RAPORT PËRFUNDIMTAR I AUDITIMIT

"Mbi Auditimin e Kontrolleve Bazë të Teknologjisë së Informacionit në Kolegjin e Mbrojtjes dhe Sigurisë"

Tiranë, dhjetor 2025

LISTA E SHKURTIMEVE

Shkurtimi	Emërtimi i plotë
KLSH	Kontrolli i Lartë i Shtetit
KMS	Kolegji i Mbrojtjes dhe Sigurisë
SHPFA	Shtabi i Përgjithshëm i Forcave të Armatosura
FARSH	Forcat e Armatosura të Republikës së Shqipërisë
ASNI	Agjencia e Sistemeve të Ndërlidhjes dhe të Informacionit
KKN	Komanda Kibernetike dhe e Ndërlidhjes
AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit
AKCESK	Autoriteti Kombëtar për Sigurinë Kibernetike
TI(IT)	Teknologjia e Informacionit
TIK	Teknologjia e Informacionit dhe Komunikimit
LAN	Rrjet i zonës lokale
WAN	Rrjet i zonës së gjerë
PSV(SOP)	Procedura Standarde të Veprimit
VKM	Vendim i Këshillit të Ministrave
ISO	International Organization for Standardization
COBIT	Objektivat e Kontrollit për Informacionin dhe Teknologjinë përkatëse
ISSAI	Standardet Ndërkombëtare të Institucioneve Supreme të Auditimit

I. PËRMBLEDHJE EKZEKUTIVE

KLSH mbështetur në Ligjin nr. 154, datë 27.11.2014 "*Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit*", zhvilloi auditimin e Kontrolleve Bazë të Teknologjisë së Informacionit, nga data 26.06.2025 deri në 21.07.2025.
Grupi i auditimit pasi mblodhi informacione të mjaftueshme, zhvilloi pyetësorë e intervista për caktimin e zonave me risk të lartë, mbështetur në këto të dhëna hartoi drejtimet e auditimit.
Kërkesat për informacion për fushat përkatëse u hartuan në përputhje me manualin e Auditimit të Teknologjisë së Informacionit.

1. Përshkrim i shkurtër i Projektit të Auditimit

Auditimi me objekt "Auditimi i Kontrolleve Bazë të Teknologjisë së Informacionit", në KMS, është pjesë e Planit Vjetor 2025 të auditimit të KLSH-së, miratuar nga Kryetari i KLSH-së.
Përzgjedhja e këtij subjekti është bërë bazuar në një analizë risku, si gjatë hartimit të planit vjetor, po ashtu edhe gjatë hartimit të Programit të Projektit të Auditimit, ku KLSH, ka vlerësuar si të rëndësishëm auditimin e kontrolleve bazë të teknologjisë së informacionit në KMS. Pas marrjes së ambienteve të përshtatshme, grupi audites filloi fazën e studimit paraprak, ku u dërgua pyetësori i hartuar nga grupi i auditimit, bazuar në Manualin e Auditimit të Teknologjisë së Informacionit. Programi i auditimit është miratuar nga Kryetari i Kontrollit të Lartë të Shtetit me nr. 584/1, me datë 24.06.2025.

2. Përshkrimi i gjetjeve kryesore dhe rekomandimeve:

Paraqitja e gjetjeve kryesore:
- Nga auditimi u konstatua se, KMS nuk disponon një rregullore të brendshme në të cilën të përcaktohen rregullat e organizimit dhe funksionimit të veprimtarisë institucionale, si dhe detyrat funksionale të punonjësve duke përfshirë edhe teknologjinë e informacionit.
Grupit të auditimit iu vendos në dispozicion një rregullore e cila është akoma në versionin draft, pasi nuk është e miratuar me urdhër të Komandantit të Kolegjit. Gjithashtu draft rregullorja e vendosur në dispozicion grupit të auditimit nuk është në përputhje me përshkrimet e miratuara për çdo pozicion pune, sipas Urdhrit nr. 262/1, datë 27.12.2023 "*Për miratimin e përshkrimit të pozicioneve të punës në Kolegjin e Mbrojtjes dhe Sigurisë*".
- Nga auditimi u konstatua se, KMS për periudhën objekt auditimi për vitet 2023-2024 nuk ka identifikuar, planifikuar dhe realizuar trajnime mbi sigurinë dhe teknologjinë e informacionit, duke pasur parasysh elementët më të rëndësishëm si ruajtja e të dhënave, të drejtat dhe detyrimet mbi mjetet teknologjike që disponon institucioni, etj., si për burimet njerëzore të cilët mbulojnë fushën e TI dhe për punonjësit të cilët janë përdorues të pajisjeve dhe sistemeve teknologjike, kjo në kundërshtim me Ligjin nr.10296 datë 08.07.2010 "*Për menaxhimin financiar dhe kontrollin*" i ndryshuar, si dhe standardet ndërkombëtare të TI për rritjen e kapaciteteve.
- Nga auditimi u konstatua se, nuk janë dokumentuar politikat e sigurisë të implementuara për përdoruesit e rrjetit kompjuterik që KMS përdor mbi detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre, si dhe nuk është hartuar një rregullore ose dokument mbi parametrizimin e fjalëkalimeve që të përcaktojë përmbajtjen, gjatësinë, mos përsëritjen e të njëjtit fjalëkalim etj. Forcimi i kritereve të fjalëkalimit konsiderohet element sigurie në standardet mbi sigurinë e informacionit, rreziqet që lidhen me fjalëkalimet e dobëta çojnë në akses të autorizuar, shkelje të sigurisë etj. Nga auditimi konstatohet se përdoruesit nuk ndjekin një politikë të qartë, për përdorimin e fjalëkalimeve të forta dhe ndërrimin e tyre periodik sipas përcaktimeve rregullatore të AKCESK, duke e lehtësuar për sulmuesit realizimin e sulmeve brute-force, credential stuffing, dictionary attacks ose password spraying për të fituar akses të paautorizuar.
- Nga auditimi mbi sistemet e operimit (OS) dhe versionet e tyre, për periudhën objekt auditimi u konstatua se KMS ka në total 66 kompjutera ku rezultuan të jenë si më poshtë:
  - 12 kompjutera janë me sistemin operativ Windows 11 – të cilët aktualisht janë në suport.

- 44 kompjutera janë me sistemin operativ Windows 10 - të cilët janë në suport, që përfundon më 14 tetor 2025. Pas kësaj date Microsoft nuk do të ofrojë më përditësime sigurie, rregullime të gabimeve apo mbështetje teknike për Windows 10. Nëse Windows 10 do të vazhdojë të funksionojë, ai do të bëhet gjithnjë e më i prekshëm ndaj kërcënimeve të sigurisë dhe mund të sjellë dhe probleme të përputhshmërisë me software dhe hardware më të reja;
- 10 kompjutera janë me sistemin operativ Windows 7 - të cilët janë me sistem operimi Windows 7, për të cilat nuk ofrohen më përditësime sigurie, duke e bërë përdorimin e tyre një rrezik të madh për sigurinë, bazuar në zhvillimet teknologjike të sistemeve të operimit dhe Standardet Ndërkombëtare të Sigurisë së Informacionit ISO/IEC 27001:2022.

Paraqitja e rekomandimeve kryesore:

Me qëllim zgjidhjen e problematikave të konstatuara nga gjetjet, janë dhënë disa rekomandime si vijon:

- Kolegji i Mbrojtjes dhe Sigurisë të marrë masa për hartimin dhe miratimin e rregullores së brendshme të institucionit sipas përshkrimeve të miratuara për çdo pozicion pune, në funksionim të përmbushjes së veprimtarisë institucionale.
- Kolegji i Mbrojtjes dhe Sigurisë të marrë masa për trajnimin e gjithë punonjësve në fushën e teknologjisë së informacionit dhe në mënyrë të veçantë punonjësit e ngarkuar me sigurinë e saj.
- Kolegji i Mbrojtjes dhe Sigurisë në koordinim me Shtabin e Përgjithshëm të Forcave të Armatosura të marrin masa për të dokumentuar dhe aplikuar politikat e sigurisë të implementuara për përdoruesit, si dhe detyrimet që nevojiten të aplikohen për fjalëkalimet sipas përcaktimeve rregullatore të Autoritetit Kombëtar për Sigurinë Kibernetike.
- Kolegji i Mbrojtjes dhe Sigurisë në bashkëpunim me Shtabin e Përgjithshëm të Forcave të Armatosura të marrë masa për planifikimin dhe kalimin në sistemin e operimit Windows 11 për të gjitha kompjuterat që KMS ka në përdorim, për të siguruar që pajisjet e tyre të vazhdojnë të marrin përditësime sigurie nga prodhuesi Microsoft dhe të jenë të mbrojtura ndaj kërcënimeve të mundshme.

