Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit e Kosovës
Nacionalna Kancelarija Revizije Kosova
Kosovo National Audit Office

MANUALI I AUDITIMIT TË TEKNOLOGJISË SË INFORMACIONIT

Prishtinë, prill 2022

PËRMBAJTJA

Parathënie **3**

Hyrje **4**

KAPITULLI 1 Auditimi i Teknlogjisë së Informacionit (TI) **6**

KAPITULLI 2 Qeverisja e TI **22**

KAPITULLI 3 Zhvillimi dhe blerja **30**

KAPITULLI 4 Operacionet e TI-së **34**

KAPITULLI 5 Nënkontraktimi **40**

KAPITULLI 6 Plani i vazhdimësisë së biznesit (PVB) dhe plani i rimëkëmbjes nga fatkeqësia (PRF) **46**

KAPITULLI 7 Siguria e informacionit **55**

KAPITULLI 8 Kontrollet e aplikacioneve **65**

KAPITULLI 9 Çështje të tjera me interes **75**

Shtojca II. Matrica e sugjeruar e auditimit mbi Qeverisjen e TI **80**

Shtojca III. Matrica e sugjeruar e auditimit mbi Zhvillimin dhe Blerjet **88**

Shtojca IV. Matrica e sugjeruar e auditimit mbi Operacionet e TI **96**

Shtojca V. Matrica e sugjeruar e auditimit mbi kontraktimin **106**

Shtojca VI. Matrica e sugjeruar e auditimit mbi PVB//PRF **118**

Shtojca VII. Matrica e sugjeruar e auditimit mbi Sigurnië e Informacionit **128**

Shtojca VIII. Matrica e sugjeruar e auditimit mbi Kontrollet e Aplikacioneve **143**

Parathënie

Manuali i Auditimit të Teknologjisë së Informacionit është botimi i parë i botimeve të Zyrës Kombëtare të Auditimit të Republikës së Kosovës në fushën e teknologjisë së informacionit. Ky botim është produkt i grupeve punuese të teknologjisë së informacionit të EUROSAI-t (WGITA) si dhe Iniciativës për Zhvillim të INTOSAI-t (IDI) për caktimin e rregullave dhe standardeve të Auditimit të Teknologjisë së Informacionit. Manuali i Auditimit të Teknologjisë së Informacionit është përkthyer në gjuhën shqipe nga Kontrolli i Lartë i Shtetit të Shqipërisë i cili më pas është përshtatur nga auditorët e Zyrës Kombëtare të Auditimit të Kosovës.

Teknologjia e Informacionit dhe Komunikimit është pjesë integrale e një Organizate Buxhetore dhe një nga drejtuesit kryesor e cila ndihmon në arritjen e misionit dhe objektivave të saj. Përdorimi i saj mundëson rritjen e efikasitetit dhe efektivitetit të Institucioneve të Republikës së Kosovës në ofrimin e shërbimeve publike ndaj qytetarëve.

Derisa teknologjia e informacionit ka përparuar, organizatat janë bërë gjithnjë e më të varura nga sistemet e kompjuterizuara të informacionit për të kryer operacionet dhe proceset e tyre, të mirëmbajnë dhe të raportojnë informacion thelbësor. Përdorimi i sistemeve të informacionit ofron përparësitë si: stabilitetin, efiqiencën, efektivitetin, privatësinë, mbrojtjen e të dhënave, etj.

Besueshmëria dhe siguria e sistemeve të kompjuterizuara të cilat procesojnë, mirëmbajnë dhe raportojnë të dhëna janë një shqetësim për audituesit dhe për organizatat. Kjo për arsye se, këto sisteme kanë sfidat dhe rreziqet e tyre, prandaj edhe janë të rëndësishme auditimet e sistemeve të informacionit, në mënyrë që qytetarët dhe Kuvendi i Kosovës të sigurohen se këto sisteme janë në funksion të objektivave dhe ofrimit të shërbimeve më të mira.

Duke marr parasysh rëndësinë e tyre, Zyra Kombëtare e Auditimit ka fuqizuar auditimet e sistemeve të informacionit, përmes vendosjes në përdorim të këtij manuali dhe zhvillimit profesional të kapaciteteve njerëzore. Krahas zhvillimit profesional, ZKA-ja ka kryer një numër të auditimeve të teknologjisë së informacionit si kombinim i auditimeve të performancës, atij financiar e tashmë edhe si auditime të veçanta të sistemeve të informacionit. Në këto auditime, është kryer ekzaminimi dhe rishikimi i sistemeve të informacionit dhe kontrolleve të lidhura për të fituar siguri ose identifikuar shkelje të parimeve të ligjshmërisë, efikasitetit, ekonomisë dhe efektivitetit të sistemeve dhe kontrolleve. Në Planin Strategjik për vitet 2022-2025, Zyra Kombëtare e Auditimit do ti jep prioritet zhvillimit dhe rritjes së mëtutjeshme të kapaciteteve në fushën e auditimit të teknologjisë së informacionit.

Andaj, besoj se Manuali i Auditimit të Teknologjisë së Informacionit do t'i shërbej fuqizimit të mëtejmë të kryerjes së auditimeve cilësore të cilat do të ndikojnë në rritjen e efikasitetit dhe efektivitetit dhe besueshmërisë së sistemeve të cilat përdoren nga sektori publik.

Shfrytëzoj rastin të falënderoj punonjësit e Zyrës Kombëtare të Auditimit për punën e pakursyer në zhvillimin e auditimeve të teknologjisë së informacionit si dhe Kontrollin e Lartë të Shtetit të Shqipërisë për bashkëpunimin e shkëlqyer me Zyrën Kombëtare të Auditimit të Kosovës në fushën e auditimit të teknologjisë së informacionit.

Vlora Spanca 

Auditore e Përgjithshme

Hyrje

Zhvillimi i Teknologjisë së Informacionit ka ndryshuar mënyrën se si ne punojmë në shumë mënyra, ku nuk përjashtohet as auditimi. Kompjuteri gjithëpërfshirës, që është padyshim një nga mjetet më efektive të biznesit, ka sjellë gjithashtu edhe dobësi të mjedisit të automatizuar të biznesit. Çdo dobësi e re ka nevojë të identifikohet, minimizohet dhe të kontrollohet; duke vlerësuar mjaftueshmërinë e çdo kontrolli nevojiten metoda të reja të auditimit.

