Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

KONTROLLI I LARTË
I SHTETIT

Raporti i përbashkët
në Auditimin Paralel

SISTEMET E INFORMACIONIT NË UJËSJELLËSIT E TIRANËS DHE PRISHTINËS

Prishtinë, Dhjetor 2023

Ky publikim është i:
Zyrës Kombërare të Auitimit – Departamenti për Auditim të Teknologjisë së Informacionit; dhe
Kontrollit të Lartë të Shtetit – Departamenti i Auditimit të Teknologjisë së Informacionit.

RAPORTI I PËRBASHKËT NË AUDITIMIN PARALEL

Sistemet e Informacionit në Ujësjellësit e Tiranës dhe Prishtinës

Prishtinë, dhjetor 2023

Ky raport i përbashkët paraqet rezultatet e dy raporteve nga auditimi paralel dhe vlerësimet e përgjithshme.

Zyra Kombëtare e Auditimit e Republikës së Kosovës dhe Kontrolli i Lartë i Shtetit të Shqipërisë kanë zhvilluar auditim paralel në Ujësjellësin e Tiranës dhe Prishtinës me fokus në sistemet e informacionit.

Auditimi është organizuar dhe zhvilluar në pajtim me kërkesat për auditimet e përbashkëta ndërmjet ISA-ve. Si dhe proceset audituese janë zhvilluar sipas SNISA 3000, GUID 5100 dhe manualet dhe metodologjitë përkatëse të dyja institucioneve. Procesi auditues është zhvilluar gjatë vitit 2022 duke përfunduar në pjesën e parë të vitit 2023. Gjatë këtij procesi janë shkëmbyer përvoja dhe janë zhvilluar takime të përbashkëta të ekipeve audituese përfshirë palët relevante në auditim.

Auditimi është fokusuar në kompanitë për furnizim me ujë të pijshëm përkatësisht sistemet e tyre të informacionit. Në ujësjellësin e Tiranës fokusi ishte shtrirë edhe në kontratat dhe pajtueshmërinë e tyre.

Kosova: Furnizimi me ujë të pijshëm është esenciale për mirëqenien, zhvillimin social dhe ekonomik të popullsisë. Në Kosovë, furnizimi me ujë të pijshëm bëhet përmes shtatë Kompanive Rajonale të Ujit të cilat sigurojnë shërbime të ujësjellësit për rreth 79% të popullatës në Kosovë. KRU Prishtina ofron shërbimet e ujit dhe kanalizimit për komunën e Prishtinës, Fushë Kosovës, Obiliqit, Shtimes, Lipjanit, Podujevës, Drenasit dhe Graqanicës. Kjo kompani është ofruesi më i madh i shërbimit të ujit në Kosovë dhe ka të regjistruar 153,509 konsumatorë apo 37% nga totali i konsumatorëve në të gjithë Kosovën. Krahas kësaj, KRU Prishtina ka numrin më të madh të ankesave komerciale/ financiare nga ana e qytetarëve.

Shqipëria: Ujësjellës Kanalizime Tiranë Sh.A është institucioni përgjegjës për shërbimin e furnizimit me ujë të pijshëm, grumbullimit, largimit dhe trajtimit të ujërave të ndotura në Bashkinë e Tiranës. Objekti i veprimtarisë së shoqërisë në zonën e shërbimit, për të cilin është licencuar nga Enti Rregullator i Ujit është:

- Shërbimi i furnizimit me ujë të pijshëm i konsumatorëve dhe shitja e tij;
- Mirëmbajtja e sistemit/sistemeve të furnizimit me ujë të pijshëm;
- Prodhimi dhe/ose blerja e ujit për plotësimin e kërkesës së konsumatorëve;
- Shërbimi i grumbullimit, largimit dhe trajtimit të ujërave të ndotura;
- Mirëmbajtja e sistemeve të ujërave të ndotura si dhe të impianteve të pastrimit të tyre;
- Kryerja e aktiviteteve laboratorike.

Tabela e përmbajtjes

Lista e shkurtesave

ARRU	Autoriteti Rregullator i Shërbimeve të Ujit
BD	Bordi i Drejtorëve
ERP	Aplikacioni për burime të ndërmarrjes
KE	Kryeshefi Ekzekutiv
KRU	Kompania Rajonale e Ujësjellësit
ME	Ministria e Ekonomisë
NP	Ndërmarrje Publike
PB	Plani i biznesit
PVB	Plani i vazhdimësisë së Biznesit
SIG	Sistemi Informativ Gjeografik
SHA	Shoqëri Aksionare
TI	Teknologjia e Informacionit
ZKA	Zyra Kombëtare e Auditimit
KLSH	Kontrolli i Lartë i Shtetit
VKM	Vendim i Këshillit të Ministrave
VPN	Virtual Private Network - Rrjet Privat Virtual
UKT	Ujësjellës Kanalizime Tiranë
MNSH	Marrëveshje në Nivel Bashkëpunimi
ERU	Enti Rregullator i Ujit

PËRMBLEDHJE E PËRGJITHSHME

Përmbledhje e përgjithshme

Kosova-Zyra Kombëtare e Auditimit (ZKA): KRU Prishtina nuk ka siguruar një mjedis efektiv të kontrollit për të ruajtur integritetin dhe vazhdimësinë e sistemeve të TI-së, duke ndikuar negativisht në arritjen e plotë të qëllimeve të ndërmarrjes dhe duke zbehur besueshmërinë e sistemeve te ndërmarrjes.

Qeverisja e teknologjisë së informacionit në Kompaninë Rajonale të Ujësjellësit Prishtina nuk ka rezultuar të jetë efektive. Mungon planifikimi strategjik i TI-së, politikave dhe procedurave si dhe nuk ka vendosur strukturë organizative të TI-së adekuate.

Lidhur me sigurinë e informacionit, Ndërmarrja nuk ka ndërmarrë masat dhe nuk ka zhvilluar mekanizmat e duhur në mënyrë që të siguroj se informacioni të mos ekspozohet ndaj kompromet imit dhe zbulimeve të paautorizuara. Mangësitë në këtë fushë pamundësojnë të identifikohet mënyra se si siguria përcaktohet, konfigurohet dhe zbatohet në sistemet e ndërmarrjes.

Poashtu, ndërmarrja nuk ka siguri të mjaftueshme se mund të vazhdojë operimin e saj duke përdorur teknologjinë e informacionit dhe asetet e saj në rast të ndonjë fatkeqësie natyrore apo të ngjashme. Mungesa e masave parandaluese si dhe kontrolleve në ambientin ku ruhen të dhënat, rrit rrezikun e qasjeve të paautorizuara, humbjen, dëmtimin apo kërcënimet tjera.