3. Konkluzioni i përgjithshëm dhe Opinioni i Auditimit

Mbështetur në Standardet Ndërkombëtare të Auditimit përkatësisht në, ISSAI 100, Parimet themelore të auditimit në sektorin publik, ISSAI 5300, Udhëzime për auditimin e IT-së, ISSAI 5310, Metodologjia e Rishikimit të Sigurisë së Sistemit të Informacionit, si dhe nenet 3 dhe 14 të ligjit nr. 154, datë 27.11.2014 *"Për Organizimin dhe Funksionimin e KLSH",* si dhe "Bazuar në procedurat e kryera dhe evidencat e mbledhura gjatë auditimit të Kontrolleve Bazë të Teknologjisë së Informacionit, ne konkludojmë se kontrollet IT të institucionit funksionojnë në mënyrë të pranueshme dhe ofrojnë një nivel të mjaftueshëm sigurie për mbrojtjen e të dhënave dhe funksionimin e sistemeve kritike.

Gjatë auditimit u identifikuan disa dobësi me ndikim mesatar, që lidhen kryesisht me menaxhimin e aksesit, kushtet e infrastrukturës së TI dhe dokumentimin e procedurave.

Në përgjithësi, mjedisi IT është i kontrolluar mirë dhe në përputhje me politikat dhe standardet përkatëse, por rekomandojmë adresimin e gjetjeve të shënuara për të rritur më tej nivelin e sigurisë dhe efektivitetin operacional."

II. HYRJA

Mbështetur në ligjin 154/2014 *"Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit"*, në zbatim të programit nr. 584/1, me datë 24.06.2025, miratuar nga Kryetari i KLSH-së, nga data 26.06.2025 deri më datë 21.07.2025, në subjektin "Kolegji i Mbrojtjes dhe Sigurisë", u krye auditimi me objekt *"Auditimi i Kontrolleve Bazë të Teknologjisë së Informacionit"*, nga grupi i auditimit me përbërje:

1. K.S, përgjegjës grupi;
2. M.P, audituese;
3. A.K, audituese.

1. Objektivat dhe qëllimi i auditimit

Kontrolli i Lartë i Shtetit mbështetur në nenet 3 dhe 14 të ligjit 154 "*Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit*", zhvilloi auditimin e teknologjisë së informacionit në KMS, nga data 26.06.2025 deri më datë 21.07.2025. Kërkesat për informacion sipas drejtimeve të programit të auditimit, u hartuan në përputhje me Manualin e Auditimit të Teknologjisë së Informacionit.
Objekti i Auditimit TIK është verifikim nëse burimet TIK ndihmojnë objektivat e institucionit të arrihen në mënyrën e duhur, përfshirë pajtueshmërinë me kërkesat ligjore dhe rregullative, konfidencialitetin, integritetin si dhe disponueshmërinë e informacionit.
Qëllimi i Auditimit TIK është vlerësimi nëse ekzistojnë kontrollet bazë dhe mekanizmat e kontrollit për përdorimin e burimeve IT.

2. Identifikimi i çështjes

Drejtimet e këtij auditimi janë bazuar në programin me nr. 584/1 Prot., datë 24.06.2025:

1. Verifikimi i politikave, standardeve dhe vlerësimi i burimeve njerëzore në TIK
2. Auditimi i përdorimit të infrastrukturës në Teknologjinë e Informacionit

3. Përgjegjësitë e strukturave drejtuese të subjektit të audituar

Kolegji i Mbrojtjes dhe Sigurisë (KMS) është njësi në varësi të Shtabit të Përgjithshëm të Forcave të Armatosura. KMS është strukturë më vete arsimore brenda Forcave të Armatosura, ka lidhje të drejtpërdrejtë me karrierën e personelit ushtarak dhe civil në përshtatje me zhvillimet e fundit në fushën e Sigurisë dhe Mbrojtjes. Në këtë strukturë planifikohen, zhvillohen dhe drejtohen kurset e karrierës si: Kursi Themelor i Oficerit të Shtabit (KTHOSH), Kursi i Komandës dhe Shtabit të Përgjithshëm (KKSHP), Kursi i Lartë i Oficerit (KLO) dhe Kursi i Lartë për Sigurinë dhe Mbrojtjen (KLSM).

4. Përgjegjësitë e audituesve

Kontrolli i Lartë i Shtetit auditoi KMS mbi periudhën e veprimtarisë nga 01.01.2023 deri në 31.12.2024, në drejtim të kontrolleve bazë të Teknologjisë së Informacionit.
Nga grupi i auditimit, me përgjegjësi të plotë, janë analizuar të gjitha çështjet që përmban programi i auditimit nr. 584/1 Prot., datë 24.06.2025 miratuar nga Kryetari i KLSH-s. Në realizimin e këtij Projekt Auditimi, grupi i auditimit është mbështetur në bazën ligjore mbi të cilën funksionon KLSH, standardet e auditimit, legjislacionin e fushës në të cilën operon institucioni nën auditim si dhe legjislacionin për Teknologjinë e Informacionit në vendin tonë. Gjithashtu, gjatë veprimtarisë audituese është siguruar një evidencë e përshtatshme e mjaftueshme dhe e besueshme auditimi, në të cilën jemi mbështetur në dhënien e konkluzioneve dhe rekomandimeve.

5. 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);
- Ligji nr. 154/2014 *"Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit"*;
- Ligji nr. 10296, datë 08.07.2010 "*Për menaxhimin financiar dhe kontrollin";*
- Ligji nr. 64/2014 *"Për pushtetet dhe autoritetet e drejtimit e të komandimit të Forcave të Armatosura të Republikës së Shqipërisë,* i ndryshuar;
- Ligji nr. 59/2014 *"Për karrierën ushtarake në Forcat e Armatosura të Republikës së Shqipërisë,* i ndryshuar.
- Rregulloret përkatëse të KMS, etj.

6. Standardet e auditimit

Auditimi është kryer në përputhje me Kodin Etik, Standardet dhe teknikat e auditimit të teknologjisë së informacionit, duke përfshirë pyetësorë, intervista, testime dhe procedura, të cilat u gjykuan se ishin të nevojshme, për të dhënë një vlerësim sa më objektiv, profesional e të pavarur, të saktë, të plotë e të qartë duke u fokusuar veçanërisht në standardet e fushës së auditimit të Teknologjisë së Informacionit dhe Komunikimit si: COBIT 4.1, Manuali i Auditimit IT, ISSAI 5310, si dhe ISSAI 5300 Udhëzime për auditimin e IT-së, ISSAI 100 Parimet themelore të auditimet në sektorin publik, etj.

7. Metodat e auditimit

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

- Shqyrtimi i dokumentacionit rregullatorë të institucionit;
- Shqyrtimi i dokumentacioneve për infrastrukturën informatike që institucioni disponon;
- Shqyrtimi i informacioneve dhe raporteve të institucionit në auditim;
- Intervista të zhvilluara me personelin kyç të KMS;
- Verifikimi dhe analizimi i të dhënave, etj.

8. Dokumentimi i auditimit

Dokumentimi i auditimit është bazuar në rregulloren e brendshme të 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 dhe informacione të ndryshme të gjeneruara nga institucioni;
- Letrat e punës mbajtur nga audituesit sipas detyrave të përcaktuara gjatë fazës së auditimit në terren.

III. PËRSHKRIMI I AUDITIMIT

1. Informacioni i përgjithshëm mbi subjektin nën auditim

Kolegji i Mbrojtjes dhe Sigurisë, në ushtrimin e veprimtarisë së tij ka si mision edukimin dhe kualifikimin e personelit ushtarak e civil nëpërmjet programit mësimor, në nivelet e larta të drejtimit të Forcave të Armatosura dhe të institucioneve të tjera të sigurisë kombëtare, për përdorimin kreativ dhe me efikasitet të elementëve të fuqisë kombëtare në kohë paqe, krize dhe lufte, si dhe arsimimin e lidërve civilë e ushtarakë të vendeve partnere dhe të NATO-s.