Kompjuterët janë zhvilluar nga sisteme procesuese të të dhënave në atë që sot ata grumbullojnë, ruajnë dhe ofrojnë qasje ndaj sasive të mëdha të të dhënave. Këto të dhëna përdoren në vendim marrje dhe në shkëmbim informacioni përgjatë rrjeteve si publike ashtu edhe private.

Në fakt, me zhvillimin dhe rritjen e sistemeve të rrjetit kompjuterik, sistemet kompjuterike janë tashmë sisteme informacioni. Si një provë e këtij evolucioni, termi 'EDP audit' (Electronic Data Process audit-Auditimi i procesimit elektronik të të dhënave) është zëvendësuar me terma të tilla si 'Auditimi i Teknologjisë së Informacionit' dhe 'Auditimi i Sistemeve të Informacionit'.

Me rritjen në investime dhe varësinë në sistemet kompjuterike nga subjektet e audituara, është bërë e domosdoshme për audituesin e TI-së të adoptojë një metodologji dhe qasje të saktë në mënyrë që të identifikojë rreziqet e integritetit të të dhënave, abuzimet dhe privatësinë, si dhe të ofrojnë siguri se ekzistojnë kontrollet e minimizimit të këtyre rreziqeve. Në një sistem TI-së, sidomos kur është i implementuar në një mjedis me kontrolle jo të sakta, subjekti i audituar ndeshet me shumë rreziqe, të cilat duhet të identifikohen nga audituesi i TI-së. Edhe kur subjekti i audituar, ka implementuar disa masa të reduktimit të rreziqeve, një auditues i pavarur duhet të japë siguri se kontrollet e duhura (Kontrollet e Përgjithshme Kompjuterike[1] ose/dhe Kontrollet e Aplikacionit[2]) janë projektuar dhe operojnë për të minimizuar ekspozimin ndaj rreziqeve të ndryshme.

Përmbajtja dhe struktura e këtij Manuali

Ky Manual është hartuar për të pajisur audituesin e TI-së me udhëzim të detajuar mbi fusha të ndryshme të Auditimit të TI-së ashtu si edhe të udhëzojë hap pas hapi se si të planifikojë këto auditime.

Në kapitullin e parë, lexuesit do të gjejnë një përmbledhje të përkufizimit të auditmit të TI-së, mandatit të ISA-t, qëllimi dhe objektivat e audituesit të TI-së. Tregon gjithashtu edhe një shpjegim të Kontrolleve të Përgjithshëm të TI-së dhe Kontrolleve te Aplikacionit si dhe marrëdhënien në mes tyre. Këto fusha kontrolli janë zhvilluar më tej në kapitujt pasardhës. Kapitulli 1 përshkruan gjithashtu proceset e auditimit të TI-së dhe metodologjinë e vlerësimit bazuar në rrezik për auditimet e përzgjedhura të TI-së. Përshkrimi i proceseve të auditmit të TI-së është i përgjithshëm dhe bazohet mbi metodat standarde të auditimit që ndiqen gjatë një auditimit tipik të TI-së. Përdoruesit e Manualit duhet t'i referohen

1 Kontrollet e përgjithshme të sisteme informative nuk janë specifike për një rrjedhe të transaksionit apo aplikacionit individual dhe janë kontrolle mbi proceset e zbatimit të teknologjisë informativei cili mbështet zhvillimin, zbatimin dhe funksionimin e një sistemi informativ. Ato përfshijnë qeverisjen e TI-së, organizimin dhe strukturën, kontrollet fizike dhe mjedisore, funksionimin e TI-së, sigurinë e SI dhe vazhdimësia e biznesit.

2 Kontrollet e aplikacionit janë kontrolle specifike për një sistem të TI-së, dhe përfshijnë planifikimin e rregullave të biznesit në aplikacion duke siguruar kështu kontrollet e hyrjes, përpunimit, daljes dhe "Master data".

manualeve dhe udhëzimeve procedurale të auditimit të ISA-ve respektiv për planifikimin dhe udhëheqjen e auditimeve.

Kapitujt 2-8 tregojnë përshkrim të detajuar të fushave të ndryshme të TI-së të cilat ndihmojnë audituesit e TI-së në identifikimin e zonave të mundshme të auditimit. Rreziqet e nivelit organizativ të lidhura me fushën e TI-së janë listuar në fund të çdo kapitulli; këto rreziqe do të ndihmojnë audituesit të identifikojnë fushat me rrezik të lartë. Udhëzimet e parashtruara në çdo fushë do të ndihmojnë audituesit e TI-së në planifikimin e auditimeve të tyre, në një fushë të caktuar ose në një kombinim fushash në varësi të qëllimit dhe objektivave të auditimit të TI-së që planifikohet (financiar ose performance). Për shembull, udhëzimi i auditimit të qeverisjes së TI-së, mund të përdoret për të planifikuar një auditim të mekanizmit qeverisës të TI-së në subjekt ose për të vlerësuar kontrollet e përgjithshme në mjedisin auditues, pjesë e rëndësishme e të cilave është edhe qeverisja e TI.

Çdo kapitull mbështetet hap pas hapi nga udhëzime mbi zhvillimin e një matrice auditimi e paraqitur në Shtojcat II-VIII. Matrica e auditimit liston çështjet e auditimit, kriteret, informacionin e nevojshëm dhe metodat e analizimit. Përdoruesit duhet të kenë parasysh se çështjet e listuara në matrica janë vetëm treguese dhe jo gjithëpërfshirëse dhe se përdoruesit janë të inkurajuar të zhvillojnë matrica sipas kërkesave të auditimit të tyre. Formati i matricës së auditimit është i përgjithshëm dhe mund të përdoret si mjet pune nga ISA-t, ose mund të modifikohet sipas standardeve të ISA-ve.

Si përfundim, ky Manual përfshin një pamje të përgjithshme të fushave të reja në Auditimin e TI-së. Kapitulli 9 thekson disa nga fushat të cilat mund të jenë në interes të audituesve të TI-së, siç janë /ueb faqet dhe portalet, E-Qeverisja, auditimi bazuar në Forenzikën Kompjuterike t Kompjuterikë Mobile etj. Ky kapitull përmban një listë me shembuj të fushave të auditimit dhe paraqet referenca për lexim më të thelluara për përdoruesit e interesuar.