Kontrollet hyrëse të aplikacionit nuk janë të vendosura krahas rregullave të Autoritetit Rregullator për Shërbimet e Ujit (ARRU) duke lejuar të futen të dhëna jo të sakta dhe të plota si dhe mungon ndërlidhje mes sistemeve. Si rezultat përveç që ka shkaktuar punë shtesë për përdoruesit duke ulur efikasitetin e tyre, ndërmarrja nuk është në gjendje të identifikoj keqpërdoruesit e ujit dhe t'i ndjekë ata sipas ligjeve në fuqi. Kjo ndikon direkt në mos arkëtimin e të hyrave, rritjen e borxheve si dhe në humbje financiare.

Aktivitetet e përdoruesve (gjurmët audituese) nuk ishin të plota nëpër sisteme si dhe nuk kishte monitorim të vazhdueshëm të këtyre aktiviteteve. Kjo pamundëson identifikimin me kohë të aktiviteteve jonormale, gabimeve, keqpërdorimeve të mundshme apo mos identifikimin fare të tyre, të cilat mund të kenë ndikim financiar e gjithashtu ekspozim të informacionit të paautorizuar.

Me qëllim të adresimit të çështjeve të identifikuara rreth qeverisjes së TI-së, sigurisë së informacionit, vazhdimësisë së biznesit dhe kontrolleve të aplikacionit ne kemi dhënë 18 rekomandime për Kompaninë Rajonale të Ujësjellësit Prishtina.

Shqipëria-Kontrolli i Lartë I Shtetit (KLSH): Ujësjellës Kanalizime Tiranë Sh.A nuk disponon strategji institucionale si dhe një strategji mbi teknologjinë e informacionit, mungesa e të cilave sjell mangësi në vendosjen e prioriteteve të institucionit, politikave të sigurisë si dhe përmirësimin e infrastrukturës të TI të cilat do duhet të jenë në mbështetje të objektivave institucionale.

Gjurma elektronike e auditimit nuk është e plotë për përdoruesit punonjës të institucionit që e aksesojnë sistemin nga ndërfaqja si dhe nuk ruhet asnjë gjurmë veprimesh për përdoruesit e krijuar në bazën e të dhënave.

Puna në sistemin informatik zhvillohet në mungesë të rregulloreve mbi përdorimin e sistemit, sistemit të veprimeve, diagrameve të qarkullimit të informacionit, kodit në burim si dhe dokumentacionit udhëzues mbi ndërtimin e sistemit.

Nuk është kryer një monitorim efektiv i zbatimit të kontratave të aksesimit të informacionit nga palët e treta nëpërmjet lidhjeve VPN.

Me qëllim adresimin e çështjeve të identifikuara rreth qeverisjes së TI-së, sigurisë së informacionit dhe kontrolleve të aplikacionit ne kemi dhënë 15 rekomandime për shoqërinë e Ujësjellës Kanalizime Tiranë Sh.A.

OBJEKTIVA DHE FUSHËVEPRIMI

01

1. Objektiva dhe fushëveprimi

Auditimet janë fokusuar në kompanitë për furnizim me ujë të pijshëm përkatësisht sistemet e tyre të informacionit. Në ujësjellësin e Tiranës fokusi ishte shtrirë edhe në kontratat dhe pajtueshmërinë e tyre.

Fushat e mbuluara të auditimit janë prezantuar si në vijim:

Fushat e auditimit	Çështjet e auditmit të përfshira nga ISA i Kosovës	Çështjet e auditimit të përfshira nga ISA i Shqipërisë
Qeverisja e TI-së :	Identifikimi, drejtimi dhe monitorimi i nevojave të ndërmarrjes;	
	Planifikimi dhe strategjia e Teknologjisë Informative;	
	Struktura organizative, Standardet, politikat dhe procedurat e TI-së;	Struktura organizative Standarde, politikat dhe procedurat e TI-së dhe vazhdimësia e ofrimit të shërbimit
Siguria e Informacionit:	Vlerësimi i rrezikut;	
	Politikat e sigurisë së informacionit;	
	Menaxhimi i aseteve;	
	Burimet njerëzore dhe siguria e TI-së;	Përdoruesit e sistemeve dhe të drejtat
	Kontrollet e qasjeve;	
Plani për vazhdimësi së proceseve të TI-së:	Kontrolli i mjedisit;	
	Plani i rimëkëmbjes nga fatkeqësitë;	
Kontrollet e aplikacioneve:	Kontrollet e të dhënave hyrëse;	Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Outpu
	Kontrollet për siguri të aplikacioneve.	Gjurmët e veprimeve në sistem

Zyra Kombëtare e Auditimit: Auditimi i kryer nga ZKA-ja kishte objektivë të vlerësohet nëse strukturat udhëheqëse të ndërmarrjes sigurohen se burimet e TI-së mbështesin qëllimet dhe strategjinë e ndërmarrjes duke ofruar një mjedis efektiv për të ruajtur integritetin e të dhënave dhe vazhdimësinë e sistemeve të TI-së.

Kontrolli i Lartë i Shtetit: Auditimi i kryer nga KLSH synon të vlerësojë nëse objektivat e subjektit arrihen në mënyrën e duhur duke përdorur burimet TI, duke përfshirë pajtueshmërinë me kërkesat ligjore dhe rregullatorë, konfidencialitetin, integritetin si dhe disponueshmërinë e sistemeve të informacionit dhe të dhënave që gjenden në të.

GJETJET E AUDITIMIT

02

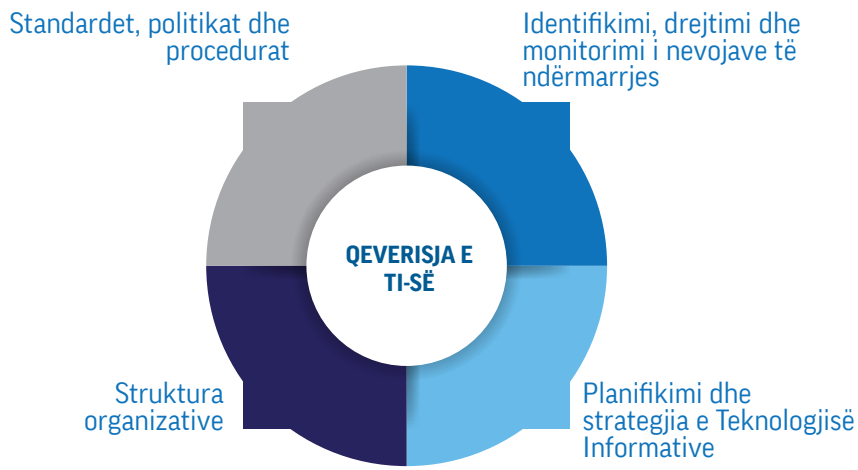
2. Gjetjet e auditimit

Në këtë kapitull janë paraqitur gjetjet e auditimit për KRU Prishtina dhe Ujësjellësin e Tiranës, që ndërlidhen me qeverisjen, sigurinë e informacionit, vazhdimësinë e proceseve/sistemeve të TI-së si dhe çështjet që ndërlidhen me kontrollet e aplikacionit.