Detyra e KMS-ës janë:

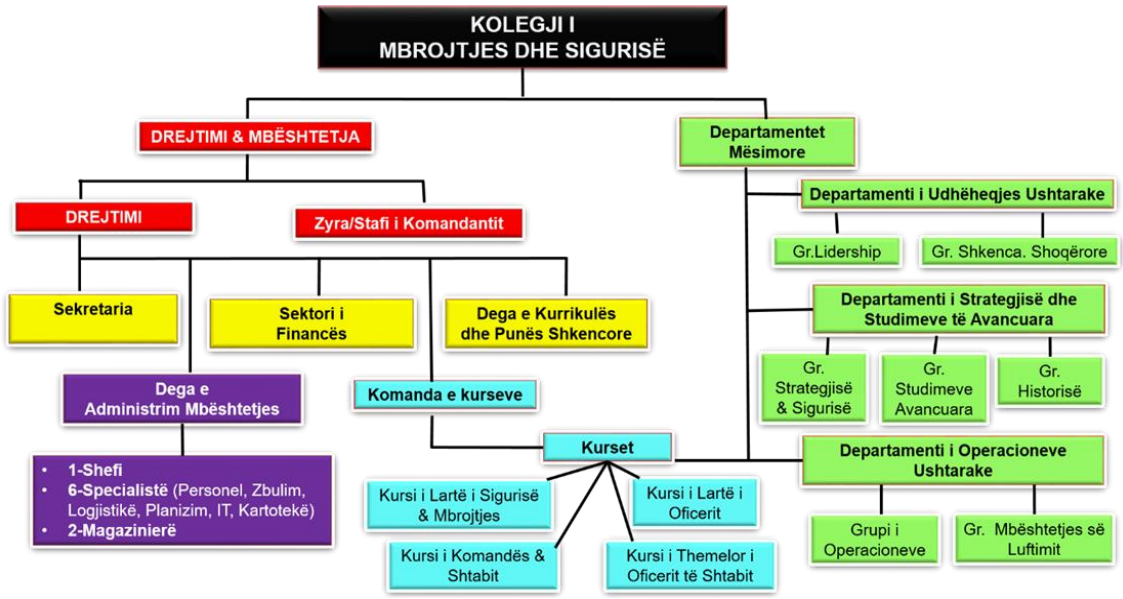
- Të përgatisë, arsimojë e kualifikojë specialist dhe drejtues të lartë të personelit ushtarak e civil për të gjitha nivelet e drejtimit të FA për fushën e sigurisë e mbrojtjes;

- Të përgatisë, arsimojë e kualifikojë specialist të lartë të personelit të institucioneve të tjera të sigurisë në vend, në fushën e sigurisë;
- Të përgatisë, arsimojë e kualifikojë lider civilë e ushtarak të vendeve partnere dhe të NATO-s në fushën e sigurisë dhe të mbrojtjes, për të krijuar një klimë të mirë besimi reciproke për promovimin e paqes dhe sigurisë në rajon e më gjerë;
- Të hartojë dhe realizojë programe arsimimi dhe kualifikimi duke i mbështetur në aplikimin e mendimit kritik, në përputhje me tendencat dhe ndryshime që ndodhin në fushën e sigurisë rajonale e ndërkombëtare;
- Të realizojë çdo vit rishikimin e kurrikulave dhe programeve mësimore, në përputhje me ndryshimet, objektivat, mësimet e nxjerra dhe eksperiencën e vendeve të tjera të NATO;
- Të drejtojë dhe organizojë punën kërkimore shkencore në fushën e sigurisë dhe të mbrojtjes për të formuar studiues të rinj ushtarakë dhe për të promovuar kërkimin shkencor e akademik.

2. Përshkrimi i auditimit, sipas drejtimeve të auditimit

2.1 Verifikimi i politikave, standardeve dhe vlerësimi i burimeve njerëzore në TIK

Kolegji i Mbrojtjes dhe Sigurisë (KMS) është një institucion ushtarak i cili zhvillon arsimimin e liderëve civilë e ushtarakë të vendeve partnere dhe të NATO-s si dhe edukimin e kualifikimin e personelit ushtarak e civil në nivelet e larta të drejtimit të Forcave të Armatosura dhe të institucioneve të tjera të sigurisë kombëtare për përdorimin kreativ dhe me efikasitet të elementëve të fuqisë kombëtare në kohë paqe, krize dhe lufte.
KMS (Reparti Ushtarak nr. 6680) është një strukturë organizative, në varësi të Shtabit të Përgjithshëm të Forcave të Armatosura (SHPFA), e cila është e organizuar si në figurën e mëposhtme:



Në këtë strukturë planifikohen, zhvillohen dhe drejtohen kurset e karrierës:
- *Kursi Themelor i Oficerit të Shtabit (KTHOSH):* Kursi ka si qëllim përgatitjen e oficerit të shtabit të batalionit (ose ekuivalente), dhënien e njohurive në nivelin e brigadës, si dhe përzgjedhjen e oficerëve më të mirë për të vijuar karrierën si oficerë profesionistë. Ky kurs zgjat 14 javë dhe përfundimi i këtij kursi mundëson marrjen e gradës major/kapiten i rangut III;

- *Kursi i Komandës dhe Shtabit të Përgjithshëm (KKSHP):* Kursi ka si qëllim përgatitjen e oficerit të karrierës për të plotësuar detyra në nivel komandant batalioni dhe shtab brigade /force dhe jep njohuri për nivelin operativo - strategjik. Ky kurs zgjat 1 vit akademik dhe përfundimi i këtij kursi mundëson marrjen e gradës nënkolonel/kapiten i rangut II;
- *Kursi i Lartë i Oficerit (KLO):* Kursi ka si qëllim përgatitjen e oficerit të karrierës për të plotësuar detyra në nivel operativo-strategjik. Ky kurs zgjat 1 vit akademik dhe përfundimi i këtij kursi mundëson marrjen e gradës kolonel/kapiten i rangut I;
- *Kursi i Lartë për Sigurinë dhe Mbrojtjen (KLSM):* Kursi ka si qëllim aftësimin e ushtarakëve dhe civilëve të niveleve strategjike në Ministrinë e Mbrojtjes, Forcat e Armatosura dhe institucionet e tjera të sigurisë së vendit dhe atyre analoge të vendeve të tjera. Ky kurs zhvillohet në një periudhë 3 mujore dhe për ushtarakët e karrierës është kusht për marrjen e gradës gjeneral brigade/underadmiral.

Numri i përgjithshëm i punonjësve të KMS është gjithsej 52 duke përfshirë stafin drejtues, mbështetës dhe pedagogjik, nga të cilët 39 janë personel ushtarak dhe 13 personel civil.
Specialisti i TI në KMS është pjesë përbërëse e Degës së Administrimit Mbështetës.

Tabela nr.1: Struktura e KMS sipas pozicioneve që ka secili punonjës aktualisht

Nr.	**Pozicioni**	**Nr. i punonjësve**	
		Plan	Fakt
1	Oficer	50	34
2	Nënoficerë	8	5
3	Civilë	0	13
Totali		**58**	**52**

Burimi: KMS, përpunuar nga grupi i auditimit

KMS për kryerjen e detyrave dhe përshkrimet e punës së punonjësve bazohet në Urdhrin nr. 262/1, datë 27.12.2023 "*Për miratimin e përshkrimit të pozicioneve të punës në Kolegjin e Mbrojtjes dhe Sigurisë".*

Nga auditimi i përshkrimeve të punës u konstatua se disa nga detyrat nuk realizohen nga specialisti TI, pasi sipas komunikimeve me institucionin këto detyra kryhen nga Komanda Kibernetike dhe e Ndërlidhjes (KKN) sipas Procedurave Standarde të Veprimit (PSV/SOP) të kësaj Komande, të cilat janë të miratuara nga Shtabi i Përgjithshëm i Forcave të Armatosura (SHPFA), konkretisht:

- Të planëzojë masa për kompleksitetin dhe mbajtjen në gatishmëri të pajisjeve kompjuterike dhe rrjetet e punës LAN/WAN të KMS-së;
- Mban dhe plotëson dokumentacionin e nevojshëm, për rrjetet kompjuterike për çdo incident që mund të ndodhë si dhe të kërkojë nga administratorët lokal të institucioneve të njëjtën gjë;
- Krijon dhe përditëson standardet e konfigurimit sipas udhëzimeve të paracaktuara për të përcaktuar dhe mirëmbajtur një nivel të përshtatshëm të shërbimeve të rrjetit kompjuterik LAN-WAN dhe sistemeve të komunikimit;
- Implementon dhe integron sistemet e reja dhe i përshtat me sistemet ekzistuese të institucionit;
- Kontrollon në mënyrë periodike problemet e administrimit, programimit, të ruajtjes, të mirëmbajtjes së informacionit në KMS.