Udhëzimet teknike mbi përdorimin e Teknikave Kompjuterike Ndihmëse në Auditim (CAATS) janë përtej fushëveprimit të qëllimit të këtij Manuali. ISA-t inkurajohen të organizojnë trajnime të veçanta mbi CAATS për personelin e tyre. ISA-t gjithashtu mund të propozojnë pjesëmarrës në programin e zhvillimit të kapaciteteve IDI (INTOSAI Development Initiative) mbi trajnime të audituesve të TI-së me temë CAATS.

Ju lutemi vizitoni ueb faqen e WGITA si dhe ueb faqen e IDI për informacion të mëtejshëm mbi burimet dhe programet e trajnimit që do të zhvillohen së shpejti.

WGITA http://www.intosaiitaudit.org

IDI http://www.idi.no

Shpresojmë që ISA-t dhe stafi i tyre i auditimit të TI-së do ta shikojnë këtë Manual si mjet të dobishëm në shtimin e njohurive dhe kuptimit të çështjeve të auditimit të TI-së, si dhe do TI-së përdorin ato në planifikimin e auditimeve të tyre.

KAPITULLI 1

Auditimi i Teknologjisë së Informacionit (TI)

Hyrje

Nën dritën e mundësive kompjuterike të gatshme nëpër botë, organizatat i janë referuar fuqimisht automatizimit të aktiviteteve të tyre si dhe menaxhimit të informacionit. Ky fakt vendos sfondin që audituesit të përfitojnë siguri në këto mekanizma dhe të shfrytëzojnë informacionin e disponueshëm në këto mekanizma për gjenerimin e konkluzioneve të duhura të auditimit.

Ky kapitull paraqet një pamje të përgjithshme të proceseve të auditimit TI-së. Shërben edhe si një prezantim ashtu edhe si një përmbledhje e kapitujve 2-8. Për këtë arsye ky kapitull ndryshon nga të tjerët në termat e formatit dhe detajeve. Proceset e auditimit të TI-së të përshkruara në këtë kapitull nuk janë të dokumentuara në ndonjë standard ndërkombëtar por është një pasqyrim i metodologjisë së zbatuar në ISSAI-t dhe në standarde të tjera ndërkombëtare po aq sa në praktikat audituese të pranuara dhe të ndjekura nga ISA-t.

ÇFARË ËSHTË AUDITIMI I TI-së

Ndërkohë që nuk ka asnjë përcaktim unik të auditimit të Teknologjisë së Informacionit, Ron Weber e ka përkufizuar auditimin e TI-së si procesi i sigurimit nëse zhvillimi, implementimi dhe mirëmbajtja e sistemeve të TI-së përmbush qëllimet e biznesit, ruan asetet e informacionit dhe ruan integritetin e të dhënave dhe nëse përdor burimet në mënyrë efikase. Me fjalë të tjera, auditimi i TI-së është një ekzaminim i implementimit të sistemeve të TI-së për tu siguruar se ato mbështesin nevojat e biznesit pa kompromentuar sigurinë, privatësinë, koston dhe elemente të tjera kritike të biznesit.

Mandati për auditimin e TI-së

Mandati i ISA për të udhëhequr auditimin e sistemeve të TI-së përshkruhet në ISSAI 1-Deklarata e Limës[3]. Për më shumë, mandati i një ISA për auditimin e TI-së rrjedh nga mandati i përgjithshëm i përcjellë nga ISA për të udhëhequr auditimin financiar, të pajtueshmërisë, të performancës ose një kombinim të tyre. Disa ISA gjithashtu mund të kenë mandat specifik për ndërmarrjen e auditimit të TI-së. Për shembull, nëse ISA ka një mandat për të audituar funksionet e të ardhurave nga taksat, ISA duhet të auditoj pjesën e automatizuar të funksionit të hyrjeve nga taksat përmes derivimit nga mandati i tyre origjinal.

Objektivat e auditimit të TI-së

Objektivë e auditimit të TI-së është që të sigurojë se burimet e TI-së lejojnë të arrihen qëllimet e organizatës efektivisht dhe përdorimin në mënyrë efikase të këtyre burimeve. Auditimet e TI-së mund të mbulojnë sistemet ERP (Enterprise Resource Planing - Planifikimi i burimeve të ndërmarrjes), sigurinë e sistemeve të informacionit, përvetësimin e zgjidhjeve të biznesit, zhvillimet e sistemeve,

[3] INTOSAI *Lima Declaration*, Part VII Section 22

vazhdimësinë e sistemeve që janë fushë specifike e implementimit të Sistemeve të Informacionit (SI) ose mund të jenë për të vëzhguar pjesën e vlerës që SI kanë përmbushur.

Disa shembuj të objektivave të TI-së janë:

- Rishikim i kontrolleve të sistemeve të TI-së për tu siguruar mbi mjaftueshmërinë dhe efektivitetin e tyre;
- Vlerësimin e proceseve të përfshira në operacionet e një fushe të caktuar si sistemi i pagave, sistemi i kontabilitetit financiar;
- Vlerësimi i performancës të një sistemi dhe sigurisë së tij, për shembull, sistemi i rezervimit të trenit;
- Ekzaminimi i procesit të zhvillimit të sistemit dhe të procedurave.

Qëllimi i auditimit të TI-së

Përgjithësisht ISA-t kryejnë auditimin e TI-së njëkohësisht me auditimin e pasqyrave financiare, rishikimin e kontrolleve të brendshme ose si auditim performance të sistemeve të TI-së ose të aplikacioneve të TI-së. Në terma më të përgjithshëm, auditimet e TI-së shtrihen në auditmet financiare (për të vlerësuar saktësinë e pasqyrave financiare të subjektit); në auditimet e pajtueshmërisë/operacioneve (vlerësimi i kontrolleve të brendshme); në auditimet e performancës (përfshirë çështjet e sistemeve të informacionit); auditmet e forenzikës dhe auditmet e projekteve zhvilluese të sistemeve të informacionit.

Pavarësisht llojit të auditimit, audituesit të TI-së do t'i nevojitet të vlerësojë politikat dhe procedurat që udhëzojnë mjedisin e përgjithshëm të TI-së të subjektit të audituar, duke siguruar se ekzistojnë kontrollet përkatëse dhe mekanizmat e zbatimit. Qëllimi i auditimit të TI-së do të përfshijë zgjedhjen e shtrirjes së shqyrtimit të auditimit, mbulimin e sistemeve të TI-së dhe funksioneve të tyre, proceset e TI-së që do të auditohen, vendndodhjet e sistemeve të TI-së që do të mbulohen, si dhe periudha që do të shtrihet. Do të jetë, në fakt, vendosja ose tejkalimi i limiteve të auditimit.