2.1. Qeverisja e teknologjisë së informacionit

Qeverisja e TI-së përkufizohet si strukturë e përgjithshme që udhëheq operacionet e TI-së të një institucioni dhe siguron që sistemet e TI-së mbështesin dhe mundësojnë arritjen e objektivave të institucionit, si dhe luan një rol kyç në përcaktimin e një mjedisi kontrollues dhe raportues. Elementet kyçe të qeverisjes së TI-së janë: strategjia dhe planifikimi i TI-së; strukturat, standardet, politikat dhe procedurat, zhvillimi dhe blerja, burimet njerëzore[1].

Figura 1: Qeverisjes së TI-së, çështjet e trajtuara në auditim



1 Manuali i auditimit të teknologjisë së informacionit, kapitulli 2, Qeverisja e TI-së, Identifikimi, Drejtimi dhe Monitorimi i nevojave

Më poshtë kemi paraqitur gjetjet lidhur me qeverisjen e teknologjisë së informacionit.

Zyra Kombëtare e Auditimit:

KRU Prishtina nuk ka plan strategjik të TI-së si dhe nuk ka të vendosur struktura adekuate, plane dhe procedura të qarta për identifikimin e kërkesave të saj në fushën e TI-së

Ndërmarrja nuk ka planifikim në nivel strategjik të TI-së (ose ekuivalent), i cili përkthen objektivat e biznesit në qëllime dhe kërkesa të TI-së dhe adreson burimet e nevojshme për të mbështetur ndërmarrjen. Në nivel të përgjithshëm të ndërmarrjes, KRU Prishtina në baza vjetore përgatit planin e biznesit, përmes të cilit përcaktohen objektivat strategjike dhe caqet e ndërmarrjës si dhe janë paraparë investimet në fushën e TI-së, megjithatë, nuk ka ndërlidhje të investimeve në fushën e TI-së më arritjen e caqeve të ndërmarrjes.

Plani i biznesit përmban rreziqet dhe treguesit e performancës në terme të përgjithshme, mirëpo nuk kemi vërejtur vlerësim të rreziqeve në fushën e TI-së. Poashtu, sa i përket monitorimit për ecurinë e planit të biznesit, nuk ka informata lidhur me ecurinë e projekteve të TI-së.

Gjithashtu, KRU Prishtina nuk ka procedurë për identifikimin dhe specifikimin e kërkesave apo nevojave të TI-së si dhe nuk ka plan të detajuar me të gjitha kërkesat apo nevojat e TI-së. Përmes këtyre dokumenteve do të lehtësohej vendimmarrja e menxhmentit për investimet e TI-së.

KRU Prishtina nuk ka strukturë të plotë organizative dhe ndarje të qartë të detyrave dhe përgjegjësive si dhe mungojnë politikat dhe procedura e TI-së

Aktualisht, departamenti i TI-së në ndërmmarrje është i pozicionuar si divizion, menaxhohet nga udhëheqësi i divizionit si dhe raporton drejtpërdrejt te Kryeshefi Ekzekutiv (tutje KE). Mirëpo, sipas përshkrimit të detyrave në rregulloren për sistematizim dhe në kontratë, udhëheqësi i divizionit të TI-së raporton te KE-ja dhe Zyrtari Kryesor Financiar (tutje ZKF) duke krijuar kështu paqartësi për formën dhe mënyrën e raportimit. Është vërejtur se ndër vite ka pasur ndryshime të vazhdueshme në departament të TI-së sa i përket pozicionimit dhe raportimit, duke qenë disa vite

si shërbim, divizion, departament, rrjedhimisht ka pasur ndryshime edhe në raportim. Kjo si pasojë e ndryshimeve të vazhdueshme edhe të BD-ve dhe prioriteteve.

Po ashtu, kemi vërejtur se divizioni i TI-së nuk i ka të plotësuara të gjitha pozitat e parapara me rregulloren për organizimin e brendshëm dhe sistematizimin e vendit të punës.

Për më tepër, gjatë viteve 2021 dhe 2022 pozitat e udhëheqësit të divizionit dhe shefit shërbimit të TI-së ishin me ushtrues detyre. Gjithashtu, edhe përshkrimi i detyrave të punës në mes të punësuarve në divizionin e TI-së nuk përcakton qartë ndarjen e detyrave të punës.

Kjo krijon konflikt të pozitave siç ishte rasti kur zyrtari për administrim të rrjetit kishte qasje të plota në bazat e të dhënave ashtu edhe në aplikacion. Po ashtu, mungon zyrtari për siguri të informacionit, i cili do të ishte përgjegjës për identifikim e kërcënimeve, vlerësimin e cenueshmërisë, përcaktimin e rrezikut, zbatimin e strategjive të kontrollit etj.

KRU nuk ka hartuar politika dhe procedura të brendshme që rregullojnë çështjen e TI-së në rastet e fillimit dhe/apo ndërprerjes së punës, trajnimeve, ruajtjes së dokumenteve, identifikimin e nevojave/kërkesave, sigurisë së informacionit, menaxhimin e rrezikut, testimin e kopjeve rezervë, menaxhimin e fjalëkalimeve, qasjeve logjike dhe fizike etj. Janë identifikuar raste kur edhe pas ndërprerjes së punës nuk janë ndaluar qasjet e përdoruesve.

Kontrolli i Lartë i Shtetit:

Struktura organizative

Shoqëria UKT Sh.A nuk ka një plan mbi trajnimin e stafit të TI në fusha specifike të cilat do të ndihmonin në rritjen profesionale dhe kualifikimin e mëtejshëm të tyre me qëllim përmbushjen e detyrave në nivel të lartë profesional.

Po ashtu, specialistët e TI nuk kanë zhvilluar trajnime, kualifikime profesionale brenda apo jashtë vendit, gjatë periudhës objekt auditimi.

Standarde, politikat dhe procedurat e TI-së

Shoqëria Ujësjellës Kanalizime Tiranë Sh.A nuk disponon një strategji institucionale si dhe një strategji mbi teknologjinë e informacionit, mungesa e të cilave sjell mangësi në vendosjen e prioriteteve të institucionit, politikave të sigurisë si dhe përmirësimin e infrastrukturës të TI të cilat do duhet të ishin në mbështetje të objektivave institucionale.

Gjithashtu, Ujësjellës Kanalizime Tiranë Sh.A nuk ka identifikuar dhe nuk ka dokumentuar rreziqet lidhur me teknologjinë e informacionit.

2.2. Siguria e Informacionit

Siguria e informacionit është një nga aspektet themelore të qeverisjes së TI-së për të siguruar disponueshmërinë, konfidencialitetin dhe integritetin e të dhënave. Për menaxhim më të mirë të sigurisë së informacionit, institucioni, duhet të krijojë mekanizma që të mundësojë menaxhimin e rreziqeve të lidhura me sigurinë, marrjen e masave të duhura dhe garancinë se informacioni është i disponueshëm, i përdorshëm, i plotë dhe i pa kompromentuar.