Nga auditimi u konstatua se përshkrimet e punës për pozicionin Specialist TI LAN/WAN janë të mbivendosura pasi ky punonjës nuk ka autorizimin për kryerjen e tyre. Përshkrimet e punës duhen rishikuar dhe përditësuar me qëllim përcaktimin e saktë të detyrave dhe përmbushjen e objektivave për pozicionin specialist TI.

Grupit të auditimit i është vendosur në dispozicion një rregullore e cila është akoma në versionin draft pasi nuk është e miratuar me urdhër të Komandantit të Kolegjit. KMS për

kryerjen e detyrave funksionale për çdo pozicion pune bazohet vetëm në Urdhrin nr. 262/1, datë 27.12.2023 "*Për miratimin e përshkrimit të pozicioneve të punës në Kolegjin e Mbrojtjes dhe Sigurisë*". Gjithashtu draft rregullorja e vendosur në dispozicion grupit të auditimit nuk është në përputhje me përshkrimet e çdo pozicioni sipas përshkrimeve të punës të miratuara.

Nga auditimi u konstatua se, KMS nuk disponon një rregullore të brendshme në të cilën të përcaktohen rregullat e organizimit dhe funksionimit të veprimtarisë institucionale si dhe detyrat funksionale të punonjësve duke përfshirë edhe teknologjinë e informacionit.

- ***Strategjia, procedurat dhe rregulloret në TIK***

Strategjia e TI përfaqëson lidhjen e përbashkët midis objektivave të Strategjisë së TI dhe atyre të strategjisë së institucionit. Objektivat e strategjisë së TI duhet të marrin parasysh nevojat e tashme dhe të ardhshme të biznesit, kapacitetin aktual të TI për të ofruar shërbime dhe kërkesat e burimeve. Strategjia duhet të marrë në konsideratë ekzistencën e infrastrukturës dhe arkitekturës së TI, investimeve, modelit të ofrimit, burimet duke përfshirë stafin, si dhe paraqitjen e strategjisë që integron këto elementë në një qasje të përbashkët për të mbështetur objektivat e institucionit.
- *Nga auditimi u konstatua se,* KMS nuk ka miratuar një strategji institucionale si dhe nuk ka një plan strategjik mbi teknologjinë e informacionit duke mos bërë planifikime strategjike mbi sigurinë e informacionit si dhe infrastrukturën TI në të cilën do duhej të ishin pasqyruar objektivat e lidhura me burimet dhe instrumentet e nevojshme për matjen e tyre, me qëllim identifikimin e proceseve për zhvillimin në mbështetje të objektivave institucionale.
Mungesa e një plani strategjik institucional të lidhur edhe me teknologjinë e informacionit mbart riskun e keq adresimit të burimeve të nevojshme të cilat mund të mbështesin mbarëvajtjen e punës dhe arritjen e objektivave të institucionit.

Grupi i auditimit, me qëllim auditimin e nivelit të dokumentimit të politikave dhe procedurave në lidhje me teknologjinë e informacionit, verifikoi rregulloret dhe dokumentacionin e vënë në dispozicion nga institucioni, si dhe udhëzime të tjera të brendshme. Auditimi për këtë çështje pati në konsideratë risqet që vijnë nga mungesa e politikave dhe procedurave të shkruara, si dhe nga praktikat me të cilat institucioni zhvillon aktivitetin e tij.
- *Nga auditimi u konstatua se,* Teknologjia e Informacionit në KMS zhvillohet duke ndjekur dhe zbatuar urdhrat dhe udhëzimet/udhëzuesit e ardhura nga strukturat eprore Ministria e Mbrojtjes dhe SHPFA.

- ***Trajnimet***

Zhvillimi i trajnimeve ka një rëndësi të veçantë për menaxhimin e kapaciteteve njerëzore në institucion. Është e nevojshme që të identifikohen nevojat e stafit për trajnime mbi teknologjinë e informacionit.
Nga auditimi nuk u administruan dokumentacione mbi propozimet përkatëse, për zhvillimin e trajnimeve specifike. Nuk dokumentohet procesi i kërkesave, nevojave dhe analizimi i tyre për trajnim duke mos plotësuar kështu nevojat për trajnim mbi sistemet dhe teknologjinë e informacionit.
- *Nga auditimi u konstatua se,* për periudhën objekt auditimi KMS nuk i ka vendosur grupit të auditmit në dispozicion asnjë dokumentacion në lidhje me zhvillimin e ndonjë trajnimi nga specialisti i TI, si dhe trajnime që mund të ketë zhvilluar stafi në lidhje me teknologjinë e informacionit si përdorues të rrjeteve kompjuterike në të cilat KMS është përdorues.
- *Nga auditimi u konstatua se,* KMS për periudhën objekt auditimi 2023-2024, nuk ka pasur plan trajnimi vjetor për burimet njerëzore të cilët mbulojnë fushën e teknologjisë së informacionit si dhe punonjës të cilët janë përdorues të pajisjeve dhe sistemeve teknologjike.

- ***Identifikimi dhe adresimi i risqeve në TIK***

Monitorimi dhe kontrolli i riskut është procesi i identifikimit, analizimit dhe planifikimit për zbulimin e rreziqeve të reja të identifikuara, monitorimit të rreziqeve të identifikuara më parë dhe vlerësimit të atyre ekzistuese për të verifikuar strategjitë e reagimit ndaj rreziqeve të planifikuara për efektivitetin e tyre.
Regjistri i Riskut përbën 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 rrezikut 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 KMS.
- *Nga auditimi u konstatua se,* KMS nuk disponon regjistër risku për teknologjinë e informacionit, në asnjë formë nuk rezulton të jenë dokumentuar risqe të identifikuara për periudhën e audituar. Kjo mungesë e dokumentacionit e bën të pamundur vlerësimin e efektivitetit të kontrolleve ekzistuese dhe planifikimin e masave të nevojshme për përmirësimin e sigurisë. Për rrjedhojë, subjekti mbetet i ekspozuar ndaj risqeve të paidentifikuara dhe të pa menaxhuara. Kjo në kundërshtim me nenin 11, pika 2: "*Identifikimin dhe krijimin e regjistrit të riskut, vlerësimin, kontrollin e risqeve që vënë në rrezik arritjen e objektivave dhe realizimin me sukses të veprimtarive të strukturave që ata drejtojnë*", 12 pika 3/d: "*Identifikimin dhe krijimin e regjistrit të riskut, vlerësimin, kontrollin e risqeve që vënë në rrezik arritjen e objektivave dhe realizimin me sukses të veprimtarive të strukturave që ata drejtojnë*" si dhe nenin 19-21 të ligjit nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar me ligjin nr. 110/2015, datë 23.10.2015. Udhëzimin nr. 30, datë 27.12.2011 "*Për menaxhimin e aktiveve në njësitë e sektorit publik*", i ndryshuar, udhëzimi nr. 21, datë 25.10.2016 "*Për nëpunësit zbatues të gjitha niveleve*", Udhëzimi i Ministrit të Financave nr. 16, datë 20.07.2016 "*Për përgjegjësitë dhe detyrat e koordinatorit të menaxhimit financiar dhe kontrollit dhe koordinatorit të riskut në njësitë publike",* KMS duhet të kishte hartuar regjistrin e riskut ku të përfshiheshin edhe risqet që lidhen me teknologjinë e informacionit.

2.2 Auditimi i përdorimit të infrastrukturës në Teknologjinë e Informacionit

Në zbatim të pikës 2 "*Auditimi i përdorimit të infrastrukturës në Teknologjinë e Informacionit*" të Programit të Auditimit nr. 584/1, datë 24.06.2025 u shqyrtua dokumentacioni si më poshtë:

- Përshkrim i përgjithshëm i teknologjisë së informacionit në KMS;
- Intervista me punonjës që kryejnë shërbime të caktuara në sistem;
- Vizita në terren;
- Indikatorë dhe statistika, etj;
- Skema e komunikimit të network-ut;
- Konsultim me faqen e web-it të KMS, etj.