Kontrollet e TI-së

Një kontroll është kombinimi i metodave, politikave dhe procedurave që sigurojnë mbrojtjen e aseteve të organizatës, saktësinë dhe besueshmërinë e regjistrimeve të tyre, si dhe përputhjes operacionale me standardet e menaxhimit.

Në kontekstin e TI-së, kontrollet ndahen në dy kategori: të përgjithshëm dhe të aplikacioneve. Kategoria varet nga shtrirja e ndikimit dhe nëse është e lidhur me ndonjë aplikacion në veçanti.

Kontrollet e përgjithshme të TI-së janë baza e strukturës së kontrollit të TI-së. Ato kanë të bëjnë me mjedisin e përgjithshëm në të cilin sistemet e TI-së janë zhvilluar, operuar, menaxhuar dhe mirëmbajtur. Kontrollet e përgjithshëm të TI-së vendosin një strukturë gjithëpërfshirëse për aktivitetet e TI-së dhe garantojnë siguri se objektivat e përgjithshëm të kontrollit do të arrihen.

Kontrollet e përgjithshëm janë implementuar duke përdorur një sërë mjetesh siç janë politikat, udhëzimet dhe procedurat ashtu si edhe duke vendosur një strukturë të dobishme menaxhimi, duke përfshirë edhe atë për menaxhimin e sistemeve të TI-së të organizatës. Shembuj të kontrolleve të përgjithshëm përfshijnë zhvillimin dhe implementimin e Strategjisë të Sistemeve Informative (SI) dhe një Politikë Sigurie të SI, vendosjen e komitetit drejtues të TI-së, organizimin e stafit të TI-së për ndarjen e detyrave konfliktuese dhe planifikimin e parandalimit dhe rimëkëmbjes nga fatkeqësitë.

Kontrollet e aplikacioneve janë kontrolle specifike unike për çdo aplikacion të kompjuterizuar. Ato aplikohen në segmente aplikacionesh dhe merren me të dhënat e transferueshme dhe ato të qëndrueshme. Kontrollet e aplikacioneve përfshijnë vlefshmërinë e futjes së të dhënave, enkriptimi i të dhënave për tu transmetuar, kontrollet proceduese etj. Për shembull, në një aplikacion pagese online, një kontroll hyrës mund të jetë data e skadencës së kartës së kreditit e cila duhet shtrihet përtej datës së transaksionit dhe të dhënat e futura duhet të jenë të enkriptuara.

Kontrollet e përgjithshme të TI-së dhe kontrollet e aplikacioneve dhe marrëdhëniet e tyre

Kontrollet e përgjithshëm të TI-së nuk janë specifikë ndaj niveleve të transaksioneve ose ndaj paketave të caktuara të kontabilitetit ose ndaj aplikacioneve financiare. Objektivi i kontrolleve të përgjithshëm të TI-së është të siguroj zhvillimin dhe implementimin e duhur të aplikacioneve, ashtu si edhe të programeve, skedarëve të të dhënave dhe operacioneve kompjuterike.[4]

Dizajni dhe implementimi i kontrolleve të përgjithshëm të TI-së mund të kenë një ndikim mbi efektivitetin e kontrolleve të aplikacioneve. Kontrollet e përgjithshëm pajisin aplikacionet me burimet e nevojshme për operim dhe sigurojnë se ndryshime të paautorizuara nuk mund të ndodhin as në aplikacione (për shembull, ato i mbrojnë nga riprogramimi) ose në bazat e të dhënave të lidhura me to (grumbullimi i madh i transaksioneve të të dhënave).

Kontrollet e përgjithshëm të TI-së më të zakonshëm të cilat rrisin kontrollet e aplikacioneve janë:[5]

-kontrollet e qasjes logjike mbi infrastrukturën, aplikacionet dhe të dhënat,

[4] ISACA, IS Auditing Guidelines-Applications Systems Review-Document GI4, f3
[5] Global Technological Audit Guide (GTAG) 8- Auditing Applications Controls

-kontrollet e zhvillimit të ciklit të jetës së sistemit,

-kontrollet e programit të menaxhimit të ndryshimit,

-kontrolli i qasjes fizike mbi qendrën e të dhënave,

-kontrollet e backup-it dhe rimëkëmbjes të sistemit dhe të të dhënave,

-kontrollet e operacioneve kompjuterike.

Kontrollet e aplikacioneve operojnë në transaksione individuale dhe sigurojnë se hyrja (inputi), përpunimi dhe rezultati/dalja (outputi) kryhen në mënyrë të saktë. Dizajnimi dhe efektiviteti i operimit të kontrolleve të përgjithshme të TI-së ndikojnë në nivelin në të cilin kontrollet e aplikacioneve mund të mbështeten, që menaxhmenti të kontrollojë rreziqet.

Pse janë të rëndësishëm kontrollet e TI-së për audituesin e TI-së

Përgjithësisht, audituesi i TI-së thirret për të testuar kontrollet e lidhura me teknologjinë ndërkohë që audituesit e tjerë testojnë kontrollet financiare, rregullatore dhe të pajtueshmërisë. Sa më shumë organizatat mbështeten në operacionet e automatizuara ose të kompjuterizuara, kufiri ndarës në mes të audituesit TI-së dhe audituesit e tjerë gjithnjë e më shumë është duke u zvogëluar. Të paktën, të gjithë audituesit duhet të kuptojnë mjedisin e kontrollit të subjektit nën auditim, në mënyrë që të japin siguri të arsyeshme mbi kontrollet e brendshme që operojnë në subjekt. Sipas Parimeve themelore të ISSAI për Auditimin Publik: “audituesit duhet të kenë njohuri të natyrës së subjektit/programit nën auditim”. Kjo përfshin njohjen e kontrolleve të brendshme, ashtu si edhe objektivave, operacioneve, mjedisit rregullator, sistemeve si dhe proceseve të biznesit. Çdo fushë e biznesit bazohet në një grup objektivash kontrolli që një organizatë vendos për të zvogëluar rreziqet. Detyra e audituesit është të njohë dhe të kuptojë rreziqet e mundshme të biznesit dhe të TI-së që mund të hasë subjekti dhe si përfundim të vlerësojë nëse këto kontrolle janë të duhurat për arritjen e objektivave të kontrollit. Në rastin e kontrolleve të përgjithshëm të TI-së, është e rëndësishme për audituesin të njohë kategoritë kryesore dhe nivelin e kontrolleve të përgjithshëm në operacione, të vlerësojë mbikëqyrjen e menaxhimit dhe ndërgjegjësimin e personelit në organizatë, si dhe të zbulojë sesa efektivë janë kontrollet për të dhënë siguri të arsyeshme. Ashtu siç thekson edhe ISSAI 1315, që edhe në subjektet më të vogla ku sistemet e informacionit dhe proceset e biznesit krahasuar me ato financiarë janë më pak të sofistikuar, roli i tyre është domethënës. Nëse kontrollet e përgjithshëm janë të dobët, ata zvogëlojnë besueshmërinë e kontrolleve lidhur me aplikacionet individuale të TI.