Figura 2: Siguria e informacionit- elementet e sigurisë së informacionit të mbuluara nga auditimi

Çështjet e ndërlidhura me sigurinë e informacionit janë shpalosur në vijim.

Zyra Kombëtare e Auditimit:

KRU Prishtina nuk ka vendosur mekanizma efektiv për të vlerësuar rrezikun e sigurisë së informacionit si dhe mungon regjistri i pasurive të TI-së

Ndërmarrja nuk ka bërë identifikimin, analizimin dhe vlerësimin e rreziqeve që ndërlidhen me sigurinë e informacionit. Rrjedhimisht nuk ka hartuar ndonjë strategji të përshtatshme apo procedura për reduktimin e rrezikut apo menaxhimin e rreziqeve kritike.

Si rrjedhojë, ndërmarrja nuk ka përcaktuar forma të kontrollit të domosdoshëm. Mungon dokumentacioni që përmban përshkrime të rreziqeve kryesore dhe identifikimin e pikave kyçe për sistemet e ndërmarrjes dhe për infrastrukturën e saj.

Nuk dihen masat që duhet të ndërmerren për ulje të rrezikut, rolet dhe përgjegjësitë e personave që duhet të përfshihen në rast të shfaqjes së ndonjë rreziku të mundshëm.

Divizioni i TI-së në ndërmarrje nuk ka regjistër të saktë për të gjitha pasuritë e TI-së, regjistër i cili përfshinë bazat e të dhënave, kontratat dhe marrëveshjet, dokumentacionin e sistemit, manualet e përdoruesit, materialet e trajnimit, procedurat operacionale ose mbështetëse, planet e vazhdimësisë së biznesit, gjurmët e auditimit, softuerët, pajisjet fizike, shërbimet etj.

Ndërmarrja nuk ka hartuar rregulla/procedura të veçanta apo nuk janë përfshirë në rregulloren e ndërmarrjes për pasuri, lidhur me përdorimin e pasurive të TI-së të cilat duhet të përmbajnë dhe klasifikojnë asetet/pasuritë e TI-së bazuar në rëndësinë e pasurisë dhe klasifikimin e sigurisë, duke identifikuar edhe nivelin e mbrojtjes në përputhje me rëndësinë e pasurisë.

Përdoruesit e sistemeve të informacionit të KRU Prishtinës nuk janë të ndërgjegjësuar mjaftueshëm lidhur me sigurinë e informacionit

Përveç zyrtarëve të TI-së, personeli tjetër i ndërmarrjes nuk kanë informacionet e nevojshme se si duhet të mbrohen nga sulmet e mundshme kibernetike si nga brenda apo nga jashtë ndërmarrjes dhe nuk ka një proces të shkruar për personelin lidhur me sigurinë e informacionit.

Zyrtarët e TI-së kishin instaluar softuer për parandalimin e sulmeve të mundshme kibernetike, si dhe në vazhdimësi kanë përdorur mekanizma të ndryshme parandalues për të pamundësuar tentimet e qasjeve nga jashtë, si dhe bëhej monitorimi i tyre, megjithatë këto përpjeke nuk ishin të mjaftueshme. Poashtu, ndërmarrja deri më tani nuk kishte organizuar trajnime apo fushata që të ndërgjegjësoj personelin rreth rëndësisë së sigurisë së informacionit për të krijuar një kulturë pozitive të sigurisë. Disa nga mangësitë e identifikuara:

- mundësia e lejimit të fjalëkalimit me vetëm një karakter;
- mos aplikimi i ndryshimit të fjalëkalimit në baza të rregullta kohore;
- përdorimin e kredencialeve gjeneralë apo të pa personalizuar;
- mungesë e administrimit të llogarive të përdoruesve e në veçanti mungesa e mbylljes së llogarive të zyrtarëve që nuk ishin më pjesë e ndërmarrjes;

- lejimin e qasjeve të plota në aplikacione për zyrtar, detyrat dhe përgjegjësit e të cilëve nuk korrespondojnë me rolet e dhëna në këto sisteme/baza të shënimeve.

Kompleksiteti i fjalëkalimit nuk është vendosur në të gjitha Sistemet e informacionit të KRU–Prishtinës si dhe janë identifikuar mangësi në menaxhimin e llogarive

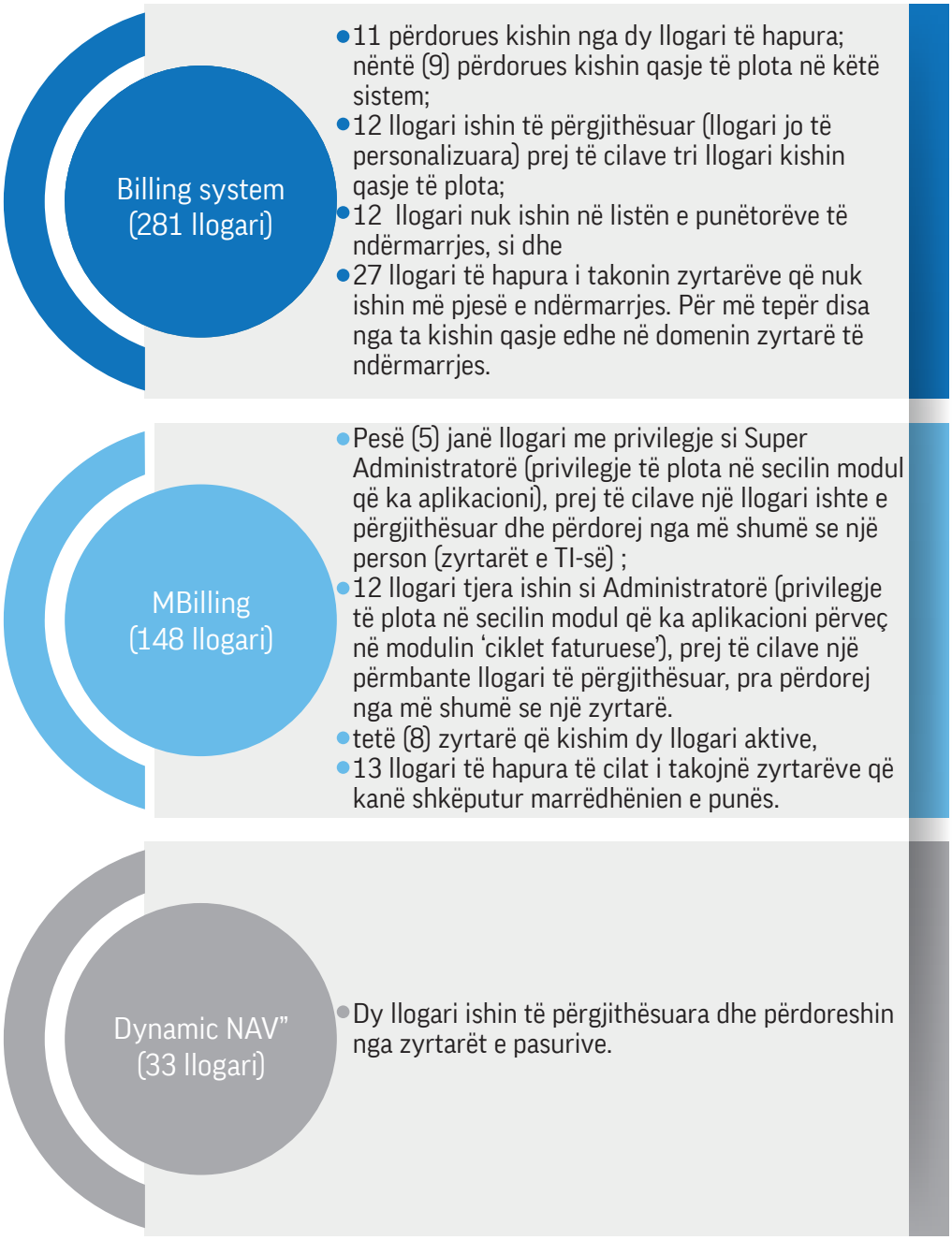
Gjatë auditimit, kemi vërejtur që aplikacioni i faturimit "Billing system" nuk ofron siguri në autentifikimin e llogarive. Ky aplikacion lejon që përdoruesit për llogaritë/ID e tyre të përdorin fjalëkalim me gjatësi vetëm një karakter. Gjithashtu, në aplikacionet e ndërmarrjës nuk ka funksion që detyron që shfrytëzuesit të ndërrojnë fjalëkalimet në periudha të rregullta.

