAMS në tablespace Audit_Aux nuk ka hapësira të nevojshme të alokuara në memorie (HDD); kjo mungesë e hapësirës (në tablespace) ka sjellë ulje të performancës dhe gabime në databazë.
-Nga auditimi i sistemit DMAIS në lidhje me performancën e veprimeve, duke u bazuar në treguesit si: Koha e përgjigjes, koha e përpunimit, përdorimi i burimeve të sistemit, u konstatua se DMAIS i përgjigjet me vonesë kërkesave të përdoruesve.
(Më hollësisht trajtuar në pikën 2.4 faqet 24-31 të Raportit Përfundimtar të Auditimit)
9.1 Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa që në vijim të kryejë sistemimet e nevoshme në databazën e sistemeve duke u bazuar në problematikat e shfaqura vazhdimisht nga njoftimet për gabime të ndodhura në sistem.

Menjëherë dhe në vijimësi

10. Gjetje nga auditimi: Nga auditimi u konstatua se për sistemet CMIS dhe DMAIS nuk ka një ambient test për menaxhimin e ndryshimeve që të sigurojë që çdo ndryshim i bërë në sistemin të mos ndikojë negativisht në performancën e përgjithshme të sistemit. Mungesa e një ambient testi do të thotë që nuk ka mënyra për të verifikuar nëse ndryshimet e bëra në sistem funksionojnë.
(Më hollësisht trajtuar në pikën 2.4 faqet 24-31 të Raportit Përfundimtar të Auditimit)

10.1.Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa për zhvillimin e një ambienti test në servera për aplikimin e ndryshimeve përpara se ato të kalojnë në live, si dhe hartimin e një akti rregullator për përcaktimin e hapave konkret për menaxhimin e ndryshimeve në sisteme (kush i inicion, autorizon, zbaton, etj.).

Në vijimësi

11. Gjetje nga auditimi: Nga auditimi u konstatua se infrastruktura e përdorur për operimin e sistemeve (PCAMS, CMIS, DMAIS) si: (Red Hat Enterprise Linux (RHEL) 5, Windows server 8, Databaza në Oracle 11g, Cisco asa5520-bun), është në statusin end of life (ka arritur fundin e jetës), që do të thotë se prodhuesi i këtyre pajisjeve dhe softeve nuk ofron më asistencë teknike, përditësime të sigurisë ose rregullim të gabimeve për këto versione, duke ndikuar në plotësimin e nevojave aktuale si dhe rritjen e kapaciteteve në të ardhmen.

(Më hollësisht trajtuar në pikën 2.4 faqet 24-31 të Raportit Përfundimtar të Auditimit)

11.1 Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me AKSHI-n, të marrin masa për përditësimin dhe standardizimin e infrastrukturës IT, si dhe të monitorojnë sistemet që nuk përditësohen më për çdo tregues të mundshëm të shkeljeve të sigurisë ose dështimeve të sistemit.

Menjëherë dhe në vijimësi

12.Gjetje nga auditimi: Nga auditimi u konstatua se sistemet (CMIS, DMAIS, PCAMS) nuk ndërveprojnë me njëri-tjetrin. Mungesa e ndërveprimit ndërmjet sistemeve rezulton në çështje të shumta, duke përfshirë: Mospërputhje e të dhënave, procese që konsumojnë kohë, rreziqe të sigurisë. Çdo sistem menaxhohet veçmas, duke çuar në rreziqe të mundshme sigurie për shkak të kontrolleve të ndryshme të aksesit, mekanizmave të vërtetimit dhe dobësive në secilin sistem. Pamundësia për të ndarë të dhënat ndërmjet sistemeve nënkupton që subjekti humb mundësitë për të fituar njohuri mbi operacionet e tyre, për të optimizuar proceset dhe për të marrë vendime të bazuara në të dhëna.

(Më hollësisht trajtuar në pikën 2.4 faqet 24-31 të Raportit Përfundimtar të Auditimit)

12.1 Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa për të vendosur në funksionim të plotë ndërveprimin ndërmjet sistemeve që ISSH disponon me qëllim rritjen e efikastitetit për mirëmenaxhimin e skemës së pensioneve, si dhe për të llogaritur përfitimet, menaxhuar kontributet, digjitalizuar dokumentet dhe çdo aspekt tjetër që lidhet me veprimtarinë e institucionit.