Në kapitujt pasardhës, disa nga fushat kryesore të Kontrolleve të Përgjithshëm të TI-së dhe Kontrolleve të Aplikacioneve, janë diskutuar në detaje. Gjithashtu për çdo lloj fushe kontrolli janë paraqitur edhe matrica kontrolli, të cilat gjenden në seksionin e shtojcave.

PROCESET E AUDITIMIT TË TI-së

Planifikimi për auditimet e TI-së

Planifikimi i auditimit është pjesë kryesore e çdo lloj auditimi, duke përfshirë këtu edhe auditimin e TI-së. Në shumë ISA, planifikimi i auditimit shtrihet në tre nivele: Planifikimi Strategjik, Planifikimi Makro ose Vjetor dhe Planifikimi Mikro ose në nivel Subjekti.

Planifikimi strategjik

Një plan strategjik i ISA-t është një parashikim afatgjatë (3-5 vjet) i synimeve të auditimit si dhe objektivave të tij, përfshirë ato të sistemeve të TI-së si dhe të organizatave respektive nën juridiksionin e ISA-s.

Në disa ISA vetëm fushat e reja dhe të shfaqura të auditimit lidhur me TI-së mund të përfshihen në planin strategjik. Kjo mund të përfshijë përqendrimin drejt metodave të reja të zhvillimit të sistemeve (për shembull, programimin e shpejtë) si dhe blerjes ose "Cloud Computing" në sektorin publik.

Në çdo lloj rasti, procesi i planifikimit strategjik si dhe plani strategjik i ISA-s ofron theksin dhe drejtimin e një ISA drejt qëllimeve të Auditimit të TI-së për të ardhmen.

Planifikimi Makro

Niveli Makro i planifikimit të auditimit zakonisht kryhet në baza vjetore në nivel të ISA-s për përzgjedhjen e fushave të auditimit. Me shtimin e shpejtë të sistemeve moderne të informacionit në qeveri të ndryshme dhe me kufizimin e burimeve të disponueshme ndaj ISA-ve, një qasje e bazuar në rrezik për përcaktimin e përparësive dhe çështjeve të duhura, është e përshtatshme. Për më tepër, ISA duhet gjithashtu të përfshijë këto auditime të detyrueshme, si ato të kërkuara me ligj ose të kërkuara nga parlamenti ose subjektet mbikëqyrëse.

Qasje bazuar në rrezik

Zakonisht, ISA-t kanë në mandatin e tyre një numër organizatash që përdorin sistem të ndryshëm informacioni. Ekzistojnë aplikacione të ndryshme për funksione dhe aktivitete të ndryshme, ekzistojnë një numër i madh instalimesh kompjuterike në vendndodhje të ndryshme gjeografike.

Ndërkohë që ka rreziqe të natyrshme ndaj sistemeve të informacionit, këto rreziqe prekin sisteme të ndryshme në mënyra të ndryshme. Rreziku i mos-disponueshmërisë qoftë edhe për një orë, mund të jetë shumë serioz për një sistem faturimi në një dyqan të madh shitjesh. Rreziku i ndryshimeve të paautorizuara, mund të jetë burim mashtrimesh dhe humbjesh të mundshme në një sistem bankar online. Një sistem i përpunimit të grupeve, ose një sistem i bashkimit të të dhënave mund të jetë relativisht me rrezik më të ulët në krahasim me rreziqe të tjerë. Mjediset teknike në të cilat janë të vendosura sistemet, gjithashtu mund të ndikojnë rreziqet që janë të lidhura me sistemet.

Një qasje e bazuar në rrezik në përzgjedhjen e sistemeve të TI-së për auditim, ndihmon audituesit në përcaktimin e prioriteteve të auditimit. Për përdorimin e strukturës së vlerësimit të rrezikut, një ISA duhet të ketë informacione mbi subjektet, zakonisht të grumbulluara nëpërmjet sondazheve.

Hapat në qasjen e bazuar në rrezik

1. Identifikoni universin e auditimit, i cili do të përbëhet nga një listë e të gjitha organizatave të audituesshme ose të njësive nën juridiksionin e ISA;
2. Listoni sistemet e informacionit në përdorim në njësitë/organizatat që do të auditohen;
3. Identifikoni faktorët të cilët prekin gjendjen kritike të sistemit në një organizatë për realizimin e funksioneve të saj dhe ofrimin e shërbimit;
4. Përcaktoni peshën ndaj secilit faktor, gjë e cila mund të kryhet në bashkëpunim me organizatën nën auditim;
5. Përpiloni informacionin për të gjithë sistemet, nëpër të gjitha organizatat dhe bazuar në përfundimet e grumbulluara, vendosni sistemet/organizatat sipas prioritetit për auditim;
6. Përgatisni një plan vjetor auditimi i cili duhet të theksojë prioritetin, qasjen dhe programin e auditimit të TI-së. Ky veprim mund të kryhet në intervale vjetore dhe në këtë mënyrë mund të jetë një plan i përsëritur.

Ndërkohë që një proces i vlerësimit të rrezikut është një mënyrë për përzgjedhjen e subjektit për auditim të TI-së, ISA gjithashtu përzgjedh subjektet në baza ciklike, duke shfrytëzuar mandatin, ose sipas kërkesës së organeve mbikëqyrëse (Parlamentit).