Për qasje në bazën e të dhënave përdoren llogarit me qasje të plota të administratorit, të cilat nuk janë të personalizuara. Poashtu, zyrtarët që kanë qasje të plota në bazat e të dhënave kanë qasje të plota edhe në aplikacione.

Kredencialet e llogarive të administratorëve për sisteme të teknologjisë së informacionit nuk janë të ruajtura në ambiente të sigurta që të shfrytëzohen vetëm atëherë kur zyrtari përgjegjës i sistemit të mungojë, pra këto llogari shfrytëzohen në vazhdimësi dhe jo vetëm nga një zyrtar, ndërsa aktivitetet e tyre nuk monitorohen.

KRU-ja nuk ka një metodologji/matricë të dhënies së qasjeve në resurset e ndryshme të teknologjisë së informacionit bazuar në rolin dhe përgjegjësinë e personelit si dhe mungon një proces i definuar lidhur me aprovimin e qasjeve në sisteme, të dhëna/informacione, pajisje etj. Mangësitë e identifikuar janë si në vijim:

Figura 3: çështjet e dala nga testimi i qasjeve të zyrtarëve në tri aplikacionet e KRU-Prishtinës



Poashtu, në këto tri aplikacione nuk kishte standardizim të kredencialeve të përdoruesve. Të dhënat e regjistruara për përdorues nuk ishin në harmoni me të

dhënat nga lista zyrtare e punëtorëve, përfshirë emrin, mbiemrin dhe pozitën e punës si të dhëna kyçe për identifikimin nëse rolet në aplikacione janë në harmoni me pozitat që ata mbajnë.

Kontrolli i Lartë i Shtetit:

Përdoruesit e sistemeve dhe të drejtat

Nga auditimi u konstatua se UKT Sh.A nuk disponon një rregullore të miratuar për procesin e menaxhimit të përdoruesve në sistemet që disponon me qëllim përcaktimin e atributeve si krijimi, fshirja, ndryshimi i roleve, të drejtave, ndryshimi i fjalëkalimeve.

Çështjet e dala nga testimi i qasjeve të zyrtarëve në aplikacionin kryesor tw UKT Sh.A Billing me 327 llogari aktive:

- Për përdoruesin me të drejta të plota, në rolin e administratorit, nuk ka të dhëna të punonjësit që posedon ketë llogari;
- Janë aktiv katër përdorues me kredenciale të pa identifikuara me të dhëna mbi emrin dhe mbiemrin;
- Në shumë raste të krijimit të përdoruesve, nuk janë ruajtur gjurmët se kush nga përdoruesit ka vepruar;
- Në disa raste një punonjës ka më shumë se një llogari aktive në sistem;
- Funksionalitetet e përdoruesve në sistem nuk janë të paracaktuara me rolin që i caktohet, ato përzgjidhen manualisht.

Nga auditimi mbi përdoruesit në bazën e të dhënave u konstatua se për drejtorin e IT-s janë aktivë dy përdorues të krijuar në bazën e të dhënave, si dhe rezultuan aktivë përdoruesit e operatorit që ka ofruar shërbim të mirëmbajtjes së sistemit të faturim-arkëtimit, megjithëse kontrata për këtë shërbim ka përfunduar.

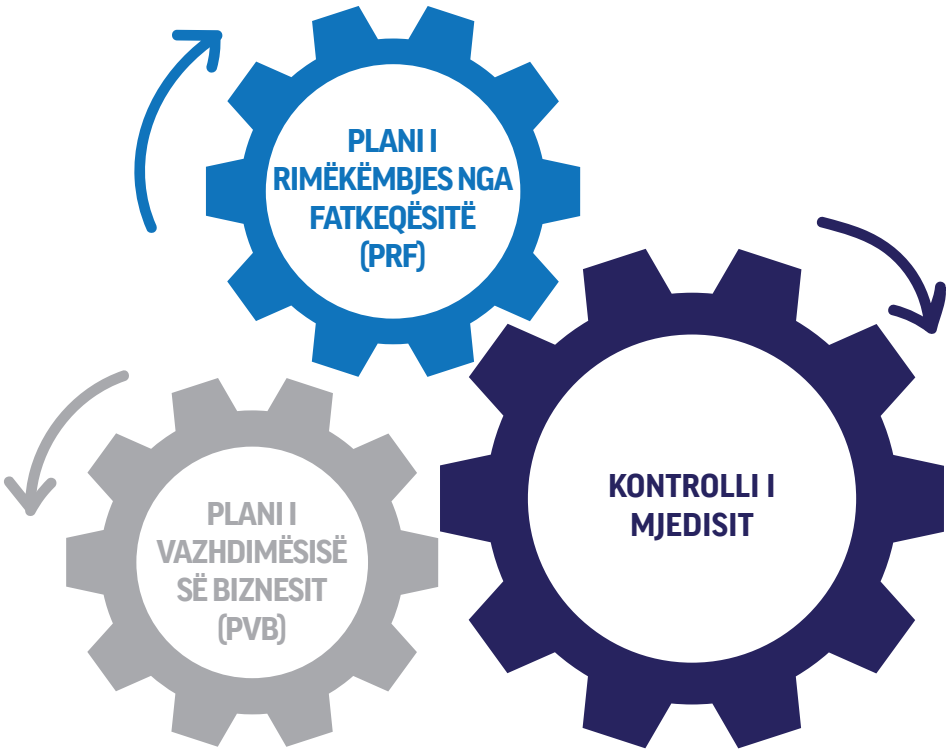
Fjalëkalimi i secilit përdorues të sapo krijuar në sistemin Billing formohet manualisht sipas një modeli standard, por kur përdoruesi logohet për herë të parë (first log-in) ndryshimi i fjalëkalimit fillestar nuk kërkohet në mënyrë të detyrueshme të ndryshohet. Ky ndryshim mbetet në dëshirën apo njohuritë e punonjësit. Ky fjalëkalim 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.

