KONTROLLI I LARTË I SHTETIT

RAPORT PËRFUNDIMTAR AUDITIMI
I
TEKNOLOGJISË SË INFORMACIONIT

Mbi Auditimin e Sistemeve të Teknologjisë së Informacionit, në Shoqërinë Ujësjellës Kanalizime Durrës Sh.A.

Tiranë, Dhjetor 2022

RAPORT PËRFUNDIMTAR AUDITIMI

"MBI AUDITIMIN E SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT NË SHOQËRINË UJËSJELLËS KANALIZIME DURRËS SH.A."

Tiranë, Dhjetor 2022

PËRMBAJTJA

✂ LISTA E SHKURTIMEVE

KLSH	- Kontrolli i Lartë i Shtetit
INTOSAI	- Organizata Ndërkombëtare e Institucioneve Supreme të Auditimit.
AKSHI	- Agjencia Kombëtarë e Shoqërisë së Informacionit
VKM	- Vendim i Këshillit të Ministrave
UMF	- Urdhri i Ministrit të Financave
UKD	- Ujësjellës Kanalizime Durrës
Flare ERP	- Sistemi i menaxhimit të proceseve në UKD
Mobiread	- Sistemi i menaxhimit të leximeve të matëseve në UKD
Oxana	- Sistemi i fiskalizimit të faturave në UKD
TIK	- Teknologjia e Informacionit dhe Komunikimit
ID	- Numri personal i identifikimit
DDOS	- Distributed Denial-of-Service
MNSH	- Marrëveshje Nivel Shërbimi
TI (IT)	- Teknologji Informacioni
BCP	- Business Continuity Plan
BCC	- Business Continuity Center
DRC	- Disaster Recovery Center
RTO	- Objektivat e Kohës së Rimëkëmbjes
RPOs	- Objektivat e Punës së Ripërtëritjes
OE	- Operator Ekonomik
AK	- Autoriteti Kontraktor
IP	- Internet Protocol
VPN	- Virtual Private Network
LAN	- Local Area Netwrok
VLAN	- Virtual Local area network
MFK	- Menaxhimi Financiar dhe Kontrollit
DVR	- Digital video recorder
NVR	- Network video recorder
NAS	- Network Attached Storage
SAN	- Storage Area Network
ALCIRT	- Agjencisë Kombëtare për Sigurinë Kompjuterike
AKCESK	- Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
ISACA	- Information Systems Audit and Control Association
IPS	- (Immovable Property System)

I. 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 "Ujësjellës Kanalizime Durrës Sh.A.", nga data 26.09.2022 deri më datë 18.11.2022.

Grupi i auditimit mblodhi informacione, zhvilloi pyetësorë e intervista për caktimin e zonave me risk të lartë dhe mbështetur në to si dhe në modulet e përzgjedhura bashkërisht me kolegët Norvegjezë, 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

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 auditimin teknologjisë së informacionit në Ujësjellës Kanalizime Durrës Sh.A., nga data 26.09.2022 deri më datë 18.11.2022. Auditimi i Sistemeve të Teknologjisë së Informacionit, në Ujësjellës Kanalizime Durrës Sh.A., ka qenë pjesë e planit të auditimit të KLSH-së, miratuar me shkresën 37/9, datë 05.10.2022 për muajin Tetor nga Kryetari i KLSH.

Ky auditim është një auditim i cili është mbështetur nga ekspertet e SAI-t të Norvegjisë dhe po zhvillohet në kuadër të projektit të bashkëpunimit ndërmjet dy institucioneve supreme të auditimit të KLSH-së dhe Zyrës së Audituesit të Përgjithshëm të Norvegjisë, bashkëpunim i cili ka filluar që në fillim të vitit 2022.
Në kuadër të këtij bashkëpunimi dhe në vijimësi të trajnimeve të zhvilluara me ekspertët Norvegjezë, pjesë e planit të bashkëpunimit është dhe zhvillimi i një auditimi pilot me ndihmën e ekspertëve Norvegjezë, me qëllim vënien në praktikë të njohurive të përfituara nga trajnimet e zhvilluara dhe forcimin e kapaciteteve audituese lidhur me teknologjinë e informacionit dhe përdorimin e mjeteve IT përgjatë auditimeve të TI-së. Shoqëria Ujësjellës Kanalizime Durrës Sh.A si pjesë e planit të veprimtarisë audituese përgjatë vitit 2022 që do të zhvillojë Departamenti i Auditimit të Teknologjisë së Informacionit, është përzgjedhur si subjekt për zhvillimin e këtij auditimi pilot që në fazat e para të fillimit të bashkëpunimit, ndërmjet dy institucioneve. Grupi i auditimit në çdo fazë nëpër të cilat ka kaluar dhe do kalojë projekti i auditimit ka zhvilluar takime online me ekspertët Norvegjezë duke bashkë diskutuar dhe trajtuar çdo çështje të dalë përgjatë auditimit.

Pas marrjes së ambienteve të përshtatshme, grupi auditues filloi fazën e studimit paraprak, ku u dërgua pyetësori i hartuar nga grupi i auditimit, bazuar në Manualin e Auditimit të Teknologjisë së Informacionit, si dhe në modulet e përcaktuara bashkërisht me kolegët Norvegjezë, bazuar në trajnimet e zhvilluara më parë me ta, mbi hartimin e programit të auditimit. Programi i auditimit me nr. 817/1 u miratua nga Kryetari i Kontrollit të Lartë të Shtetit me datë 23.09.2022.

Objektivat e këtij projekt auditimi, u vendosën në koherencë me veprimtarinë, vizionin, qëllimin dhe objektivat e shoqërisë, duke marrë në konsideratë të gjithë kuadrin rregullator në bazë të të cilit institucioni zhvillon veprimtarinë e tij.

I.2. Përshkrim i gjetjeve kryesore dhe rekomandimeve

Gjetjet kryesore, të paraqitura në këtë Raport Përfundimtar Auditimi në mënyrë të përmbledhur sipas drejtimeve të auditimit, rezultuan si më poshtë:

Gjetja Nr.	Përmbledhje e Gjetjes	Referenca me Raportin Përfundimtar	Rëndësia	Rekomandimi
1	Nga auditimi u konstatua se ambienti fizik i dhomës së serverave ku janë hostuar serverat e sistemeve Flare ERP, Mobiread dhe Oxana si dhe disa pajisje të tjera nuk është në përputhje me standardet e përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (Versioni 1.0, datë 02.12.2008) miratuar nga AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit).	faqe 13-26	e lartë	UKD të marrë masa për planifikimin dhe ngritjen e një infrastrukture IT (ambienteve të dhomës të serverëve dhe rrjetin network) në përputhje me kushtet teknike të përcaktuara në rregulloren e miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK si dhe në përputhje me udhëzimet, standardet dhe praktikat më të mira kombëtare dhe ndërkombëtare.
2	Nga administrimi i dokumentacionit u konstatua se: -UKD, ka investuar në ngritjen e Active Directory për menaxhimin e userave, pajisjeve, aplikacioneve dhe marrjen e shërbimeve me anë të një autentifikimi të vetëm "single sign in", por nuk e ka vënë në përdorim akoma Active Directory. duke mos përdorur të gjitha përfitimet e saj. -Të gjitha konfigurimet e Active Directory janë by default, pra konfigurimi i politikave të sigurisë mbi fjalëkalimet, të drejtat e përdoruesve, të dhënat e sigurisë, etj, janë në gjendjen fillestare të lënë nga sistemi në momentin e implementimit të aplikacionit. Disa nga risqet që vijnë si rezultat i konfigurimeve default i active directory: -Ekziston rreziku i mos menaxhimit të politikave që mund t'i lejojë përdoruesit të marrin shumë të drejta; -Rreziku që politikat e fjalëkalimit nuk janë në përputhje me kërkesat e entitetit ose praktikat më të mira. Kjo mund ta bëjë më të lehtë për personat e paautorizuar qasjen në rrjet dhe sisteme; -Fjalëkalimet që nuk skadojnë kurrë mund të rezultojnë në akses të paautorizuar. Ky është veçanërisht një rrezik nëse ka llogari të përbashkëta përdoruesish ose llogari të sistemit me privilegje administratori. Kështu, ish-punonjësit mund të abuzojnë me këto të drejta; - Llogaria e një përdoruesi me një fjalëkalim bosh mund të rezultojë në akses të paautorizuar; -Nëse kompania ka vetëm një politikë fjalëkalimi, ajo duhet t'i përshtatet të gjitha nevojave, dhe për këtë arsye mund të jetë e dobët, etj.	faqe 13-26	e lartë	UKD të marrë masa për konfigurimin dhe vendosjen në përdorim të Active Directory, me qëllim standardizimin e infrastrukturës IT, rritjen e sigurisë së rrjetit si dhe garantimin e një identifikimi të qendërzuar dhe të sigurt. Për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhim të shërbimeve, konfigurimi i politikave të sigurisë së Active Directory duhet të realizohet sipas rëndësisë dhe në përputhje me standardet më të mira, në mënyrë që të rritet niveli i sigurisë së aksesit.
3	Nga auditimi u konstatua se funksionimi dhe organizimi i strukturës së IT-së në nivel zyre nën varësi të Drejtorisë ligjore dhe me një staf shumë të vogël, nuk i përgjigjet shtrirjes së teknologjisë së informacionit në UKD duke sjellë uljen e ndikimit të IT-së në qeverisjen e shoqërisë si dhe zbeh ndikimin e varësisë direkt nga menaxhimi i lartë.	faqe 13-26	e lartë	Strukturat drejtuese të UKD, duke marrë në konsideratë kohën, burimet e nevojshme të analizojnë mundësinë e ndryshimeve strukturore të strukturës ekzistuese IT me qëllim rritjen e rolit të saj dhe të marrin masa për ngritjen në nivel të strukturës së IT nga nivel zyre në nivel Drejtorie.

4	Nga auditimi u konstatua se: -Administrimi dhe menaxhimi i databazës së sistemit Flare ERP dhe Mobiread realizohet nga OE. Ky OE gjithashtu është duke ofruar suport për këtë sistem. Në sistemin Flare ERP administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Sys admin". Sys Admin ushtron funksionet viewer dhe ka të drejta mbi përdoruesit. Në sistemin Mobiread administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Admin" dhe ka të drejta të plota mbi çdo gjë në sistem. -Detyra e Administratorit të sistemit dhe Administratorit të bazës së të dhënave nuk janë atribuar me anë të një shkrese zyrtare nga organet drejtuese të UKD, ku punonjësit e zyrës IT të janë emëruar zyrtarisht si Administratorë për administrimin e bazës së të dhënave për të ushtruar atributet e përcaktuara sipas funksioneve të tyre dhe të gjitha detyrat e administratorit mbi administrimin e bazës së të dhënave të sistemit.	faqe 27-51	e lartë	1.Strukturat drejtuese në UKD në bashkëpunim me specialistët TIK, të marrin masa për adresimin e këtyre çështjeve tek OE që ka implementuara sistemet Flare ERP dhe Mobiread me qëllim marrjen e kodit në burim të sistemeve, në funksion të përmbushjes të përcaktimeve ligjore si dhe krijimin e kushteve të barabarta për operatorët ekonomik që dëshirojnë të marrin pjesë në procedurat e prokurimit, duke mos penguar konkurrencën e lirë si dhe të stimulojnë pjesëmarrjen e biznesit të vogël dhe të mesëm. 2. Administratori i UKD të marri masa për përcaktimin e detyrës së Administratorit të sistemit dhe Administratorit të bazës së të dhënave, ku të jenë emëruar zyrtarisht Administratorët për administrimin e sistemit dhe bazës së të dhënave duke përcaktuar dhe atributet specifike sipas funksioneve të tyre dhe të gjitha detyrat e administratorit.
5	Nga auditimi mbi sistemin Flare ERP u konstatua se: -Për shkak të mbingarkesës dhe shtimit të shërbimeve, të abonentëve, si dhe për shkak të performancës së dobët të sistemit, ky sistem vazhdimisht punon me ndërprerje dhe ka probleme me ecurinë normale të punës duke ndikuar në veprimtarinë e specialistëve dhe institucionit në ofrimin e shërbimeve kundrejt qytetarëve dhe bizneseve por edhe vetë administratës së UKD; -Sistemi krijon vonesa në shqyrtimin dhe gjenerimin e raporteve të ndryshme; -Kur gjenerohet një raport pivot, në qoftë se tenton të gjenerosh dhe një tjetër, raporti i dytë nuk mund të gjenerohet pa e mbyllur me parë aplikacionin dhe të futesh përsëri; -Sistemi krijon errore dhe nuk gjeneron të dhëna në qoftë se përzgjedhim raporte për periudha më shumë se një muaj; -Shfaqet error kur kërkohet të ekstraktohen të dhënat mbi rolet në sistemin Flare ERP; -Kur tentohet ekstraktimi i klientëve nga sistemi me të gjitha opsionet e zgjedhura të kolonave sistemi bllokohet dhe nuk u përgjigjet komandave dhe nuk ekstrakton asgjë sepse bën crash; -Kur sistemi aksesohet me anë të VPN, jashtë rrjetit të brendshëm, shpeshherë hasen pengesa në aksesimin e tij, pasi sistemi shfaq error. Në momentin që aksesohet është shumë e vështirë të punohet në të pasi është shumë i ngadaltë në veprime; -Sinkronizimi ndërmjet dy sistemeve Flare ERP dhe Mobiread, realizohet çdo një muaj, çka rrit riskun e mospasjes së informacionit të përditësuar për abonentët dhe ndryshimet e kontratave ndërmjet dy sistemeve.	faqe 27-51	e lartë	Strukturat drejtuese në UKD së bashku me specialistët e IT-së, të analizojnë dhe adresojnë tek ofruesi i shërbimit të mirëmbajtjes, parregullsitë, mangësitë e konstatuara nga auditimi dhe të ofrojnë zgjidhje për to me qëllim përmirësimin e performancës së funksionimit të sistemit Flare në ofrimin e shërbimeve, si dhe të merren masa për shtimin e funksionaliteteve të reja sipas nevojës së përdoruesve në sistem.

I.3. Konkluzioni i përgjithshëm 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 154 "*Për Organizimin dhe Funksionimin e KLSH*" datë 27.11.2014 konstaton se, mungesa e kontrolleve dhe mekanizmave të duhur me qëllim krijimin, mirëmbajtjen, zhvillimin e burimeve IT dhe mungesa e akteve rregullatorë të përditësuar në drejtim të sistemeve të teknologjisë së informacionit kanë ndikuar në një zhvillim të pa monitoruar të aktivitetit institucional dhe pa deleguar përgjegjësitë individuale për veprimet e kryera.

Investimet në sistemet e informacionit nuk kanë zgjidhur përfundimisht problemet e sigurisë së informacionit si dhe sigurimin e vazhdueshmërisë së biznesit. Zhvillimi i shërbimeve dhe infrastrukturës duhet të mbështetet në praktikat më të mira si dhe në rekomandimet e AKSHI-t.

Performanca e funksionimit të sistemit Flare ERP është jo e kënaqshme, pasi sistemi vazhdimisht punon me ndërprerje dhe ka probleme me ecurinë normale të punës duke ndikuar në veprimtarinë e specialistëve dhe institucionit në ofrimin e shërbimeve kundrejt qytetarëve dhe bizneseve por edhe vetë administratës së UKD. Sistemi krijon vonesa në shqyrtimin dhe gjenerimin e raporteve të ndryshme, Sistemi krijon errore dhe nuk gjeneron të dhëna në qoftë se përzgjedhim raporte për periudha më shumë se një muaj.

Organizimi i strukturës së IT-së në nivel zyre dhe me një staf shumë të vogël, nuk i përgjigjet shtrirjes së teknologjisë së informacionit në UKD duke sjellë uljen e ndikimit të IT-së në qeverisjen e shoqërisë UKD si dhe zbeh ndikimin e varësisë direkt nga menaxhimi i lartë.

Nga analizimi i të dhënave me teknikat CAAT, rezultoi se sistemi nuk ka mekanizmat e nevojshme për kontrollin e inputit, duke rritur riskun e popullimit të sistemit me të dhëna të gabuara, e për pasojë nxjerrjen e raporteve të pasakta.

Në gjykimin tonë, identifikimi dhe administrimi i elementëve kritikë në ofrimin e shërbimeve kundrejt qytetareve dhe bizneseve dhe garantimin e sigurisë së të dhënave si dhe vazhdimësisë në ofrimin e shërbimit pa ndërprerje nëpërmjet teknologjisë së informacionit është i pamjaftueshëm.

Zbatimi i rekomandimeve të këtij raporti si dhe mbështetja e zhvillimit të TI në UKD nga organet drejtuese të UKD do të rris stabilitetin dhe do të sigurojë qasje efektive dhe në mbështetje të qytetarëve.

II. HYRJA

Mbështetur në Ligjin 154/2014, datë 27.11.2014 "*Për Organizimin dhe Funksionimin e KLSH*", në zbatim të Programit të Auditimit nr. 817/1 prot, datë 23.09.2022 miratuar nga Kryetari i KLSH, me afat auditimi 26.09.2022 deri në 18.11.2022, në subjektin e auditimit "Ujësjellës Kanalizime Durrës Sh.A.", ku periudha e audituar është 01.01.2020 deri në 31.12.2021, u krye auditimi me objekt "*Auditimi i Sistemeve të Teknologjisë së Informacionit*", nga audituesit:

1. B. H., *përgjegjës grupi*
2. M. H., *anëtar*
3. A. K., *anëtare*

II.1. Objekti i auditimit:

Objektivi i auditimit IT është përcaktimi nëse sistemet e teknologjisë së informacionit në Ujësjellës Kanalizime Durrës Sh.A., mbrojnë asetet e informacionit; ruajnë integritetin e të dhënave; sigurojnë disponueshmërinë dhe konfidencialitetin e informacionit dhe mbështeten në kontrolle të duhura

II.2. Qëllimi i auditimit:

Qëllimi i auditimit IT është Vlerësimi nëse objektivat e subjektit arrihen në mënyrë efektive duke përdorur burimet IT, duke përfshirë pajtueshmërinë me kërkesat ligjore dhe rregullative, si dhe disponueshmërinë e sistemeve të informacionit dhe të dhënave që gjenden në të.

Objektivat e këtij projekt auditimi, u vendosën në koherencë me veprimtarinë, vizionin, qëllimin dhe objektivat e shoqërisë, duke marrë në konsideratë të gjithë kuadrin rregullator në bazë të të cilit institucioni zhvillon veprimtarinë e tij.
Për të arritur në dhënien e një opinioni, janë mbledhur informacione, të dhëna dhe prova, për të përcaktuar nëse nëpërmjet sistemeve të 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.

II.3. Identifikimi i çështjeve:

Duke qenë se ky auditim është një auditim i cili është mbështetur nga ekspertet e SAI-t të Norvegjisë, siç e kemi theksuar dhe më lart, modulet e përzgjedhura u përcaktuan bashkërisht me kolegët Norvegjezë dhe në koherencë të plotë me trajnimet e zhvilluara më përpara si rezultat i bashkëpunimit me qëllim vënien në praktikë të njohurive të përfituara nga trajnimet e zhvilluara. Bazuar në fushat e identifikuara, drejtimet e këtij auditimi u konsoliduan në programin e auditimit të protokolluar në KLSH me shkresën nr. 817/1, datë 23.09.2022:

1. Auditimi i Sigurisë së Informacionit

- Identifikimi dhe menaxhimi i risqeve në TIK;
- Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet;
- Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit.

2. Auditimi i sistemeve

-Të drejtat e përdoruesve dhe menaxhimi i tyre;
-Verifikim i kontrolleve të aplikacioneve për të dhënat Input/Output.

II.4. Përgjegjësitë e strukturave drejtuese të subjektit të audituar:

Shoqëria Ujësjellës Kanalizime Durrës Sh.A. e zhvillon aktivitetin e saj mbështetur në ligjin nr. 9901, datë 14.04.2008 "*Për tregtarët dhe shoqëritë tregtare*", i ndryshuar; ligjin nr. 8102 datë 28.03.1996 "*Për kuadrin rregullator të sektorit të furnizimit me ujë dhe largimit e përpunimit të ujërave të ndotura*", i ndryshuar; VKM nr. 63 datë 27.01.2016 "*Për riorganizimin e operatorëve që ofrojnë shërbimin e furnizimit me ujë të pijshëm, grumbullimin, largimin dhe trajtimin e ujërave të ndotura*"; Kodin e punës në RSH, i ndryshuar, etj

Shoqëria Ujësjellës Kanalizime Durrës Sh.A ofron shërbimin e furnizimit me ujë dhe largimit të ujërave të ndotura për 355,298 banorë të Bashkisë Durrës, Shijak dhe Njësitë Administrative Bubq (Bashkia Krujë), Thumane (Bashkia Krujë), Fushë-Kuqe (Bashkia Kurbin), Prezë (Bashkia Vorë), si dhe përpunimin e ujërave të ndotura në ITUN Durrës me një kapacitet për rreth 250,000 banorë të qytetit të Durrësit, zonës së plazhit dhe fshatrat përreth tij.

Organet drejtuese të Shoqërisë Ujësjellës Kanalizime Durrës Sh.A. janë: Asambleja e Përgjithshme, Këshilli i Administrimit si dhe Administratori.

Strategjia kryesore e veprimtarisë së Shoqërisë Ujësjellës-Kanalizime Durrës është realizimi i një performance në drejtim të përmbushjes së detyrave, rritjes së kapaciteteve njerëzore për të ofruar një shërbim sa më cilësor për konsumatorin, duke synuar përmirësimin e menaxhimit në sektorin e furnizimit me ujë dhe kanalizimeve në qytet, për ta bërë atë më efiçent, të qëndrueshëm dhe efektiv në përputhje me ligjet dhe rregulloret në fuqi në Shqipëri.

Objektet e Veprimtarisë janë:

- 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;
- Shoqëria duhet të realizojë çdo lloj operacioni financiar apo tregtar që lidhet direkt apo indirekt me objektin e saj, brenda kufijve të parashikuar nga legjislacioni në fuqi. Shoqëria ushtron veprimtarinë e saj në përputhje me lejet, autorizimet, licencat sipas legjislacionit në fuqi.

Misioni kryesor i Shoqërisë Ujësjellës-Kanalizime Durrës sh.a në zonën e shërbimit me ujë të pijshëm është:

- Garantimi i një sistemi teknikisht të përshtatshëm të furnizimit me ujë, përfshirë dhe mbrojtjen e burimeve ujore;
- Largimi i kontrolluar i ujërave të ndotura që prodhohen në zonën e shërbimit nga konsumatorët;
- Sigurimin e furnizimit me ujë të pijshëm sasior dhe cilësor për konsumatorët;
- Zvogëlimi i humbjeve dhe i sasisë së ujit të pafaturuar në sistemin e furnizimit me ujë;
- Rritjen e të ardhurave nga faturimi, si dhe zvogëlimin e shpërdorimeve në sistem;
- Mirëmbajtja e elementeve përbërës të sistemit të kanalizimit;
- Mirëmbajtja e impiantit të trajtimit të ujërave të ndotura;
- Mbledhja e tarifës nga konsumatorët për këto shërbime.

II.5. Përgjegjësitë e audituesve:

Kontrolli i Lartë i Shtetit, auditoi Ujësjellës Kanalizime Durrës Sh.A, për periudhën e veprimtarisë nga 01.01.2020 deri në 31.12.2021, duke i kushtuar vëmendje çështjeve që lidhen me cilësinë e shërbimeve të ofruara nëpërmjet sistemeve të teknologjisë së informacionit, sigurisë së të dhënave dhe arritjes së objektivave institucional nëpërmjet përdorimit të burimeve të TIK.

Nga grupi i auditimit, me përgjegjësi të plotë, janë analizuar të gjitha çështjet që përmban Programi i Auditimit nr. 817/1, datë 23.09.2022, miratuar nga Kryetari i KLSH. Në realizimin e këtij Projekt Auditimi, grupi i auditimit është mbështetur në bazën ligjore mbi të cilën funksionon KLSH, standardet e auditimit si dhe në legjislacionin e fushës në të cilën operon Ujësjellës Kanalizime Durrës Sh.A. Gjithashtu, gjatë veprimtarisë audituese, është siguruar një evidencë e përshtatshme auditimi, në të cilën jemi mbështetur për nxjerrjen e konkluzioneve dhe dhënien e 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:

- Kushtetuta e Republikës së Shqipërisë (*nenet 162-165 si dhe nenet 78, 83*);
- Ligji nr. 154/2014 "*Për Organizimin dhe Funksionimit e Kontrollit të Lartë të Shtetit*";
- Ligji Nr. 10325, datë 23.09.2010, "*Për Bazat e të Dhënave Shtetërore*";
- Ligji nr. 9887, datë 10.03.2008 "*Për Mbrojtjen e të Dhënave Personale*" i ndryshuar;
- Ligji nr. 2/2017, "*Për Sigurinë Kibernetike*";
- Ligji nr.1029, datë 8.7.2010 për "*Menaxhimin Financiar dhe Kontrollin*";
- Ligj**i** nr.114/2015 për "*Auditimin e brendshëm në sektorin publik*";
- Ligji Nr. 119/2014 "*Për të drejtën e informimit*";
- Ligji Nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*" i ndryshuar;
- Ligji nr. 9901, datë 14.04.2008 "*Për tregtarët dhe shoqëritë tregtare*" i ndryshuar;
- Ligji nr. 7691 datë 12.07.1995 "*Kodi i punës*" i ndryshuar;
- VKM nr. 673, datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*", i ndryshuar;
- VKM nr. 710, datë 21.08.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit*", i ndryshuar;
- VKM nr. 945, datë 02.11.2012 "*Për miratimin e rregullores administrimi i sistemit të bazave të të dhënave shtetërore*", etj;
- VKM nr. 63, datë 27.01.2016 "*Për riorganizimin e operatorëve që ofrojnë shërbimin e furnizimit me ujë të pijshëm, grumbullimin, largimin, dhe trajtimin e ujërave të ndotura*", Statutin e Shoqërisë, Kontratës Kolektive.
- VKM nr. 1304, datë 11.12.2009 "*Për miratimin e modelit të rregullores për furnizimin me ujë dhe për kanalizimet në zonën e shërbimit të ujësjellës kanalizimeve sh.a.*",
- 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;
- Rregullore për organizimin dhe funksionimin e Shoqërisë U. K. Durrës Sh.A
- Rregulloret përkatëse të Agjencisë Kombëtare të Shoqërisë së Informacionit;
- Aktet ligjore/nënligjore/rregullative që përcaktojnë regjistrimin dhe ruajtjen e të dhënave;
- Standardet e miratuara nga CESK, etj.
- Standardet Ndërkombëtare të Auditimit (ISSAI) të INTOSAI-t;
- Udhëzues dhe Manuale të Auditimit të Teknologjisë së Informacionit si: ISSAI 5300, Manuali Aktiv i Auditimit TI si dhe Standardet e COBIT.

II.7. Standardet e auditimit:

Auditimi është kryer, në përputhje me Kodin Etik, Standardet dhe teknikat e auditimit, 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 si dhe standardet ndërkombëtare të teknologjisë së informacionit.

II.8. Metodat e auditimit:

Grupi i auditimit, me qëllim arritjen e objektivave të auditimit, ka përdorur metoda si intervista me gojë zhvilluar në subjekt me personat përgjegjës, testime me zgjedhje, shqyrtimin e dokumentacionit rregullativ të institucionit, ka verifikuar dokumentacionin e nevojshëm të kërkuar dhe të paraqitur nga subjekti i audituar me qëllim përmbushjen e drejtimeve të auditimit, ka testuar me teknikat CAAT të dhënat e sistemeve, si dhe ka kryer testime dhe verifikime mbi shkallën e sigurisë së rrjetit dhe sistemeve që subjekti i audituar përdor,

analizimi i të dhënave të eksportuara nga sistemi, analizimi i të dhënave të raportuara nga ana e subjektit.

II.9. Dokumentimi i auditimit:

Dokumentimi i auditimit është bazuar në rregulloren e procedurave të auditimit në KLSH si dhe në manualin e 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;
- Pyetësorë dhe përgjigje të punonjësve që veprojnë nëpërmjet sistemit.