KMS është institucion fundor (*end user*), i cili ndjek dhe zbaton rregullat/udhëzimet dhe Procedurat Standarde të Veprimit të miratuara nga SHPFA. Gjithashtu është pjesë e rrjetit kompjuterik të SHPFA në dy rrjete të klasifikuar dhe pa klasifikuar. Këto rrjete, administrohen nga Komanda Kibernetike dhe e Ndërlidhjes (KKN), ku SHPFA është autoriteti operues i të dy rrjeteve për çdo element të këtyre rrjeteve kompjuterike, duke përfshirë pjesën *hardware, software,* si dhe aplikacionet e ndryshme që zbatohen në këto sisteme.

SHPFA është Autoriteti Operues i Sistemit, për çdo sistem, rrjetet kompjuterike dhe infrastrukturën hardware, software të menaxhuar nga Drejtoria e Ndërlidhjes (J6) pjesë e SHPFA dhe nën administrimin logjik dhe fizik të centralizuar nëpërmjet Agjencisë së Sistemeve të Ndërlidhjes dhe të Informacionit (ASNI). ASNI është autoriteti i administrimit logjik dhe fizik të rrjeteve kompjuterike të SHPFA dhe sistemeve të tjera që mbështesin strukturat e FA-së me shërbime të qendërzuara. ASNI realizion administrimin fizik dhe logjik

të Sistemeve dhe të pajisjeve që lidhen me to si dhe mbështet mirëmbajtjen e software-ve dhe hardware-ve ekzistuese për operimin normal të rrjeteve kompjuterike të SHPFA.

KMS në lidhje me përdorimin e infrastrukturës në Teknologjinë e Informacionit si institucion fundor (*end user*) ndjek dhe zbaton rregullat dhe Procedurat Standarde të Veprimit (PSV/SOP) të miratuara nga SHPFA, konkretisht:

- PSV nr. 601 *"Për hapjen e aksesit në rrjetin e klasifikuar";*
- PSV nr. 602 *"Për hapjen e aksesit në rrjetin e pa klasifikuar"*;
- PSV nr. 603 *"Për konfigurimin dhe instalimin e kompjuterëve që përdorin Forcat e Armatosura"*;
- PSV nr. 605 *"Për të drejtat e administratorëve lokal dhe help desk në rrjetet kompjuterike të Forcave të Armatosura të Republikës së Shqipërisë"*;
- PSV nr. 606 *"Për Përdorim të Softit Unified Endpoint Management & Security Solution nga administratorët lokal";*
- PSV nr. 617 *"Për përdorimin e email-it në rrjetin e paklasifikuar të Forcave të Armatosura"*;
- PSV nr. 618 *"Për menaxhimin pas incidentit të ndodhur në rrjetin e klasifikuar" (e klasifikuar me nivel "Konfidencial"*.

Specialisti TI i KMS merret me kontrollin dhe mirëmbajtjen lokale të pajisjeve që ka në përdorim duke ndjekur dhe zbatuar udhëzimet e SHPFA, ku KMS ka në përdorim 55 kompjuterë, nga të cilët 52 janë të pa klasifikuar (në sistemin e SHPFA *aaf.mil.al*) dhe 3 të klasifikuar.
Mjedisi i konektimit të rrjetit kompjuterik të KMS me serverat e SHPFA, realizohet nëpërmjet mjedisit fizik, me fibër optike. Gjithashtu programet si: antivirus, Windows 10 dhe 11, paketa office 16, Microsoft Edge, ManagementEngine UEMS, etj, vijnë të licencuara nga SHPFA, të cilat instalohen nga Specialisti i TI i KMS.

KMS ka akses si *end user* në sistemin e Qendrës së Personelit, i cili është sistem i Klasifikuar dhe administrohet nga Qendra e Personel Rekrutimit dhe SHPFA.

KMS nuk ka administrator sistemesh por ka administrator lokal, ku atributet, rolet dhe përgjegjësitë (e admin. lokal) janë të përcaktuara në PSV nr. 605 *"Për të drejtat e administratorëve lokal dhe help desk në rrjetet kompjuterike të Forcave të Armatosura të Republikës së Shqipërisë (FARSH)"*, si më poshtë:

- Instalimi i softeve të miratuara;
- Menaxhimi i *share folder* të krijuar nga Qendra Fikse e Komandës Kibernetike;
- Krijimi i database me pajisjet kompjuterike sipas vitit, nr.serial dhe *mac* adresës, etj.

Administratori lokal pasi emërohet me urdhër të Ministrit të Mbrojtjes, i jepet e drejta nga Drejtoria J6 e SHPFA, duke plotësuar Aneksin A (për rrjetin e klasifikuar) dhe B (për rrjetin e paklasifikuar).
Administratorët lokal kanë të drejtë të përdorin softin remote kontroll Unified endpoint management E& security solution, me qëllim evidentimin dhe zgjidhjen e problematikave që mund të hasin si: antivirus, instalim të softit, përdorimi i USB-ve të palejuara në rrjet, evidentimi i gjendjes së kompjuterit etj.

Administratori lokal është pjesë e grupit kryesor të përdorimit të sistemit Aaxes, remote desktop me të drejta për të parë si dhe të drejta për të kryer veprime me përdoruesit, kompjuterat dhe grupet e sigurisë. Administratori ka privilegjin të veprojë vetëm në objektet e OU (Njësi Organizative) në të cilën ushtron detyrën e tij sipas privilegjeve të përcaktuara nga SHPFA (Drejtoria e J6) dhe të aplikuara nga Qendra Fikse TIT (ASNI).
Të drejtat e specialistit TI si administrator lokal janë:

- Krijimi i një llogarie;
- Fshirja e një llogarie;
- Rivendosja e fjalëkalimit;

- Transferimi i një llogarie;
- Marrja dhe aktivizimi e një llogarie të transferuar;
- Remote Control.

Të gjitha të drejtat më sipër inciohen nga administratori lokal dhe kalojnë më pas në procesin e aprovimit nga Drejtoria J6. Specialisti i TI në KMS nuk ka të drejta për fshirjen dhe ndryshimin e përdoruesve në rrjetin kompjuterik, fjalëkalimet ndryshohen nga vetë përdoruesi në çdo kohë, si dhe i vjen një sms rikujtues për ndryshim të detyruar të fjalëkalimit çdo 3 muaj.

Nga auditimi konstatohet se detyrat dhe përgjegjësitë përkatëse për administratorin lokal në KMS nuk janë atribuar me anë të një shkrese zyrtare me qëllim realizimin dhe zbatimin e udhëzuesve PSV të vendosura në dispozicion nga strukturat SHPFA dhe Ministria e Mbrojtjes, referuar PSV 605 *"Për Përdorim të Softit Unified Endpoint Management & Security Solution nga administratorët lokal",* miratuar me urdhër nr. 285, datë 18.03.2025 nga SHPFA, pika 2.2 Zbatueshmëria, citohet: *"Të drejtat administrative për administratorët lokal do të aktivizohen në momentin kur personeli i emëruar në këtë detyrë është i i pajisur me certifikatë dhe ka plotësuar aneksin A bashkëlidhur kësaj PSV. Më pas J6 miraton të drejtën si administrator"*.

Nga auditimi u konstatua se, nuk janë dokumentuar politikat e sigurisë të implementuara për përdoruesit e rrjetit kompjuterik që KMS përdor mbi detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre si dhe nuk është hartuar një rregullore ose dokument mbi parametrizimin e fjalëkalimeve që të përcaktojë përmbajtjen, gjatësinë, mos përsëritjen e të njëjtit fjalëkalim etj. Forcimi i kritereve të fjalëkalimit konsiderohet element sigurie në standardet mbi sigurinë e informacionit, rreziqet që lidhen me fjalëkalimet e dobëta çojnë në akses të autorizuar, shkelje të sigurisë etj.
Nga auditimi konstatohet se përdoruesit nuk ndjekin një politikë të qartë, për përdorimin e fjalëkalimeve të forta dhe ndërrimin e tyre periodik, duke e lehtësuar për sulmuesit realizimin e sulmeve brute-force, credential stuffing, dictionary attacks ose password spraying për të fituar akses të paautorizuar.