Planifikimi Mikro (ose në nivel subjekti)

Planifikimi mikro përfshin zhvillimin e planeve të detajuara të auditimit për subjektin e përzgjedhur duke filluar nga theksimi i objektivave të auditimit. Plani i auditimit do të ndihmojë audituesit në përgatitjen e programit të auditimit të TI-së. Hapi i domosdoshëm në zhvillimin e programit të auditimit, do të jetë njohja e subjektit dhe sistemeve të tij të informacionit. Ky Manual do të ndihmojë audituesit pasi plani është hartuar në popullimin e matricës së auditimit me objektiva specifikë për çdo fushë (qeverisje, siguria e informacionit etj) që do të inspektohet. Planifikimi në nivel mikro kërkon njohjen e subjektit dhe disa vlerësime paraprake të kontrolleve për lehtësimin e planifikimit të detajuar të auditimit.

i. Njohja e organizatës

Niveli i njohurisë mbi organizatën dhe proceseve të saj, të kërkuara nga audituesit e TI-së do të përcaktohen nga natyra e organizatës dhe nivelit të detajeve të punës audituese që është duke u kryer. Njohja e organizatës duhet të përfshijë rreziqet e biznesit, financiarë dhe të brendshëmme të cilët përballet organizata dhe sistemet e saj të TI-së. Duhet gjithashtu të përfshijë masën që shpreh varësinë e organizatës nga blerja e zgjidhjeve teknologjike nga tregtarët për arritjen e objektivave të saj dhe sesi janë pozicionuar proceset e plota të biznesit në mjedisin e TI-së. Audituesi duhet të përdorë këtë informacion në identifikimin e problemeve të mundshme, në formulimin e objektivave dhe të qëllimit të punës, në kryerjen e punës dhe në marrjen parasysh të veprimeve të menaxhimit për të cilët audituesi duhet të jetë vigjilent.

Një paraqitje karakteristike e SI në një organizatë jepet si më poshtë:

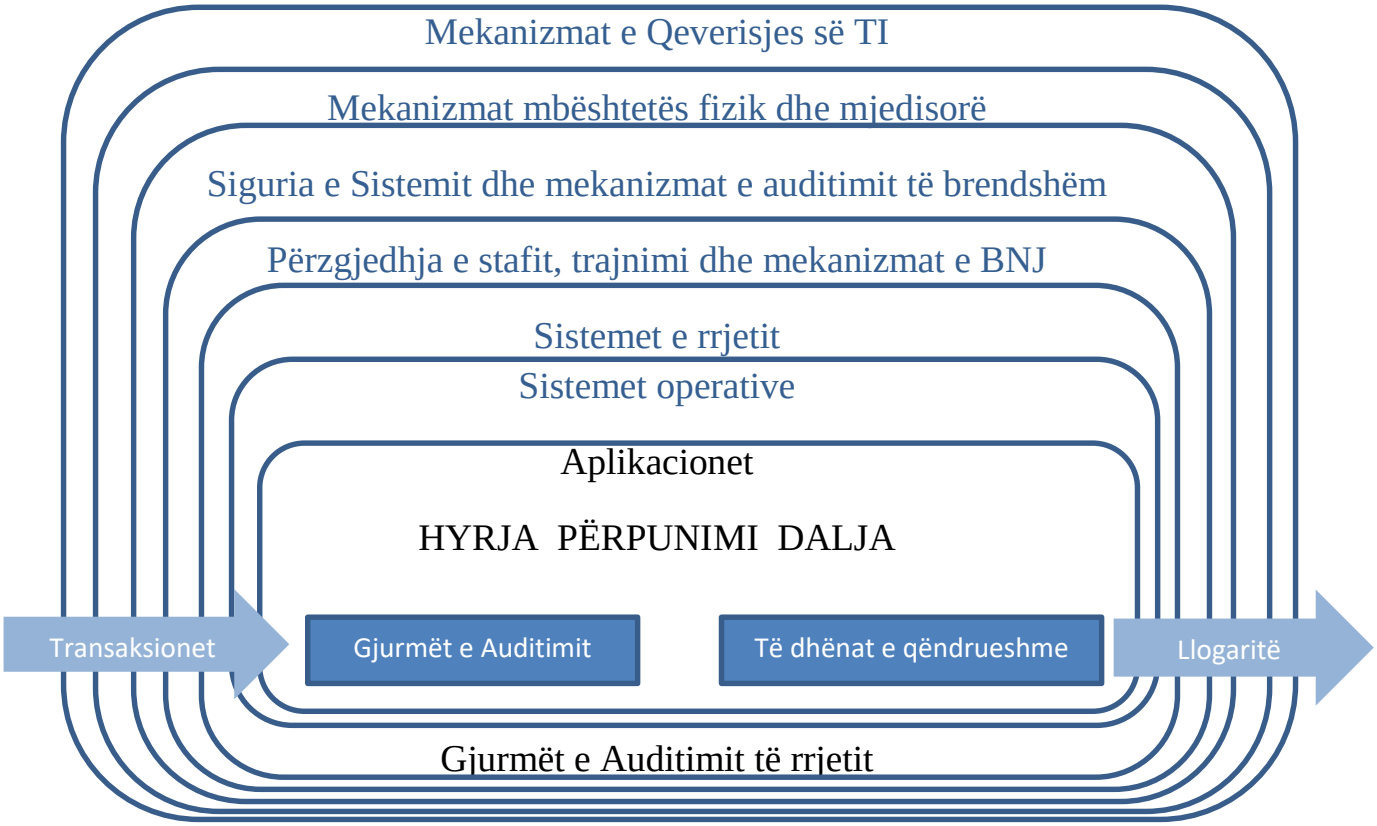


Figura 1.2: Paraqitja e TI-së në një organizatë

Një aplikacion tipik, i cili është bërthama e SI në një organizatë të kompjuterizuar, do të ketë kombinimin e sistemit të menaxhimit të bazës së të dhënave me baza të dhënash specifike, programe aplikative që pozicionojnë rregullat e biznesit në sistem nëpërmjet moduleve të ndryshme, ndërfaqe përdoruesish të mbështetura nga programi aplikativ i rrjetit nëse ka një mjedis rrjet. Bazat e të dhënave dhe programet aplikative qëndrojnë në servera, të cilët janë kompjutera me kapacitet të lartë të aftë për të mbajtur baza të dhënash të shumëfishta si dhe aplikacione. Serverat mund të jenë specifikë ndaj kërkesave të ndryshme të përdoruesve si servera të të dhënave, servera të aplikacioneve, servera të internetit si dhe Proxy servera.