-Për çështjen e auditimit "*Auditimi i Sigurisë së Informacionit*", grupi i auditimit shqyrtoi dokumentacionin: Verifikime onsite të dhomës së serverave të UKD dhe infrastrukturës network të ujësjellësit; 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; Planet e menaxhimit të incidenteve; Planet e menaxhimit të ndryshimeve; etj.

-Për çështjen e auditimit "*Auditimi i Sistemeve*", grupi i auditimit shqyrtoi dokumentacionin: Përshkrim i përgjithshëm i sistemit të teknologjisë së informacionit në UKD; Të dhënat e gjeneruara nga sistemi për shërbimet e ofruara; U mor akses me përdorues me të drejta "lexues" në sistemin Flare ERP; Aktet rregullative të shoqërisë që lidhen me sistemet dhe veprimet operacionale brenda dhe jashtë sistemit; Manualet e përdorimit të sistemeve; Intervista të drejtpërdrejta me punonjësit që kryenin apo administronin shërbime të caktuara; Të dhënat për përdoruesit e sistemeve Flare ERP dhe Mobiread; Vizita në terren; Analizë e performancës së sistemit; etj.

III. PËRSHKRIMI I AUDITIMIT

III.1. Informacion i përgjithshëm mbi subjektin nën auditim:

Shoqëria Ujësjellës Kanalizime Durrës Sh.A. e zhvillon aktivitetin e saj mbështetur në ligjin nr. 9901, datë 14.04.2008 "*Për tregtarët dhe shoqëritë tregtare*", i ndryshuar; ligjin nr. 8102 datë 28.03.1996 "*Për kuadrin rregullator të sektorit të furnizimit me ujë dhe largimit e përpunimit të ujërave të ndotura*", i ndryshuar; VKM nr. 63 datë 27.01.2016 "*Për riorganizimin e operatorëve që ofrojnë shërbimin e furnizimit me ujë të pijshëm, grumbullimin, largimin dhe trajtimin e ujërave të ndotura*"; VKM nr. 1304, datë 11.12.2009 "*Për miratimin e modelit të rregullores për furnizimin me ujë dhe për kanalizimet në zonën e shërbimit të ujësjellës kanalizimeve Sh.A.*", Kodin e punës në RSH, i ndryshuar, etj

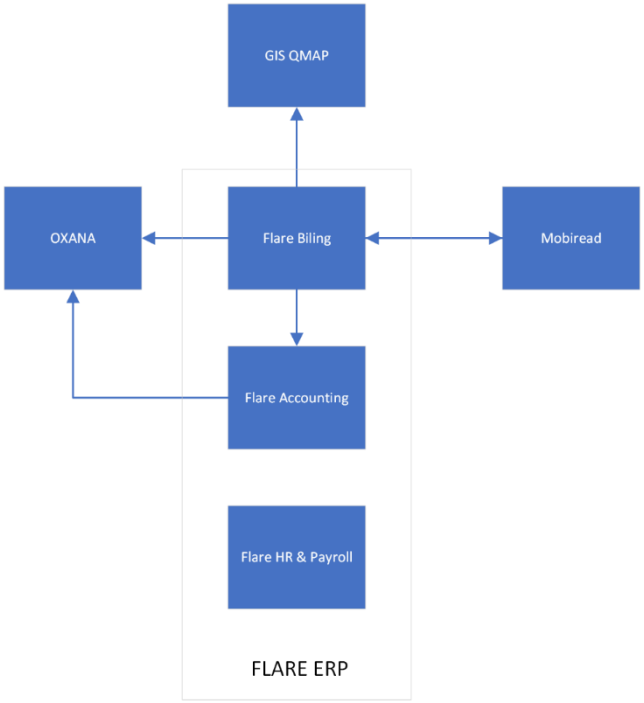
Shoqëria Ujësjellës Kanalizime Durrës Sh.A ofron shërbimin e furnizimit me ujë dhe largimit të ujërave të ndotura për 355,298 banorë të Bashkisë Durrës, Shijak dhe Njësitë Administrative Bubq (Bashkia Krujë), Thumane (Bashkia Krujë), Fushë-Kuqe (Bashkia Kurbin), Prezë

(Bashkia Vorë), si dhe përpunimin e ujërave të ndotura në ITUN Durrës me një kapacitet për rreth 250,000 banorë të qytetit të Durrësit, zonës së plazhit dhe fshatrat përreth tij.

Organet drejtuese të Shoqërisë Ujësjellës Kanalizime Durrës Sh.A. janë: Asambleja e Përgjithshme, Këshilli i Administrimit si dhe Administratori.

Strategjia kryesore e veprimtarisë së Shoqërisë Ujësjellës-Kanalizime Durrës është realizimi i një performance në drejtim të përmbushjes së detyrave, rritjes së kapaciteteve njerëzore për të ofruar një shërbim sa më cilësor për konsumatorin, duke synuar përmirësimin e menaxhimit në sektorin e furnizimit me ujë dhe kanalizimeve në qytet, për ta bërë atë më efiçent, të qëndrueshëm dhe efektiv në përputhje me ligjet dhe rregulloret në fuqi në Shqipëri.

Për periudhën objekt auditimi UKD ka pasur në përdorim një sërë sistemesh të cilat ndihmojnë në mbarëvajtjen e veprimtarisë së UKD. Sistemet kryesore mbi të cilat grupi i auditimit u fokusua janë Sistemi Flare ERP, Sistemi Mobiread, sistemi Oxana si dhe sistemi GIS QMAP. Të tre këto sisteme komunikojnë dhe ndërveprojnë me njëri tjetrin sipas diagramës së më poshtme.



Sistemi Flare ERP:
Sistemi Flare ERP është implementuar për herë të parë në vitin 2014, dhe është i përbërë nga modulet Flare Accounting, Flare HR & Payroll, Flare Billing. Programi është i ndërtuar mbi katër menu bazë që janë: a) Kontabiliteti b) Inventari c) Punonjësit d) Opsionet.

Sistemi Mobiread:
Sistemi Mobiread është implementuar në vitin 2016 për mbledhjen dhe hedhjen e leximeve të matësve, nga lexuesit e UKD.
Sistemi Mobiread është i ndërtuar në platformën PHP, MySQL, html/javscript, si dhe sistemi Android për pajisjet PDA që përdorin lexuesit për hedhjen e të dhënave të leximeve të matësave. Qëllimi kryesor i këtij sistemi është marrja e leximeve nga pajisjet PDA dhe dërgimi i këtyre të dhënave në sistemin Flare ERP, Moduli Billing në mënyrë që të realizohet faturimi i saktë i konsumatorëve. Për të bërë të mundur këtë proces, sistemi "Mobiread" merr të dhënat fillestare nga sistemi Flare, Moduli Billing. PDA-të marrin të dhënat e abonentëve që ju nevojiten dhe i kthejnë sërish sistemit të dhënat e përditësuara me leximet përkatëse. Në fund të këtij procesi, sistemi i dërgon këto të dhëna në sistemin Flare, Moduli Billing.

Sistemi Oxana:
Sistemi i fiskalizimit është një aplikacion online, i cili mbulon procesin e shitjeve dhe realizon fiskalizimin e faturave për abonentët e UKD. Ky sistem është implementuar në vitin 2021. Në këtë sistem gjithashtu mund të menaxhohen të dhënat e nevojshme për çdo artikull, shitje dhe çdo detaj për sa i përket shitjeve apo klient, etj. Ky sistem aksesohet online në adresën "fiscalization.oxana.al".

III.2. PËRSHKRIM I REZULTATEVE SIPAS DREJTIMEVE TË AUDITIMIT:

III.2.1.Auditimi i Sigurisë së Informacionit

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

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

a. Identifikimi dhe menaxhimi i risqeve në TIK

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 TI është aplikimi i metodave të menaxhimit të riskut në teknologjinë e informacionit për të menaxhuar rrezikun e TI-së, pra: Rreziku i institucionit që lidhet me përdorimin, pronësinë, operimin, përfshirjen, ndikimin dhe adoptimin e TI në UKD.
-Nga administrimi i dokumentacionit se si UKD, identifikon dhe menaxhon risqet institucionale dhe risqet në teknologjinë e informacionit, u konstatua se UKD nuk disponon regjistër risku të përgjithshëm institucional, ku të përfshihen edhe risqet mbi IT dhe të mbulohen të gjithë aktivitet duke përfshirë këtu risqet mbi sistemet Flare ERP dhe Mobiread, proceset e menaxhimit të ndryshimit, etj. UKD nuk ka identifikuar dhe vlerësuar ngjarjet e mundshme që mund të kenë efekt negativ përsa i përket arritjes së objektivave të shoqërisë.
Nisur sa më sipër dhe mbështetur në 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*", UKD nuk disponon regjistër risku ku të përfshiheshin edhe risqet që lidhen me teknologjinë e informacionit.

b. Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet

Verifikimi i shkallës së sigurisë së dhomës së serverëve me qëllim parandalimin e vjedhjes ose të dëmtimit të pajisjeve kompjuterike, aksesit të paautorizuar, kopjimit ose shikimit të informacionit sensitiv.

- ***Ambienti fizik i dhomave të serverave***

Auditimi mbi shkallën e sigurisë së dhomës së serverave, u krye në bazë të manualit të auditimit TI, 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.
Duke qenë se dhoma e serverëve është pika më 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 zyrës së IT-së, zhvilloi verifikimin e dhomës së serverave të lokalizuar në katin e dytë të një prej godinave të UKD ku janë hostuar rack-et me serverat e sistemeve: Flare ERP, Mobiread, Oxana si dhe servera dhe pajisje të tjera.

Nga auditimi u konstatuan u konstatuan disa problematika konkretisht si më poshtë:

-Ambienti ku janë lokalizuar serverat e sistemeve të UKD dhe infrastruktura e network-ut, nga karakteristika ka qenë një zyrë ekzistuese e cila është përshtatur për tu përdorur si dhomë serverësh;
- Ambienti nuk ka të instaluar një sistem akses kontrolli i cili garanton hyrjen e personave të autorizuar, (pra aksesi në ambientin e dhomës së serverëve nuk është i kontrolluar me teknologji të tilla si: skanime, lexues karte, etj);
- Nuk ka një rregullore të miratuar për personat e autorizuar që mund të hyjnë në dhomën e serverëve;
- Kabllimet dhe lidhjet e rrjetit në switch dhe patch panel nuk janë të sistemuar;
- Ambienti kishte prani të lagështirës dhe hyrja në këtë ambient ishte e përbërë nga një derë druri, faktor i cili ul sigurinë për në dhomën e serverëve;
- Nuk ka një plan testimi të sensorëve të zjarrit si dhe mirëmbajtje për sistemin elektrik dhe sistemin backup UPS;
- Nuk bëhen kolaudime për sistemin antizjarr;
- Nuk ka të instaluar BMS (Building Managment System).

-Bëhet regjistrimi me video (*kamera sigurie*) për monitorimin e portave hyrëse për në dhomën e serverave dhe në pjesë të tjera të perimetrit të ndërtesës;

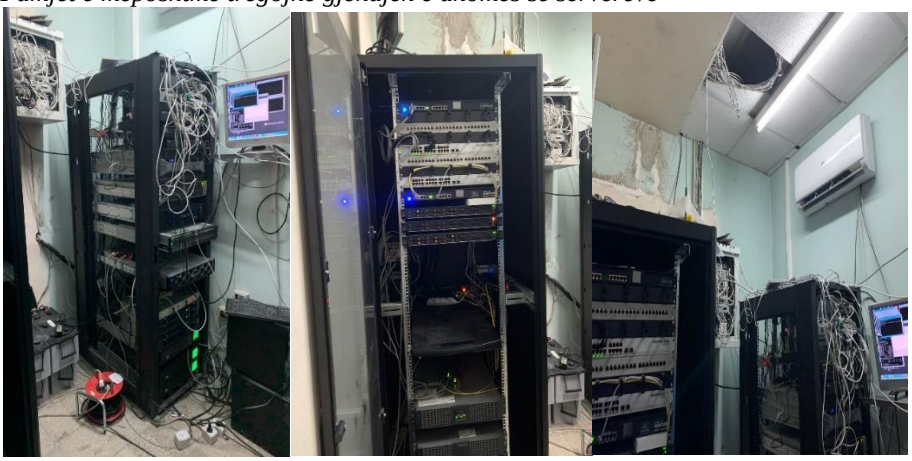
-Dhoma duhet të jetë e pajisur me një sistem të përshtatshëm kundër zjarrit; dhoma duhet të jetë rezistente ndaj zjarrit nëse kabllot dhe sistemet e ftohjes kombinohen në të njëjtën hapësire sipër tavanit ose nën dysheme;

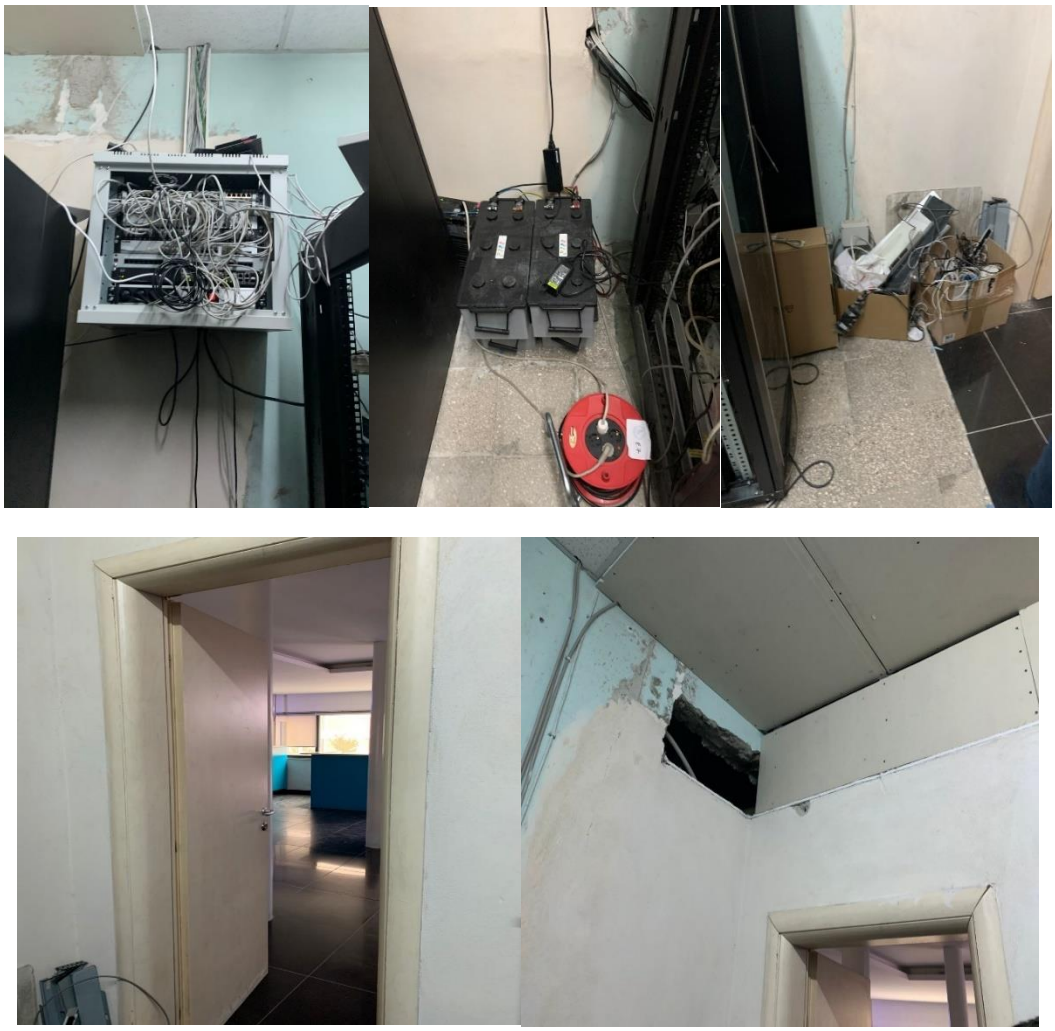
-Instalimi elektrik i dhomës së serverëve nuk është veçmas instalimit të përgjithshëm;

-Mungon sistemi i alarmit, i cili duhet të jenë të tillë që të sinjalizojnë problemet me rrymën elektrike, me ambientin fizik, sensor për rrjedhjen e ujit, sensor për parandalimin e dëmtimeve fizike të strukturës së dhomës.

Si konkluzion, ambienti fizik i dhomës së serverave ku janë hostuar serverat e sistemeve Flare ERP, Mobiread dhe Oxana si dhe disa pajisje të tjera nuk është në përputhje me standardet e përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (*Versioni 1.0, datë 02.12.2008*) miratuar nga AKSHI (*Agjencia Kombëtare e Shoqërisë së Informacionit*).

Figura nr.1: *Pamjet e mëposhtme tregojnë gjendjen e dhomës së serverëve*



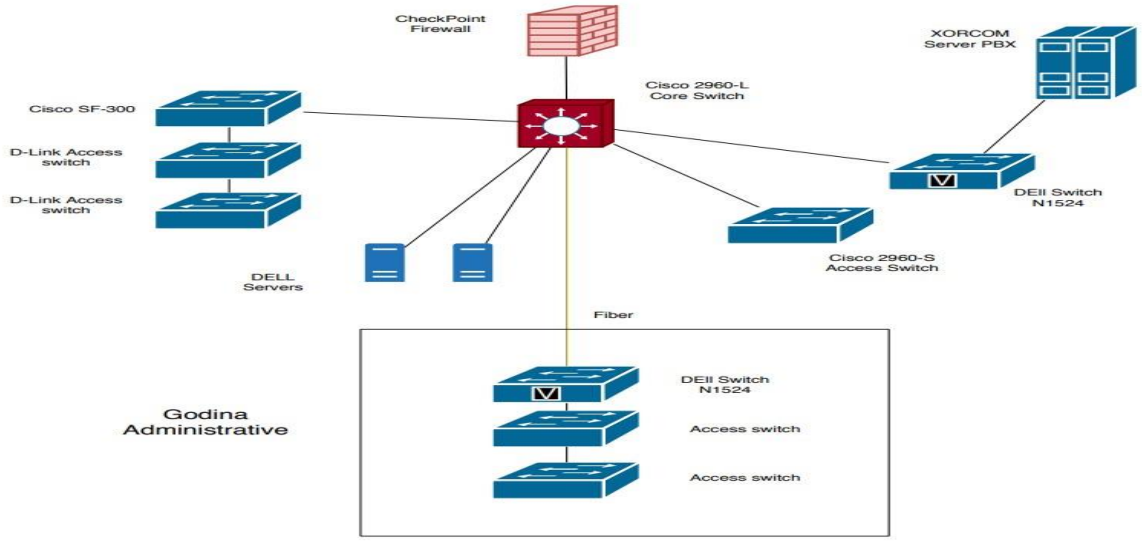


Burimi: *Grupi i Auditimit*

- ***Auditimi mbi pajisjet Firewall të UKD***

Infrastruktura aktuale e godinës kryesore të UKD është e shpërndarë në tre godina të vendosura brenda një perimetri të afërt me njëra-tjetrën. Shërbimet janë të qendërzuara në një godinë brenda një dhome e cila është përshtatur si dhomë serverash për infrastrukturat: infrastruktura e rrjetit, infrastruktura e përdorimit dhe ruajtjes së të dhënave, infrastruktura e shërbimit të përdoruesve, sistemi i monitorimit, sistemi i telefonisë etj.
Ndërlidhja e kësaj qendre shërbimesh me ndërfaqen WAN (*komunikimet e jashtme*) mundësohet nëpërmjet një Firewall Checkpoint. Ky firewall ka të ngritura politikat e komunikimit të shërbimeve dhe mbrojtjes nga jashtë rrjetit. Ky firewall përfundon me dy switch-e të cilët shërbejnë për infrastrukturën e shërbimeve të përdoruesve. Infrastruktura e përdorimit të të dhënave përbëhet nga dy servera: HPE DL 380 G9 dhe DELL EMC PowerEdge R740 dhe një storage DELL EMC SC 2020, të gjitha këto pajisje komunikojnë me ndërfaqe iSCSI. Mbi këta servera është ndërtuar një infrastrukturë virtuale e bazuar në teknologjinë VMware, mbi të cilat janë ngritur shërbimet e nevojshme për të realizuar gjithë proceset punës.

Figura nr. 2: *Topologjia fizike e logjike e Infrastrukturës TI të UKD*



Burimi: *UKD Sh.A*

UKD e merr internetin nga një ISP lokale, e cila i siguron dhe një linjë backup në rast të ndërprerjes së linjës primare. Për shpërndarjen e internetit në pikat e tjera përdoret opsioni dark fibër që do të thotë që përdoret infrastruktura e ISP për ofrimin e shërbimit network për pikat e shërbimit të UKD.

Nga auditimi mbi konfigurimet aktuale për switch-et kryesore u konstatua se:
-Nuk janë marrë masat e nevojshme që useri admin të limitohet në logimin vetëm nga IP-të brenda rrjetit privat dhe nuk është e bllokuar që useri admin të logohet nga jashtë rrjetit, pra nga një rrjet publik;
-Nuk janë krijuar group users me nivele të ndara menaxhim/monitorim. Çdo veprim bëhet nga useri admin;
-Nuk janë krijuar zona me limite të caktuara për brenda LAN si dhe rrjeti nuk është i ndarë në VLAN (rrjete virtuale) çka do të bënte të mundur menaxhimin dhe lejimin e grupeve të IP-ve në shërbime të ndryshme sipas nevojave. Gjithashtu nuk është krijuar edhe një zonë Untrust e cila sipas konfigurimeve shërben për bllokimin e portave të shërbimeve si dhe bllokimin e IP-ve të cilat mund të paraqesin problematika ose sulme;
-Pajisja firewall ka të aktivizuar log çka bën të mundur për të verifikuar një sërë procesesh që routeri kryen si edhe ruajtjen e tyre.

c. Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit

Bazuar në standardet ndërkombëtare, siguria e informacionit garantohet duke siguruar gatishmërinë, konfidencialitetin dhe integritetin e të dhënave. Politikat e sigurisë së organizatës janë rregulla, praktika që rregullojnë sesi një institucion menaxhon, mbron dhe shpërndan burimet për të arritur objektivat specifikë të sigurisë. Këto rregulla dhe praktika duhet të identifikojnë kriteret për autoritetin përkatës. Disa nga elementët në Sigurinë e TI janë:
- Planet e vazhdueshmërisë së institucionit;
- Përdorimi i aseteve të teknologjisë së informacionit;
- Procedurat e backup-it;
- Elemente të trajnimit dhe të edukimit mbi sigurinë;
- Procesi për raportimin e incidenteve të dyshimta të sigurisë;
- Metodat e komunikimit me stafin mbi politikat dhe procedurat e përshtatura për sigurinë e Sistemeve të Informacionit etj.

- ***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.
Backup i infrastrukturës virtuale në UKD mundësohet nga platforma Veeam Backup & Replication. Serveri i Veeam është ngritur si makinë virtuale në infrastrukturën ekzistuese Vmware, si dhe ka dy particione. Particioni i parë është përcaktuar si Virtual Disk me kapacitet 60Gb në të cilin ndodhet i instaluar sistemi dhe particioni i dytë me kapacitet 1.2 TB ndodhet në Storage dhe i është paraqitur serverit me iSCSI. Particioni i dytë është dhe particioni në të cilin ruhet dhe backup i makinave virtuale. Makina Virtuale e Serverit të VM disponon tre karta rrjeti. Karta e parë ka dhe IP e menaxhimit ndërsa dy kartat e tjera janë të dedikuara për trafikun iSCSI. Për trafikun iSCSI janë përdorur dy karta rrjeti virtuale që janë në VLAN të ndryshme dhe në Switch fizike të ndryshme për të ofruar redundancë edhe në rastin kur një nga switch-at është me probleme. Çdo backup është konfigururar që të ekzekutohet çdo ditë të javës pas orës 23:00.

Nga auditimi u konstatua se:
-Procedura e ndjekur për kryerjen e backup-ve nuk është e pasqyruar apo e dokumentuar në një dokument administrativ si Rregullore e Brendshme apo dokument tjetër TIK ku të përcaktohet mënyra e kryerjes së backup-ve, procesin e ruajtjes së të dhënave për sistemet në përdorim nga punonjësit e UKD;
-Procedurat e backup ndiqen nga operatori ekonomik që kryen mirëmbajtjen;
-Procedurat e rikthimit (restore) të të dhënave nuk testohen për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar për sistemet e sipërpërmendura;
-Ruajtja e backup në vende në distancë nuk realizohet;
-Në rastet kur të dhënat e backup-it janë të panevojshme nuk ekzistojnë procedura për mënyrën e nxjerrjes së tyre jashtë përdorimit;
-Nuk është e qartë nëse kontrollohet statusi i backup-it nëse procedura është kryer me sukses.

- ***Active Directory***

Nga auditimi i sigurisë së të dhënave që UKD administron në sistemin e saj rezulton se: Siguria e rrjetit të UKD është e kompromentuar pasi nuk ka Active Directory dhe Domain Controller për një identifikim të qendërzuar dhe të sigurtë. Pa Active Directory, çdo kompjuter në rrjet ka bazën e të dhënave të veta të vogla të emrave të përdoruesve dhe fjalëkalimeve. Microsoft e quan këtë lloj krijimi një GRUP PUNE (WORKGROUP), domethënë çdo kompjuter vepron më vete dhe nuk ka kontroll qendror. Ky lloj konfigurimi krijon një sfidë kur kemi shumë kompjutera dhe një përdorues duhet të ketë qasje në njërën prej tyre ose kur ai ndryshon fjalëkalimin ose emrin e përdoruesit. Active Directory mban në një memorie të centralizuar, emrat, përdoruesit dhe fjalëkalimet. Çdo ndryshim në emrat e përdoruesit dhe fjalëkalimet regjistrohen nga Active Directory dhe të gjithë kompjuterat në rrjet kanë qasje në këtë informacion. Prandaj Active Directory:

- Është një bazë të dhënash;
- Siguron kontroll të centralizuar;
- Regjistron të gjitha ndryshimet e fjalëkalimeve;
- Mund të shpërndahet në të gjithë botën;
- Ruan burimet në share folders;
- Shërbimet si e-mail mund të përdorin Active Directory.

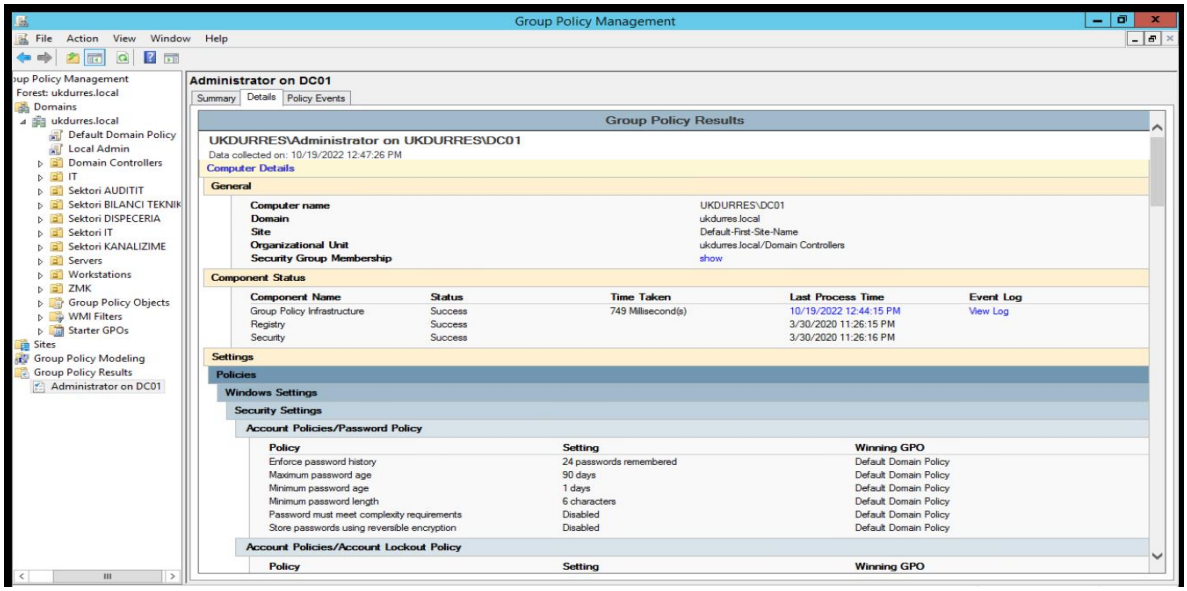
Administratorët e rrjetit e përdorin Active Directory për të ruajtur dhe organizuar objekte në një rrjet (të tilla si përdoruesit, kompjuterët, pajisjet, etj.) Në një strukturë të sigurt hierarkike të kontrollit që njihet si strukturë logjike.