Bazuar në Planin e Arsimimit dhe Kualifikimit të Personelit të FARSH për vitet akademike, si dhe urdhrave të dala nga Ministri i Mbrojtjes, në KMS kryhet procesi mësimor, ku për çdo vit akademik administrohet në arkivin kompjuterik (të dhëna në excel) dhe të printuara të dhënat e mëposhtme për çdo kursant:
- Lista e Notave;
- Të dhëna të përgjithshme;
- Kopje e diplomës;
- Tabela e mesatares;
- Listë-merita për rezultatet e arritura në vitin akademik.

KMS bazuar në dokumentacionin e vendosur në dispozicion grupit të auditimit, rezulton se pas përfundimit të kursit i dorëzon një kopje të dosjes së secilit kursant Qëndrës së Personel Rekrutimit e cila hedh të dhënat në sistemin e qendrës së personelit dhe një kopje e dosjes dërgohet me shkresë përcjellëse në repartin përkatës ku emërohet kursanti. KMS më pas ruan në format excel tabelën përmbledhëse sipas mesatares me nr 'nr.amze' përkatëse.

➢ Nga auditimi mbi sistemet e operimit (OS) dhe versionet e tyre, për periudhën u konstatua se KMS ka në total 66 kompjutera ku rezultuan të jenë si më poshtë:
- 10 kompjutera janë me sistemin operativ Windows 7 - të cilët janë me sistem operimi Windows 7, për të cilat nuk ofrohen më përditësime sigurie, duke e bërë përodrimin e tyre një rrezik të madh për sigurinë;
- 44 kompjutera janë me sistemin operativ Windows 10 - të cilët janë në suport, që përfundon më 14 tetor 2025. Pas kësaj date Microsoft nuk do të ofrojë më përditësime sigurie, rregullime të gabimeve apo mbështetje teknike për Windows 10. Nëse Windows 10 do të vazhdojë të funksionojë, ai do të bëhet gjithnjë e më i prekshëm ndaj kërcënimeve të sigurisë dhe mund të sjellë dhe probleme të përputhshmërisë me software dhe hardware më të reja.

- 12 kompjutera janë me sistemin operativ Windows 11 – të cilët aktualisht janë në suport.

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

Objektivi: Vlerësimi i efektivitetit të menaxhimit të politikave dhe procedurave të menaxhimit të problemeve dhe incidenteve.

Vlerësimi mbi risqet në KMS dokumentohet sipas PSV nr. 618 *"Për menaxhimin pas incidentit të ndodhur në rrjetin e klasifikuar",* e klasifikuar me nivel "Konfidencial".
Nga auditimi u konstatua se, KMS nuk disponon procedura mbi administrimin e incidenteve dhe problemeve në rrjetin e pa klasifikuar ku është përdorues, si dhe nuk ka të dokumentuar një plan masash për identifikimin, trajtimin e gabimeve, problemeve dhe incidenteve që mund të ndodhin në infrastrukturën TI. Nga intervistat e zhvilluara me personat përgjegjës në KMS, konstatohet se nuk disponohet një procedurë për inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve në proceset e punës operacionale të KMS.
Për periudhën objekt auditimi, risqet menaxhohen mbi bazë ngjarjesh, ku suporti dhe komunikimi i brendshëm institucional si dhe mbështetja teknike dhe logjike për operacionet TI që ndihmojnë mbarëvajtjen e strukturave të institucionit kryhen nga specialisti TI nëpërmjet komunikimeve verbale apo me telefon.
Nisur nga rëndësia e procesit të menaxhimit të ndryshimit, i cili duhet të sigurojë që ndryshimet janë regjistruar, vlerësuar, autorizuar, prioritarizuar, planifikuar, testuar, implementuar, dokumentuar dhe rishikuar në përputhje me procedurat e dokumentuara dhe të aprovuara të menaxhimit të ndryshimit, grupit të auditimit nuk i është vënë në dispozicion asnjë dokumentacion. Nga intervistat e zhvilluara me personat përgjegjës në KMS, konstatohet se nuk disponohet një procedurë për inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve në proceset e punës operacionale të KMS.

- ***Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet***

Topologjia e rrjeteve kompjuterike të KMS, si pjesë e rrjeteve kompjuterik të SHPFA, është e tipit STAR dhe menaxhohet nga servera të instaluar në Qendrën e Ndërlidhjes së SHPFA.
Serveri ndodhet në Qendrën Fikse të Komandës Kibernetike si dhe Firewall të Komandës Kibernetike. Në KMS IP-të merren nga Drejtoria e Ndërlidhjes në SHPFA, të cilët janë user fundorë.
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 serverave (versioni 1.0, datë 02.12.2008) miratuar nga AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit).
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.
Përsa më sipër, grupi i auditimit verifikoi infrastrukturën hardware dhe network që disponon KMS.
Nga auditimi u konstatua se KMS nuk disponon një dhomë serverësh të mirëfilltë pasi nuk ka sisteme dhe infrastrukturë serverësh të tijën. Në ambientet e katit të dytë të godinës janë lokalizuar dy rack, në të cilin janë instaluar kryesisht infrastrukturë network si patch panel, switch Layer 3, switch Layer 2 etj. Gjithashtu, në katin e tretë është lokalizuar një rack për pjesën e rrjetit për KMS-ën, ku konstatohet se kabllimet dhe lidhjet e rrjetit nuk janë të sistemuara. Nga auditimi u konstatua se ambienti ku janë lokalizuar rack-et që përmban infrastrukturën network, swich, etj, nuk përmbush kushtet standarde të përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (Versioni 1.0, datë 02.12.2008) miratuar nga AKSHI.

Për sa është trajtuar në këtë pikë të Raportit Përfundimtar të Auditimit, nga subjekti i audituar është paraqitur observacioni me shkresë nr. 696/9 prot., datë 22.10.2025 "Observacion mbi projektraportin e auditimit", ku janë shprehur objeksionet si më poshtë:

Pretendimi i subjektit: … Me ristrukturimin e KMS bazuar në urdhrin e klasifikuar të Ministrit të Mbrojtjes (MM) nr. 75, datë 08.09.2025, "Për riorganizimin e strukturës organizative të KMS"], do të zbatohen rekomandimet e gjetjes së auditimit Tuaj, ku do të specifikohen dhe të përditësohen përshkrimet e punës për të gjithë personelin e IT në organikë, duke i përshtatur ato me detyrat funksionale dhe përgjegjësitë reale të secilit post pune, në funksion të objektivave të veprimtarisë së institucionit tonë.

***

… Me ristrukturimin e KMS (bazuar në urdhrin e klasifikuar të MM të cituar më sipër), do të punohet për përditësimin e draft-rregullores së brendshme të institucionit, si dhe miratimin e saj, në funksion të përmbushjes së veprimtarisë të KMS-së.

***

...KMS si institucion i vartësisë së SHPFA, nuk harton Strategji Institucionale për IT dhe Mbrojtjen Kibernetike, por MM ka hartuar vetëm Strategjinë e Mbrojtjes Kibernetike (*linku:* strategjia-Mbrojtje-Kibernetike-2024-2028-290324.pdf), e cila zbatohet nga të gjitha repartet e Forcave të Armatosura të Republikës së Shqipërisë (FARSH) dhe si rrjedhojë edhe nga KMS, si *end user*.

***

…KMS në vijim ka marrë masa për identifikimin e trajnimeve për burimet njerëzore në fushën e IT, por duhet të kalojë në proces miratimi në Shtabin e Përgjithshëm të Forcave të Armatosura (SHPFA) dhe MM, e cila më pas të financohet nga KMS.

***

… KMS si *end user*, nuk disponon sisteme të ndërlidhjes dhe IT në inventar të saj, pasi ato janë të centralizuara në SHPFA (Drejtoria e Ndërlidhjes- J6). J6 kryen çdo vit kalendarik analizën e riskut për sistemet e IT të FARSH (në të cilën përfshihet edhe KMS). Sjellim në vëmendjen Tuaj se kjo analizë është informacion i klasifikuar.

***

KMS ka marrë masa për caktimin e administratorit lokal me shkresë zyrtare.

***

...KMS si *end user*, nuk disponon sisteme të ndërlidhjes dhe IT në inventar të saj, pasi ato janë të centralizuara në SHPFA (J6). J6 sipas PSV përkatëse, si strukturë eprore, përcakton politikat për fjalëkalimet e të gjithë *user*-at e FARSH, të cilat zbatohen nga KMS. Në Procedurën Standarde të Veprimit (PSV) nr. 601 dhe 602 është e specifikuar dhe aktualisht veprohet sipas tyre, ku për çdo 3 muaj sistemi të kërkon ndryshimin e fjalëkalimit, ku ky i fundit nuk duhet të jetë i ripërtërirë, si dhe të ketë karaktere të ndryshme (gërma e madhe, e vogël, numra, shenja pikësimi) dhe për çdo 3 herë fjalëkalim të gabuar, *user-i* bllokohet.