Bazuar në njohjen e zhvillimit të Sistemit të Informacionit dhe të subjektit nën auditim, audituesit e TI-së mund të vendosin qasjen e tyre në auditimin e TI-së. Auditimi i TI-së përfundimisht do të përfshijë auditimin e kontrolleve të përgjithshëm dhe apkikacioneve.

ii. Materialiteti

Materialiteti i një çështje të auditimit të TI-së duhet të përcaktohet nën një kuadër të përgjithshëm për vendosjen e politikave të materialitetit në një ISA. Në formulimin e raportit të auditimit, audituesi duhet të konsiderojë materialitetin në përmbajtje të pasqyrave financiare (auditimi i rregullsisë) ose në natyrën e subjektit apo aktivitetit.

Audituesi i Sistemeve të Informacionit duhet të përcaktojë nëse ndonjë mangësi e përgjithshme e TI-së mund të shndërrohet në materiale. Rëndësia e kontrolleve të tilla të mangëta të përgjithshme të TI-së duhet të vlerësohet në lidhje me ndikimin e kontrolleve të aplikacioneve, për shembull, nëse kontrollet e aplikacioneve të ndërlidhur me të janë gjithashtu joefektive. Nëse mangësia në aplikacion është e shkaktuar nga kontrolli i përgjithshëm i TI-së, atëherë ato janë materiale. Për shembull, nëse një llogaritje takse e bazuar mbi një aplikacion është gabim material dhe është shkaktuar nga një kontroll i dobët ndryshimi në tabelat e taksës, atëherë vendimi i menaxhmentit për mos-rregullimin e mangësive në kontrollet e përgjithshëm të TI-së dhe lidhja e tij me mjedisin kontrollues, mund të shndërrohen në materiale kur ato bashkohen me mangësi të tjera që prekin mjedisin kontrollues.

iii. Shpërndarja e burimeve

Auditimi i TI-së kërkon shpërndarje specifike të burimeve, sidomos forcën punëtore, e cila duhet të jetë e pajisur me njohuri të mira të sistemeve tipikë të TI-së, proceseve dhe mekanizmave të cilat udhëheqin një impelementim të suksesshëm të TI-së. Përveç burimeve njerëzore të përshtatshme[6], buxhetit të mjaftueshëm, infrastrukturës[7], çdo nevojë tjetër e identifikuar duhet të garantohet. Kohështrirja e auditimit duhet të përcaktohet, nëse është e mundur, duke u këshilluar me subjektin e audituar.

iv. Angazhimi me subjektin nën auditim

Subjekti nën auditim duhet të jetë i informuar rreth qëllimit, objektivave dhe kriteret e vlerësimit të auditimit duhet të diskutohen me ta sipas nevojës. ISA mundet, nëse është e nevojshme, të hartojë një dokument angazhimi për subjektin nën auditim, ku të cilësojë gjithashtu edhe termat e angazhimit. ISA duhet të sigurojë se nëpërmjet bashkëpunimit dhe mbështetjes së subjektit nën auditim, të përmbyllë auditimin, duke përfshirë qasjen ndaj regjistrimeve dhe informacionit, qoftë manual ose elektronik.

v. Grumbullimi i evidencave të auditimit

1. Vlerësimi paraprak i kontrolleve të TI-së

Audituesi i TI-së duhet të ndërmarrë një vlerësim paraprak të kontrolleve të TI-së në sistemin që po auditohet për të nxjerrë një kuptim të sigurisë se kontrollet ekzistuese (Kontrollet e përgjithshme dhe të aplikacioneve) janë të besueshme. Vlerësimi i kontrolleve në këtë nivel do të përfshijë:

a. Vlerësimi se mekanizmat e përshtatshëm të Qeverisjes së TI-së ekzistojnë dhe janë funksionalë.
b. Vlerësimi se objektivat e TI-së janë te lidhura/ me objektivat e biznesit.
c. Vlerësimi se ekzistojnë mekanizma të përshtatshëm për blerjen e zgjidhjeve TI-së (ku përfshihen aplikacionet e TI-së, harduer, softuer, burimet njerëzore, rrjeti, shërbime etj)
d. Kontrollet në nivel të organizatës të përfshira në operacionet e TI-së që udhëheqin çdo ditë funksionet e TI-së, procedurat e sigurisë së informacionit të organizatës, vazhdimësinë e biznesit

[6] Burimet e përshtatshme të personelit do të nënkuptojnë personelin që kanë një kuptim të Sistemeve të Informacionit dhe mund të kryejnë nxjerrjen dhe analizimin e të dhënave nëse kërkohet, pasi Auditimet e TI-së pa ndryshim do të kërkonin përdorimin e aftësive të TI-së për kryerjen e kontrolleve. SAI duhet t'i referohet ISSAI 100 paragrafi 52 mbi sigurimin e kompetencës së nevojshme për stafin e saj përpara se të ndërmarrë një Auditim TI

[7] Do të përfshinin platformat e harduerit, sistemet operative, sistemi i menaxhimit te bazave te te dhenave, si dhe pajisjet e ruajtjes, pajisjet kompjuterike si PC, laptopë etj., që të jenë në gjendje të nxjerrin dhe analizojnë informacionin.

dhe procedurat e backup-it, menaxhimin e ndryshimit, ofrimin e shërbimit dhe informatave kthyese.

Të mësipërmet përfshijnë kontrollet e përgjithshme të TI-së të cilët nuk janë specifikë ndaj çdo transaksioni të veçantë ose aplikacioni, por kanë lidhje me infrastrukturën e përgjithshme të TI-së në organizatë, përfshirë këtu politikat e TI-së, procedurat dhe praktikat e punës. Testimet duhet të jenë veçanërisht të dizajnuara duke përdorur teknika përfshirë intervista, sondazhe me pyetësorë, vëzhgime/verifikime, "walk through"[8] marrja e të dhënave dhe analizimi i tyre,etj.

2. Testimet Substanciale (Substantive Testing)

Në testimet substanciale, testet janë dizajnuar të vërtetojnë pohimet sipas objektivave të auditimit. Testimet substanciale përfshijnë teste të detajuara të kontrolleve të TI-së që përdorin teknika dhe mjete të ndryshme për hetimin, nxjerrjen dhe analizimin e të dhënave.

Analizimi i të dhënave përfshin elementët e listuara më poshtë:

- Identifikimin e qëllimit të analizës ose projektit[9]:
- Njohjen e mostrës nën studim;
- Njohja e paraqitjes dhe formatit të të dhënave;
- Vendosja e një identifikuesi të vetëm nëse ka dyfishime ose bashkime;
- Deklarimi i objektivave të auditimit dhe pyetjeve të kërkimit;
- Metodat e përdorura për përgjigjen e pyetjeve të kërkimit
    - Kriteret e vlerësimit
    - Evidencat
    - Analizat
    - Konkluzionet
- Procedurat e ristrukturimit të dosjeve (krijimi i sintaksës, shtimi i parametrave të tjerë sipas nevojës);
- Procedurat e pastrimit të të dhënave (për shembull heqja e kufijve).