Nga administrimi i dokumentacionit u konstatua se UKD, ka investuar në ngritjen e Active Directory për menaxhimin e userave, pajisjeve, aplikacioneve dhe marrjen e shërbimeve me anë të një autentifikimi të vetëm "*single sign in*" për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhimin e shërbimeve në përputhje me standardet me të mira, por nuk e ka vënë në përdorim akoma Active Directory, duke mos përdorur të gjitha përfitimet e saj për:
-Përfitimin e një performance më të mirë të aplikacionit;
-Garantimin e vazhdimësisë së shërbimeve të ofruara;
-Krijim dhe logimin e përdoruesve dhe marrjen e shërbimeve me anë të një autentifikimi të vetëm "*single sign in*". Përdoruesit mund të logohen me adresën e emailit në pc, në email, në rrjet etj me anë të domain controller-it duke patur një autentifikim të sigurt. Me anë të "single sign in" përdoruesit mund të logojnë: *në PC; në network (wifi me pajisjet, laptop, smartphone, tablet, etj); në email; në apps, etj*.
Në opinionin e grupit të auditimit përdorimi i një zgjidhje të tillë do të sillte lehtësira për stafin e UKD në procesin e punës si dhe rritjen e sigurisë së të dhënave.
Në momentin e hartimit të këtij raporti, nga ana e specialistëve të zyrës IT në UKD ka filluar puna për popullimin e active directory, krijimi i ndarjeve, drejtorive, sektorëve, ndarjen e roleve dhe përgjegjësive, etj. Nisur sa më sipër grupi i auditimit për ti ardhur në ndihmë subjektit në këtë fazë fillestare, këqyri dhe mori të dhëna mbi politikat e sigurisë të konfiguruara në active directory.

Nga auditimi u konstatua se të gjithë konfigurimet e Active Directory janë by default, pra konfigurimi i politikave të sigurisë mbi fjalëkalimet, të drejtat e përdoruesve, të dhënat e sigurisë, etj, janë në gjendjen fillestare të lënë nga sistemi në momentin e implementimit të aplikacionit. Këto politika të sigurisë konfigurohen sipas rëndësisë që i kushtohet këtyre elementëve, në mënyrë që rritet niveli i sigurisë së aksesit.

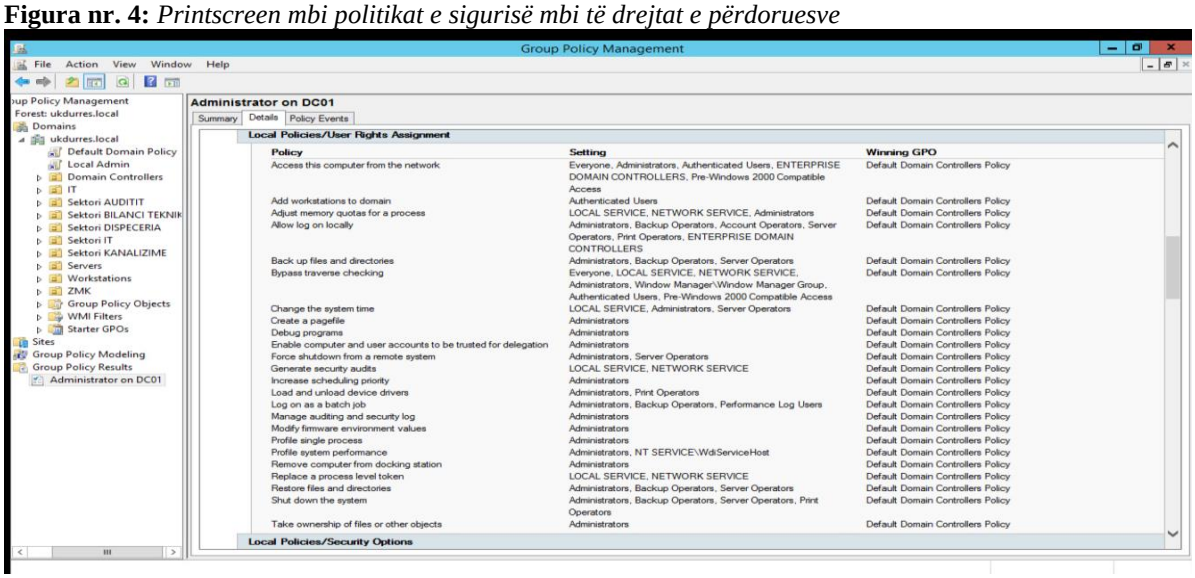
Disa nga risqet që vijnë si rezultat i konfigurimeve default i active directory:
-Ekziston rreziku i mos menaxhimit të politikave që mund t'i lejojë përdoruesit të marrin shumë të drejta;
-Rreziku që politikat e fjalëkalimit nuk janë në përputhje me kërkesat e entitetit ose praktikat më të mira. Kjo mund ta bëjë më të lehtë për personat e paautorizuar qasjen në rrjet dhe sisteme;
-Fjalëkalimet që nuk skadojnë kurrë mund të rezultojnë në akses të paautorizuar. Ky është veçanërisht një rrezik nëse ka llogari të përbashkëta përdoruesish ose llogari të sistemit me privilegje administratori. Kështu, ish-punonjësit mund të abuzojnë me këto të drejta;
- Llogaria e një përdoruesi me një fjalëkalim bosh mund të rezultojë në akses të paautorizuar;
-Nëse kompania ka vetëm një politikë fjalëkalimi, ajo duhet t'i përshtatet të gjitha nevojave, dhe për këtë arsye mund të jetë e dobët, etj.

Figura nr. 3: *Printscreen mbi politikat e sigurisë së fjalëkalimeve*



Burimi: *Grupi i auditimit*

Figura nr. 4: *Printscreen mbi politikat e sigurisë mbi të drejtat e përdoruesve*



Burimi: *Grupi i auditimit*

- ***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 planin e vazhdueshmërisë së biznesit 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 kundërshtim me këtë VKM, Ujësjellës Kanalizime Durrës si institucion që ka si synim kryesor realizimin e një shërbimi sa më cilësor për konsumatorin, duke synuar përmirësimin e menaxhimit në Sektorin e Furnizimit me Ujë dhe Kanalizimeve në qytet, për ta bërë atë më efiçent, të qëndrueshëm dhe efektiv në përputhje me ligjet dhe rregulloret në fuqi në Shqipëri, që posedon sistemin Flare Billing (*Sistemi për faturimin, shitjen dhe arkëtimin*), Mobiread *(Sistem për administrimin e procesit të mbledhjes së leximit të matësve të ujit*) etj, nuk ka marrë masa konkretisht sa më poshtë:
-Nga auditimi u konstatua se, Ujësjellës Kanalizime Durrës nuk disponon një infrastrukturë DRC (*disaster recovery center*) për rikuperimin dhe vazhdimësinë e punës pa ndërprerje si dhe sigurinë e ruajtjes së të dhënave në rastet e dështimit të qendrës së të dhënave primare[1], duke mbartur riskun për humbjen e të dhënave.
- Nuk disponon dokument të planeve 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;
-Nuk ka identifikuar sistemet ose pjesët e tyre të cilat janë kritike për ofrimin e shërbimit 24 orë në 7 ditë të javës.

Nisur sa më sipër dhe duke marrë parasysh që shoqëria UKD vitin tjetër do ristrukturohet në shoqëri Rajonale të Ujësjellës Kanalizime, ndryshim i cili do të sjellë bashkim me ujësjellësit e tjerë të Krujës, Kavajës dhe Rrogozhinës në një të vetëm. Në këtë mënyrë sistemi Flare ERP dhe Mobiread do të popullohen edhe me më shumë të dhëna mbi abonentët, duke e bërë më jetike nevojën për hartimin e këtyre planeve si dhe marrjen e masave afatgjata mbi ndërtimin e një qendre dytësore në rast të ndodhjes së ndonjë fatkeqësie në dhomën e serverëve primare.

- ***Menaxhimi i Incidenteve dhe Problemeve***

Për periudhën e audituar, në mungesë të procedurave të shkruara, risqet menaxhohen mbi bazë ngjarjesh. Suporti dhe mbështetja teknike dhe logjike për operacionet TI që ndihmojnë mbarëvajtjen e strukturave të institucionit kryhen nëpërmjet shkëmbimeve verbale dhe nëpërmjet e-mail-eve. Nga auditimi u konstatua se institucioni nuk ka hartuar politika të ruajtjes së dokumenteve dhe nuk ka të dokumentuar një plan masash për identifikimin, trajtimin e gabimeve, problemeve dhe incidenteve që mund të ndodhin në infrastrukturën TI. Duke mos realizuar identifikimin e risqeve, ujësjellësi rrezikon që ngjarjet të përsëriten dhe mënyra dhe koha e zgjidhjes së tyre është e papërcaktuar duke rrezikuar mbarëvajtjen e punës së sistemeve, ndërprerjen e shërbimeve etj. Identifikimi i risqeve çon në gjetjen e zgjidhjeve për t'i trajtuar ato dhe për të parandaluar ndodhjen e incidenteve të ngjashme në të ardhmen dhe në mënyrë që funksionet e institucionit të jenë të mbrojtura.
Mungesa e masave dhe mungesa e rregullores për trajtimin e incidenteve bën që UKD të mos identifikojë dhe menaxhojë risqet me efekt negativ në TI dhe në proceset e punës si dhe sjell mos dokumentim dhe mos lënie gjurmësh për trajtimin e gabimeve ose incidenteve nga punonjësit e TI.

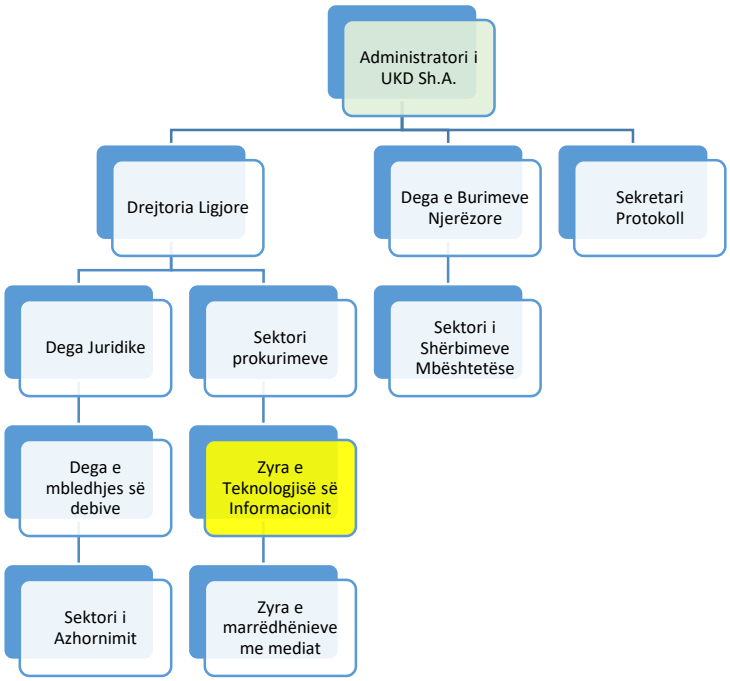
[1] *Dhoma e serverëve e UKD e lokalizuar në katin e dytë tek një prej godinave qendrore të UKD*

-Menaxhimi i ndryshimeve.
Nga auditimi u konstatua se Ujësjellës Kanalizime Durrës nuk disponon procedura për inicimin, rishikimin dhe aprovimin e ndryshimeve, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve.

➢ ***Vlerësimi i Burimeve Njerëzore në TIK***

Për kryerjen e funksioneve, përgjegjësive, UKD ka një strukturë organizative e cila është e ndërtuar mbi bazën e Drejtorive, sektorëve dhe njësive të varësisë dhe veprimtaria e të cilave rregullohet nëpërmjet dokumenteve të rregullores së UKD.
Numri i përgjithshëm i punonjësve të Ujësjellës Kanalizime Durrës Sh.A për vitin 2021 është gjithsej 763 punonjës.

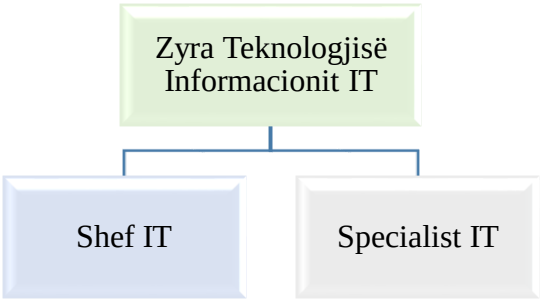
Figura nr. 5: *Në figurën e mëposhtme paraqitet pozicionimi i zyrës së IT-së, në strukturën organike të UKD.*



Burimi: *UKD. Punoi grupi i auditimit.*

Shoqëria UKD Sh.a ka të miratuar në organigramën e saj Zyrën IT. Zyra e IT referuar strukturës së miratuar ka në përbërjen e saj 2 punonjës: Shefin e IT dhe specialistin e IT, i cili gjatë fazës së auditimit në terren iku nga puna dhe struktura e zyrës së IT-së mbeti vetëm me përgjegjësin e sektorin.

Figura nr. 6: *Struktura e zyrës së Teknologjisë së Informacionit*



Burimi: *UKD. Punoi grupi i auditimit*

Duke vlerësuar rëndësinë e menaxhimit të burimeve njerëzore IT në UKD nga auditimi u konstatua se:

Nisur nga objektivat e UKD, nga shtrirja e teknologjisë së informacionit në institucion si dhe nga rëndësia e të dhënave që ruhen dhe përpunohen nga zyra e Teknologjisë së Informacionit për mirëmbajtjen administrimin dhe menaxhimin e sistemeve të informacionit Flare ERP, Mobiread, Oxana si dhe sistemi GIS QMAP, grupi i auditimit gjykon që organizimi i strukturës së IT-së në nivel zyre në varësi direkte nga Drejtoria Ligjore dhe me një staf shumë të vogël, nuk i përgjigjet shtrirjes së teknologjisë së informacionit në UKD duke sjellë uljen e ndikimit të IT-së në qeverisjen e shoqërisë UKD si dhe zbeh ndikimin e varësisë direkt nga menaxhimi i lartë.
Gjithashtu, detyrat e specialistëve të zyrës së TI-së janë jo të mire përcaktuara dhe nuk përputhen me detyrat reale që ata kryejnë.

Për sa është trajtuar në këtë pikë të Raportit Përfundimtar të Auditimit është mbajtur Aktkonstatimi nr. 1, datë 11.11.2022, protokolluar në UKD me shkresën nr. 7607/1, datë 11.11.2022, si dhe është trajtuar në faqet 10-23 të Projektraportit të Auditimit mbi të cilin janë paraqitur observacione mbi Aktkonstatimin nr. 1, me shkresën nr. 7607/3, datë 18.11.2022, protokolluar në KLSH me nr. 817/3, datë 05.12.2022. Në shkresën e sipërpërmendur subjekti i audituar shprehet se, i ka pranuar të gjitha konstatimet e auditimit dhe do të marrë masat përkatëse për plotësimin e rekomandimeve.

1. Titulli i gjetjes: UKD Sh.A. nuk disponon regjistër risku institucional ku të përfshiheshin edhe risqet që lidhen me teknologjinë e informacionit

Situata: Nga administrimi i dokumentacionit për identifikimin dhe menaxhimin e riskut në teknologjinë e informacionit, u konstatua se UKD nuk disponon regjistër risku të përgjithshëm institucional, ku të përfshihen edhe risqet mbi IT dhe të mbulohen të gjithë aktivitet duke përfshirë këtu risqet mbi sistemet Flare ERP dhe Mobiread, proceset e menaxhimit të ndryshimit, etj. UKD nuk ka identifikuar dhe vlerësuar ngjarjet e mundshme që mund të kenë efekte negative përsa i përket arritjes së objektivave të shoqërisë.
Nisur sa më sipër rezulton se shoqëria UKD Sh.A. nuk ka hartuar regjistrin e riskut ku të përfshiheshin edhe risqet që lidhen me teknologjinë e informacionit, kjo mbështetur në nenin 11, pika 2, neni 12 pika 3/d si 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*", 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*".
Kriteri: 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*", 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*".
Ndikimi/efekti: Mos identifikimi i ndikimit të risqeve cënon ecurinë normale të punës së sistemeve, ndërprerjen e shërbimeve etj, si dhe rrezikon që mënyra dhe koha e zgjidhjes së problemeve të jetë e papërcaktuar.
Shkaku: Mos marrja e masave për identifikimin dhe dokumentimin e risqeve mbi TI.
Rëndësia: E Lartë
1.1.Rekomandim: Administratori i shoqërisë në bashkëpunim me Drejtorët e Drejtorive dhe Degëve të marrin masa për identifikimin dhe hartimin e regjistrit të riskut me qëllim analizimin dhe vlerësimin e risqeve, për të mos riskuar përmbushjen e objektivave të shoqërisë në përputhje me përcaktimet ligjore e nënligjore, në të cilin të përcaktohen edhe risqet në teknologjinë e informacionit. Gjithashtu të marrin masa për hartimin dhe dokumentimin e një

plani veprimi për minimizimin/ parandalimin e risqeve të identifikuara, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave.

2. Titulli i gjetjes: Dhoma e serverave në UKD nuk plotëson standardet e përcaktuara.
Situata: Nga auditimi u konstatua se ambienti fizik i dhomës së serverave ku janë hostuar serverat e sistemeve Flare ERP, Mobiread dhe Oxana si dhe disa pajisje të tjera nuk është në përputhje me standardet e përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (*Versioni 1.0, datë 02.12.2008*) miratuar nga AKSHI (*Agjencia Kombëtare e Shoqërisë së Informacionit*).
Kriteri: Rregullorja për ndërtimin e dhomës së serverëve (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI.
Ndikimi/efekti: Cënim i sigurisë, hyrje e paautorizuara dhe risk humbje të të dhënave
Shkaku: Mos njohje e bazës rregullatore mbi standardet dhe sigurinë fizike të ambienteve të infrastrukturave kritike.
Rëndësia: E Lartë
2.1.Rekomandim: UKD të marrë masa për planifikimin dhe ngritjen e një infrastrukture IT (ambienteve të dhomës të serverëve dhe rrjetin network) në përputhje me kushtet teknike të përcaktuara në rregulloren e miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK si dhe në përputhje me udhëzimet, standardet dhe praktikat më të mira kombëtare dhe ndërkombëtare.

3.Titulli i gjetjes: Problematika mbi sigurinë e aksesit dhe infrastrukturën network
Situata: *Nga auditimi mbi konfigurimet aktuale për switch-et kryesore u konstatua se:*
-Nuk janë marrë masat e nevojshme që useri admin të limitohet në logimin vetëm nga IP-të brenda rrjetit privat dhe nuk është e bllokuar që useri admin të logohet nga jashtë rrjetit, pra nga një rrjet publik;
-Nuk janë krijuar group users me nivele të ndara menaxhim/monitorim. Çdo veprim bëhet nga useri admin;
-Nuk janë krijuar zona me limite të caktuara për brenda LAN si dhe rrjeti nuk është i ndarë në VLAN (rrjete virtuale) çka do të bënte të mundur menaxhimin dhe lejimin e grupeve të IP-ve në shërbime të ndryshme sipas nevojave. Gjithashtu nuk është krijuar edhe një zonë Untrust e cila sipas konfigurimeve shërben për bllokimin e portave të shërbimeve si dhe bllokimin e IP-ve të cilat mund të paraqesin problematika ose sulme;
-Pajisja firewall ka të aktivizuar log çka bën të mundur për të verifikuar një sërë procesesh që routeri kryen si edhe ruajtjen e tyre.
Kriteri: Ligji nr. 2/2017 ‘’Për Sigurinë Kibernetike’; ISO/IEC 27001.
Ndikimi/efekti: Aksesi i paautorizuar dhe thyerje e mundshme e sigurisë së infrastrukturës network
Shkaku: Implementim i konfigurimeve jo të përshtatshme të sigurisë
Rëndësia: E Lartë
3.1.Rekomandim: Zyra IT pranë UKD të marrë masat e nevojshme për krijimin e konfigurimeve përkatëse në rrjetin e institucionit mbi logimin, konfigurimin dhe sigurinë e switch-ve dhe firewall-it. Të krijohen zona me limite të caktuara brenda LAN si dhe rrjeti të konfigurohet në VLAN (rrjete virtuale) për menaxhimin dhe lejimin e grupeve të IP-ve në shërbime të ndryshme sipas nevojave. Gjithashtu të merren masa për administrimin dhe implementimin e të gjitha konfigurimeve të nevojshme të evidentuara nga auditimi dhe të tjera të mundshme, me qëllim rritjen e sigurisë së infrastrukturës network.

4.Titulli i gjetjes: Mungesa e procedurave të backup-it dhe Planeve të vazhdimësisë së punës me qëllim garantimin e vazhdueshmërisë së ofrimit të shërbimeve në raste të jashtëzakonshme emergjencash.
Situata 1: *Nga auditimi u konstatua se:*

-Procedura e ndjekur për kryerjen e backup-ve nuk është e pasqyruar apo e dokumentuar në një dokument administrativ si Rregullore e Brendshme apo dokument tjetër TIK ku të përcaktohet mënyra e kryerjes së backup-ve, procesin e ruajtjes së të dhënave për sistemet në përdorim nga punonjësit e UKD;
-Procedurat e backup ndiqen nga operatori ekonomik që kryen mirëmbajtjen;
-Procedurat e rikthimit (restore) të të dhënave nuk testohen për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar për sistemet e sipërpërmendura;
-Ruajtja e backup në vende në distancë nuk realizohet;
-Në rastet kur të dhënat e backup-it janë të panevojshme nuk ekzistojnë procedura për mënyrën e nxjerrjes së tyre jashtë përdorimit;
-Nuk është e qartë nëse kontrollohet statusi i backup-it nëse procedura është kryer me sukses.
Situata 2: Nga auditimi u konstatua se, Ujësjellës Kanalizime Durrës nuk disponon një infrastrukturë DRC (*disaster recovery center*) për rikuperimin dhe vazhdimësinë e punës pa ndërprerje si dhe sigurinë e ruajtjes së të dhënave në rastet e dështimit të qendrës së të dhënave primare, duke mbartur riskun për humbjen e të dhënave.
- Nuk disponon dokument të planeve 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;
-Nuk ka identifikuar sistemet ose pjesët e tyre të cilat janë kritike për ofrimin e shërbimit 24 orë në 7 ditë të javës.
Kriteri: Standardet nga Autoriteti Kombëtar Për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) dhe praktikat më të mira kombëtare dhe ndërkombëtare (*COBIT dhe Manuali i Auditimit IT*).
Ndikimi/efekti: Humbje e të dhënave dhe risk për vazhdimësinë e punës dhe ndërprerjes së shërbimeve.
Shkaku: Mos zbatim i standardeve të sigurisë mbi ruajtjen dhe përpunimin e informacionit
Rëndësia: E Lartë
4.1.Rekomandim: Strukturat drejtuese në UKD në bashkëpunim me zyrën e IT-së të marrin masa për ndërtimin dhe hartimin e planeve të vazhdimësisë së biznesit duke përfshirë planet për backup për sistemet, pajisjet kompjuterike dhe të dhënat, me qëllim garantimin e sigurisë së informacionit dhe uljen e riskut për ndërprerjen e shërbimeve dhe vazhdimësisë së punës.

4.2.Rekomandim: UKD duke marrë në konsideratë që në të ardhmen do të ristrukturohet në një shoqëri Rajonale të Ujësjellës Kanalizime, ndryshim i cili do të sjellë bashkim me ujësjellësit e tjerë në një të vetëm, të bëjë të mundur marrjen e masave afatgjata për planifikimin dhe ngritjen e një infrastrukture DRC në përputhje me kushtet teknike të përcaktuara aktet ligjore dhe nënligjore, që parashikojnë përcaktimin e standardeve të TIK si dhe në përputhje me udhëzimet, standardet dhe praktikat më të mira kombëtare dhe ndërkombëtare në lidhje me ndërtimin e një site dytësor, me qëllim mundësimin e ofrimit të shërbimit pa ndërprerje dhe parandalimin e humbjes ose të shkatërrimit aksidental të të dhënave, në rastet e dështimit të qendrës së të dhënave primare.

5.Titulli i gjetjes: Siguria e rrjetit të UKD është e kompromentuar pasi nuk ka Active Directory dhe Domain Controller për një identifikim të qendërzuar dhe sigurt.

Situata: Nga administrimi i dokumentacionit u konstatua se:
-UKD, ka investuar në ngritjen e Active Directory për menaxhimin e userave, pajisjeve, aplikacioneve dhe marrjen e shërbimeve me anë të një autentifikimi të vetëm "*single sign in*", por nuk e ka vënë në përdorim akoma Active Directory. duke mos përdorur të gjitha përfitimet e saj.
-Të gjitha konfigurimet e Active Directory janë by default, pra konfigurimi i politikave të sigurisë mbi fjalëkalimet, të drejtat e përdoruesve, të dhënat e sigurisë, etj, janë në gjendjen fillestare të lënë nga sistemi në momentin e implementimit të aplikacionit.
Disa nga risqet që vijnë si rezultat i konfigurimeve default i active directory:
-Ekziston rreziku i mos menaxhimit të politikave që mund t'i lejojë përdoruesit të marrin shumë të drejta;
-Rreziku që politikat e fjalëkalimit nuk janë në përputhje me kërkesat e entitetit ose praktikat më të mira. Kjo mund ta bëjë më të lehtë për personat e paautorizuar qasjen në rrjet dhe sisteme;
-Fjalëkalimet që nuk skadojnë kurrë mund të rezultojnë në akses të paautorizuar. Ky është veçanërisht një rrezik nëse ka llogari të përbashkëta përdoruesish ose llogari të sistemit me privilegje administratori. Kështu, ish-punonjësit mund të abuzojnë me këto të drejta;
- Llogaria e një përdoruesi me një fjalëkalim bosh mund të rezultojë në akses të paautorizuar;
-Nëse kompania ka vetëm një politikë fjalëkalimi, ajo duhet t'i përshtatet të gjitha nevojave, dhe për këtë arsye mund të jetë e dobët, etj.
Kriteri: Politikat e sigurisë së informacionit mbulojnë të gjithë risqet operacionale dhe ka mundësi të mbrojë në mënyrë të arsyeshme të gjithë asetet e informacioneve kritike kundrejt humbjeve, dëmtimit dhe abuzimit.
Politikat e sigurisë së informacionit janë të afta të mbrojnë të gjithë informacionin konfidencial lidhur me palët e brendshme dhe të jashtme detyra dhe përgjegjësi të qarta të IT lidhur me Politikat e Sigurisë së Informacionit (Referuar ISO 27000). ISO/IEC 27002:2013
Për praktikat më të mira mbi konfigurimin e politikave të sigurisë (GPO) së Active Directory, referojuni sa më poshtë:
http://technet.microsoft.com/en-us/library/cc773365(WS.10).aspx
Strong passwords: http://technet.microsoft.com/en-us/library/cc728372(WS.10).aspx
Password requirements: http://technet.microsoft.com/en-us/library/cc772803(WS.10).aspx
Complex password: http://technet.microsoft.com/en-us/library/cc786468(WS.10).aspx
http://technet.microsoft.com/en-us/library/cc773388(WS.10).aspx
http://technet.microsoft.com/en-us/library/cc780182(WS.10).aspx
Ndikimi/Efekti: Kompromet im i qasjes në sisteme, humbje të informacionit, etj.
Shkaku: Mos zbatim praktikave më të mira (Ref. ISO 27000 Sistemi i menaxhimit të sigurisë së informacionit). ISO/IEC 27002:2013, *http://technet.microsoft.com/en-us/library/cc773365(WS.10).aspx*
Rëndësia: E Lartë
5.1.Rekomandim: UKD të marrë masa për konfigurimin dhe vendosjen në përdorim të Active Directory, me qëllim standardizimin e infrastrukturës IT, rritjen e sigurisë së rrjetit si dhe garantimin e një identifikimi të qendërzuar dhe të sigurt.
Për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhim të shërbimeve, konfigurimi i politikave të sigurisë së Active Directory duhet të realizohet sipas rëndësisë dhe në përputhje me standardet me të mira, në mënyrë që rritet niveli i sigurisë së aksesit.