***

... KMS është në proces furnizimi me kompjuterë të rinj, pasi kompjuterët aktual nuk kishin parametrat teknikë të duhur për të instaluar sistemin e përditësuar windows 11. Po vijon puna në bashkëpunim me SHPFA për eliminimin e pa përputhshmërinë me soft dhe hardware.

***

...Aktualisht SHPFA (J6), është duke marrë masa për hartimin e një PSV (draft PSV nr. 621) "Për incidentet kibernetike dhe probleme të ndryshme", e cila pas miratimit të saj, do të zbatohet në të gjithë FARSH dhe si rrjedhojë edhe në KMS.

***

... Aktualisht KMS po vijon punën për sistemimin e kabllimeve dhe etiketimin e tyre në *Rack*-et përkatës. Për sa i përket investimit sipas rekomandimit për rregulloren e ndërtimit të dhomës së serverit, KMS nuk mund të marrë masa për investim, pasi aktualisht godina është

në administrim të Akademisë së Forcave të Armatosura (AFA), por pavarësisht kësaj, për këtë qëllim po bashkëpunohet me AFA.
Qëndrimi i grupit të auditimit: Në lidhje me observimet mbi gjetjet nr. 1, nr. 2, nr. 4, nr. 6, nr. 8, nr. 9 dhe nr. 10, KMS është përgjigjur se do të marrë masa për realizimin e tyre.

Në lidhje me observacionin mbi caktimin e administratorit lokal me shkresë zyrtare, duke qenë se nuk ka vendosur në dispozicion asnjë shkresë të miratuar, grupi i auditimit do të mbaj të njëjtin qëndrim.
Përsa i përket pjesës tjetër të observacioneve sqarojmë se argumentet e parashtruara janë në tërësi shpjeguese, si dhe një pjesë e konsiderueshme është diskutuar me grupin e auditimit gjatë fazës së terrenit. Sqarojmë se, duke qenë se kompetencën e miratimit të dokumentacioneve e ka SHPFA këto rekomandime janë lënë në bashkëpunim duke qenë se është domosdoshmëri pasja e tyre në mirëfunksionim të institucionit.

IV. REKOMANDIME

B. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi u konstatua se, KMS nuk ka miratuar një strategji institucionale zhvillimi, e cila do të duhej të përfshinte edhe komponentët e teknologjisë së informacionit që mbështesin realizimin e objektivave institucionale, kjo në kundërshtim me Ligjin nr. 10296 datë 08.07.2010 "*Për menaxhimin financiar dhe kontrollin*" i ndryshuar. Mungesa e një strategjie mbart riskun e keq adresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së institucionit.
(Më hollësisht trajtuar në pikën 2.1 faqet 8-11 të Raportit Përfundimtar të Auditimit)
1.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë në bashkëpunim me Shtabin e Përgjithshëm të Forcave të Armatosura të marrë masa për hartimin dhe miratimin e një strategjie institucionale në të cilën të integrojë edhe komponentët e teknologjisë së informacionit, si një faktor mbështetës për përmbushjen e objektivave të institucionit.

Menjëherë

2. Gjetje nga auditimi: Nga auditimi u konstatua se disa nga detyrat e përcaktuara në përshkrimet e punës për pozicionin Specialist TI LAN/WAN i cili është pjesë përbërëse e Degës së Administrimit Mbështetës nuk realizohen nga specialisti TI, në kundërshtim me Urdhrin nr. 262/1, datë 27.12.2023 "*Për miratimin e përshkrimit të pozicioneve të punës në Kolegjin e Mbrojtjes dhe Sigurisë*".
Detyrat të cilat nuk mund të realizohen nga specialist TI janë:
- Të planëzojë masa për kompleksitetin dhe mbajtjen në gatishmëri të pajisjeve kompjuterike dhe rrjetet e punës LAN/WAN të KMS-së;
- Mban dhe plotëson dokumentacionin e nevojshëm, për rrjetet kompjuterike për çdo incident që mund të ndodhë si dhe të kërkojë nga administratorët lokal të institucioneve të njëjtën gjë;
- Krijon dhe përditëson standardet e konfigurimit sipas udhëzimeve të paracaktuara për të përcaktuar dhe mirëmbajtur një nivel të përshtatshëm të shërbimeve të rrjetit kompjuterik LAN-WAN dhe sistemeve të komunikimit;
- Implementon dhe integron sistemet e reja dhe i përshtat me sistemet ekzistuese të institucionit;
- Kontrollon në mënyrë periodike problemet e administrimit, programimit, të ruajtjes, të mirëmbajtjes së informacionit në KMS.

Sipas komunikimeve me institucionin këto detyra kryhen nga Komanda Kibernetike dhe e Ndërlidhjes (KKN) sipas Procedurave Standarde të Veprimit (PSV/SOP) të kësaj Komande, të cilat janë të miratuara nga Shtabi i Përgjithshëm i Forcave të Armatosura (SHPFA).
(Më hollësisht trajtuar në pikën 2.1 faqet 8-11 të Raportit Përfundimtar të Auditimit)

2.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë të marrë masa për përditësimin e përshkrimeve të punës për specialistin TI duke i përshtatur ato me detyrat funksionale dhe përgjegjësitë reale të këtij pozicioni në funksion të përmbushjes së objektivave të veprimtarisë së institucionit.

Menjëherë

3. Gjetje nga auditimi: Nga auditimi u konstatua se, KMS nuk disponon një rregullore të brendshme në të cilën të përcaktohen rregullat e organizimit dhe funksionimit të veprimtarisë institucionale, si dhe detyrat funksionale të punonjësve duke përfshirë edhe teknologjinë e informacionit.
Grupit të auditimit iu vendos në dispozicion një rregullore e cila është akoma në versionin draft, pasi nuk është e miratuar me urdhër të Komandantit të Kolegjit. Gjithashtu draft rregullorja e vendosur në dispozicion grupit të auditimit nuk është në përputhje me përshkrimet e miratuara për çdo pozicion pune, sipas Urdhrit nr. 262/1, datë 27.12.2023 "*Për miratimin e përshkrimit të pozicioneve të punës në Kolegjin e Mbrojtjes dhe Sigurisë*".
(Më hollësisht trajtuar në pikën 2.1 faqet 8-11 të Raportit Përfundimtar të Auditimit)
3.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë të marrë masa për hartimin dhe miratimin e rregullores së brendshme të institucionit sipas përshkrimeve të miratuara për çdo pozicion pune, në funksionim të përmbushjes së veprimtarisë institucionale.

Menjëherë

4. Gjetje nga auditimi: Nga auditimi u konstatua se, KMS për periudhën objekt auditimi për vitet 2023-2024 nuk ka identifikuar, planifikuar dhe realizuar trajnime mbi sigurinë dhe teknologjinë e informacionit, duke pasur parasysh elementët më të rëndësishëm si ruajtja e të dhënave, të drejtat dhe detyrimet mbi mjetet teknologjike që disponon institucioni, etj., si për burimet njerëzore të cilët mbulojnë fushën e TI dhe për punonjësit të cilët janë përdorues të pajisjeve dhe sistemeve teknologjike, kjo në kundërshtim me Ligjin nr.10296 datë 08.07.2010 "*Për menaxhimin financiar dhe kontrollin*" i ndryshuar, si dhe standardet ndërkombëtare të TI për rritjen e kapaciteteve.
(Më hollësisht trajtuar në pikën 2.1 faqet 8-11 të Raportit Përfundimtar të Auditimit)
4.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë të marrë masa për trajnimin e gjithë punonjësve në fushën e teknologjisë së informacionit dhe në mënyrë të veçantë punonjësit e ngarkuar me sigurinë e saj.