2.3. Plani i vazhdimësisë së biznesit dhe plani i rimëkëmbjes nga fatkeqësia

Organizatat qeveritare gjithnjë e më shumë mbështeten në disponueshmërinë dhe funksionimin korrekt të sistemeve të tyre kompjuterike për të përmbushur detyrimet e tyre ligjore.

Planifikimi i vazhdimësisë së biznesit (PVB) është proces gjatë së cilës një organizatë planifikon dhe teston rimëkëmbjen e proceseve të biznesit (veprimtarisë) pas një ndërprerjeje. Ky proces përshkruan se si një organizatë do të vazhdojë të funksionojë në kushte të pafavorshme që mund të shfaqen (për shembull, fatkeqësi natyrore ose fatkeqësi të tjera). **Planifikimi i rimëkëmbjes nga fatkeqësitë (PRF)** është proces i planifikimit dhe testimit të rimëkëmbjes së infrastrukturës së teknologjisë informative pas një fatkeqësie natyrore ose ngjashëm. Është nën-grup i planifikimit të vazhdimësisë së biznesit. PVB vlen për funksionet e biznesit organizativ ndërsa PRF për burimet e TI-së që mbështesin funksionet e biznesit.

Figura 4: elementet e mbuluara nga auditimit



Më poshtë kemi paraqitur gjetjet lidhur me kontrollet mjedisore, planifikimi i vazhdimësisë së biznesit dhe planifikimi i rimëkëmbjes nga fatkeqësitë (PRF).

Zyra Kombëtare e Auditimit:

KRU – Prishtina nuk ka krijuar mekanizmat parandaluese kundrejt rreziqeve fizike në ambientet ku ruhet informacioni i ndërmarrjes nuk ka plan të vazhdimësisë së proceseve të punës në rast të ndonjë fatkeqësie natyrore apo dëmtime tjera të sistemeve të informacionit.

KRU-Prishtina në mungesë të një dhome adekuate (dhomë të serverëve) për ruajtjen e infrastrukturës kompjuterike, kishe adaptuar një mjedis për ruajtjen e pajisjeve të përpunimit të të dhënave të kësaj ndërmarrje. Kjo hapësirë/zyre nuk plotësonte kushtet mjedisore elementare ashtu që të parandalojë ose pamundësoj dëmtimin e mundshëm të infrastrukturës kompjuterike dhe ndërprerjeve të shërbimeve në rast të ndonjë fatkeqësie natyrore apo dëmtimi të qëllimshëm.

Në dhomën e serverëve janë vendosur vetëm disa kontrolle minimale parandaluese mjedisore.

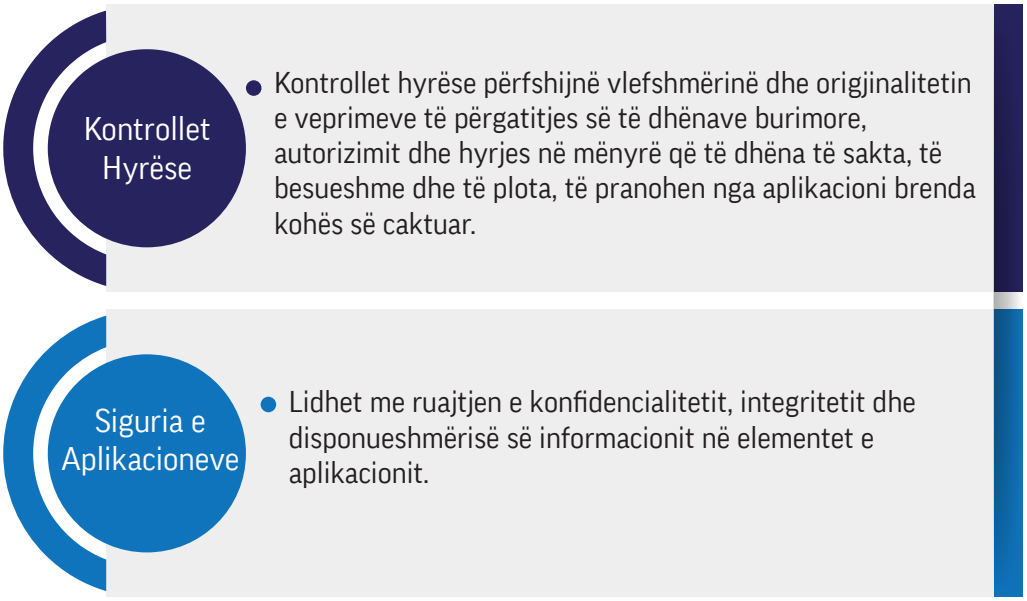
Për më tepër, KRU-Prishtina nuk ka zhvilluar një plan të vazhdimësisë së biznesit dhe të rimëkëmbjes nga fatkeqësitë, i cili do të ishte udhëzues i detajuar për reagim emergjent në rast të ndonjë fatkeqësie natyrore apo dëmtime tjera që mund të ndikojnë në dështimin e proceseve të punës dhe burimeve të teknologjisë së informacionit. Poashtu, ndërmarrja nuk ka një plan që të adresojë rimëkëmbjen e pasurive kritike të teknologjisë.

Megjithëse për sistemet e përdorura bëhen backup (kopje rezervë), por ato ruhen në të njëjtin lokacion me sistemet primare që paraqesin rrezik të humbjeve në rast të ndonjë fatkeqësie.

2.4. Kontrollet e aplikacionit

Kontrollet e aplikacioneve janë kontrolle specifike unike për çdo aplikacion.

Figura 5: Kontrollet e përfshira në auditim



Më poshtë janë prezantuar gjetjet lidhur me kontrollet hyrëse dhe sigurinë e aplikacionit.

Zyra Kombëtare e Auditimit:

Në aplikacionet që përdorë KRU-Prishtina kishte mungesë të vendosjes së kontrolleve të vlefshmërisë, mungon ndërlidhja si dhe të dhënat nuk janë cilësore

Gjatë testimit të aplikacioneve që përdoren në ndërmarrje, kontrollet e vlefshmërisë për të dhënat hyrëse ishin të vendosura minimalisht. Aplikacionet mundësonin procedimin e të dhënave që nuk ishin të sakta dhe të plota.