6.Titulli i gjetjes: Mos menaxhim i incidenteve dhe ndryshimeve, dhe mungesa e plan veprimit për minimizimin e risqeve.
Situata: Për periudhën e audituar, u konstatua se UKD nuk ka politika të ruajtjes së dokumenteve dhe nuk ka të dokumentuar një plan masash për identifikimin, trajtimin e gabimeve dhe incidenteve që mund të ndodhin në infrastrukturën IT, dhe në mungesë të procedurave të shkruara, risqet menaxhohen mbi bazë ngjarjesh. Suporti, mbështetje teknike

dhe logjike për operacionet IT që ndihmojnë mbarëvajtjen e strukturave të institucionit, kryhen nëpërmjet shkëmbimeve verbale dhe nëpërmjet e-mail-eve.
Ndikimi/efekti: Mos realizim i objektivave, shkelje të sigurisë, humbje të të dhënave.
Shkaku: Mos zbatim i 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".
Rëndësia: E lartë
6.1.Rekomandim: Strukturat Drejtuese në UKD në bashkëpunim me zyrën IT të marrin masa për identifikimin, dokumentimin dhe monitorimin e incidenteve si dhe menaxhimin e ndryshimeve dhe dokumentimin e tyre.

7. Titulli i gjetjes: Hierarkia dhe organizimi i strukturës TIK.
Situata: Nga auditimi u konstatua se funksionimi dhe organizimi i strukturës së IT-së në nivel zyre nën varësi të Drejtorisë ligjore dhe me një staf shumë të vogël, nuk i përgjigjet shtrirjes së teknologjisë së informacionit në UKD duke sjellë uljen e ndikimit të IT-së në qeverisjen e shoqërisë si dhe zbeh ndikimin e varësisë direkt nga menaxhimi i lartë.
Kriteri: Standardet ndërkombëtare të TIK në organizimin funksional të strukturave.
Ndikimi/efekti: Mos pasqyrimin e qartë të objektivave të shoqërisë lidhur zhvillimet teknologjike dhe zbehje e ndikimit të strukturave TIK në vendimmarrje.
Shkaku: Paqartësi mbi rëndësinë e strukturave TIK dhe mos zbatim i praktikave më të mira të fushës.
Rëndësia: E Lartë
7.1.Rekomandim: Strukturat drejtuese të UKD, duke marrë në konsideratë kohën, burimet e nevojshme të analizojnë mundësinë e ndryshimeve strukturore të strukturës ekzistuese IT me qëllim rritjen e rolit të saj dhe të marrin masa për ngritjen në nivel të strukturës së IT nga nivel zyre në nivel Drejtorie.

III.2.2. Auditimi i Sistemeve

Objektivi i auditimit të sistemeve dhe kontrolleve të aplikacioneve, për të dhënat Input / Output që UKD administron, është vlerësimi mbi efektivitetin e ndërtimit, operimit të kontrolleve të brendshme dhe saktësinë e funksionaliteteve që lidhen me procese të automatizuara si rezultat i zhvillimit informatik, që shoqëria ka pasur gjatë viteve. Po ashtu dhe auditimin mbi menaxhimin e përdoruesve dhe të drejtat e tyre në sistemin informatik.

Në përmbushje të drejtimit të auditimit "*Auditimi i sistemeve*", u shqyrtuan dokumentacionet e mëposhtme:

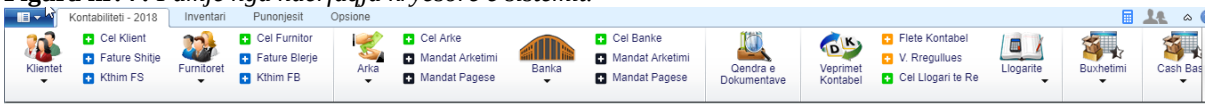
- Përshkrim i përgjithshëm i sistemit të teknologjisë së informacionit në UKD;
- Të dhënat e gjeneruara nga sistemi për shërbimet e ofruara;
- U mor akses me përdorues me të drejta "lexues" në sistemin Flare ERP;
- Aktet rregullative të shoqërisë që lidhen me sistemet dhe veprimet operacionale brenda dhe jashtë sistemit;
- Manualet e përdorimit të sistemeve;
- Intervista të drejtpërdrejta me punonjësit që kryenin apo administronin shërbime të caktuara;
- Të dhënat për përdoruesit e sistemeve Flare ERP dhe Mobiread;
- Vizita në terren;
- Analizë e performancës së sistemit;
- Etj.

Hyrje:

Sistemi Flare ERP:

Sistemi Flare ERP është implementuar për herë të parë në vitin 2014, dhe është i përbërë nga modulet Flare Accounting, Flare HR & Payroll, Flare Billing.

Figura nr. 7: *Pamje nga ndërfaqja kryesore e sistemit.*

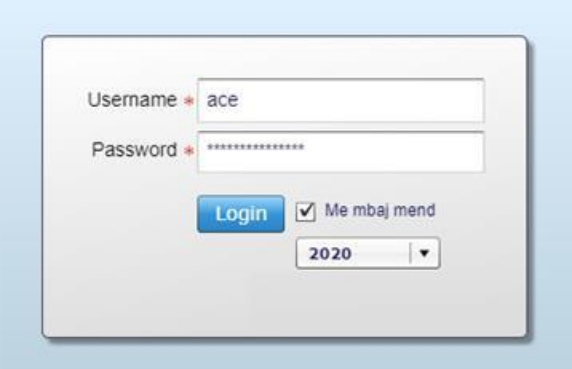


Burimi: *UKD, sistemi Flare ERP*

Programi është i ndërtuar mbi katër menu bazë që janë: a) Kontabiliteti b) Inventari c) Punonjësit d) Opsionet.

Moduli Flare Billing ose Moduli i Faturimit është një aplikacion që aksesohet online, i cili mundëson regjistrimin e të dhënave për klientët që do të faturohen; krijon artikujt dhe përcakton nivelet e çmimeve të tyre; krijon plane tarifore me mundësi të ndryshme të mënyrës së llogaritjes; gjeneron faturat; menaxhon procesin e mbledhjes së pagesave; është i integruar me sisteme të palëve të treta për marrje të detyrimeve dhe pagesave; gjeneron raporte etj.

Hyrja në modulin e faturimit paraqitet si më poshtë



Programi funksionon në bazë të roleve dhe të drejtave. Nëse një përdorues ka të drejta atëherë ai mund të logohet kudo ku ndodhet, ndërkohë që e drejta mund të kufizohet nga administratori i sistemit për të patur akses të programit, vetëm nga vendet e punës.

Figura nr. 8: *Pas logimit ndërfaqja fillestare paraqitet si më poshtë.*

Burimi: *UKD, sistemi Flare ERP*

Për të aksesuar sistemin fillimisht duhet të instalohet lokalisht në çdo pc aplikacioni përkatës, bashkë me konfigurimet përkatëse dhe pasi hapet aplikacioni, shfaqet mundësia për të hyrë në sistem (duhet shkruar username ose emrin e përdoruesit me të cilin identifikohen në sistem, i cili është regjistruar më parë dhe password-in ose fjalëkalimin i cili është personal për secilin përdorues). Të dyja këto të dhëna "Username" dhe "Password" janë të domosdoshme. Nuk mund të fitohet akses në sistem në rast se këto të dhëna nuk shkruhen saktësisht.

-Moduli Flare Accounting

Moduli i kontabilitetit përdoret nga Arka për pagesat, debitë etj,

-Moduli Flare HR & Payroll

Moduli Flare HR & Payroll përdoret për të menaxhuar të dhënat e nevojshme për çdo punonjës të kompanisë, kontratat e tyre, koha e punës, llogaritja e pagave në kushte të ndryshme, menaxhimi i dokumenteve dhe performancën e punonjësve.

Sistemi Mobiread:

Sistemi Mobiread është implementuar në vitin 2016 për mbledhjen dhe hedhjen e leximeve të matësve, nga lexuesit e UKD. Kjo platformë është një platformë proprietare më të drejta autori të zotëruara nga OE që e ka zhvilluar dhe implementuar atë.

Sistemi Mobiread është i ndërtuar në platformën PHP, MySQL, html/javscript, si dhe sistemi Android për pajisjet PDA që përdorin lexuesit për hedhjen e të dhënave të leximeve të matësave. Qëllimi kryesor i këtij sistemi është marrja e leximeve nga pajisjet PDA dhe dërgimi i këtyre të dhënave në sistemin Flare ERP, Moduli Billing në mënyrë që të realizohet faturimi i saktë i konsumatorëve. Për të bërë të mundur këtë proces, sistemi "Mobiread" merr të dhënat fillestare nga sistemi Flare, Moduli Billing. PDA-të marrin të dhënat e abonentëve që ju nevojiten dhe i kthejnë sërish sistemit të dhënat e përditësuara me leximet përkatëse. Në fund të këtij procesi, sistemi i dërgon këto të dhëna në sistemin Flare, Moduli Billing. Për të aksesuar sistemin Mobiread është e njëjta procedurë sikurse edhe aksesimi i sistemit Flare ERP dhe më pas kërkohen të dhënat si username dhe password.

Sistemi Oxana:

Sistemi i fiskalizimit është një aplikacion online, i cili mbulon procesin e shitjeve dhe realizon fiskalizimin e faturave për abonentët e UKD. Ky sistem është implementuar në vitin 2021. Në këtë sistem gjithashtu mund të menaxhohen të dhënat e nevojshme për çdo artikull, shitje dhe çdo detaj për sa i përket shitjeve apo klient, etj. Ky sistem aksesohet online në adresën "fiscalization.oxana.al".

a. Të drejtat e përdoruesve dhe menaxhimi i tyre

Përdoruesit e sistemit Flare ERP

Administrimi dhe menaxhimi i përdoruesve të sistemeve Flare ERP realizohet nga përgjegjësi i zyrës së IT, në UKD, duke ushtruar atributet dhe funksionet e përcaktuara nga sistemi.

Përdoruesit e sistemit Flare ERP janë të kategorizuar në role dhe përgjegjësi për secilin përdorues. Në sistemin Flare ERP administratori i sistemit është i kategorizuar në rolin "Sys admin". Sys Admin ushtron funksionet viewer dhe ka të drejta mbi përdoruesit.

Sistemi Flare ERP ka 87 usera aktiv. Secili user është i kategorizuar sipas rolit të tij. Rolet e përcaktuara në sistem janë në total 53 role të ndryshme që kategorizohen sipas pozicionit të punës që ushtron përdoruesi. Disa nga rolet janë:

- Admin
- Admin viewer
- DBNJ - Llogaritje Paga
- DBNJ - Shef I Departamentit Burime Njerëzore
- Dega e mbledhjes se debive - Operator
- Dega e Shitjes - Kryetar/e Dega e shitjes
- Dega e Shitjes - Llogaritare e Pare
- Dega e Shitjes - Operator Faturimi
- Dega Teknike - Operator
- Finance - Billing
- Finance - Operator
- Finance - Operator Blerje + Shitje + Arke + Banke
- Finance - Operator Magazine
- Finance - përgjegjës kontabilitet
- Finance - Viewer
- Finance Viewer Only
- IT Management
- Etj.

➢ ***Manualet e sistemit Flare ERP:***

Këto manuale shërbejnë si udhëzues për të gjithë përdoruesit që kanë të drejtë të aksesojnë sistemin Flare ERP. Sistemi i mundëson shoqërisë trajtimin dhe menaxhimin e abonentëve, matësave, tarifave, artikujve, nivelet e çmimeve, leximet e matësave dhe menaxhimin e abonentëve në qytetin e Durrësit dhe zonave që UKD menaxhon. Çdo përdorues identifikohet në sistem me një username përkatës. Regjistrimi i tyre realizohet nga administratori i sistemit, i cili është përgjegjës për konfigurimet e ndryshme të sistemit dhe userave.

1. *Manual përdorimi për modulin "Flare Accounting"*
2. *Manual përdorimi për modulin "Flare Billing"*
3. *Manual përdorimi për modulin "Flare HR and Payroll"*

Këto manuale përdorimi u shpjegojnë përdoruesve se si të kryejnë të gjithë proceset e përdorimit të sistemit duke filluar që nga hapja e userave sipas roleve përkatës deri në shpjegimin e menuve dhe nënmenuve përkatëse në sistem. Sistemi është i përbërë nga 4 module dhe secili modul ka manualin përkatës.

Nga auditimi mbi aktet rregullatore të manualeve të përdorimit të sistemit Flare ERP u konstatua se dy nga tre manualet e moduleve të sistemit nuk janë të përditësuara.

<u>Përdoruesit e sistemit Mobiread</u>

Administrimi dhe menaxhimi i përdoruesve të sistemit Mobiread realizohet nga përgjegjësi dhe specialisti i zyrës së IT, në UKD, duke ushtruar atributet dhe funksionet e përcaktuara nga sistemi. Përdoruesit e sistemit Mobiread janë të kategorizuar në role dhe përgjegjësi për secilin përdorues. Në sistemin Mobiread administratori i sistemit është i kategorizuar në rolin "Admin" dhe ka të drejta të plota mbi çdo gjë në sistem.

Sistemi Mobiread ka 115 usera aktiv. Secili user është i kategorizuar sipas rolit të tij. Rolet e përcaktuara në sistem janë në total 18 role të ndryshme që kategorizohen sipas pozicionit të punës që ushtron përdoruesi. Më konkretisht rolet janë:

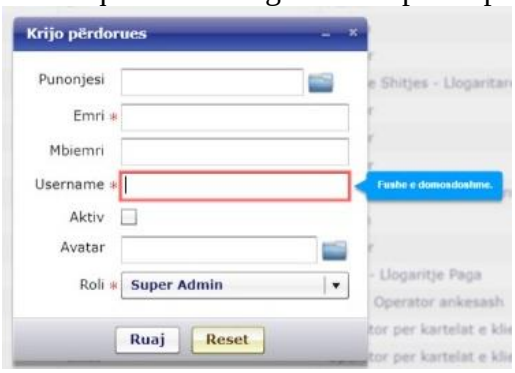
- Admin
- Admin Viewer

- Administrimi i anomalive
- Ankesa
- Azhornimi - Anomalite
- Azhornues
- Billing
- Dega teknike - Anomalite
- Inspektoriati - Anomalite
- Lexues
- Manager
- Office manager
- READONLY
- Sektori i matesave - Anomalite
- SSHK - Anomalite
- SSHK - Rol i avancuar
- Verifikues
- Viewer - photo

Duke qenë se shoqëria UKD, vitin tjetër ndryshon strukturën dhe mënyrën e funksionimit si dhe shtimin e zonave të tjera me abonentë, duke u konvertuar në shoqëri rajonale, duhet që këto manuale të pësojnë ndryshime, përditësime në përputhje me bazën ligjore të funksionimit të shoqërisë; funksionalitet e sistemit në qoftë se do shtohen; ndryshimet strukturore të burimeve njerëzore; sistemi mund të pësojë ndryshime në ndërfaqe dhe funksionalitete etj, të gjitha këto duhen reflektuar apo përditësuar në manualet e sistemit, nga ku rolet dhe përgjegjësitë mund të pësojnë ndryshime.

- ***Mënyra e çeljes së përdoruesve dhe politikat e vendosjes së fjalëkalimeve të përdoruesve dhe siguria e tyre***

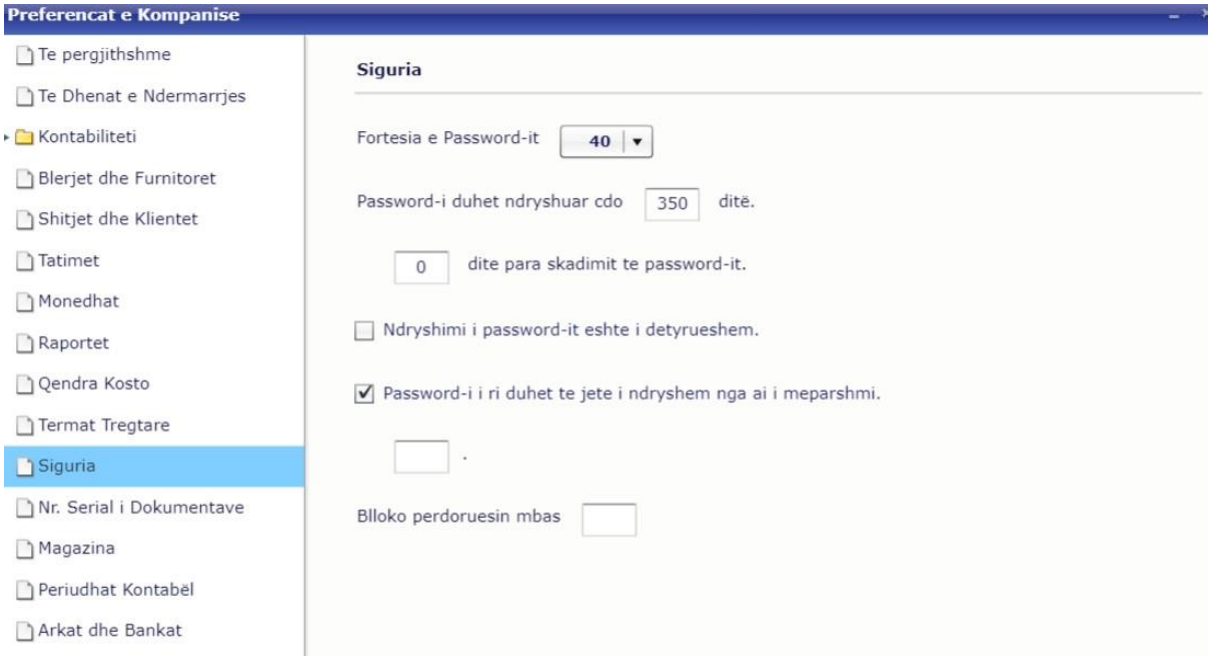
Të dhënat që kërkohet nga sistemi për tu plotësuar në rast të krijimi të një useri të ri:



Çelja e përdoruesit në sistemin Flare ERP
(*Të dhënat që kërkohen*)

Çelja e përdoruesit në sistemin Mobiread
(*Të dhënat që kërkohen*)

Figura nr. 9: *Opsionet e kompleksitetit të sigurisë së fjalëkalimit në sistemin Flare ERP.*



Burimi: *UKD, sistemi Flare ERP*

Hapja e userave në sistemet ERP dhe Mobiread realizohet vetëm për ata punonjës që janë të destinuar për të patur aktivitet dhe funksione në sistemet përkatëse sipas pozicionit të emërimit. Çelja e përdoruesve në sistemin Flare ERP dhe Mobiread realizohet si më poshtë:

-pasi punonjësi merr emërimin e punësimit në UKD, kjo shkresë i dërgohet edhe zyrës së IT, e cila njoftohet për emërimin e punonjësit. Regjistrimin e parë të punonjësit në sistemin ERP e bëjnë burimet njerëzore të cilat shtojnë përdoruesin e ri me anë të modulit *Flare HR and Payroll*, punonjësin bashkë më të dhënat (*emër, mbiemër dhe ID personale*).

-kur shkresa e emërimit vjen, zyrës së IT-së nuk i përcaktohet se çfarë funksioni konkret duhet të realizojë punonjësi, kështu që specialistëve të IT-së u duhet të pyesin verbalisht burimet njerëzore për të saktësuar dhe përcaktuar rolin në sistem të punonjësit dhe më pas të realizojnë hapjen e userit në sistem duke e zgjedhur atë në listën e punonjësve që më parë është shtuar nga burimet njerëzore.

-për krijimin e userit nga specialisti i IT-së popullohen të dhënat manualisht, edhe username popullohet manualisht nga specialisti. Passwordin e userit, sistemi e merr automatikisht siç është username i përdoruesit dhe sistemi nuk të lejon të menaxhosh këtë funksion.

-pasi popullohen të dhënat e përdoruesit dhe përcaktohet roli i tij, punonjësit të sapo emëruar u kërkohet emaili personal dhe numri i telefonit në mënyrë që ti dërgohen kredencialet e emailit të punës dhe userit të hapur në sistemet përkatëse. Në këtë email, punonjësi informohet gjithashtu edhe për ndryshimin e passwordit.

Fjalëkalimi i secilit përdorues në sistemin ERP në momentin e çeljes vendoset automatikisht nga sistemi i njëjtë me username-in e përdoruesit dhe nuk gjenerohet nga sistemi një password automatik i tipit kompleks. Përdoruesi sapo logohet (*first log-in*) me fjalëkalim fillestar, nuk i shfaqet automatikisht nga sistemi tabela e cila të kërkon vendosjen e fjalëkalimit të ri, ruajtjen e tij dhe rilogimin përsëri me anë të fjalëkalimit të ri por punonjësi informohet me email nga specialisti i IT që të ndërrojë passwordin. Pas një periudhe të standardizuar 350 ditore, sistemi kërkon rigjenerimin e një fjalëkalimi të ri. Në rast se punonjësi nuk e ndryshon fjalëkalimin fillestar dhe vazhdon të përdorë të njëjtin password, sistemi i jep akses pavarësisht se përdoruesi se ka ndryshuar passwordin. Kjo gjë rrit riskut për akses të paautorizuar dhe fshirje apo modifikim të të dhënave të populluara.

Nga intervistimi i specialistit të IT-së në UKD u konstatua se për sistemet Flare ERP dhe Mobiread nuk ka përdorues të jashtëm.

Nga auditimi mbi politikat e sigurisë së përdoruesve në sistemet ERP dhe Mobiread u konstatua se:

- Passwordin e userit, sistemi e merr automatikisht siç është username i përdoruesit dhe sistemi nuk të lejon të menaxhosh këtë funksion;
- Përdoruesi sapo logohet (*first log-in*) me fjalëkalim fillestar, nuk i shfaqet automatikisht nga sistemi tabela e cila të kërkon vendosjen e fjalëkalimit të ri;
- Në rast se punonjësi nuk e ndryshon fjalëkalimin fillestar dhe vazhdon të përdorë të njëjtin password, sistemi i jep akses pavarësisht se përdoruesi se ka ndryshuar passwordin. Nga të dhënat e ekstraktuara mbi përdoruesit e sistemeve vihet re se edhe pse kërkohet shumë herë reset të paswordit, përdoruesit vazhdojnë sërish me të njëjtat passworde;
- Siguria e vendosjes së fjalëkalimit nuk është e tipit kompleks ku të kërkohen të ketë minimumi 8 karaktere, të ketë të paktën 1 shkronje dhe 1 shifër.
- Nuk janë dokumentuar politikat e sigurisë të implementuara për përdoruesit e sistemit, si dhe detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre, bazuar në pikën 4 "*Kërkesat e Sigurisë*" pika a. të rregullores për "*Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike*" të miratuar nga AKCESK[2] me urdhrin nr. 86, datë 23.08.2019.
- Nuk janë dokumentuar politikat e sigurisë të implementuara për fjalëkalimet e sistemeve qendrore dhe administrimit bazuar në pikën 4 "*Kërkesat e Sigurisë*" pika b. Të rregullores për "Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike" miratuara nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

➢ ***Analizimi i përdoruesve sipas roleve dhe atributeve në sistemin Flare ERP***

Përdoruesit e sistemit Flare ERP janë të kategorizuar në role dhe përgjegjësi për secilin përdorues. Në sistemin Flare ERP administratori i sistemit është i kategorizuar në rolin "Sys admin". Sys Admin ushtron funksionet viewer, si dhe ka të drejta mbi përdoruesit.

Sistemi Flare ERP ka në total 215 usera aktiv dhe jo aktiv. Përdoruesit Aktiv janë 87 usera aktiv në sistem të cilët janë të ndarë sipas roleve përkatëse. Rolet e përcaktuara në sistem janë në total 53 role të ndryshme që kategorizohen sipas pozicionit të punës që ushtron përdoruesi.

Figura nr. 10: *Figura e mëposhtme përmbledh llojet e atributeve për secilin rol në sistem.*

Roli	Pershkrimi	Krijuar
Super Admin	Ka te drejta te plota mbi cdo gje.	11/08/2011
Finance - Drejtor Ekonomik	Finance - Drejtor Ekonomik	11/08/2011
Dega e Shitjes - Operator Faturimi	Dega e Shitjes - Operator Faturimi	11/08/2011
ZMK - pergjegjes e Zyres se Mardhenies se Klientit	ZMK - pergjegjes e Zyres se Mardhenies se Klientit	11/08/2011
DBNJ - Shef I Departamentit Burime Njerezore	DBNJ - Shef I Departamentit Burime Njerezore	11/08/2011
DBNJ - Llogaritje Paga	personi qe punon me llogaritjen e pagave	11/08/2011
itrack_team_member	Anetar skuadre	11/08/2011
itrack_admin	Administrator i modulit iTrack	11/08/2011
ITrack + billing		13/11/2012
itrak_team_leader	Drejtor skuadre per iTrack	16/01/2013
itrack_team_member_complaints	Hapje ankesash	16/01/2013
ZMK - Operator per kontratat e reja	ZMK - Operator per kontratat e reja	11/08/2011
Dega e Shitjes - Kryetar/e Dega e shitjes	Dega e Shitjes - Kryetar/e Dega e shitjes	11/08/2011
test	test	11/08/2011
ZMK - Operator	ZMK - Operator	11/08/2011
ZMK - Operatore Arke	Operator per hedhjen e arketimeve	11/08/2011
ZMK - Operator Ndryshim Emri	Te drejta mbi ndryshimin e emrit dhe mbylljen e kontrates	11/08/2011
ZMK - Operator per hedhjen e dokumentacionit	Operator per hedhjen e dokumentacionit	11/08/2011
Finance - Kontabilitet	Ka te drejta te plota mbi kontabilitetin.Te drejtat e modulit billing per klientet,arka dhe moduli baze	11/08/2011
Dega e Shitjes - Llogaritare e Pare	Dega e Shitjes - Llogaritare e Pare	11/08/2011
Viewer	thjesht shikues	11/08/2011
Finance - Operator Arke	Finance - Operator Arke	11/08/2011
Finance - Operator Magazine	Finance - Operator Magazine	11/08/2011

Burimi: *UKD, sistemi Flare ERP*

Nga auditimi mbi përdoruesit aktiv, të ndarë sipas roleve përkatëse në sistemin Flare ERP u konstatua se:

[2] *Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike*

-Detyra e administratorit të sistemit nuk është e atribuar me anë të shkresës zyrtare nga organet drejtuese të UKD në mënyrë që të përcaktohen qartë atributet dhe të gjitha detyrat e administratorit të sistemit.
-Në sistemin ERP nuk është e mirë përcaktuar forma e username, duke qenë se ajo popullohet manualisht, disa username kanë shkronjën e parë të emrit dhe pastaj mbiemrin, disa username kanë vetëm emrin e përdoruesit, disa emrin dhe një numër, disa vetëm një shkronjë, etj. Username-t nuk janë të standardizuar çka tregon që sistemi nuk ka mekanizma të kontrollit të inputit. Ka raste që username nuk lidhet fare me emrin e përdoruesit pasi username ka vetëm një shkronjë. Si më poshtë:

Përdoruesit aktiv të ndarë sipas roleve

Roli	Username	Status	Emri
Admin	a	1	Enor
	ace	1	Sistemi
	MarsiKx	2	Marsi
	sistemi	1	sistemi
Admin viewer	kasti.b	1	Kasem
DBNJ - Llogaritje Pa..	dervishrustemi	1	Dervish
DBNJ - Shef I Depart..	genti	1	Gentian
Dega e mbledhjes se	armando	1	Armando
debive - Operator	genta	1	Gentiana
	jdajko	1	Julinda
Dega e Shitjes - Krye..	m.xhaferi	1	Michela
Dega e Shitjes -	aida	1	Aida
Llogaritare e Pare	e.huqi	1	Erisa
	sonila.leka	1	Sonila
Dega e Shitjes -	anulakau	1	Anula
Operator Faturimi	arbiana	1	Arbiana
	doralda	1	Doralda
	enerjeta	1	Enerjeta
	irena	1	Irena
	jona.s	1	Jona
	klevisguce	1	Klevis
	maxi	1	Maxheliana
	morena	1	Morena

-Në rolin "*Admin*", janë aktiv 4 administrator me atributin që kanë të drejta mbi çdo gjë. Nga auditimi u konstatua se këta usera nuk identifikohet se çfarë procesesh mbulojnë në sistem, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Përdoruesit me username "*sistemi*", "*MarsiKx*" si dhe "*ace*" nuk identifikohen se çfarë procesesh mbulojnë në sistem dhe kujt useri i përkasin, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Kjo gjë përsëritet edhe në rolin Financë – operator. Gjithashtu ka përdorues që kanë rolin "Admin", ndërkohë që pozicioni i punës së këtyre përdoruesve nuk përputhet me rolin që kanë në sistem.