Menjëherë dhe në vijimësi

5. Gjetje nga auditimi: Nga auditimi u konstatua se, KMS nuk disponon regjistër risku për teknologjinë e informacionit, si dhe për periudhën e audituar nuk rezulton në asnjë formë të jenë të dokumentuara risqe të identifikuara. Kjo sjell mungesë të identifikimit dhe adresimit të problematikave potenciale, si dhe rrit riskun për shkelje në fushën e sigurisë së informacionit. Kjo në kundërshtim me nenin 11, pika 2, nenin 12 pika 3/d dhe nenet 19-21 të ligjit nr. 10296, datë 08.07.2010, "*Për menaxhimin financiar dhe kontrollin*", i ndryshuar me ligjin nr. 110/2015, datë 23.10.2015, Udhëzimi i Ministrit të Financave 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 faqet 8-11 të Raportit Përfundimtar të Auditimit)
5.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë të marrë masa për identifikimin, vlerësimin, ndjekjen dhe adresimin tek personat përgjegjës të risqeve, për analizimin, vlerësimin e tyre dhe përmbushjen e objektivave të institucionit.

Menjëherë dhe në vijimësi

6. Gjetje nga auditimi: Nga auditimi u konstatua se, detyrat dhe përgjegjësitë përkatëse për administratorin lokal në KMS kryhen nga specialisti TI, detyra të cilat nuk i janë vendosur me rregullore ose shkresa zyrtare me qëllim realizimin dhe zbatimin e udhëzuesve të Procedurave Standarde të Veprimit (PSV) të vendosura në dispozicion nga strukturat e Shtabit të

Përgjithshëm të Forcave të Armatosura dhe Ministria e Mbrojtjes, referuar PSV 605 *"Për Përdorim të Softit Unified Endpoint Management & Security Solution nga administratorët lokal",* miratuar me urdhër nr. 285, datë 18.03.2025 nga SHPFA, pika 2.2 Zbatueshmëria.
(Më hollësisht trajtuar në pikën 2.2 faqet 11-16 të Raportit Përfundimtar të Auditimit)
6.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë të marrë masa për përcaktimin e administratorit lokal, për kryerjen e detyrave administrative për teknologjinë e informacionit, duke përcaktuar përgjegjësitë, aksesit, gjurmueshmërisë dhe sigurisë së të dhënave.

Menjëherë

7. Gjetje nga auditimi: Nga auditimi u konstatua se, nuk janë dokumentuar politikat e sigurisë të implementuara për përdoruesit e rrjetit kompjuterik që KMS përdor mbi detyrimet që nevojiten të aplikohen në fjalëkalimet e tyre, si dhe nuk është hartuar një rregullore ose dokument mbi parametrizimin e fjalëkalimeve që të përcaktojë përmbajtjen, gjatësinë, mos përsëritjen e të njëjtit fjalëkalim etj. Forcimi i kritereve të fjalëkalimit konsiderohet element sigurie në standardet mbi sigurinë e informacionit, rreziqet që lidhen me fjalëkalimet e dobëta çojnë në akses të autorizuar, shkelje të sigurisë etj.
Nga auditimi konstatohet se përdoruesit nuk ndjekin një politikë të qartë, për përdorimin e fjalëkalimeve të forta dhe ndërrimin e tyre periodik sipas përcaktimeve rregullatore të AKCESK, duke e lehtësuar për sulmuesit realizimin e sulmeve brute-force, credential stuffing, dictionary attacks ose password spraying për të fituar akses të paautorizuar.
(Më hollësisht trajtuar në pikën 2.2 faqet 11-16 të Raportit Përfundimtar të Auditimit)
7.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë në koordinim me Shtabin e Përgjithshëm të Forcave të Armatosura të marrin masa për të dokumentuar dhe aplikuar politikat e sigurisë të implementuara për përdoruesit, si dhe detyrimet që nevojiten të aplikohen për fjalëkalimet sipas përcaktimeve rregullatore të Autoritetit Kombëtar për Sigurinë Kibernetike.

Menjëherë dhe në vijimësi

8. Gjetje nga auditimi: Nga auditimi mbi sistemet e operimit (OS) dhe versionet e tyre, për periudhën objekt auditimi u konstatua se KMS ka në total 66 kompjutera ku rezultuan të jenë si më poshtë:
- 12 kompjutera janë me sistemin operativ Windows 11 – të cilët aktualisht janë në suport.
- 44 kompjutera janë me sistemin operativ Windows 10 - të cilët janë në suport, që përfundon më 14 tetor 2025. Pas kësaj date Microsoft nuk do të ofrojë më përditësime sigurie, rregullime të gabimeve apo mbështetje teknike për Windows 10. Nëse Windows 10 do të vazhdojë të funksionojë, ai do të bëhet gjithnjë e më i prekshëm ndaj kërcënimeve të sigurisë dhe mund të sjellë dhe probleme të përputhshmërisë me software dhe hardware më të reja;
- 10 kompjutera janë me sistemin operativ Windows 7 - të cilët janë me sistem operimi Windows 7, për të cilat nuk ofrohen më përditësime sigurie, duke e bërë përdorimin e tyre një rrezik të madh për sigurinë, bazuar në zhvillimet teknologjike të sistemeve të operimit dhe Standardet Ndërkombëtare të Sigurisë së Informacionit ISO/IEC 27001:2022.
(Më hollësisht trajtuar në pikën 2.2 faqet 11-16 të Raportit Përfundimtar të Auditimit)
8.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë në bashkëpunim me Shtabin e Përgjithshëm të Forcave të Armatosura të marrë masa për planifikimin dhe kalimin në sistemin e operimit Windows 11 për të gjitha kompjuterat që KMS ka në përdorim, për të siguruar që pajisjet e tyre të vazhdojnë të marrin përditësime sigurie nga prodhuesi Microsoft dhe të jenë të mbrojtura ndaj kërcënimeve të mundshme.

Në vijimësi

9. Gjetje nga auditimi: Nga auditimi u konstatua se, KMS nuk disponon procedura mbi administrimin e incidenteve dhe problemeve në rrjetin e pa klasifikuar ku është përdorues, si dhe nuk ka të dokumentuar një plan masash për identifikimin, trajtimin e gabimeve, problemeve dhe incidenteve që mund të ndodhin në infrastrukturën TI. Nga intervistat e zhvilluara me personat përgjegjës në KMS, konstatohet se nuk disponohet një procedurë për

inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve në proceset e punës operacionale të KMS, sipas praktikave dhe standardeve më të mira.
(Më hollësisht trajtuar në pikën 2.2 faqet 11-16 të Raportit Përfundimtar të Auditimit)
9.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë në bashkëpunim me Shtabin e Përgjithshëm të Forcave të Armatosura të marrë masa për hartimin e një plan veprimi për identifikimin, dokumentimin dhe monitorimin e incidenteve, problemeve, si dhe menaxhimin e ndryshimeve, me qëllim njohjen dhe minimizimin e riskut të incidenteve që mund të sjellin humbje, tjetërsim apo transferim të informacionit konfidencial që akseson dhe administron institucioni në përputhje me aktivitetin e tij.

Menjëherë dhe në vijimësi

10. Gjetje nga auditimi: Nga auditimi u konstatua se KMS nuk disponon një dhomë serverësh të mirëfilltë, pasi nuk ka sisteme dhe infrastrukturë serverësh të tijën. Në ambientet e katit të dytë të godinës janë lokalizuar dy rack, në të cilin janë instaluar kryesisht infrastrukturë network si patch panel, switch Layer 3, switch Layer 2 etj. Gjithashtu, në katin e tretë është lokalizuar një rack për pjesën e rrjetit për KMS-ën, ku konstatohet se kabllimet dhe lidhjet e rrjetit nuk janë të sistemuara. Nga auditimi u konstatua se ambienti ku janë lokalizuar rack-et që përmban infrastrukturën network, swich, etj, nuk përmbush kushtet standarde të përcaktuara në Rregulloren për ndërtimin e dhomës së serverëve (Versioni 1.0, datë 02.12.2008) miratuar nga AKSHI.
(Më hollësisht trajtuar në pikën 2.2 faqet 11-16 të Raportit Përfundimtar të Auditimit)
10.1 Rekomandimi: Kolegji i Mbrojtjes dhe Sigurisë në koordinim me Shtabin e Përgjithshëm të Forcave të Armatosura të marrë masa për përmirësimin e ambienteve të dhomës së serverave në përputhje me udhëzimet, standardet dhe praktikat më të mira kombëtare dhe ndërkombëtare për shmangien e shkeljes së sigurisë, humbjes së informacionit, shkatërrimit të aseteve dhe mos garantimit të vazhdimësisë së punës.

Menjëherë

Për sa më sipër paraqitet ky Raport Auditimi.

KONTROLLI I LARTË I SHTETIT