Menjëherë dhe në vijimësi

13.Gjetje nga auditimi: Nga auditimi i Sistemit elektronik për menaxhimin e kontributeve (CMIS), sistem i cili komunikon nëpërmjet webservice-ve me Sistemin e Tatimeve, u konstatuan problematika si:

- Raste të vendosjes gabim të Numrit Personal NID, të cilat kanë sjellë një problem në sistemin CMIS, si dhe nuk shfaqen akoma listëpagesat e periudhave të personave gjyqfitues.
- Në sistemin CMIS nuk shfaqen muaj të veçantë për subjekte të ndryshme dhe individë të ndryshëm, në vite të ndryshme, periudha të cilat ndërkohë shfaqen në sistemin tatimor.
- Në rastet kur subjektet kryejnë pagesa pjesore dhe për punëmarrës të veçantë, të dhënat e kontributeve të paguara nuk shfaqen në sistemin CMIS.
- Në rastet kur subjektet kryejnë korigjimin e deklaratës tatimore listëpagesat ESIG-25, krijon probleme të mundshme sidomos lidhur me kushtet e përfitimeve afatshkurtra, pasi subjektet "luajnë" me deklarimet e punonjësve (për shembull një punonjës merr përfitimin nga ISSH, më pas bëhet rivlerësim i listëpagesës duke ndryshuar pagën ose duke e hequr fare punonjësin nga listëpagesa).
- Janë evidentuar raste të sjelljes në listëpagesa të personave që kanë ndërruar jetë.
- Në shumë raste, sidomos tek pagat minimale njëra nga pagat, vlera e pagës bruto (gross_salary) ose pagës kontributive (gross_salary_contib) vjen me vlerën "0" (zero lekë). Në disa listëpagesa,

vlera e pagës bruto (gross_salary) ose pagës kontributive (gross_salary_contib) vjen nën pagën minimale edhe pse numri i ditëve të punuara është 22 ose 26.

- Evidentohen raste të vendosjes gabim të Numrit Personal NID.

(Më hollësisht trajtuar në pikën 2.4 faqet 24-31 të Raportit Përfundimtar të Auditimit)

13.1 Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me Drejtorinë e Përgjithshme të Tatimeve, të marrin masa të nevojshme që të optimizojnë sistemet elektronike që shfrytëzohen nga të dyja palët, me qëllim shkëmbimin e saktë të të dhënave midis tyre.

Menjëherë dhe në vijimësi

14.Gjetje nga auditimi Nga auditimi i përdoruesve të sistemeve PCAMS (Sistemi elektronik i kalkulimit dhe pagesës së përfitimeve), CMIS (Sistemi elektronik për menaxhimin e kontributeve) DMAIS (Sistemi elektronik për digjitalizimin e dokumenteve të Arkivit Qendror) u konstatua se nuk ka të dhëna se cilat janë personat e autorizuar që ushtrojnë rolin e adiministratorit të sistemeve (CMIS, ADMIN, DMAIS, DATALOD PCAMS).

Fjalëkalimi në sistemet (PCAMS, CMIS, DMAIS) nuk është i parametrizuar për nga kompleksiteti dhe gjatësia e tij. Për kriteret e fjalëkalimit të përdoruesve fundor nuk janë hartuar apo implementuar standarde me qëllim forcimin e tij.

(Më hollësisht trajtuar në pikën 2.4 faqet 24-31 të Raportit Përfundimtar të Auditimit)

14.1 Rekomandimi: Instituti i Sigurimeve Shoqërore të marrë masa për hartimin dhe miratimin e rregullores për krijimin dhe administrimin e përdoruesve të brendshëm, ku të jenë të pasqyruara saktë të drejtat dhe detyrimet për të gjithë përdoruesit.

Gjithashtu, ISSH të marrë masa për hartimin dhe miratimin e politikave mbi fjalëkalimin e përdoruesve në sistemet (PCAMS, CMIS, DMAIS) ku të përcaktohet kompleksiteti minimal në gjatësi, karaktere speciale apo numra si dhe periodiciteti për ndryshimin e tij.

Menjëherë

15.Gjetje nga auditimi Nga auditimi u konstatua se ISSH nuk ka hartuar akte rregullatore për menaxhimin e log-eve digjitale ku specifikohen kërkesat për ruajtjen e log-eve përkatëse për çdo sistem/pajisje të institucionit, procedurat e administrimit dhe përgjegjësitë, 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).

(Më hollësisht trajtuar në pikën 2.4 faqet 24-31 të Raportit Përfundimtar të Auditimit)

15.1.Rekomandimi: Instituti i Sigurimeve Shoqërore, në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit, të marrin masa për rritjen e sigurisë dhe mbrojtjes së të dhënave duke hartuar 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 tjetër që i shërben sigurisë së të dhënave dhe parandalimit në tjetërsimin e tyre.

Menjëherë dhe në vijimësi

Për sa më sipër paraqitet ky Raport Përfundimtar Auditimi

KONTROLLI I LARTË I SHTETIT