-Në rolin "Admin viewer", është aktiv vetëm një përdorues me atribute për të parë në sistem.

-Në rolin "Sys Admin" është aktiv një përdorues që është njëkohësisht përgjegjësi i zyrës së IT, dhe ka të drejta Viewer si dhe të drejta mbi përdoruesit. Pra përgjegjësi i zyrës IT që duhet të ishte në rolin e Super Admin, duke qenë së është administratori i sistemit, nuk ka të drejta të plota në sistem.

-Atributet dhe rolet e userave në sistemin ERP nuk janë të përcaktuara sipas detyrave dhe përgjegjësive të përcaktuara në rregulloren e brendshme për funksionimin e UKD por sipas funksionaliteteve që punonjësi ushtron në praktikë përgjatë procesit të punës;
-Një përdorues aktiv mund të autentifikohet në më shumë së një kompjuter. Pra me një username mund ta hapësh sistemin Flare ERP në të njëjtën kohë në më shumë se një kompjuter.

- ***Analizimi i përdoruesve sipas roleve dhe atributeve në sistemin Mobiread***

Administrimi dhe menaxhimi i përdoruesve të sistemit Mobiread realizohet nga përgjegjësi dhe specialisti i zyrës së IT, në UKD, duke ushtruar atributet e përcaktuara sipas funksioneve të tyre në sistem.

Përdoruesit e sistemit Mobiread janë të kategorizuar në role dhe përgjegjësi për secilin përdorues. Në sistemin Mobiread administratori i sistemit është i kategorizuar në rolin "Admin" dhe ka të drejta të plota mbi çdo gjë në sistem.
Sistemi Mobiread ka në total 189 usera aktiv dhe jo aktiv. Përdoruesit Aktiv janë 115 usera aktiv në sistem të cilët janë të ndarë sipas roleve përkatëse. Rolet e përcaktuara në sistem janë në total 18 role të ndryshme që kategorizohen sipas pozicionit të punës që ushtron përdoruesi.

Figura nr. 11: *Figura e mëposhtme përmbledh llojet e atributeve për secilin rol në sistem.*

Roli	Pershkrimi	Të Gjitha Krijuar
Admin	Ka te drejta te plota mbi cdo gje.	11/08/2011
Office user	Office user	11/08/2011
READONLY	User me me te drejta vetem lexim	11/08/2011
Manager	Te drejta menaxhuese	11/08/2011
Lexues	Roli Lexues nuk ka asnje te drejte ne sistem. Perdoret vetem per te mbajtur lexuesit qe punojne ne terren.	11/08/2011
Verifikues	Verifikues Leximesh	11/08/2011
Office manager	Monitoron konsumatoret, leximet, anomalite	11/08/2011
Azhornues	Azhornues	27/04/2015
Azhornimi - Anomalite	Ndjekja e anomalive nga azhornimi	11/08/2011
SSHK - Anomalite	Ndjekja e anomalive nga SSHK	11/08/2011
Inspektoriati - Anomalite	Ndjekja e anomalive nga inspektoriati	11/08/2011
Sektori i matesave - Anomalite	Ndjekja e anomalive nga sektori i matesave	11/08/2011
Dega teknike - Anomalite	Ndjekja e anomalive nga dega teknike	11/08/2011
SSHK - Rol i avancuar	SSHK - Rol i avancuar	11/08/2011
Viewer - photo	Shikon vetem foto per ankesat	12/08/2015
Billing	Kontroll mbi konsumet negative dhe shume here te larta se muaji i fundit	11/08/2011
Ankesa	Ankesa	02/12/2015
IT Management	IT Management	15/12/2015
Administrimi i anomalive	Administrimi i anomalive	11/08/2011
Admin Viewer	Ka te drejta te shohi te dhena ne sistem	11/08/2011

Burimi: *UKD, sistemi Mobiread*

Nga auditimi mbi përdoruesit aktiv, të ndarë sipas roleve përkatëse në sistemin Mobiread u konstatua se:

-Detyra e administratorit të sistemit nuk është e atribuuar me anë të shkresës zyrtare nga organet drejtuese të UKD në mënyrë që të përcaktohen qartë atributet dhe të gjitha detyrat e administratorit të sistemit.

-Në sistemin Mobiread nuk është e mirë përcaktuar forma e username, duke qenë se ajo popullohet manualisht, disa username kanë shkronjën e parë të emrit dhe pastaj mbiemrin, disa username kanë vetëm emrin e përdoruesit, disa emrin dhe një numër, disa vetëm një shkronjë, etj. Username-t nuk janë të standardizuar çka tregon që sistemi nuk ka mekanizma të kontrollit të inputit. Ka raste që username nuk lidhet fare me emrin e përdoruesit pasi username ka vetëm një shkronjë. Si më poshtë:

Përdoruesit aktiv të ndarë sipas roleve

Roli	Username	Status	Emri
Admin	ace	1	a
	denisgjoni	1	Denis
	mikela	1	Mikela
	s.kuqi	2	Sokol
Admin Viewer	mirela.h	1	Mirela
	suport	1	suport
Administrimi i anom..	amansaku	1	Arbiana
Ankesa	kllaftiu	1	Klodiana
Azhornimi - Anomali..	jdajko	1	Juli
Azhornues	azhornues1	1	azhornues 1
	azhornues2	1	azhornues 2
Dega teknike - Anom..	lfacja	1	Lorenc
	mballa	1	Marsida
Inspektoriati - Anom..	amyshketa	1	Aida
	ghoxha	1	Gentiana
Lexues	a.cerri	1	Adriana
	acapoku	1	Agetina
	admirtarko	1	Admir
	aidahoxha	1	Aida
	albanaselishta	1	Albana
	alfred	1	alfred
	ameta	1	albert
	andi.h	1	Andi
	anilakapedani	1	Anila
	aurel	1	Aurel
	ballanca	1	Albana
	buqe	1	Burbuqe
	dritagjoni	1	Drita

-Në rolin "*Admin*", janë aktiv 4 administrator me atributin që kanë të drejta mbi çdo gjë. Nga auditimi u konstatua se këta usera nuk identifikohet se çfarë procesesh mbulojnë në sistem, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Përdoruesit me username "*m.*" si dhe "*ace*" nuk identifikohen se çfarë procesesh mbulojnë në sistem dhe kujt useri i përkasin, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Kjo gjë përsëritet edhe në rolin Azhornues për userat "*azhornues 1 dhe 2*", në rolin Lexues për userat "lexues 2 dhe 3", në rolin Verifikues për userat "verifikues 1". Gjithashtu ka përdorues që kanë rolin "Admin", ndërkohë që pozicioni i punës së këtyre përdoruesve nuk përputhet me rolin që kanë në sistem.

-Rolin "Admin", e posedon edhe username "d.gj.", i cili sipas informacionit të dhënë ushtron pozicionin e drejtorit tregtar në UKD Sh.a, pra këtij useri i janë dhënë atributet e administratorit të sistemit, në mospërputhje me aktivitetin e punës që ushtron në sistem.

-Në rolin "Admin viewer", janë aktiv dy përdorues me atribute për të parë në sistem. Përdoruesi me username "suport" nuk identifikohet në sistem se kujt useri i përket, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor.

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

Auditimi mbi sistemet e teknologjisë së informacionit u fokusua në sistemet e quajtur Flare ERP dhe Mobiread të cilët janë sistemet kryesore për administrimin e procesit të regjistrimit, faturimit, leximit të konsumatorëve si dhe menaxhimit të shërbimit të furnizimit me ujë të pijshëm të konsumatorëve dhe shitja e tij, në UKD.

Për përdorimin e sistemeve Flare ERP dhe Mobiread, fillimisht duhet që të instalohen si program në kompjuter në mënyrë që të aksesohen dhe përdoren. Specifikë tjetër e këtij sistemi është që mund të aksesohet vetëm në rrjetin e infrastrukturës së UKD ose me VPN dhe nuk mund të aksesohen jashtë rrjetit me ip ose webservice.

Sistemi Flare ERP

Sistemi Flare ERP është implementuar për herë të parë në vitin 2014, dhe është i përbërë nga modulet Flare Accounting, Flare HR & Payroll, Flare Billing.
Sistemi Flare ERP është një platformë proprietare me të drejta autori të zotëruara nga OE që ka ndërtuar dhe implementuar këtë sistem. Ai është i ndërtuar në PHP, MySQL.
Ky sistem është i ndërtuar mbi katër module bazë që janë a) Kontabiliteti b) Inventari c) Punonjësit d) Opsionet. Moduli Flare Billing ose Moduli i Faturimit është një program që aksesohet online, i cili mundëson regjistrimin e të dhënave për klientët që do të faturohen; krijon artikujt dhe përcakton nivelet e çmimeve të tyre; krijon plane tarifore me mundësi të ndryshme të mënyrës së llogaritjes; gjeneron faturat; menaxhon procesin e mbledhjes së pagesave; është i integruar me sisteme të palëve të treta për marrje të detyrimeve dhe pagesave; gjeneron raporte etj.

Hyrja dhe identifikimi i përdoruesve të sistemit Flare ERP kryhet me emër përdoruesi dhe fjalëkalim. Fjalëkalimet për përdoruesin janë trajtuar gjerësisht më lart në materialin mbi politikat e përdoruesve.

Nga auditimi u konstatua se:
-Administrimi dhe menaxhimi i databazës së sistemit Flare ERP realizohet nga OE. Ky OE gjithashtu është duke ofruar suport për këtë sistem.
Në sistemin Flare ERP administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Sys admin". Sys Admin ushtron funksionet viewer dhe ka të drejta mbi përdoruesit.

-Detyra e Administratorit të sistemit dhe Administratorit të bazës së të dhënave nuk janë atribuuar me anë të një shkrese zyrtare nga organet drejtuese të UKD, ku punonjësit e zyrës IT të janë emëruar zyrtarisht si Administratorë për administrimin e bazës së të dhënave për të ushtruar atributet e përcaktuara sipas funksioneve të tyre dhe të gjitha detyrat e administratorit mbi administrimin e bazës së të dhënave të sistemit.

Të dhënat input dhe output:

Të dhëna Input:
- Të dhënat e abonenteve, matësve, tarifave, leximeve të matësve;
- Të dhënat financiare dhe kontabile;
- Të dhënat e punonjësve, koeficientet dhe logjika e skemës së pagave;
- Të dhënat e faturave;
- Leximet e matësve të ujit të abonentëve me PDA.

Të dhënat output:
- Leximet e dërguara në sistemin Flare ERP, moduli i Billing, raporte të ndryshme;
- Faturat mujore;
- Raporte financiare;
- Raporte Pivot;
- Raporte që lidhen me zërat e pagave, raporte që lidhen me të dhënat e punonjësve;
- Fiskalizimi i faturave.

➢ **Ndërveprimi i sistemit Flare ERP me sisteme të tjera (web service-et):**

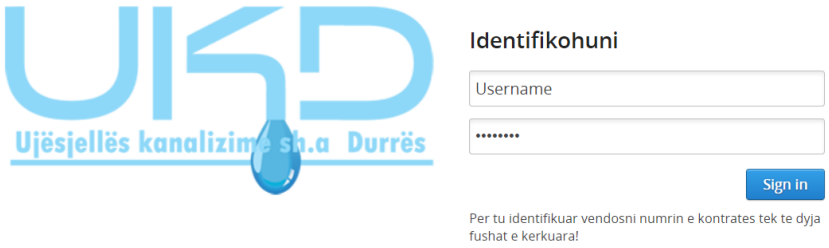
Sistemet Flare ERP dhe Mobiread shkëmbejnë të dhëna me njëri tjetrin vetëm për sa i përket abonentëve dhe të dhënave që lexohen nga PDA-të pra të dhënat e leximit ose të dhënat afrofe ose kur plotësohen manualisht vlerat e leximit. Nga sistemi Flare Billing dërgohen në Mobiread të dhëna mbi abonentët; të dhënat mbi matësat e ujit për lexim; zonat etj. Nga sistemi i Mobiread dërgohen në sistemin Flare Billing leximet e matësave të ujit të abonentëve.

Sistemi Flare ERP me anë të modulit Flare Billing komunikon me institucionet e pagesave siç janë bankat e nivelit të dytë dhe institucione financiare jo banka. Lidhja bëhet me anë të komunikim me VPN.
Ndërsa nga sistemi i Oxana kryhet fiskalizimi i faturave mujore te shitjes së ujit.

Shërbimet që ofrohen online:
Webservice selfcare për abonentët e UKD:
Abonentët e UKD për të konsultuar dhe për të parë faturat mujore por edhe historikun e konsumit dhe llojin e taksave që paguajnë ju ofrohet shërbimi online për të kontrolluar faturën online.

Për ta aksesuar këtë shërbim abonentët duhet të shkojnë tek faqja web zyrtare e UKD https://www.shuk.al/durres.

Në këtë portal është bërë e mundur lidhja me një webservice që të dërgon tek portali selfcare për të aksesuar faturat mujore. Ky portal është i hostuar në një server virtual në dhomën e serverëve të UKD. Po të klikohet në dritaren "Kontrollo Faturën Online", ajo të dërgon tek portali si më poshtë:

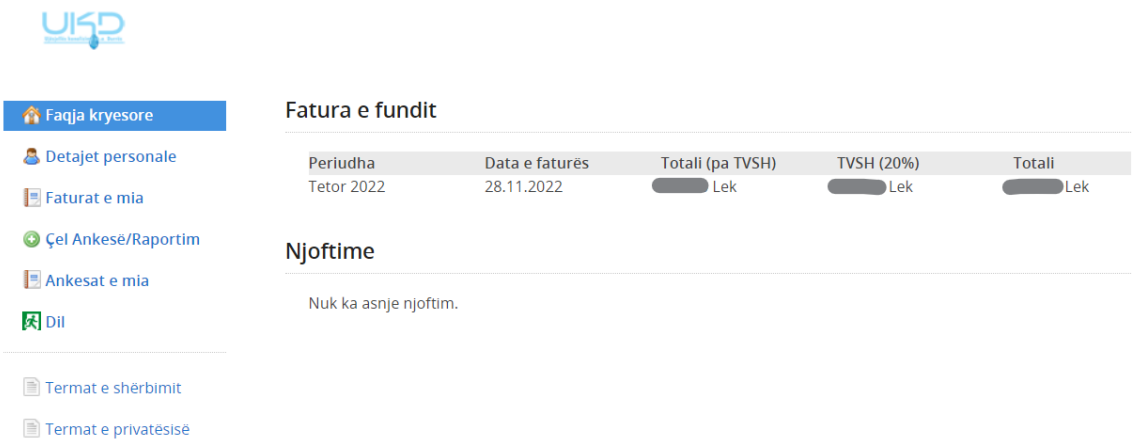


Nga auditimi u konstatua se:

-Nivel shumë i ulët i sigurisë së autentifikimit në portal. Për tu identifikuar në këtë portal abonenti apo klienti duhet të vendosi në të dyja dritaret numrin e kontratës, pra edhe username edhe password janë numri i kontratës.

-Mungesa e elementëve të sigurisë në ndërfaqen e portalit "selfcare". Pasi është log-uar për herë të parë në portal, abonenti nuk ka asnjë mundësi që të ndryshojë fjalëkalimin, pra fjalëkalimi mbetet i njëjtë me numrin e kontratës.

-Risk i lartë për modifikimin e të dhënave si dhe risk për humbjen apo përdorimin e të dhënave personale. Nëse dikush ka ose gjen numrin e kontratës të një abonenti tjetër atëherë ai mund të logohet, të shohë faturat, historikun e faturave, si më poshtë:



-Mungesë e popullimit të fushave të kërkuara. Të gjithë ata abonentë në mënyrë rastësore që grupi i auditimit, i kontrolloi në sistem, rezultuan që asnjë prej tyre nuk i kishte të populluara detajet personale, apo të kishte ndonjë historik ankesash, çka nënkupton që këta abonentë nuk e kanë vizituar ndonjëherë këtë portal, apo nuk e kanë aksesuar ndonjëherë kontratën e tyre.

Sistemi Mobiread

Sistemi Mobiread është implementuar në vitin 2016 për mbledhjen dhe hedhjen e leximeve të matësve, nga lexuesit e UKD. Kjo platformë është një platformë proprietare më të drejta autori të zotëruara nga OE që e ka zhvilluar dhe implementuar atë.
Sistemi Mobiread është e ndërtuar në platformën MySQL, si dhe sistemi Android për pajisjet PDA që përdorin lexuesit për hedhjen e të dhënave të leximeve të matësave. Qëllimi kryesor i këtij sistemi është marrja e leximeve nga pajisjet PDA dhe dërgimi i këtyre të dhënave në sistemin Flare ERP, Moduli Billing në mënyrë që të realizohet faturimi i saktë i konsumatorëve. Për të bërë të mundur këtë proces, sistemi "Mobiread" merr të dhënat fillestare nga sistemi Flare, Moduli Billing. PDA-të marrin të dhënat e abonentëve që ju nevojiten dhe i kthejnë sërish sistemit të dhënat e përditësuara me leximet përkatëse. Në fund të këtij procesi, sistemi i dërgon këto të dhëna në sistemin Flare, Moduli Billing. Për të aksesuar sistemin Mobiread është e njëjta procedurë sikurse edhe aksesimi i sistemit Flare ERP dhe më pas kërkohen të dhënat si username dhe password.

Nga auditimi u konstatua se:
-Administrimi dhe menaxhimi i databazës së sistemit Mobiread realizohet nga OE. Ky OE gjithashtu është duke ofruar suport për këtë sistem. Në sistemin Mobiread administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Admin" dhe ka të drejta të plota mbi çdo gjë në sistem.
-Detyra e Administratorit të sistemit dhe Administratorit të bazës së të dhënave nuk janë atribuuar me anë të një shkrese zyrtare nga organet drejtuese të UKD, ku punonjësit e zyrës IT të janë emëruar zyrtarisht si Administratorë për administrimin e bazës së të dhënave për të ushtruar atributet e përcaktuara sipas funksioneve të tyre dhe të gjitha detyrat e administratorit mbi administrimin e bazës së të dhënave të sistemit.

Të dhënat input dhe output:

Të dhëna Input:
- Leximet e matësve të ujit të abonentëve me PDA.

Të dhënat output:
- Leximet e dërguara në sistemin Flare ERP, moduli i Billing;
- Raporte të ndryshme.

- **Kodi i burimit (source code):**

Nga administrimi i dokumentacionit në fazën e auditimit në terren, grupi i auditimit nuk vërejti asnjë dokumentacion që të faktonte marrjen e kodit burim, për të dy sistemet Flare ERP dhe Mobiread.
Nisur sa më sipër dhe në zbatim të rekomandimeve të VKM nr. 710, datë 21.8.2013, të Ministrit për Inovacionin, Teknologjinë e Informacionit dhe të Komunikimit, është nxjerrë Udhëzimi nr. 2, datë 02.09.2013 "*Për standardizimin e Hartimin e termave të Referencës për Projektet TIK në Administratën Publike".* Në germën "e", të pikës 8, të kreut II, të këtij udhëzimi përcaktohet se, për propozimet e kërkuara, institucionet gjatë hartimit të termave të referencës për projektet TIK duhet të marrin në konsideratë çështjet si më poshtë:
"*Të sigurojnë pronësinë e Kodeve Burimore (source code) dhe /ose të drejtën për të blerë Kodet Burimore. Pronësinë e Kodeve Burimore, analiza e projektimit, burimi dhe programet e ekzekutueshme të të gjitha sistemeve të aplikimit të zhvilluara do ti kalojnë institucionit pa asnjë kosto shtesë*".
Në zbatim me sa më sipër Kodi i Burimit për të dy sistemet duhet të jetë në pronësi të UKD.

- ***e-maili i UKD:***

UKD për përdorimin e e-mailit ka blerë domainin "@ukdurres.al" dhe më pas hostimin e e-maili e kanë bërë në serverat e Google me anë të platformës "google cloud", në të cilën ka bërë një abonim një vjeçar i cili rinovohet çdo vit. Pagesa për këtë shërbim mund të shkojë deri në 60 euro në vit. Çdo punonjës i administratës së UKD i cili dëshiron të aksesojë e-mailin e tij të punës duhet të shkojë në google.com, ku me anë të kredencialeve personale mund ta aksesojë emailin e tij nga çdo vend.

Nga auditimi u konstatua se nuk ka një akt rregullues në të cilin të përcaktoheshin rregullat standarde mbi përdorimin e emailit të punës, përgjegjësitë e gjithsecilit, siguria, administrimi, etj.

- ***Infrastruktura harware dhe software e Sistemeve Flare ERP dhe Mobiread***

Sistemi elektronik Flare ERP është ngritur në gjuhën e programimit PHP, MySQL. Kodi i burimit nuk disponohet akoma nga institucioni por posedohet nga OE që e ka zhvilluar dhe implementuar atë. Sistemi është një aplikacion që duhet të instalohet në çdo pc në mënyrë që të aksesohet dhe nuk është i aksesueshëm nga web-i. Kredencialet Emër Përdoruesi/ fjalëkalimi krijohen nga administratori dhe i dorëzohen përdoruesit. Ky sistem është i hostuar në një nga godinat e UKD, ku ndodhen dhe serverat e tjerë. E njëjta situatë përsëritet edhe për sistemin Mobiread.

Infrastruktura e përdorimit të të dhënave përbëhet nga dy servera: HPE DL 380 G9 dhe DELL EMC PowerEdge R740, Model: PowerEdge R530 si dhe një storage DELL EMC SC 2020. Të gjitha këto pajisje komunikojnë me ndërfaqe iSCSI. Mbi këta servera është ndërtuar një infrastrukturë virtuale e bazuar në teknologjinë VMware, mbi të cilat janë ngritur shërbimet e nevojshme për të realizuar gjithë proceset punës.

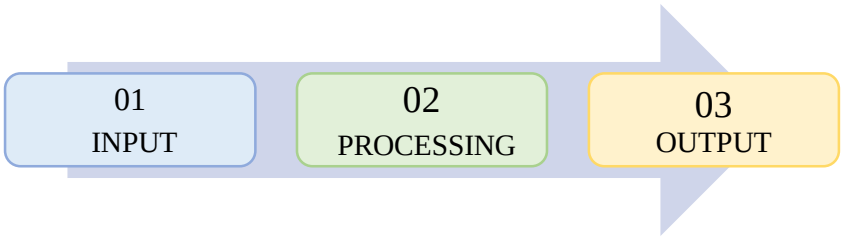
Të dhënat e hardware për të dy serverat fizikë:

Model: PowerEdge R740 (viti i prodhimit 2017)
Serveri Fizik: 192.168.xxx.xxx
Makina virtuale: xxx.xxx.x.xxx
Kapacitetet:
RAM: 128 GB
Processor: Intel® Xeon® Gold 5118 CPU @ 2.30 GHz
Kapaciteti: 6 TB

Model: PowerEdge R530 (viti i prodhimit 2014)
Serveri Fizik: 192.168.xxx.xxx
Makina virtuale: xxx.xxx.x.xxx
Kapacitetet:
RAM: 64 GB
Processor: Intel® Xeon® CPU E5-2650 v4 @ 2.20 GHz
Kapaciteti: 8.5 TB

➢ *Diagrama e rrjedhës së informacionit për sistemet TIK (workflow[3])*

Nga auditimi u konstatua se nuk janë dokumentuar, diagramat e rrjedhës së informacionit , për çdo produkt apo shërbim të konfiguruar në sistemin Flare ERP. Gjithashtu nga grupi i auditimit nuk u administrua një dokumentim skematik mbi proceset, rregullat dhe procedurat e implementuara për çdo modul apo shërbim që është informatizuar në sistemin Flare ERP.
Nga grupi i auditimit përgjatë fazës së auditimit në terren është administruar vetëm diagrama se si ndërveprojnë dhe komunikojnë sistemet me njëri tjetrin, e cila është cituar dhe më lart në këtë akt konstatim.
Tre proceset kryesore që përfshihen në Workflow ilustruar dhe në figurën e mëposhtme janë: Hyrja e të dhënave (Input); Procesimi i tyre dhe Rezultati (Output)



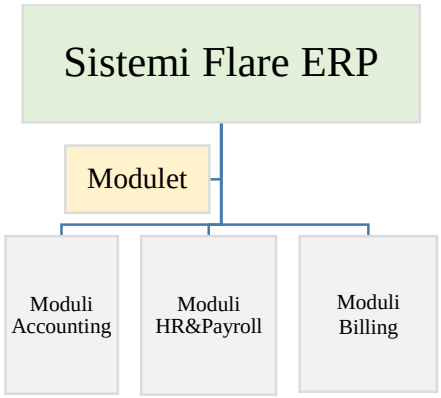
Burimi: *Përgatitur nga grupi i auditimit*

Mungesa e dokumentimit të diagrameve shpjeguese se si informacioni rrjedh në sistemet e TI që mbështesin proceset e institucionet në vazhdimësi të plotësimit të gjurmës së auditimit, krijojnë pengesa në të paktën 3 drejtime, për:
- *Kuptimin*: Diagrami nxjerr në pah zona ku mungon kuptimi i sistemit dhe kontrolleve që janë implementuar në të.
- *Vlerësimin*: Nëpërmjet diagrameve, vetë punonjësit apo strukturat monitoruese mund të zbulojnë pikat e forta dhe dobësitë e kontrollit që është implementuar në sistem.
- *Gjurmimin*: Nëpërmjet diagrameve dokumentohet rruga që përshkon informacioni i regjistruar në sistem, deri në raportimin e të dhënave përfundimtare që janë institucionet tek të cilat shoqëria raporton. Ky gjurmim tek UKD nuk realizohet plotësisht nëpërmjet aplikacionit.

➢ ***Mbi funksionalitet e sistemit Flare ERP***

Sistemi Flare ERP është një sistem modular i ndërtuar në module të ndryshme. Modulet që përfshihen në sistemin Flare ERP janë: Moduli Flare Accounting, Moduli HR&Payroll, Moduli Billingut.

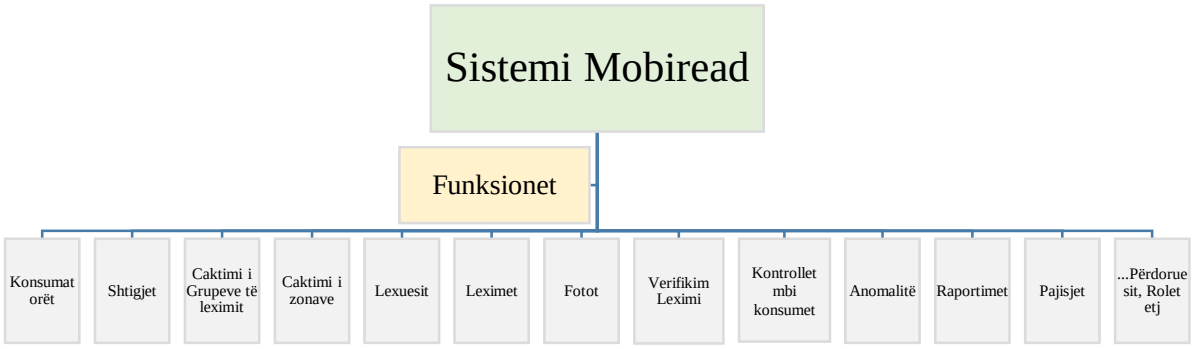
[3] *Termat që përdoren në gjuhën e TI për rrjedhën e informacionit janë: Workflow, Flowchart*



Burimi: *UKD. Punoi Grupi i Auditimi.*

➢ ***Mbi funksionalitet e sistemit Mobiread***

Sistemi Mobiread është e ndërtuar në platformën MySQL, si dhe sistemi Android për pajisjet PDA që përdorin lexuesit për hedhjen e të dhënave të leximeve të matësave. Qëllimi kryesor i këtij sistemi është marrja e leximeve nga pajisjet PDA dhe dërgimi i këtyre të dhënave në sistemin Flare ERP, Moduli Billing në mënyrë që të realizohet faturimi i saktë i konsumatorëve.