- Nga testimet në aplikacionin "Dynamic NAV" në modulet për regjistrimin e pagave, aplikacioni lejonte futjen e një punëtori me numër të letërnjoftimit gabim dhe të pa verifikuar, me

llogari bankare jo ekzistuese apo të një banke tjetër, me një ditëlindje data e se cilës nuk kishe ndodhur ende. Po ashtu, në këtë aplikacion për asnjë lloj të transaksionit nuk kërkohej aprovim shtesë. Kontrollet e transaksioneve bëheshin në mënyrë manuale nga udhëheqësit ndaj vartësve të tyre.

- Në aplikacionin "Billing system", gjatë testimeve për regjistrim të konsumatorëve, pronës, adresës, inkasantit, fushat në të gjitha këto module nuk kishte kufizime që të lejohet të regjistrohen vetëm të dhëna të sakta dhe të plota.
  Po ashtu, ky aplikacion lejonte regjistrimin e të dhënave që konsiderohen me rëndësi për ndërmarrjen pa ndonjë aprovim shtesë, për të siguruar saktësinë dhe plotësinë e informacionit të regjistruar.

Për të verifikuar nëse regjistri i konsumatorëve përmban së paku shënimet siç janë përcaktuar me rregulla të ARRU-së, ne kemi analizuar bazën e të dhënave dhe kemi identifikuar se shumë të dhëna nuk janë regjistruar sipas këtyre kërkesave.

Nga 176,814 konsumatorë[2] të regjistruar deri në fund të vitit 2022, janë identifikuar mangësitë si në vijim

- 71,732 konsumatorë aktiv[3]nuk kishin të regjistruar numër identifikues (numër personal, numër fiskal, numër të biznesit etj). Sipas zyrtarëve të ndërmarrjes, këta konsumatorë janë regjistruar në kohën kur nuk kishin të zbatuara standarde të regjistrimit në aplikacione, megjithatë që nga viti 2020 ishin të regjistruar 842 konsumatorë pa të dhënat bazë.
- Janë identifikuar shumë numra të ID-ve të regjistruara që ishin të pavlefshëm, me karaktere (".", ",","/","*"), shkronja, kishin karaktere me pak apo më shumë se sa që janë të përcaktuara me standarde. Kishte poashtu raste kur në vend të ID ishin të regjistruar numra të telefonit, adresa elektronike apo të tjera.
- Regjistrimi i konsumatorëve nuk bëhej siç duhej sipas kategorive të përcaktuar nga ARRU-ja. Kishte biznese që

2 Numri i përgjithshëm i konsumatorëve ishte 176,814, prej tyre 161,923 konsumatorë aktiv dhe 14,891 konsumatorë pasiv

3 Nga gjithsej 83,083 konsumatorë pa ID

ishin regjistruar si konsumator fizik si dhe ishin klasifikuar si amvisëri. Kishte raste kur në vend të numrit identifikues të një shkolle, objekti fetarë apo institucioni tjetër ishe regjistruar me numër personal.

- Rreth 4000 numra personal të regjistruar me shumë se dy here në sistem që përmbajnë emër dhe mbiemër ndryshe, gjë që e pamundëson identifikim e saktë të poseduesit të ujëmatësve.

Më tej, mungon edhe ndërlidhja mes aplikacioneve që ka ndërmarrja dhe kjo ka shkaktuar punë shtesë për përdoruesit, duke rritur mundësin e gabimeve dhe vështirësi në identifikimin e dhënave të konsumatorëve apo përdoruesve.

Kualiteti i ulët i të dhënave të regjistruara ishte si pasojë e mungesës së planifikimit dhe inicimit që gjatë krijimit të aplikacioneve të dizajnohen kontrollet shtesë si dhe të bëhet ndërlidhja me të dhënat nga Agjencia për Regjistrim Civil si dhe me Agjencisë për Regjistrimin e Bizneseve të Kosovës ashtu që regjistrat të përmbajnë vetëm të dhëna të sakta.

KRU-Prishtina nuk ka monitorim të aktiviteteve në sistemet e informacionit

Gjatë verifikimit nëse ekzistojnë gjurmë të auditimit në sisteme, ne kemi verifikuar dy sistemet bazë "Dynamic NAV" dhe "ERP dhe Billing system". Për një pjesë të tabelave në bazën e të dhënave si dhe për disa module ekzistonin gjurmët audituese. Mirëpo, ndërmarrja nuk kishte identifikuar se cilat janë tabelat kritike në bazën e të dhënave si dhe modulet kritike të aplikacioneve për të cilat duhet që patjetër të ruhen gjurmët audituese, përfshirë këtu edhe ruajtjen automatike në tabela të datës së krijimit të transaksionit (të dhënës) dhe ID/llogarinë e përdoruesit i cili ka krijuar transaksionin.

Gjithashtu, gjatë verifikimit të bazës së të dhënave në "Dynamic NAV", Billing system"dhe 'Mbilling", nëse secilit transaksion i është shoqëruar një numër unik dhe sekuencial, ne kemi gjetur se vetëm tabela e realizimit të transaksioneve financiare në "Dynamic NAV" ishte e plotë dhe nuk i mungonte asnjë e dhënë, në tabelat tjera nuk është shoqëruar ky numër.

Për më tepër, gjurmët e aktiviteteve të përdoruesve nuk monitorohen në baza të rregullta kohore, nuk monitoron as aktivitetet e përdoruesve të jashtëm të kontraktuar për mirëmbajtje si dhe përdoruesve të cilët kanë qasje të plotë si në aplikacion po ashtu edhe në bazën e të dhënave.

Kontrolli i Lartë i Shtetit:

Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output

Për sistemin informatik Billing, u konstatua se UKT Sh.A nuk disponon asnjë nga dokumentacionet e mëposhtme:

- Rregullore mbi përdorimin e sistemit;
- Rregullore operacionale mbi veprimet sistemuese që kryhen ne sistem dhe bazën e te dhënave;
- Manual përdorimi;
- Diagramet e qarkullimit të informacionit;
- Kodin në burim;
- Dokumentacion udhëzues i ndërtimit.

Nga dokumentimi i marrëveshjeve dhe konfigurimeve të VPN-ve për aksesimin e jashtëm të informacionit, u konstatua se:

- Kontratat e Ujësjellës Kanalizime Tiranë Sh.A me palët e treta nuk përmbajnë detaje teknike mbi implementimin, zbatimin dhe ndjekjen e kontratës;
- Disa nga operatorët privatë që aksesojnë të dhënat e sistemit të Ujësjellës Kanalizime Tiranë Sh.A, u konstatua se kanë më shumë se një llogari VPN aktive, ndërsa nuk ka gjurmë dokumentare nëse janë miratuar lidhjet e dyta si dhe arsyet që kanë lindur për këtë konfigurim.
- UKT nuk ka ushtruar kontrolle periodike mbi VPN që janë vënë në dispozicion të palëve të treta me qëllim kontrollin në çdo përpjekje autentifikimi, të dështuar ose të suksesshme, kohën dhe datën e secilës lidhje dhe shkëputje si dhe jo pak e rëndësishme sasia e të dhënave të transmetuara në çdo sesion.
- VPN dhe përdorues databaze të operatorit që ka ofruar shërbim mirëmbajtje, u konstatua të jenë aktive në sistem, megjithëse kontrata për shërbimin e mirëmbajtjes ka përfunduar.
- Në kontratat me palët e treta për lidhjet VPN, nuk përcaktohen kushtet teknike, mënyrat e raportimit, kontrollet periodike që

do të ushtrohen, penalitete të mundshme, persona kontakti teknik të dy palëve, etj., me qëllim informimin dhe adresimin e problematikave nga aksesime jo të sigurta.