Burimi: *UKD. Punoi Grupi i Auditimi.*

➢ **Performanca e Sistemeve Flare ERP dhe Mobiread**

Sistemi ERP është sistemi kryesor në të cilin UKD e mbështet aktivitetin e saj mbi regjistrimin e të dhënave të abonentëve; kontratave; matësave të ujit; artikujve dhe tarifave për faturim. Organizimin e zonave dhe nën-zonave; menaxhimin e procesit të pagesave pranë njësive të arkave të Ujësjellësit, pranë bankave dhe institucioneve financiare. Gjenerimin e raporteve mbi abonentët; faturimet; arkëtimet; debinë e abonentëve etj.

Mosfunksionimi i këtij sistemi do të kishte ndjeshmëri dhe ndikim të lartë ndaj qytetarëve dhe bizneseve që marrin shërbime nga UKD dhe do të sillte pasoja të rënda në vazhdimësinë normale të punës së shoqërisë UKD.

Nga auditimi mbi sistemin Flare ERP u konstatua se:

-Për shkak të mbingarkesës dhe shtimit të shërbimeve, të abonentëve, si dhe për shkak të perfomancës së dobët të sistemit, ky sistem vazhdimisht punon me ndërprerje dhe ka probleme me ecurinë normale të punës duke ndikuar në veprimtarinë e specialistëve dhe institucionit në ofrimin e shërbimeve kundrejt qytetarëve dhe bizneseve por edhe vetë administratës së UKD;

-Sistemi krijon vonesa në shqyrtimin dhe gjenerimin e raporteve të ndryshme;

-Kur gjenerohet një raport pivot, në qoftë se tenton të gjenerosh dhe një tjetër, raporti i dytë nuk mund të gjenerohet pa e mbyllur me parë aplikacionin dhe të futesh përsëri;

-Sistemi krijon errore dhe nuk gjeneron të dhëna në qoftë se përzgjedhim raporte për periudha më shumë se një muaj;

-Shfaqet error kur kërkohet të ekstraktohen të dhënat mbi rolet në sistemin Flare ERP;
-Kur tentohet ekstraktimi i klientëve nga sistemi me të gjitha opsionet e zgjedhura të kolonave sistemi bllokohet dhe nuk u përgjigjet komandave dhe nuk ekstrakton asgjë sepse bën crash;
-Kur sistemi aksesohet me anë të VPN, jashtë rrjetit të brendshëm, shpeshherë hasen pengesa në aksesimin e tij, pasi sistemi shfaq error. Në momentin që aksesohet është shumë e vështirë të punohet në të pasi është shumë i ngadaltë në veprime;
-Sinkronizimi ndërmjet dy sistemeve Flare ERP dhe Mobiread, realizohet çdo një muaj, çka rrit riskun e mospasjes së informacionit të përditësuar për abonentët dhe ndryshimet e kontratave ndërmjet dy sistemeve.

Disa problematika mbi analizimin e të dhënave mbi abonentët:

Ujësjellës kanalizime Durrës e ka zonën e shërbimit dhe faturimit të shtrirë në rrethin e Durrësit, rrethin e Shijakut dhe Fushëkuqe.
-Rrethi i Durrësit përfshin:
Qytetin, Plazhin, zonën e ish Kënetës, Shkozet, Rrashbull, Ishëm, Katund i Ri, Manzë
-Rrethi i Shijakut përfshin:
Qytetin, Shenvlashin, Xhafzotaj, një pjesë të Vorës, Prez, Maminas
-Fushe kuqe
Në këtë shtrirje janë dhe dy impiante të përpunimit të ujërave të ndotur:
Impianti i Xhafzotaj, Impianti i Lalëzit
Në total janë 117,152 abonentë aktiv, jo aktiv, afrofe. Nga ky numër total, 93,613 janë abonentë aktiv, pra janë abonentë që faturohen dhe 96% e abonentëve është e pajisur me matësa. Plani tarifor i faturimit ndahet: Sipas matësit Familje me Kanalizime; Sipas matësit Familje me Kanalizime pa tarife shërbimi; Sipas matësit Familje pa Kanalizime; Sipas matësit Institucion me Kanalizime; Sipas matësit Institucion pa Kanalizime; Sipas matësit Kompani private me Kanalizime; Sipas matësit Kompani private pa Kanalizime; Vetëm tarifa e shërbimit Familje; Vetëm tarifa e shërbimit Kompani private.

Nga auditimi dhe analizimi i të dhënave input/output të sistemit Flare ERP mbi "Abonentët" u konstatua se:
-Kodi i kontratës vendoset në mënyrë automatike nga sistemi Flare ERP dhe në mënyrë inkrementale. Gjatë kohës së vendosjes dhe implementimit të sistemit të ERP në UKD ka qenë në përdorim një tjetër databazë e ngritur me kodin e kontratave. Gjatë implementimit të sistemit Flare ERP të dhënat e mëparshme janë migruar në këtë sistem. Pra të dhënat e ekstraktuara nga sistemi ERP mbi numrat e kontratave nuk i përkasin vetëm atyre të krijuara nga sistemi ERP por edhe nga të dhënat e mëparshme të migruara. Kontratat e reja me sistemin Flare ERP kanë filluar të hapen që prej vitit 2018;
-Kur plotësohen të dhënat e një abonenti, jo të gjitha fushat e afishuara nga sistemi Flare ERP popullohen saktë nga specialistët. Si p.sh. "*Adresa e abonentit*", kur nuk dihet adresa e saktë shkruhet vetëm emri i zonës ku ndodhet abonenti.
-Rreth 40% e abonentëve kanë informacion të populluar mjaftueshëm të kontratave. Pjesa tjetër kanë informacion të pjesshëm ose nuk janë populluar fare. Ka një numër të lartë abonentësh të cilët nuk kanë një numër identifikimi, nipt (në qoftë se janë biznes) apo edhe numrin e telefonit, çka nënkupton që këta abonentë kur janë regjistruar si abonentë nuk kanë patur dokumentacionin përkatës si kartën ID dhe certifikatën e pronësisë së pronës, dokumente që nevojiten për të hapur një kontratë të re, pra informacioni mbi abonentët nuk është i populluar dhe i përditësuar.

Mbi "*Input application data set*":
-Nga analizimi i të dhënave mbi Abonentët në total të UKD, aktiv dhe jo aktiv u konstatua se në dy raste kemi dublikim të kodit të kontratës, edhe pse ky kod duhet të vendoset në mënyrë

automatike nga sistemi. Konkretisht kodi i kontratës me numër: 7777777 dhe kodi i kontratës me numër: 2147483647, janë të dublikuar.
Mbështetur sa më sipër, kjo nënkupton se sistemi nuk ka kontroll për inputin e të dhënave, çka e bën sistemin vulnerabël. Sistemi duhet të gjenerojë numrin e kontratave në mënyrë automatike dhe në rritje inkrementale.
-Tek kolona "Numri i ID", sistemi duhet të ketë kontrolle të vlefshmërisë së informacionit pasi dihet që numri i identifikimit është unik dhe ka një format të përcaktuar se si është i ndërtuar, dhe në këtë kolonë nuk mund të popullojmë të dhëna jashtë formatit të përcaktuar. Është konstatuar një numër i lartë rastesh që popullimi i kësaj fushe është bërë jo sipas përcaktimeve;
-Tek kolona "Nipt", sistemi duhet të ketë kontrolle të vlefshmërisë së informacionit pasi dihet që numri nipt është unik dhe ka një format të përcaktuar se si është i ndërtuar, dhe në këtë kolonë nuk mund të popullojmë të dhëna jashtë formatit të përcaktuar;
-Konfigurimi i fushave input të sistemit. Gjatë popullimit të të dhënave të një abonenti sistemi duhet të shfaqë për të plotësuar vetëm ato fusha me të dhënat që kërkohen sipas profilit të abonentit. P.sh. në qoftë se abonenti është familjar, nga sistemi nuk duhet të shfaqet për tu populluar fusha që kërkon niptin e kompanisë. Kjo fushë duhet të jetë aktive vetëm për abonentët biznes;
-Ka raste që lexuesit hedhin leximet e një matësi tjetër në faturimet e një abonenti që nuk është i lidhur me atë matës. Këto raste vihen re dhe verifikohen vetëm pasi abonenti i drejtohet me ankesë UKD që e ve në dijeni që është faturuar gabim. Pas verifikimit këto fatura sistemohen në sistem duke krijuar fatura me vlerë negative në mënyrë që zerohet vlera e shtuar gabim nga leximi dhe faturimi.

- ***Administrimi i log-eve të sistemit Flare ERP***

Menaxhimi i log-eve ndihmon institucionin 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:

- Të gjitha log-et janë të ruajtura në makinat fizike përkatëse, por ato nuk janë testuar, analizuar dhe monitoruar ndonjëherë, nëse janë të plota, funksionale dhe të përdorshme. Nuk është e përcaktuar se për sa kohë ruhen këto log-e dhe çfarë procedure ndiqet për analizimin e tyre. Ekstraktet e logeve të sistemit të kërkuara nga grupi i auditimit të ekstraktuara nga OE, në pamundësi për tu ekstraktuar nga specialistët e UKD, për shkak se sistemi bënte crash, u sollën jashtë afatit të kërkuar dhe ishin jo të plota, kështu që ishte e pamundur analizimi i tyre në tërësi.
-Nga verifikimi i dokumentacionit u konstatua se UKD nuk disponon akte rregullator për menaxhimin e log-eve digjitale, në kundërshtim me rekomandimet e pikës 4 shkronja a) të "Rregullores për menaxhimin e log-eve digjitale në Administratën Publike", miratuar me urdhrin nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT) Institucioni duhet të përcaktojë një rregullore të shkruar për menaxhimin e log-eve sipas kërkesave të institucionit. Kjo rregullore duhet të specifikojë qartë të gjitha kërkesat për ruajtjen e log-eve përkatëse për çdo sistem/pajisje të institucionit, procedurat e administrimit dhe përgjegjësitë në përputhje me këtë rregullore dhe legjislacionin në fuqi.
- Nuk janë përcaktuar burimet e nevojshme si dhe detyrat e personelit për menaxhimin e log-eve;

- UKD nuk zhvillon kontrolle mbi Audit Log, pavarësisht rëndësisë që kanë këto të dhëna në përmirësimin e sistemit, konstatimin dhe analizimin e problematikave të ndryshme.

Për sa është trajtuar në këtë pikë të Raportit Përfundimtar të Auditimit është mbajtur Aktkonstatimi nr. 2, datë 11.11.2022, protokolluar në UKD me shkresën nr. 7607/2, datë 11.11.2022, si dhe është trajtuar në faqet 24-48 të Projektraportit të Auditimit mbi të cilin janë paraqitur observacione mbi Aktkonstatimin nr. 2, me shkresën nr. 7607/4, datë 18.11.2022, protokolluar në KLSH me nr. 817/3, datë 05.12.2022. Në shkresën e sipërpërmendur subjekti i audituar shprehet se, i ka pranuar të gjitha konstatimet e auditimit dhe do të marrë masat përkatëse për plotësimin e rekomandimeve.

1. Titulli i gjetjes: Nga auditimi mbi aktet rregullatore të manualeve të përdorimit të sistemit Flare ERP u konstatua se dy nga tre manualet e moduleve të sistemit nuk janë të përditësuara.

Situata 1: Nga auditimi u konstatua se, dy nga tre manualet e përdorimit të moduleve të sistemit Flare ERP nuk janë të përditësuara. Këto manuale shërbejnë si udhëzues për të gjithë përdoruesit që kanë të drejtë të aksesojnë sistemin Flare ERP. Sistemi i mundëson shoqërisë trajtimin dhe menaxhimin e abonentëve, matësave, tarifave, artikujve, nivelet e çmimeve, leximet e matësave dhe menaxhimin e abonentëve në qytetin e Durrësit dhe zonave që UKD menaxhon.
- Manual përdorimi për modulin "Flare Accounting"
- Manual përdorimi për modulin "Flare Billing"
- Manual përdorimi për modulin "Flare HR and Payroll"

Këto manuale përdorimi u shpjegojnë përdoruesve se si të kryejnë të gjithë proceset e përdorimit të sistemit duke filluar që nga hapja e userave sipas roleve përkatës deri në shpjegimin e menuve dhe nënmenuve përkatëse në sistem. Sistemi është i përbërë nga 4 module dhe secili modul ka manualin përkatës.
Situata 2: Nga auditimi u konstatua se nuk ka një akt rregullues në të cilin të përcaktoheshin rregullat standarde mbi përdorimin e e-mailit të punës, përgjegjësitë e gjithsecilit, siguria, administrimi, etj.
Kriteri: Efektiviteti në përdorim të sistemit Flare ERP dhe neni 20 i ligjit nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar.
Ndikimi/efekti: Mos adresim i përgjegjësive si pasojë e keq adresimit të përcaktimit të detyrave, kompetencave dhe përgjegjësive.
Shkaku: Mos menaxhimi i ndryshimit në bazën ligjore, nënligjore dhe aktet rregullative.
Rëndësia: E Mesme.
1.1.Rekomandim: UKD, të hartojë, amendojë dhe miratojë, manualet e përdorimit të sistemit Flare ERP duke reflektuar ndryshimet institucionale, strukturore dhe kompjuterike që priten të ndodhin pas transformimit shoqërisë UKD në shoqëri rajonale.
Gjithashtu të merren masa për hartimin dhe miratimin e një rregulloreje të përgjithshme për funksionimin e sistemeve të teknologjisë së informacionit të cilët ka në përdorim UKD, në të cilat të jenë të pasqyruara saktë përgjegjësitë, detyrat dhe të drejtat për menaxhimin e përdoruesve të këtyre sistemeve. Në këtë rregullore të përcaktohen edhe rregulla për menaxhimin dhe përdorimin e e-mailit zyrtar të punës.

2. Titulli i gjetjes: Parregullsi që i adresohen politikave të sigurisë së identifikimit të përdoruesve.
Situata: Nga auditimi mbi politikat e sigurisë së përdoruesve në sistemet ERP dhe Mobiread u konstatua se:
- Passwordin e userit, sistemi e merr automatikisht siç është username i përdoruesit dhe sistemi nuk të lejon të menaxhosh këtë funksion;

- Përdoruesi sapo logohet (first log-in) me fjalëkalim fillestar, nuk i shfaqet automatikisht nga sistemi tabela e cila të kërkon vendosjen e fjalëkalimit të ri;
- Në rast se punonjësi nuk e ndryshon fjalëkalimin fillestar dhe vazhdon të përdorë të njëjtin password, sistemi i jep akses pavarësisht se përdoruesi se ka ndryshuar passwordin. Nga të dhënat e ekstraktuara mbi përdoruesit e sistemeve vihet re se edhe pse kërkohet shumë herë reset të paswordit, përdoruesit vazhdojnë sërish me të njëjtat passworde;
- Siguria e vendosjes së fjalëkalimit nuk është e tipit kompleks ku të kërkohen të ketë minimumi 8 karaktere, të ketë të paktën 1 shkronje dhe 1 shifër.
- Nuk janë dokumentuar politikat e sigurisë të implementuara për përdoruesit e sistemit, si dhe detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre, bazuar në pikën 4 "Kërkesat e Sigurisë" pika a. të rregullores për "Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike" të miratuar nga AKCESK me urdhrin nr. 86, datë 23.08.2019.
- Nuk janë dokumentuar politikat e sigurisë të implementuara për fjalëkalimet e sistemeve qendrore dhe administrimit bazuar në pikën 4 "Kërkesat e Sigurisë" pika b. Të rregullores për "Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike" miratuara nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

Kriteri: Pika 4 "*Kërkesat e Sigurisë*" pika a, e rregullores për "Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike" miratuar nga AKCESK me urdhrin nr. 86, datë 23.08.2019; Forcimin i fjalëkalimit si element sigurie është në standardin "Two Factor Authentication".

Ndikimi/efekti: Mos administrim i fjalëkalimeve të përdoruesve në rrjetet dhe sistemet kompjuterike si dhe mosnjohje e të drejtave dhe detyrimeve që kanë të gjithë përdoruesit e sistemit.

Shkaku: Mungesa e rregullave të dokumentuara dhe implementimi i tyre mbi sigurinë e fjalëkalimeve të përdoruesve.

Rëndësia: E Lartë

2.1.Rekomandim: Organet drejtuese në UKD të marrin masa për të dokumentuar politikat e sigurisë të implementuara për përdoruesit e sistemit, si dhe detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre sipas përcaktimeve rregullatore të AKCESK. Gjithashtu të merren masa për adresimin e çështjeve të konstatuara nga auditimi, me qëllim rritjen e sigurisë së identifikimit të përdoruesve. Të merren në konsideratë praktikat e përcaktuara në rregulloren për "*Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike*" miratuar nga AKCESK.

3. Titulli i gjetjes: Keq menaxhim dhe keq administrim i përdoruesve të sistemeve Flare ERP dhe Mobiread, duke krijuar kushte për shkelje të sigurisë

Situata 1: Nga auditimi mbi përdoruesit aktiv, të ndarë sipas roleve përkatëse në sistemin Flare ERP u konstatua se:

-Në sistemin ERP nuk është e mirë përcaktuar forma e username, duke qenë se ajo popullohet manualisht, disa username kanë shkronjën e parë të emrit dhe pastaj mbiemrin, disa username kanë vetëm emrin e përdoruesit, disa emrin dhe një numër, disa vetëm një shkronjë, etj. Username-t nuk janë të standardizuar çka tregon që sistemi nuk ka mekanizma të kontrollit të inputit. Ka raste që username nuk lidhet fare me emrin e përdoruesit pasi username ka vetëm një shkronjë.

-Në rolin "Admin", janë aktiv 4 administrator me atributin që kanë të drejta mbi çdo gjë. Nga auditimi u konstatua se këta usera nuk identifikohet se çfarë procesesh mbulojnë në sistem, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Përdoruesit me username "sistemi", "MarsiKx" si dhe "ace" nuk identifikohen se çfarë procesesh mbulojnë në sistem dhe kujt useri i përkasin, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Kjo gjë përsëritet edhe në

rolin Financë-operator. Gjithashtu ka përdorues që kanë rolin "Admin", ndërkohë që pozicioni i punës së këtyre përdoruesve nuk përputhet me rolin që kanë në sistem.
-Në rolin "Admin viewer", është aktiv vetëm një përdorues me atribute për të parë në sistem.
-Në rolin "Sys Admin" është aktiv një përdorues që është njëkohësisht përgjegjësi i zyrës së IT, dhe ka të drejta Viewer si dhe të drejta mbi përdoruesit. Pra përgjegjësi i zyrës IT që duhet të ishte në rolin e Super Admin, duke qenë së është administratori i sistemit, nuk ka të drejta të plota në sistem.
-Atributet dhe rolet e userave në sistemin ERP nuk janë të përcaktuara sipas detyrave dhe përgjegjësive të përcaktuara në rregulloren e brendshme për funksionimin e UKD por sipas funksionaliteteve që punonjësi ushtron në praktikë përgjatë procesit të punës;
-Një përdorues aktiv mund të autentifikohet në më shumë së një kompjuter. Pra me një username mund ta hapësh sistemin Flare ERP në të njëjtën kohë në më shumë se një kompjuter.
Situata 2: Nga auditimi mbi përdoruesit aktiv, të ndarë sipas roleve përkatëse në sistemin Mobiread u konstatua se:
-Në sistemin Mobiread nuk është e mirë përcaktuar forma e username, duke qenë se ajo popullohet manualisht, disa username kanë shkronjën e parë të emrit dhe pastaj mbiemrin, disa username kanë vetëm emrin e përdoruesit, disa emrin dhe një numër, disa vetëm një shkronjë, etj. Username-t nuk janë të standardizuar çka tregon që sistemi nuk ka mekanizma të kontrollit të inputit. Ka raste që username nuk lidhet fare me emrin e përdoruesit pasi username ka vetëm një shkronjë. Si më poshtë:
-Në rolin "Admin", janë aktiv 4 administrator me atributin që kanë të drejta mbi çdo gjë. Nga auditimi u konstatua se këta usera nuk identifikohet se çfarë procesesh mbulojnë në sistem, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Përdoruesit me username "m." si dhe "ace" nuk identifikohen se çfarë procesesh mbulojnë në sistem dhe kujt useri i përkasin, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Kjo gjë përsëritet edhe në rolin Azhornues për userat "azhornues 1 dhe 2", në rolin Lexues për userat "lexues 2 dhe 3", në rolin Verifikues për userat "verifikues 1". Gjithashtu ka përdorues që kanë rolin "Admin", ndërkohë që pozicioni i punës së këtyre përdoruesve nuk përputhet me rolin që kanë në sistem.
-Rolin "Admin", e posedon edhe username "d.gj.", i cili sipas informacionit të dhënë ushtron pozicionin e drejtorit tregtar në UKD Sh.a, pra këtij useri i janë dhënë atributet e administratorit të sistemit, në mospërputhje me aktivitetin e punës që ushtron në sistem.
-Në rolin "Admin viewer", janë aktiv dy përdorues me atribute për të parë në sistem. Përdoruesi me username "suport" nuk identifikohet në sistem se kujt useri i përket, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor.
Kriteri: Ligji 2/2017 "*Për sigurinë kibernetike*"; Neni 27, Ligji Nr. 9887, "Për Mbrojtjen e të Dhënave Personale", i ndryshuar; ISO/IEC 27001 "*Information security management*".
Ndikimi/efekti: Risk për kompromet imin e të dhënave dhe humbjes së gjurmës audituese;
- Risk për ndërhyrje të jashtme, me pasojë dëmtimin e sistemit të teknologjisë së Informacionit;
- Risk për kryerjen e veprimeve në sistem nga persona të paautorizuar;
- Risk për mos-evidentimin dhe mos-parandalimin e problematikave që lidhen me sigurinë e të dhënave.
Shkaku: Mos marrja e masave paraprake për parandalimin e problematikave që lidhen me performancën e funksionimit jo të mirë të sistemit.
Rëndësia: E Lartë
3.1.Rekomandim: Strukturat drejtuese në UKD të marrin masa për analizimin e hollësishëm të të gjithë përdoruesve aktivë në sistemet që ka në përdorim UKD me të drejta në sistem sipas pozicioneve të punës dhe të të gjithë çështjeve të konstatuar nga auditimi, me qëllim rritjen e

sigurisë së identifikimit të përdoruesve. Pas analizimit dhe evidentimit të të gjithë përdoruesve, të merren masa për bllokimin e aksesit dhe ç'aktivizimin e të gjithë përdoruesve të cilët nuk janë të lidhur me përdorues të identifikueshëm, kanë më shumë se një user, kanë më shumë atribute se pozicioni i punës, të mbyllë përdoruesit të cilët kanë përfunduar objektin e krijimit si dhe të gjitha çështjet e konstatuara nga grupi i auditimit me qëllim ruajtjen e sistemeve nga ndërhyrjet e paautorizuara. Gjithashtu të standardizohen username-t e përdoruesve.

4. Titulli i gjetjes: Kodi në burim për sistemet Flare ERP dhe Mobiread, si dhe përcaktimi i administrimit të sistemit dhe databazës së sistemeve.
Situata 1: Nga auditimi u konstatua se nuk administrohet asnjë dokumentacion që të faktojë marrjen e kodit burim, për të dy sistemet Flare ERP dhe Mobiread.
Nisur sa më sipër dhe në zbatim të rekomandimeve të VKM nr. 710, datë 21.8.2013, të Ministrit për Inovacionin, Teknologjinë e Informacionit dhe të Komunikimit, është nxjerrë Udhëzimi nr. 2, datë 02.09.2013 "Për standardizimin e Hartimin e termave të Referencës për Projektet TIK në Administratën Publike". Në germën "e", të pikës 8, të kreut II, të këtij udhëzimi përcaktohet se, për propozimet e kërkuara, institucionet gjatë hartimit të termave të referencës për projektet TIK duhet të marrin në konsideratë çështjet si më poshtë:
"*Të sigurojnë pronësinë e Kodeve Burimore (source code) dhe /ose të drejtën për të blerë Kodet Burimore. Pronësinë e Kodeve Burimore, analiza e projektimit, burimi dhe programet e ekzekutueshme të të gjitha sistemeve të aplikimit të zhvilluara do ti kalojnë institucionit pa asnjë kosto shtesë*". Në zbatim me sa më sipër Kodi i Burimit për të dy sistemet duhet të jetë në pronësi të UKD.
Situata 2: Nga auditimi u konstatua se:
-Administrimi dhe menaxhimi i databazës së sistemit Flare ERP dhe Mobiread realizohet nga OE. Ky OE gjithashtu është duke ofruar suport për këtë sistem.
Në sistemin Flare ERP administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Sys admin". Sys Admin ushtron funksionet viewer dhe ka të drejta mbi përdoruesit. Në sistemin Mobiread administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Admin" dhe ka të drejta të plota mbi çdo gjë në sistem.
-Detyra e Administratorit të sistemit dhe Administratorit të bazës së të dhënave nuk janë atribuar me anë të një shkrese zyrtare nga organet drejtuese të UKD, ku punonjësit e zyrës IT të janë emëruar zyrtarisht si Administratorë për administrimin e bazës së të dhënave për të ushtruar atributet e përcaktuara sipas funksioneve të tyre dhe të gjitha detyrat e administratorit mbi administrimin e bazës së të dhënave të sistemit.
Kriteri: VKM nr. 710, datë 21.8.2013, të Ministrit për Inovacionin, Teknologjinë e Informacionit dhe të Komunikimit, Udhëzimi nr. 2, datë 02.09.2013 "Për standardizimin e Hartimin e termave të Referencës për Projektet TIK në Administratën Publike". Germa "e", pika 8, e kreut II.
Ndikimi/efekti: Krijimi i kushteve të pabarabarta për operatorët ekonomik që dëshirojnë të marrin pjesë në procedurat e prokurimit. Mos ushtrimi i të gjithë atributeve të administratorit mbi administrimin e bazës së të dhënave të sistemit.
Shkaku: Mos marrja e kodit burim për sistemet Flare ERP dhe Mobiread.
Rëndësia: E Lartë
4.1.Rekomandim: Strukturat drejtuese në UKD në bashkëpunim me specialistët TIK, të marrin masa për adresimin e këtyre çështjeve tek OE që ka implementuara sistemet Flare ERP dhe Mobiread me qëllim marrjen e kodit në burim të sistemeve, në funksion të përmbushjes të përcaktimeve ligjore si dhe krijimin e kushteve të barabarta për operatorët ekonomik që dëshirojnë të marrin pjesë në procedurat e prokurimit, duke mos penguar konkurrencën e lirë si dhe të stimulojnë pjesëmarrjen e biznesit të vogël dhe të mesëm.

4.2.Rekomandim: Administratori i UKD të marri masa për përcaktimin e detyrës së Administratorit të sistemit dhe Administratorit të bazës së të dhënave, ku të jenë emëruar zyrtarisht Administratorët për administrimin e sistemit dhe bazës së të dhënave duke përcaktuar dhe atributet specifike sipas funksioneve të tyre dhe të gjitha detyrat e administratorit.

5. Titulli i gjetjes: Mungesa e dokumentimit të rrjedhës së informacionit "Workflow" për hapat që kryhen nëpërmjet sistemit informatik.
Situata: Nga auditimi u konstatua se nuk janë dokumentuar, diagramat e rrjedhës së informacionit , për çdo produkt apo shërbim të konfiguruar në sistemin Flare ERP. Gjithashtu nga grupi i auditimit nuk u administrua një dokumentim skematik mbi proceset, rregullat dhe procedurat e implementuara për çdo modul apo shërbim që është informatizuar në sistemin Flare ERP.
Kriteri: Standardet më të mira dhe neni 4, pika 19 të ligjit nr. 10296, datë 08.07.2010 "*Për menaxhimin financiar dhe kontrollin*", "Gjurma e auditimit".
Ndikimi/efekti: Mungesa e dokumentimit të diagrameve shpjeguese se si informacioni rrjedh në sistemet e TI që mbështesin proceset e institucionet në vazhdimësi të plotësimit të gjurmës së auditimit, krijojnë pengesa në të paktën 3 drejtime, për: *Kuptimin; Vlerësimin; Gjurmimin*.
Shkaku: Neni 16, pika 2 e ligjit nr.10296, datë 08.07.2010 "Për menaxhimin financiar dhe kontrollin", janë titullarët e njësive publike që miratojnë gjurmët e auditimit, të detajuara për procedurat kryesore dhe sigurojnë që të gjitha operacionet e njësisë publike dokumentohen në atë formë, që u mundëson audituesve të brendshëm, të jashtëm dhe autoriteteve mbikëqyrëse të kuptojnë mjedisin e kontrollit.
Rëndësia: E Lartë
5.1.Rekomandim: Strukturat Drejtuese në UKD krahas identifikimit të proceseve që nevojiten për dokumentimin e gjurmës audituese, të marrin masa që të hartojnë dhe dokumentojnë diagramat e rrjedhës së informacionit për çdo proces që realizohet nëpërmjet sistemeve me qëllim përcaktimin e të dhënave hyrëse, roleve, ndryshimin, miratimin dhe përfundimin për çdo shërbim që realizohet nëpërmjet sistemit informatik.

6. Titulli i gjetjes: Mungesa e elementëve të sigurisë në ndërfaqen e portalit "s*elfcare për abonentët e UKD*".
Situata: Nga auditimi u konstatua se:
-Nivel shumë i ulët i sigurisë së autentifikimit në portal. Për tu identifikuar në këtë portal abonenti apo klienti duhet të vendosi në të dyja dritaret numrin e kontratës, pra edhe username edhe password janë numri i kontratës.
-Mungesa e elementëve të sigurisë në ndërfaqen e portalit "selfcare". Pasi është log-uar për herë të parë në portal, abonenti nuk ka asnjë mundësi që të ndryshojë fjalëkalimin, pra fjalëkalimi mbetet i njëjtë me numrin e kontratës.
-Risk i lartë për modifikimin e të dhënave si dhe risk për humbjen apo përdorimin e të dhënave personale. Nëse dikush ka ose gjen numrin e kontratës të një abonenti tjetër atëherë ai mund të logohet, të shohë faturat, historikun e faturave, si më poshtë:
-Mungesë e popullimit të fushave të kërkuara. Të gjithë ata abonentë në mënyrë rastësore që grupi i auditimit, i kontrolloi në sistem, rezultuan që asnjë prej tyre nuk i kishte të populluara detajet personale, apo të kishte ndonjë historik ankesash, çka nënkupton që këta abonentë nuk e kanë vizituar ndonjëherë këtë portal, apo nuk e kanë aksesuar ndonjëherë kontratën e tyre.
Kriteri: Ligji nr. 2/2017, datë 26.01.2017 *"Për Sigurinë Kibernetike";* neni 27 i ligjit nr. 9887, "*Për mbrojtjen e të dhënave personale*", i ndryshuar, ISO/IEC 27001 "*Information security management*".Nenet 19-21 të ligjit nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar, si dhe praktikat më të mira.
Ndikimi/efekti: Risk për kompromentimin e të dhënave.

Shkaku: Mos marrja e masave për rritjen e elementëve të sigurisë në ndërfaqen e portalit "*selfcare*".
Rëndësia: E Lartë
6.1.Rekomandim: Strukturat përgjegjëse në UKD të analizojnë dhe adresojnë tek ofruesi i shërbimit të mirëmbajtjes parregullsitë, mangësitë e konstatuara nga auditimi mbi portalin selfcare dhe të ofrojnë zgjidhje për to me qëllim rritjen e nivelit të sigurisë së aksesit në portal dhe garantimin e marrjes së shërbimit të sigurtë për abonentët.

7. Titulli i gjetjes: Problematika mbi performancën e funksionimit të sistemit.
Situata: Nga auditimi mbi sistemin Flare ERP u konstatua se:
-Për shkak të mbingarkesës dhe shtimit të shërbimeve, të abonentëve, si dhe për shkak të performancës së dobët të sistemit, ky sistem vazhdimisht punon me ndërprerje dhe ka probleme me ecurinë normale të punës duke ndikuar në veprimtarinë e specialistëve dhe institucionit në ofrimin e shërbimeve kundrejt qytetarëve dhe bizneseve por edhe vetë administratës së UKD;
-Sistemi krijon vonesa në shqyrtimin dhe gjenerimin e raporteve të ndryshme;
-Kur gjenerohet një raport pivot, në qoftë se tenton të gjenerosh dhe një tjetër, raporti i dytë nuk mund të gjenerohet pa e mbyllur me parë aplikacionin dhe të futesh përsëri;
-Sistemi krijon errore dhe nuk gjeneron të dhëna në qoftë se përzgjedhim raporte për periudha më shumë se një muaj;
-Shfaqet error kur kërkohet të ekstraktohen të dhënat mbi rolet në sistemin Flare ERP;
-Kur tentohet ekstraktimi i klientëve nga sistemi me të gjitha opsionet e zgjedhura të kolonave sistemi bllokohet dhe nuk u përgjigjet komandave dhe nuk ekstrakton asgjë sepse bën crash;
-Kur sistemi aksesohet me anë të VPN, jashtë rrjetit të brendshëm, shpeshherë hasen pengesa në aksesimin e tij, pasi sistemi shfaq error. Në momentin që aksesohet është shumë e vështirë të punohet në të pasi është shumë i ngadaltë në veprime;
-Sinkronizimi ndërmjet dy sistemeve Flare ERP dhe Mobiread, realizohet çdo një muaj, çka rrit riskun e mospasjes së informacionit të përditësuar për abonentët dhe ndryshimet e kontratave ndërmjet dy sistemeve.
Kriteri: Ligji nr. 2/2017, datë 26.01.2017 *"Për Sigurinë Kibernetike";*neni 27 i ligjit nr. 9887, "*Për mbrojtjen e të dhënave personale*", i ndryshuar, ISO/IEC 27001 "*Information security management*". VKM Nr. 710, datë 21.08.2013 "P*ër Krijimin dhe Funksionimin e Sistemeve të Ruajtjes së Informacionit, Vazhdueshmërisë së Punës dhe Marrëveshjeve të Nivelit të Shërbimit*", i ndryshuar, praktikat më të mira.
Ndikimi/efekti: Risk për mos-evidentimin dhe mos-parandalimin e problematikave që lidhen me sigurinë e të dhënave.
Shkaku: Mos marrja e masave paraprake për parandalimin e problematikave që lidhen me performancën e funksionimit jo të mirë të sistemit.
Rëndësia: E Lartë
7.1.Rekomandim: Strukturat drejtuese në UKD së bashku me specialistët e IT-së, të analizojnë dhe adresojnë tek ofruesi i shërbimit të mirëmbajtjes, parregullsitë, mangësitë e konstatuara nga auditimi dhe të ofrojnë zgjidhje për to me qëllim përmirësimin e performancës së funksionimit të sistemit Flare në ofrimin e shërbimeve, si dhe të merren masa për shtimin e funksionaliteteve të reja në sistemin Flare sipas nevojës së përdoruesve në sistem.

8. Titulli i gjetjes: Disa problematika mbi analizimin e të dhënave mbi abonentët.
Situata: Nga auditimi dhe analizimi i të dhënave input/output të sistemit Flare ERP mbi "Abonentët" u konstatua se:
-Kodi i kontratës vendoset në mënyrë automatike nga sistemi Flare ERP dhe në mënyrë inkrementale. Gjatë kohës së vendosjes dhe implementimit të sistemit të ERP në UKD ka qenë në përdorim një tjetër databazë e ngritur me kodin e kontratave. Gjatë implementimit të sistemit Flare ERP të dhënat e mëparshme janë migruar në këtë sistem. Pra të dhënat e ekstraktuara nga

sistemi ERP mbi numrat e kontratave nuk i përkasin vetëm atyre të krijuara nga sistemi ERP por edhe nga të dhënat e mëparshme të migruara. Kontratat e reja me sistemin Flare ERP kanë filluar të hapen që prej vitit 2018;
-Kur plotësohen të dhënat e një abonenti, jo të gjitha fushat e afishuara nga sistemi Flare ERP popullohen saktë nga specialistët. Si p.sh. "Adresa e abonentit", kur nuk dihet adresa e saktë shkruhet vetëm emri i zonës ku ndodhet abonenti.
-Rreth 40% e abonentëve kanë informacion të populluar mjaftueshëm të kontratave. Pjesa tjetër kanë informacion të pjesshëm ose nuk janë populluar fare. Ka një numër të lartë abonentësh të cilët nuk kanë një numër identifikimi, nipt (në qoftë se janë biznes) apo edhe numrin e telefonit, çka nënkupton që këta abonentë kur janë regjistruar si abonentë nuk kanë patur dokumentacionin përkatës si kartën ID dhe certifikatën e pronësisë së pronës, dokumente që nevojiten për të hapur një kontratë të re, pra informacioni mbi abonentët nuk është i populluar dhe i përditësuar.
Mbi "Input application data set":
-Nga analizimi i të dhënave mbi Abonentët në total të UKD, aktiv dhe jo aktiv u konstatua se në dy raste kemi dublikim të kodit të kontratës, edhe pse ky kod duhet të vendoset në mënyrë automatike nga sistemi. Konkretisht kodi i kontratës me numër: 7777777 dhe kodi i kontratës me numër: 2147483647, janë të dublikuar.
Mbështetur sa më sipër, kjo nënkupton se sistemi nuk ka kontroll për inputin e të dhënave, çka e bën sistemin vulnerabël. Sistemi duhet të gjenerojë numrin e kontratave në mënyrë automatike dhe në rritje inkrementale.
-Tek kolona "Numri i ID", sistemi duhet të ketë kontrolle të vlefshmërisë së informacionit pasi dihet që numri i identifikimit është unik dhe ka një format të përcaktuar se si është i ndërtuar, dhe në këtë kolonë nuk mund të popullojmë të dhëna jashtë formatit të përcaktuar. Është konstatuar një numër i lartë rastesh që popullimi i kësaj fushe është bërë jo sipas përcaktimeve;
-Tek kolona "Nipt", sistemi duhet të ketë kontrolle të vlefshmërisë së informacionit pasi dihet që numri nipt është unik dhe ka një format të përcaktuar se si është i ndërtuar, dhe në këtë kolonë nuk mund të popullojmë të dhëna jashtë formatit të përcaktuar;
-Konfigurimi i fushave input të sistemit. Gjatë popullimit të të dhënave të një abonenti sistemi duhet të shfaqë për të plotësuar vetëm ato fusha me të dhënat që kërkohen sipas profilit të abonentit. P.sh. në qoftë se abonenti është familjar, nga sistemi nuk duhet të shfaqet për tu populluar fusha që kërkon niptin e kompanisë. Kjo fushë duhet të jetë aktive vetëm për abonentët biznes;
-Ka raste që lexuesit hedhin leximet e një matësi tjetër në faturimet e një abonenti që nuk është i lidhur me atë matës. Këto raste vihen re dhe verifikohen vetëm pasi abonenti i drejtohet me ankesë UKD që e ve në dijeni që është faturuar gabim. Pas verifikimit këto fatura sistemohen në sistem duke krijuar fatura me vlerë negative në mënyrë që zerohet vlera e shtuar gabim nga leximi dhe faturimi.
Kriteri: Ligji nr. 2/2017, datë 26.01.2017 *"Për Sigurinë Kibernetike",*neni 27 i ligjit nr. 9887, "*Për mbrojtjen e të dhënave personale*", i ndryshuar, ISO/IEC 27001 "*Information security management*".
Ndikimi/efekti: Risk për mos-evidentimin dhe mos-parandalimin e problematikave që lidhen me inputin e të dhënave.
Shkaku: Mos marrja e masave paraprake për parandalimin e problematikave që lidhen me popullimin e sistemit.
Rëndësia: E Lartë
8.1.Rekomandim: Strukturat drejtuese në UKD së bashku me specialistët e IT-së, të analizojnë dhe adresojnë tek ofruesi i shërbimit të mirëmbajtjes, parregullsitë, mangësitë e konstatuara nga auditimi dhe të ofrojnë zgjidhje të menjëhershme për to. Gjithashtu të ndërtohen konfigurimet përkatëse të fushave në sistem, mbi popullimin e tyre, sipas natyrës së abonentit,

duke vendosur njëkohësisht kufizime në sistem me qëllim ndalimin e hedhjeve të të dhënave jo të sakta.

8.2.Rekomandim: Struktura e teknologjisë së informacionit, të marrë masa për analizimin e situatës aktuale në lidhje me integritetin dhe plotësinë e të dhënave që përmbajnë sistemet informatike Flare ERP dhe Mobiread dhe të merren masat e nevojshme për implementimin e mekanizmave të kontrollit dhe validimit të inputit në sistemet informatik, për menaxhimin e gabimeve njerëzore dhe teknike në lidhje me përdorimin e sistemit, me qëllim parandalimin e përsëritjes së problematikave të konstatuara mbi popullimin jo të saktë të fushave si Nipt, Numri i ID apo adresa, apo fusha të tjera me qëllim automatizimin dhe rritjen e efektivitetit të shërbimeve për të cilat është investuar.

8.3.Rekomandim: Strukturat përgjegjëse në UKD të marrin masa të menjëhershme për ngritjen e një grupi pune të përbashkët për të populluar me informacionin përkatës në sistem, kontratat sipas abonentëve dhe popullimin e të gjitha fushave të kërkuara nga sistemi. Ky proces të shtrihet për të gjitha zonat që mbulon UKD me shërbim dhe të dokumentohet procesi i punës në mënyrë që të parandalohet përsëritja e problematikave të njëjta.

9. Titulli i gjetjes: Mungesa e menaxhimit të logeve
Situata: Nga auditimi u konstatua se:
- Të gjitha log-et janë të ruajtura në makinat fizike përkatëse, por ato nuk janë testuar, analizuar dhe monitoruar ndonjëherë, nëse janë të plota, funksionale dhe të përdorshme. Nuk është e përcaktuar se për sa kohë ruhen këto log-e dhe çfarë procedure ndiqet për analizimin e tyre. Ekstraktet e logeve të sistemit të kërkuara nga grupi i auditimit të ekstraktuara nga OE, në pamundësi për tu ekstraktuar nga specialistët e UKD, për shkak se sistemi bënte crash, u sollën jashtë afatit të kërkuar dhe ishin jo të plota, kështu që ishte e pamundur analizimi i tyre në tërësi.
-Nga verifikimi i dokumentacionit u konstatua se UKD nuk disponon akte rregullator për menaxhimin e log-eve digjitale, në kundërshtim me rekomandimet e pikës 4 shkronja a) të "Rregullores për menaxhimin e log-eve digjitale në Administratën Publike", miratuar me urdhrin nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT) Institucioni duhet të përcaktojë një rregullore të shkruar për menaxhimin e log-eve sipas kërkesave të institucionit.
- Nuk janë përcaktuar burimet e nevojshme si dhe detyrat e personelit për menaxhimin e log-eve;
- UKD nuk zhvillon kontrolle mbi Audit Log, pavarësisht rëndësisë që kanë këto të dhëna në përmirësimin e sistemit, konstatimin dhe analizimin e problematikave të ndryshme.
Kriteri: Rregullore për "Menaxhimin e Log-eve digjitale në administratën publike" miratuar nga AKCESK me urdhrin nr. 109, datë 10.06.2016.
Ndikimi/efekti: Pamundësi për të identifikuar ndërhyrjet në sistem nga përdoruesit e sistemit.
Shkaku: Mungesa e strukturave për të dhënat në UKD, mos zbatim i rregullores së miratuar nga AKCESK.
Rëndësia: E Lartë
9.1.Rekomandim: Strukturat drejtuese në UKD t'i japin rëndësi sigurisë dhe mbrojtjes së të dhënave duke filluar me hartimin e një procedure apo rregullore për menaxhimin e gjurmës elektronike të auditimit, me qëllim uljen e riskut mbi sigurinë e të dhënave me pasojë humbjen dhe tjetërsimin e tyre. Në këtë dokument duhet të specifikohet qartë vendi ku ruhen gjurmët, për cilat veprime të përdoruesit ruhen këto gjurmë, koha, struktura përgjegjëse për monitorimin dhe analizimin e tyre, detyrat dhe përgjegjësitë, e çdo element që i shërben sigurisë së të dhënave në përputhje me rregulloret dhe legjislacionin në fuqi.

IV. GJETJET DHE REKOMANDIMET

A. MASA ORGANIZATIVE:

1.Gjetje nga auditimi: Nga administrimi i dokumentacionit për identifikimin dhe menaxhimin e riskut në teknologjinë e informacionit, u konstatua se UKD nuk disponon regjistër risku të përgjithshëm institucional, ku të përfshihen edhe risqet mbi IT dhe të mbulohen të gjithë aktivitet duke përfshirë këtu risqet mbi sistemet Flare ERP dhe Mobiread, proceset e menaxhimit të ndryshimit, etj. UKD nuk ka identifikuar dhe vlerësuar ngjarjet e mundshme që mund të kenë efekte negative përsa i përket arritjes së objektivave të shoqërisë.
Nisur sa më sipër rezulton se shoqëria UKD Sh.A. nuk ka hartuar regjistrin e riskut ku të përfshiheshin edhe risqet që lidhen me teknologjinë e informacionit, kjo mbështetur në nenin 11, pika 2, neni 12 pika 3/d si 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*", 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*".
(Më hollësisht trajtuar në pikën (2.1) faqe (13-26) të Raportit Përfundimtar të Auditimit)
1.1.Rekomandim: Administratori i shoqërisë në bashkëpunim me Drejtorët e Drejtorive dhe Degëve të marrin masa për identifikimin dhe hartimin e regjistrit të riskut me qëllim analizimin dhe vlerësimin e risqeve, për të mos riskuar përmbushjen e objektivave të shoqërisë në përputhje me përcaktimet ligjore e nënligjore, në të cilin të përcaktohen edhe risqet në teknologjinë e informacionit. Gjithashtu të marrin masa për hartimin dhe dokumentimin e një plan veprimi për minimizimin/ parandalimin e risqeve të identifikuara, si dhe të bëhet monitorimi periodik i zbatimit të këtyre masave.

Brenda vitit 2023 dhe në vijimësi

2.Gjetje nga auditimi: Nga auditimi u konstatua se ambienti fizik i dhomës së serverave ku janë hostuar serverat e sistemeve Flare ERP, Mobiread dhe Oxana si dhe disa pajisje të tjera nuk është në përputhje me standardet e përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (*Versioni 1.0, datë 02.12.2008*) miratuar nga AKSHI (*Agjencia Kombëtare e Shoqërisë së Informacionit*).
(Më hollësisht trajtuar në pikën (2.1) faqe (13-26) të Raportit Përfundimtar të Auditimit)
2.1.Rekomandim: UKD të marrë masa për planifikimin dhe ngritjen e një infrastrukture IT (ambienteve të dhomës të serverëve dhe rrjetin network) në përputhje me kushtet teknike të përcaktuara në rregulloren e miratuar nga AKSHI, që parashikon përcaktimin e standardeve të TIK si dhe në përputhje me udhëzimet, standardet dhe praktikat më të mira kombëtare dhe ndërkombëtare.

Brenda vitit 2023 dhe në vijimësi

3.Gjetje nga auditimi: Nga auditimi mbi konfigurimet aktuale për switch-et kryesore u konstatua se:
-Nuk janë marrë masat e nevojshme që useri admin të limitohet në logimin vetëm nga IP-të brenda rrjetit privat dhe nuk është e bllokuar që useri admin të logohet nga jashtë rrjetit, pra nga një rrjet publik;
-Nuk janë krijuar group users me nivele të ndara menaxhim/monitorim. Çdo veprim bëhet nga useri admin;
-Nuk janë krijuar zona me limite të caktuara për brenda LAN si dhe rrjeti nuk është i ndarë në VLAN (rrjete virtuale) çka do të bënte të mundur menaxhimin dhe lejimin e grupeve të IP-ve në shërbime të ndryshme sipas nevojave. Gjithashtu nuk është krijuar edhe një zonë Untrust e

cila sipas konfigurimeve shërben për bllokimin e portave të shërbimeve si dhe bllokimin e IP-ve të cilat mund të paraqesin problematika ose sulme;
-Pajisja firewall ka të aktivizuar log-s çka bën të mundur për të verifikuar një sërë procesesh që routeri kryen.
(Më hollësisht trajtuar në pikën (2.1) faqe (13-26) të Raportit Përfundimtar të Auditimit)
3.1.Rekomandim: Zyra IT pranë UKD të marrë masat e nevojshme për krijimin e konfigurimeve përkatëse në rrjetin e institucionit mbi logimin, konfigurimin dhe sigurinë e switch-ve dhe firewall-it. Të krijohen zona me limite të caktuara brenda LAN si dhe rrjeti të konfigurohet në VLAN (rrjete virtuale) për menaxhimin dhe lejimin e grupeve të IP-ve në shërbime të ndryshme sipas nevojave. Gjithashtu të merren masa për administrimin dhe implementimin e të gjitha konfigurimeve të nevojshme të evidentuara nga auditimi dhe të tjera të mundshme, me qëllim rritjen e sigurisë së infrastrukturës network.

Menjëherë dhe në vijimësi

4.1.Gjetje nga auditimi: Nga auditimi u konstatua se:
-Procedura e ndjekur për kryerjen e backup-ve nuk është e pasqyruar apo e dokumentuar në një dokument administrativ si Rregullore e Brendshme apo dokument tjetër TIK ku të përcaktohet mënyra e kryerjes së backup-ve, procesin e ruajtjes së të dhënave për sistemet në përdorim nga punonjësit e UKD;
-Procedurat e backup ndiqen nga operatori ekonomik që kryen mirëmbajtjen;
-Procedurat e rikthimit (restore) të të dhënave nuk testohen për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar për sistemet e sipërpërmendura;
-Ruajtja e backup në vende në distancë nuk realizohet;
-Në rastet kur të dhënat e backup-it janë të panevojshme nuk ekzistojnë procedura për mënyrën e nxjerrjes së tyre jashtë përdorimit;
-Nuk është e qartë nëse kontrollohet statusi i backup-it nëse procedura është kryer me sukses.
4.2.Gjetje nga auditimi: Nga auditimi u konstatua se, Ujësjellës Kanalizime Durrës nuk disponon një infrastrukturë DRC (*disaster recovery center*) për rikuperimin dhe vazhdimësinë e punës pa ndërprerje si dhe sigurinë e ruajtjes së të dhënave në rastet e dështimit të qendrës së të dhënave primare, duke mbartur riskun për humbjen e të dhënave.
- Nuk disponon dokument të planeve 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;
-Nuk ka identifikuar sistemet ose pjesët e tyre të cilat janë kritike për ofrimin e shërbimit 24 orë në 7 ditë të javës.
(Më hollësisht trajtuar në pikën (2.1) faqe (13-26) të Raportit Përfundimtar të Auditimit)
4.1.Rekomandim: Strukturat drejtuese në UKD në bashkëpunim me zyrën e IT-së të marrin masa për ndërtimin dhe hartimin e planeve të vazhdimësisë së biznesit duke përfshirë planet për backup për sistemet, pajisjet kompjuterike dhe të dhënat, me qëllim garantimin e sigurisë së informacionit dhe uljen e riskut për ndërprerjen e shërbimeve dhe vazhdimësisë së punës.

Brenda vitit 2023

4.2.Rekomandim: UKD duke marrë në konsideratë që në të ardhmen do të ristrukturohet në një shoqëri Rajonale të Ujësjellës Kanalizime, ndryshim i cili do të sjellë bashkim me

ujësjellësit e tjerë në një të vetëm, të bëjë të mundur marrjen e masave afatgjata për planifikimin dhe ngritjen e një infrastrukture DRC në përputhje me kushtet teknike të përcaktuara aktet ligjore dhe nënligjore, që parashikojnë përcaktimin e standardeve të TIK si dhe në përputhje me udhëzimet, standardet dhe praktikat më të mira kombëtare dhe ndërkombëtare në lidhje me ndërtimin e një site dytësor, me qëllim mundësimin e ofrimit të shërbimit pa ndërprerje dhe parandalimin e humbjes ose të shkatërrimit aksidental të të dhënave, në rastet e dështimit të qendrës së të dhënave primare.

Në vijimësi

5.Gjetje nga auditimi: Nga administrimi i dokumentacionit u konstatua se:
-UKD, ka investuar në ngritjen e Active Directory për menaxhimin e userave, pajisjeve, aplikacioneve dhe marrjen e shërbimeve me anë të një autentifikimi të vetëm "*single sign in*", por nuk e ka vënë në përdorim akoma Active Directory. duke mos përdorur të gjitha përfitimet e saj.
-Të gjitha konfigurimet e Active Directory janë by default, pra konfigurimi i politikave të sigurisë mbi fjalëkalimet, të drejtat e përdoruesve, të dhënat e sigurisë, etj, janë në gjendjen fillestare të lënë nga sistemi në momentin e implementimit të aplikacionit.
Disa nga risqet që vijnë si rezultat i konfigurimeve default i active directory:
-Ekziston rreziku i mos menaxhimit të politikave që mund t'i lejojë përdoruesit të marrin shumë të drejta;
-Rreziku që politikat e fjalëkalimit nuk janë në përputhje me kërkesat e entitetit ose praktikat më të mira. Kjo mund ta bëjë më të lehtë për personat e paautorizuar qasjen në rrjet dhe sisteme;
-Fjalëkalimet që nuk skadojnë kurrë mund të rezultojnë në akses të paautorizuar. Ky është veçanërisht një rrezik nëse ka llogari të përbashkëta përdoruesish ose llogari të sistemit me privilegje administratori. Kështu, ish-punonjësit mund të abuzojnë me këto të drejta;
- Llogaria e një përdoruesi me një fjalëkalim bosh mund të rezultojë në akses të paautorizuar;
-Nëse kompania ka vetëm një politikë fjalëkalimi, ajo duhet t'i përshtatet të gjitha nevojave, dhe për këtë arsye mund të jetë e dobët, etj.
(Më hollësisht trajtuar në pikën (2.1) faqe (13-26) të Raportit Përfundimtar të Auditimit)
5.1.Rekomandim: UKD të marrë masa për konfigurimin dhe vendosjen në përdorim të Active Directory, me qëllim standardizimin e infrastrukturës IT, rritjen e sigurisë së rrjetit si dhe garantimin e një identifikimi të qendërzuar dhe të sigurt.
Për një identifikim të qendërzuar të sigurt të kontrollit dhe menaxhim të shërbimeve, konfigurimi i politikave të sigurisë së Active Directory duhet të realizohet sipas rëndësisë dhe në përputhje me standardet më të mira, në mënyrë që të rritet niveli i sigurisë së aksesit.

Menjëherë

6.Gjetje nga auditimi: Për periudhën e audituar, u konstatua se UKD nuk ka politika të ruajtjes së dokumenteve dhe nuk ka të dokumentuar një plan masash për identifikimin, trajtimin e gabimeve dhe incidenteve që mund të ndodhin në infrastrukturën IT, dhe në mungesë të procedurave të shkruara, risqet menaxhohen mbi bazë ngjarjesh. Suporti, mbështetje teknike dhe logjike për operacionet IT që ndihmojnë mbarëvajtjen e strukturave të institucionit, kryhen nëpërmjet shkëmbimeve verbale dhe nëpërmjet e-mail-eve.
(Më hollësisht trajtuar në pikën (2.1) faqe (13-26) të Raportit Përfundimtar të Auditimit)
6.1.Rekomandim: Strukturat Drejtuese në UKD në bashkëpunim me zyrën IT të marrin masa për identifikimin, dokumentimin dhe monitorimin e incidenteve si dhe menaxhimin e ndryshimeve dhe dokumentimin e tyre.