Gjurmët e veprimeve në sistem

Nuk gjenerohet gjurmë elektronike mbi veprimet që kryejnë përdoruesit e bazës së të dhënave, ndërsa për përdoruesit që aksesojnë sistemin nga ndërfaqja, ruhen të dhëna të pakta që janë: hyrja, dalja, IP e përdoruesit si dhe mënyra e daljes nga sistemi. Kjo gjurmë elektronike është e pamjaftueshme, për të siguruar të dhëna mbi aktivitetin e tyre.

KONKLUZIONET

03

3. Konkluzionet

Konkluzioni i përgjithshëm nga auditimi paralel nxjerr në pah mangësi të theksuara në qeverisjen e TI-së, sigurinë e informacionit dhe vazhdimësinë e shërbimeve. Përderisa, në KRU Prishtina janë identifikuar mangësi edhe në kualitetin e të dhënave në Ujësjellësin e Tiranës nuk ka pasur problematika të mëdha në të dhënat elektronike, megjithatë mundësia për humbjen e tyre, ndërprerjen apo tjetërsimin është e lartë.

KRU Prishtina nuk ka siguruar një mjedis efektiv të kontrollit për të ruajtur integritetin dhe vazhdimësinë e sistemeve të TI-së, duke ndikuar negativisht në arritjen e plotë të qëllimeve të ndërmarrjes dhe duke zbehur besueshmërinë e sistemeve te ndërmarrjes.

Në shoqërinë Ujësjellës Kanalizime Tiranë Sh.A mungojnë strategjia, politikat dhe aktet rregullativë që përcaktojnë drejtimin, përgjegjësitë dhe detyrimet mbi përdorimin e Teknologjisë së Informacionit.

Në UKT Sh.A, ka munguar një planifikim dhe zhvillim në shërbime të reja informatike, që do të ndihmonin shoqërinë për arritjen e objektivave institucionale. Hapat e ndërmarrë në drejtim të rritjes së përdorimit, përmirësimit dhe sigurisë së shërbimeve që ofrohen nëpërmjet teknologjisë së informacionit janë të pamjaftueshëm, për të hyrë në procesin e sigurisë së të dhënave dhe vazhdimësisë së ofrimit të shërbimeve pa ndërprerje. Megjithëse nuk ka pasur problematika të mëdha në të dhënat elektronike, mundësia për humbjen e tyre, ndërprerjen apo tjetërsimin është e lartë.

REKOMANDIMET

04

4. Rekomandimet

Me qëllim të adresimit të çështjeve të identifikuara rreth qeverisjes së TI-së, sigurisë së informacionit, vazhdimësisë së biznesit dhe kontrolleve të aplikacionit ne kemi dhënë 18 rekomandime për Kompaninë Rajonale të Ujësjellësit Prishtina dhe 15 rekomandime për Ujësjellësin e Tiranës.

Rekomandimet ne detaje gjenden ne raportet individuale të auditimit:

https://zka-rks.org/wp-content/uploads/2023/05/Raporti-auditimit-KRU-Prishtina-Shqip.pdf

https://panel.klsh.org.al/storage/phpsiBhgV.pdf

Shtojca I. Dizajni i auditimit

1. Pyetjet e auditimit dhe kriteret

Zyra Kombëtare e Auditimit ka parashtruar pyetjet e auditimit si në vijim:

1. KRU Prishtina a ka vendosur strukturat, politikat, proceset dhe a i ka identifikuar nevojat për burime të teknologjisë së informacionit me qëllim që të ndihmoj në arritjen e strategjisë dhe objektivave të kompanisë?
2. A ka vendosur organizata mekanizma efektiv dhe të dokumentuar për të vlerësuar rrezikun e sigurisë së informacionit?
3. A janë të vendosur mekanizmat e nevojshëm për vazhdimësi të shërbimeve të TI-së?
4. A janë dizajnuar kontrollet e aplikacioneve në atë mënyrë që të sigurojnë se sistemet në KRU Prishtina pranojnë vetëm të dhëna vlefshme dhe të proceduara nga personeli i autorizuar?

Kontrolli i Lartë i Shtetit ka patur si qëllim t'ju kthejë përgjigje pyetjeve që lindin nga drejtimet si në vijim:

1. Struktura, standarde, aktet rregulluese për teknologjinë e informacionit dhe vazhdimësia e ofrimit të shërbimit;
2. Verifikim i kontrolleve të aplikacioneve për të dhënat Input/ Output;
3. Përdoruesit e sistemeve, të drejtat dhe gjurmët e veprimeve në system.

2. Kriteret e auditimit

Kriteret e përdorura në këtë auditim rrjedhin nga ligjet dhe rregulloret vendore për Ndërmarrjet Publike përkatësisht ofruesit e shërbimeve të ujësjellësit, standardet ndërkombëtare të teknologjisë së informacionit/sistemeve të informacionit, nga objektivat e kontrollit për informacion dhe teknologji, përkatësisht:

Manuali i Auditimit të Teknologjisë së Informacionit, produkt i grupeve të punës së teknologjisë së Informacionit të EUROSAI-t (WGITA) dhe Iniciativës për zhvillim të

INTOSAI-t (IDI); si dhe Kapitulli 7, Siguria e Informacionit; CISA – Manuali i Rishikimit, Edicioni i 27-të,2019 – Kapitulli 5, Kornizat, Standardet dhe Udhëzimet e Sigurisë së Aseteve të Informacionit; Familja e standardeve ISO /IEC 27000 nga Organizata Ndërkombëtare për Standardizim (ISO) dhe Komisioni Ndërkombëtar Elektroteknik (IEC).

Po ashtu praktikat e mira dhe standardet që merren me menaxhimin e sigurisë së informacionit janë marrë parasysh.

Sistemet e Informacionit në
Ujësjellësit e Tiranës dhe Prishtinës

Zyra Kombëtare e Auditimit
Lagjja Arbëria
Rr. Ahmet Krasniqi, 210
10000 Prishtina
Republika e Kosovës

Kontrolli i Lartë i Shtetit
Rruga "Abdi Toptan" Nr.1 Tiranë
Republika e Shqipërisë