Menjëherë dhe në vijimësi

7.Gjetje nga auditimi: Nga auditimi u konstatua se funksionimi dhe organizimi i strukturës së IT-së në nivel zyre nën varësi të Drejtorisë ligjore dhe me një staf shumë të vogël, nuk i përgjigjet shtrirjes së teknologjisë së informacionit në UKD duke sjellë uljen e ndikimit të IT-

së në qeverisjen e shoqërisë si dhe zbeh ndikimin e varësisë direkt nga menaxhimi i lartë.
(Më hollësisht trajtuar në pikën (2.1) faqe (13-26) të Raportit Përfundimtar të Auditimit)
7.1.Rekomandim: Strukturat drejtuese të UKD, duke marrë në konsideratë kohën, burimet e nevojshme të analizojnë mundësinë e ndryshimeve strukturore të strukturës ekzistuese IT me qëllim rritjen e rolit të saj dhe të marrin masa për ngritjen në nivel të strukturës së IT nga nivel zyre në nivel Drejtorie.

Brenda vitit 2023

8.1.Gjetje nga auditimi: Nga auditimi u konstatua se, dy nga tre manualet e përdorimit të moduleve të sistemit Flare ERP nuk janë të përditësuara. Këto manuale shërbejnë si udhëzues për të gjithë përdoruesit që kanë të drejtë të aksesojnë sistemin Flare ERP. Sistemi i mundëson shoqërisë trajtimin dhe menaxhimin e abonentëve, matësave, tarifave, artikujve, nivelet e çmimeve, leximet e matësave dhe menaxhimin e abonentëve në qytetin e Durrësit dhe zonave që UKD menaxhon.
- Manual përdorimi për modulin "Flare Accounting"
- Manual përdorimi për modulin "Flare Billing"
- Manual përdorimi për modulin "Flare HR and Payroll"
Këto manuale përdorimi u shpjegojnë përdoruesve se si të kryejnë të gjithë proceset e përdorimit të sistemit duke filluar që nga hapja e userave sipas roleve përkatës deri në shpjegimin e menuve dhe nën menuve përkatëse në sistem. Sistemi është i përbërë nga 4 module dhe secili modul ka manualin përkatës.
8.2.Gjetje nga auditimi: Nga auditimi u konstatua se nuk ka një akt rregullues në të cilin të përcaktoheshin rregullat standarde mbi përdorimin e e-mailit të punës, përgjegjësitë e gjithsecilit, siguria, administrimi, etj.
(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)
8.1.Rekomandim: UKD, të hartojë, amendojë dhe miratojë, manualet e përdorimit të sistemit Flare ERP duke reflektuar ndryshimet institucionale, strukturore dhe kompjuterike që priten të ndodhin pas transformimit shoqërisë UKD në shoqëri rajonale.
Gjithashtu të merren masa për hartimin dhe miratimin e një rregulloreje të përgjithshme për funksionimin e sistemeve të teknologjisë së informacionit të cilët ka në përdorim UKD, në të cilat të jenë të pasqyruara saktë përgjegjësitë, detyrat dhe të drejtat për menaxhimin e përdoruesve të këtyre sistemeve. Në këtë rregullore të përcaktohen edhe rregulla për menaxhimin dhe përdorimin e e-mailit zyrtar të punës.

Brenda vitit 2023 dhe në vijimësi

9.Gjetje nga auditimi: Nga auditimi mbi politikat e sigurisë së përdoruesve në sistemet ERP dhe Mobiread u konstatua se:
- Passwordin e userit, sistemi e merr automatikisht siç është username i përdoruesit dhe sistemi nuk të lejon të menaxhosh këtë funksion;
- Përdoruesi sapo logohet (first log-in) me fjalëkalim fillestar, nuk i shfaqet automatikisht nga sistemi tabela e cila të kërkon vendosjen e fjalëkalimit të ri;
- Në rast se punonjësi nuk e ndryshon fjalëkalimin fillestar dhe vazhdon të përdorë të njëjtin password, sistemi i jep akses pavarësisht se përdoruesi se ka ndryshuar passwordin. Nga të dhënat e ekstraktuara mbi përdoruesit e sistemeve vihet re se edhe pse kërkohet shumë herë reset të paswordit, përdoruesit vazhdojnë sërish me të njëjtat passworde;
- Siguria e vendosjes së fjalëkalimit nuk është e tipit kompleks ku të kërkohet të ketë minimumi 8 karaktere, të ketë të paktën 1 shkronjë dhe 1 shifër.
- Nuk janë dokumentuar politikat e sigurisë të implementuara për përdoruesit e sistemit, si dhe detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre, bazuar në pikën 4 "*Kërkesat e Sigurisë*" pika a. të rregullores për "*Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike*" të miratuar nga AKCESK me urdhrin nr. 86, datë 23.08.2019.

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

(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)

9.1.Rekomandim: Organet drejtuese në UKD të marrin masa për të dokumentuar politikat e sigurisë të implementuara për përdoruesit e sistemit, si dhe detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre sipas përcaktimeve rregullatore të AKCESK. Gjithashtu të merren masa për adresimin e çështjeve të konstatuara nga auditimi, me qëllim rritjen e sigurisë së identifikimit të përdoruesve. Të merren në konsideratë praktikat e përcaktuara në rregulloren për "*Administrimin e fjalëkalimeve në rrjetet dhe sistemet kompjuterike*" miratuar nga AKCESK.

Brenda vitit 2023 dhe në vijimësi

10.1.Gjetje nga auditimi: Nga auditimi mbi përdoruesit aktiv, të ndarë sipas roleve përkatëse në sistemin Flare ERP u konstatua se:

-Në sistemin Flare ERP nuk është e mirë përcaktuar forma e username, duke qenë se ajo popullohet manualisht, disa username kanë shkronjën e parë të emrit dhe pastaj mbiemrin, disa username kanë vetëm emrin e përdoruesit, disa emrin dhe një numër, disa vetëm një shkronjë, etj. Username-t nuk janë të standardizuar çka tregon që sistemi nuk ka mekanizma të kontrollit të inputit. Ka raste që username nuk lidhet fare me emrin e përdoruesit pasi username ka vetëm një shkronjë.

-Në rolin "Admin", janë aktiv 4 administrator me atributin që kanë të drejta mbi çdo gjë. Nga auditimi u konstatua se këta usera nuk identifikohet se çfarë procesesh mbulojnë në sistem, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Përdoruesit me username "sistemi", "MarsiKx" si dhe "ace" nuk identifikohen se çfarë procesesh mbulojnë në sistem dhe kujt useri i përkasin, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Kjo gjë përsëritet edhe në rolin Financë-operator. Gjithashtu ka përdorues që kanë rolin "Admin", ndërkohë që pozicioni i punës së këtyre përdoruesve nuk përputhet me rolin që kanë në sistem.

-Në rolin "Admin viewer", është aktiv vetëm një përdorues me atribute për të parë në sistem.

-Në rolin "Sys Admin" është aktiv një përdorues që është njëkohësisht përgjegjësi i zyrës së IT, dhe ka të drejta Viewer si dhe të drejta mbi përdoruesit. Pra përgjegjësi i zyrës IT që duhet të ishte në rolin e Super Admin, duke qenë së është administratori i sistemit, nuk ka të drejta të plota në sistem.

-Atributet dhe rolet e userave në sistemin Flare ERP nuk janë të përcaktuara sipas detyrave dhe përgjegjësive të përcaktuara në rregulloren e brendshme për funksionimin e UKD por sipas funksionaliteteve që punonjësi ushtron në praktikë përgjatë procesit të punës;

-Një përdorues aktiv mund të autentifikohet në më shumë së një kompjuter. Pra me një username mund ta hapësh sistemin Flare ERP në të njëjtën kohë në më shumë se një kompjuter.

10.2.Gjetje nga auditimi: Nga auditimi mbi përdoruesit aktiv, të ndarë sipas roleve përkatëse në sistemin Mobiread u konstatua se:

-Në sistemin Mobiread nuk është e mirë përcaktuar forma e username, duke qenë se ajo popullohet manualisht, disa username kanë shkronjën e parë të emrit dhe pastaj mbiemrin, disa username kanë vetëm emrin e përdoruesit, disa emrin dhe një numër, disa vetëm një shkronjë, etj. Username-t nuk janë të standardizuar çka tregon që sistemi nuk ka mekanizma të kontrollit të inputit. Ka raste që username nuk lidhet fare me emrin e përdoruesit pasi username ka vetëm një shkronjë. Si më poshtë:

-Në rolin "Admin", janë aktiv 4 administrator me atributin që kanë të drejta mbi çdo gjë. Nga auditimi u konstatua se këta usera nuk identifikohet se çfarë procesesh mbulojnë në sistem,

duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Përdoruesit me username "m." si dhe "ace" nuk identifikohen se çfarë procesesh mbulojnë në sistem dhe kujt useri i përkasin, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor, duke rritur riskun e ndërhyrjes në sistem dhe duke rritur riskun e tjetërsimit të të dhënave në sistem. Kjo gjë përsëritet edhe në rolin Azhornues për userat "azhornues 1 dhe 2", në rolin Lexues për userat "lexues 2 dhe 3", në rolin Verifikues për userat "verifikues 1". Gjithashtu ka përdorues që kanë rolin "Admin", ndërkohë që pozicioni i punës së këtyre përdoruesve nuk përputhet me rolin që kanë në sistem.
-Rolin "Admin", e posedon edhe username "d.gj.", i cili sipas informacionit të dhënë ushtron pozicionin e drejtorit tregtar në UKD Sh.a, pra këtij useri i janë dhënë atributet e administratorit të sistemit, në mospërputhje me aktivitetin e punës që ushtron në sistem.
-Në rolin "Admin viewer", janë aktiv dy përdorues me atribute për të parë në sistem. Përdoruesi me username "suport" nuk identifikohet në sistem se kujt useri i përket, pra nuk lidhet me një përdorues të përvetshëm në mënyrë që të mbikëqyret se cili person e përdor.
(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)

10.1.Rekomandim: Strukturat drejtuese në UKD të marrin masa për analizimin e hollësishëm të të gjithë përdoruesve aktivë në sistemet që ka në përdorim UKD me të drejta në sistem sipas pozicioneve të punës dhe të të gjithë çështjeve të konstatuara nga auditimi, me qëllim rritjen e sigurisë së identifikimit të përdoruesve. Pas analizimit dhe evidentimit të të gjithë përdoruesve, të merren masa për bllokimin e aksesit dhe ç'aktivizimin e të gjithë përdoruesve të cilët nuk janë të lidhur me përdorues të identifikueshëm, kanë më shumë se një user, kanë më shumë atribute se pozicioni i punës, të mbyllë përdoruesit të cilët kanë përfunduar objektin e krijimit si dhe të gjitha çështjet e konstatuara nga grupi i auditimit me qëllim ruajtjen e sistemeve nga ndërhyrjet e paautorizuara. Gjithashtu të standardizohen username-t e përdoruesve.

Brenda vitit 2023 dhe në vijimësi

11.1.Gjetje nga auditimi: Nga auditimi u konstatua se nuk administrohet asnjë dokumentacion që të faktojë marrjen e kodit burim, për të dy sistemet Flare ERP dhe Mobiread. Nisur sa më sipër dhe në zbatim të rekomandimeve të VKM nr. 710, datë 21.8.2013, të Ministrit për Inovacionin, Teknologjinë e Informacionit dhe të Komunikimit, është nxjerrë Udhëzimi nr. 2, datë 02.09.2013 "*Për standardizimin e Hartimin e termave të Referencës për Projektet TIK në Administratën Publike*". Në germën "e", të pikës 8, të kreut II, të këtij udhëzimi përcaktohet se, për propozimet e kërkuara, institucionet gjatë hartimit të termave të referencës për projektet TIK duhet të marrin në konsideratë çështjet si më poshtë:
"*Të sigurojnë pronësinë e Kodeve Burimore (source code) dhe /ose të drejtën për të blerë Kodet Burimore. Pronësinë e Kodeve Burimore, analiza e projektimit, burimi dhe programet e ekzekutueshme të të gjitha sistemeve të aplikimit të zhvilluara do ti kalojnë institucionit pa asnjë kosto shtesë*". Në zbatim me sa më sipër Kodi i Burimit për të dy sistemet duhet të jetë në pronësi të UKD.

11.2.Gjetje nga auditimi: Nga auditimi u konstatua se:
-Administrimi dhe menaxhimi i databazës së sistemit Flare ERP dhe Mobiread realizohet nga OE. Ky OE gjithashtu është duke ofruar suport për këtë sistem.
Në sistemin Flare ERP administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Sys admin". Sys Admin ushtron funksionet viewer dhe ka të drejta mbi përdoruesit. Në sistemin Mobiread administratori i sistemit që është përgjegjësi i zyrës së IT-së, është i kategorizuar në rolin "Admin" dhe ka të drejta të plota mbi çdo gjë në sistem.
-Detyra e Administratorit të sistemit dhe Administratorit të bazës së të dhënave nuk janë atribuar me anë të një shkrese zyrtare nga organet drejtuese të UKD, ku punonjësit e zyrës IT të janë emëruar zyrtarisht si Administratorë për administrimin e bazës së të dhënave për të ushtruar atributet e përcaktuara sipas funksioneve të tyre dhe të gjitha detyrat e administratorit mbi administrimin e bazës së të dhënave të sistemit.

(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)
11.1.Rekomandim: Strukturat drejtuese në UKD në bashkëpunim me specialistët TIK, të marrin masa për adresimin e këtyre çështjeve tek OE që ka implementuara sistemet Flare ERP dhe Mobiread me qëllim marrjen e kodit në burim të sistemeve, në funksion të përmbushjes të përcaktimeve ligjore si dhe krijimin e kushteve të barabarta për operatorët ekonomik që dëshirojnë të marrin pjesë në procedurat e prokurimit, duke mos penguar konkurrencën e lirë si dhe të stimulojnë pjesëmarrjen e biznesit të vogël dhe të mesëm.

Brenda vitit 2023 dhe në vijimësi

11.2.Rekomandim: Administratori i UKD të marri masa për përcaktimin e detyrës së Administratorit të sistemit dhe Administratorit të bazës së të dhënave, ku të jenë emëruar zyrtarisht Administratorët për administrimin e sistemit dhe bazës së të dhënave duke përcaktuar dhe atributet specifike sipas funksioneve të tyre dhe të gjitha detyrat e administratorit.

Menjëherë

12.Gjetje nga auditimi: Nga auditimi u konstatua se nuk janë dokumentuar, diagramat e rrjedhës së informacionit , për çdo produkt apo shërbim të konfiguruar në sistemin Flare ERP. Gjithashtu nga grupi i auditimit nuk u administrua një dokumentim skematik mbi proceset, rregullat dhe procedurat e implementuara për çdo modul apo shërbim që është informatizuar në sistemin Flare ERP.
(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)
12.1.Rekomandim: Strukturat Drejtuese në UKD krahas identifikimit të proceseve që nevojiten për dokumentimin e gjurmës audituese, të marrin masa që të hartojnë dhe dokumentojnë diagramat e rrjedhës së informacionit për çdo proces që realizohet nëpërmjet sistemeve me qëllim përcaktimin e të dhënave hyrëse, roleve, ndryshimin, miratimin dhe përfundimin për çdo shërbim që realizohet nëpërmjet sistemit informatik.

Brenda vitit 2023 dhe në vijimësi

13.Gjetje nga auditimi: Nga auditimi u konstatua se:
-Nivel shumë i ulët i sigurisë së autentifikimit në portal. Për tu identifikuar në këtë portal abonenti apo klienti duhet të vendosi në të dyja dritaret numrin e kontratës, pra edhe username edhe password janë numri i kontratës.
-Mungesa e elementëve të sigurisë në ndërfaqen e portalit "selfcare". Pasi është log-uar për herë të parë në portal, abonenti nuk ka asnjë mundësi që të ndryshojë fjalëkalimin, pra fjalëkalimi mbetet i njëjtë me numrin e kontratës.
-Risk i lartë për modifikimin e të dhënave si dhe risk për humbjen apo përdorimin e të dhënave personale. Nëse dikush ka ose gjen numrin e kontratës të një abonenti tjetër atëherë ai mund të logohet, të shohë faturat, historikun e faturave.
-Mungesë e popullimit të fushave të kërkuara. Të gjithë ata abonentë në mënyrë rastësore që grupi i auditimit, i kontrolloi në sistem, rezultuan që asnjë prej tyre nuk i kishte të populluara detajet personale, apo të kishte ndonjë historik ankesash, çka nënkupton që këta abonentë nuk e kanë vizituar ndonjëherë këtë portal, apo nuk e kanë aksesuar ndonjëherë kontratën e tyre.
(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)
13.1.Rekomandimi: Strukturat përgjegjëse në UKD të analizojnë dhe adresojnë tek ofruesi i shërbimit të mirëmbajtjes parregullsitë, mangësitë e konstatuara nga auditimi mbi portalin selfcare dhe të ofrojnë zgjidhje për to me qëllim rritjen e nivelit të sigurisë së aksesit në portal dhe garantimin e marrjes së shërbimit të sigurtë për abonentët.

Menjëherë

14.Gjetje nga auditimi: Nga auditimi mbi sistemin Flare ERP u konstatua se:
-Për shkak të mbingarkesës dhe shtimit të shërbimeve, të abonentëve, si dhe për shkak të performancës së dobët të sistemit, ky sistem vazhdimisht punon me ndërprerje dhe ka probleme

me ecurinë normale të punës duke ndikuar në veprimtarinë e specialistëve dhe institucionit në ofrimin e shërbimeve kundrejt qytetarëve dhe bizneseve por edhe vetë administratës së UKD;
-Sistemi krijon vonesa në shqyrtimin dhe gjenerimin e raporteve të ndryshme;
-Kur gjenerohet një raport pivot, në qoftë se tenton të gjenerosh dhe një tjetër, raporti i dytë nuk mund të gjenerohet pa e mbyllur me parë aplikacionin dhe të futesh përsëri;
-Sistemi krijon errore dhe nuk gjeneron të dhëna në qoftë se përzgjedhim raporte për periudha më shumë se një muaj;
-Shfaqet error kur kërkohet të ekstraktohen të dhënat mbi rolet në sistemin Flare ERP;
-Kur tentohet ekstraktimi i klientëve nga sistemi me të gjitha opsionet e zgjedhura të kolonave sistemi bllokohet dhe nuk u përgjigjet komandave dhe nuk ekstrakton asgjë sepse bën crash;
-Kur sistemi aksesohet me anë të VPN, jashtë rrjetit të brendshëm, shpeshherë hasen pengesa në aksesimin e tij, pasi sistemi shfaq error. Në momentin që aksesohet është shumë e vështirë të punohet në të pasi është shumë i ngadaltë në veprime;
-Sinkronizimi ndërmjet dy sistemeve Flare ERP dhe Mobiread, realizohet çdo një muaj, çka rrit riskun e mospasjes së informacionit të përditësuar për abonentët dhe ndryshimet e kontratave ndërmjet dy sistemeve.
(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)
14.1.Rekomandim: Strukturat drejtuese në UKD së bashku me specialistët e IT-së, të analizojnë dhe adresojnë tek ofruesi i shërbimit të mirëmbajtjes, parregullsitë, mangësitë e konstatuara nga auditimi dhe të ofrojnë zgjidhje për to me qëllim përmirësimin e performancës së funksionimit të sistemit Flare në ofrimin e shërbimeve, si dhe të merren masa për shtimin e funksionaliteteve të reja sipas nevojës së përdoruesve në sistem.

Menjëherë dhe në vijimësi

15.Gjetje nga auditimi: Nga auditimi dhe analizimi i të dhënave input/output të sistemit Flare ERP mbi "Abonentët" u konstatua se:
-Kodi i kontratës vendoset në mënyrë automatike nga sistemi Flare ERP dhe në mënyrë inkrementale. Gjatë kohës së vendosjes dhe implementimit të sistemit të Flare ERP në UKD ka qenë në përdorim një tjetër databazë e ngritur me kodin e kontratave. Gjatë implementimit të sistemit Flare ERP të dhënat e mëparshme janë migruar në këtë sistem. Pra të dhënat e ekstraktuara nga sistemi ERP mbi numrat e kontratave nuk i përkasin vetëm atyre të krijuara nga sistemi ERP por edhe nga të dhënat e mëparshme të migruara. Kontratat e reja me sistemin Flare ERP kanë filluar të hapen që prej vitit 2018;
-Kur plotësohen të dhënat e një abonenti, jo të gjitha fushat e afishuara nga sistemi Flare ERP populllohen saktë nga specialistët. Si p.sh. "Adresa e abonentit", kur nuk dihet adresa e saktë shkruhet vetëm emri i zonës ku ndodhet abonenti.
-Rreth 40% e abonentëve kanë informacion të populluar mjaftueshëm të kontratave. Pjesa tjetër kanë informacion të pjesshëm ose nuk janë populluar fare. Ka një numër të lartë abonentësh të cilët nuk kanë një numër identifikimi, nipt (në qoftë se janë biznes) apo edhe numrin e telefonit, çka nënkupton që këta abonentë kur janë regjistruar si abonentë nuk kanë patur dokumentacionin përkatës si kartën ID dhe certifikatën e pronësisë së pronës, dokumente që nevojiten për të hapur një kontratë të re, pra informacioni mbi abonentët nuk është i populluar dhe i përditësuar.
Mbi "Input application data set":
-Nga analizimi i të dhënave mbi Abonentët në total të UKD, aktiv dhe jo aktiv u konstatua se në dy raste kemi dublikim të kodit të kontratës, edhe pse ky kod duhet të vendoset në mënyrë automatike nga sistemi. Konkretisht kodi i kontratës me numër: 7777777 dhe kodi i kontratës me numër: 2147483647, janë të dublikuar.
Mbështetur sa më sipër, kjo nënkupton se sistemi nuk ka kontroll për inputin e të dhënave, çka e bën sistemin vulnerabël. Sistemi duhet të gjenerojë numrin e kontratave në mënyrë automatike dhe në rritje inkrementale.

-Tek kolona “Numri i ID”, sistemi duhet të ketë kontrolle të vlefshmërisë së informacionit pasi dihet që numri i identifikimit është unik dhe ka një format të përcaktuar se si është i ndërtuar, dhe në këtë kolonë nuk mund të popullojmë të dhëna jashtë formatit të përcaktuar. Është konstatuar një numër i lartë rastesh që popullimi i kësaj fushe është bërë jo sipas përcaktimeve;
-Tek kolona “Nipt”, sistemi duhet të ketë kontrolle të vlefshmërisë së informacionit pasi dihet që numri nipt është unik dhe ka një format të përcaktuar se si është i ndërtuar, dhe në këtë kolonë nuk mund të popullojmë të dhëna jashtë formatit të përcaktuar;
-Konfigurimi i fushave input të sistemit. Gjatë popullimit të të dhënave të një abonenti sistemi duhet të shfaqë për të plotësuar vetëm ato fusha me të dhënat që kërkohen sipas profilit të abonentit. P.sh. në qoftë se abonenti është familjar, nga sistemi nuk duhet të shfaqet për tu populluar fusha që kërkon niptin e kompanisë. Kjo fushë duhet të jetë aktive vetëm për abonentët biznes;
-Ka raste që lexuesit hedhin leximet e një matësi tjetër në faturimet e një abonenti që nuk është i lidhur me atë matës. Këto raste vihen re dhe verifikohen vetëm pasi abonenti i drejtohet me ankesë UKD që e ve në dijeni që është faturuar gabim. Pas verifikimit këto fatura sistemohen në sistem duke krijuar fatura me vlerë negative në mënyrë që zerohet vlera e shtuar gabim nga leximi dhe faturimi.
(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)

15.1.Rekomandim: Strukturat drejtuese në UKD së bashku me specialistët e IT-së, të analizojnë dhe adresojnë tek ofruesi i shërbimit të mirëmbajtjes, parregullsitë, mangësitë e konstatuara nga auditimi dhe të ofrojnë zgjidhje të menjëhershme për to. Gjithashtu të ndërtohen konfigurimet përkatëse të fushave në sistem, mbi popullimin e tyre, sipas natyrës së abonentit, duke vendosur njëkohësisht kufizime në sistem me qëllim ndalimin e hedhjeve të të dhënave jo të sakta.

Menjëherë

15.2.Rekomandim: Struktura e teknologjisë së informacionit, të marrë masa për analizimin e situatës aktuale në lidhje me integritetin dhe plotësinë e të dhënave që përmbajnë sistemet informatike Flare ERP dhe Mobiread dhe të merren masat e nevojshme për implementimin e mekanizmave të kontrollit dhe validimit të inputit në sistemet informatik, për menaxhimin e gabimeve njerëzore dhe teknike në lidhje me përdorimin e sistemit, me qëllim parandalimin e përsëritjes së problematikave të konstatuara mbi popullimin jo të saktë të fushave si Nipt, Numri i ID, adresa, apo fusha të tjera me qëllim automatizimin dhe rritjen e efektivitetit të shërbimeve për të cilat është investuar.

Menjëherë dhe në vijimësi

15.3.Rekomandim: Strukturat përgjegjëse në UKD të marrin masa të menjëhershme për ngritjen e një grupi pune të përbashkët për të populluar me informacionin përkatës në sistem, kontratat sipas abonentëve dhe popullimin e të gjitha fushave të kërkuara nga sistemi. Ky proces të shtrihet për të gjitha zonat që mbulon UKD me shërbim dhe të dokumentohet procesi i punës në mënyrë që të parandalohet përsëritja e problematikave të njëjta.

Menjëherë

16.Gjetje nga auditimi: Nga auditimi u konstatua se:
- Të gjitha log-et janë të ruajtura në makinat fizike përkatëse, por ato nuk janë testuar, analizuar dhe monitoruar ndonjëherë, nëse janë të plota, funksionale dhe të përdorshme. Nuk është e përcaktuar se për sa kohë ruhen këto log-e dhe çfarë procedure ndiqet për analizimin e tyre. Ekstraktet e logeve të sistemit të kërkuara nga grupi i auditimit të ekstraktuara nga OE, në pamundësi për tu ekstraktuar nga specialistët e UKD, për shkak se sistemi bënte crash, u sollën jashtë afatit të kërkuar dhe ishin jo të plota, kështu që ishte e pamundur analizimi i tyre në tërësi.

-Nga verifikimi i dokumentacionit u konstatua se UKD nuk disponon akte rregullator për menaxhimin e log-eve digjitale, në kundërshtim me rekomandimet e pikës 4 shkronja a) të "Rregullores për menaxhimin e log-eve digjitale në Administratën Publike", miratuar me urdhrin nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT) Institucioni duhet të përcaktojë një rregullore të shkruar për menaxhimin e log-eve sipas kërkesave të institucionit.
- Nuk janë përcaktuar burimet e nevojshme si dhe detyrat e personelit për menaxhimin e log-eve;
- UKD nuk zhvillon kontrolle mbi Audit Log, pavarësisht rëndësisë që kanë këto të dhëna në përmirësimin e sistemit, konstatimin dhe analizimin e problematikave të ndryshme.
(Më hollësisht trajtuar në pikën (2.2) faqe (27-51) të Raportit Përfundimtar të Auditimit)
16.1.Rekomandim: Strukturat drejtuese në UKD t'i japin rëndësi sigurisë dhe mbrojtjes së të dhënave duke filluar me hartimin e një procedure apo rregullore për menaxhimin e gjurmës elektronike të auditimit, me qëllim uljen e riskut mbi sigurinë e të dhënave me pasojë humbjen dhe tjetërsimin e tyre. Në këtë dokument duhet të specifikohet qartë vendi ku ruhen gjurmët, për cilat veprime të përdoruesit ruhen këto gjurmë, koha, struktura përgjegjëse për monitorimin dhe analizimin e tyre, detyrat dhe përgjegjësitë, e çdo element që i shërben sigurisë së të dhënave në përputhje me rregulloret dhe legjislacionin në fuqi.

Brenda vitit 2023 dhe në vijimësi

Për sa më sipër paraqitet ky Raport Përfundimtar Auditimi

KONTROLLI I LARTË I SHTETIT