Analizat më të shumta mund të ekzekutohen direkt në një dosje pune. Disa analiza mund të kërkojnë modifikime të të dhënave të papërpunuara, grupime, ose futje të të dhënave specifike për tu përshtatur me programet statistikore. Sistemet e TI-së përdorin shumëllojshmëri të dhënash dhe formatesh (numerike, karaktere, alfa, etj). Audituesi i TI-së duhet të ketë njohuri të këtyre formateve dhe të përdorë mjetet e duhura në analizimin e të dhënave. Audituesi mund të përdorë Program të Përgjithshëm Auditimi ose Program Specifik Auditimi për të kryer analizimin e informacionit. Mjete si Microsoft Excel, Microsoft Access, IDEA, ACL etj., janë shembuj të programeve të përgjithshëm auditimi të cilët ofrojnë lehtësira në importimin dhe analizimin e të dhënave.

8 Walk through-Testet e përcjelljes kryhen për të kuptuar dhe vendosur besueshmërinë e Sistemeve të TI-së të klientit dhe procedurave të kontrollit të brendshëm. Ky test është më i përshtatshëm për të kuptuar sistemin e TI-së ose për verifikimin e gjetjeve nga testet preliminare ose rezultate të testeve të tjera substanciale. Kështu që nuk mund të jetë pikërisht një test i kontrolleve.

9 Jonathan Steinberg, *An Overview of Data Analysis*; Bruce A. Kaplan *Data Analysis Research*; Muhamad Jantan *Introduction to Data Analysis*

Pas kësaj secila prej teknikave të mëposhtme, sipas kërkesave mund të adoptohet nga audituesit e TI-së si:

a) Nxjerrjen e të dhënave duke kopjuar të dhënat nga subjekti i audituar. Audituesi TI-së mund të krijojë një mjedis të ngjashëm (sistem operativ, sistem i menaxhimit të bazës së të dhënave, harduer etj), si të subjektit nën auditim për të analizuar/nxjerrë të dhëna nga kopja e të dhënave. Audituesi i TI-së mundet gjithashtu të ketë nevojë të konvertojë të dhënat nga një lloj në tjetrin për të lehtësuar leximin dhe analizimin e tyre.
b) Shfrytëzimi i programeve të auditimit për nxjerrjen e të dhënave nga kombinime të ndryshme të sistemeve operative, sistemeve të menaxhimit të bazës së të dhënave, sistemeve aplikativë etj. Audituesit e TI-së mund të përdorin **Programe të Përgjithshme Auditimi** ose **Programe Specifike Auditimi.** Programet e përgjithshme të auditimit gjithashtu mund të përdoren për industri të veçanta ose mund të jenë softuer i shërbimeve që mund të përdoren për të vlerësuar funksionimin e shërbimeve të ndryshme të sistemeve kompjuterike. Përdorimi i secilit prej tyre, ose kombinimit të tyre është në varësi të objektivave dhe qëllimit të auditimit që do të trajtohet në Auditimin e TI.
c) Kryerja e **testimit të të dhënave** në situatat ku cilësia e programit është si synim për tu testuar. Premisat tregojnë që është e mundur të përgjithësojmë mbi besueshmërinë e plotë të një programi nëse është i besueshëm për një grup testimesh specifikë. Përdorimi i të dhënave të testimit përfshin ***Dizajnimin*** e të dhënave të testimit dhe ***Krijimin*** e të dhënave të testimit përpara se të ekzekutojmë programin me të dhënat e testimit.

Audituesi i TI-së duhet të zgjedhë vlerësimin e saktë të rrezikut dhe të përdorë teknika të marrjes së mostrave për të arritur në përfundime të përshtatshme bazuar në kontrolle të mjaftueshme statistikore mbi të dhënat e limituara. Përgjithësisht është një praktikë e mirë ndihma nga ekspertë brenda organizatës për përzgjedhjen dhe përcaktimin e mostrave.

DOKUMENTACIONI I AUDITIMIT

Dokumentacioni i auditimit të sistemeve të informacionit është regjistrimi i punës audituese të kryer si dhe të evidencave të auditimit që mbështesin gjetjet dhe përfundimet. Ruajtja e rezultateve dhe provave të auditimit duhet të sigurohet nga audituesit e TI-së, në mënyrë që të përmbushin kërkesat e besueshmërisë, plotësisë, mjaftueshmërisë si dhe saktësisë. Është gjithashtu e rëndësishme për audituesit e TI-së të sigurojnë që procesi i auditimit mirëmbahet për të siguruar verifikimin e mëtejshëm të procedurave të analizimit të auditimit. Kjo përfshin teknikat e përshtatshme të dokumentimit.

Dokumentimi përfshin regjistrim të:

- Planifikimi dhe përgatitja e qëllimeve dhe objektivave të auditimit;
- Programet e auditimit;
- Evidencat e grumbulluara mbi bazën e të cilave konkluzionet janë hartuar;
- Të gjitha letrat e punës, duke përfshirë dosjet e përgjithshme që kanë lidhje me subjektin ose sistemin;
- Çështjet e diskutuara në intervista që theksojnë qartë pikat e trajtuara, personin e intervistuar, pozicionin e punës, kohën dhe vendin;
- Verifikimi sesi audituesi vëzhgoi performancën në punë. Verifikimi mund të përfshijnë vendin dhe kohën, arsyen e verifikimit si dhe personat e përfshirë në të;
- Raporte dhe të dhëna të nxjerrë direkt nga sistemi prej audituesit ose të ofruara nga stafi nën auditim. Audituesi i SI duhet të sigurohet se këto raporte përmbajnë burimin se nga vijnë, datën, vendin dhe kushtet në të cilat është marrë;
- Në pika të ndryshme të dokumentacionit, audituesi mund të shtojë komente dhe qartësime mbi shqetësime, dyshime dhe nevoja për informacione të mëtejshme. Audituesi duhet t'u rikthehet këtyre komenteve më vonë dhe të shtojë shënime sesi dhe kur ato janë marrë;
- Për ruajtjen e të dhënave elektronike, ISA-t duhet të garantojnë backup të të dhënave të marra nga subjekti i audituar, si dhe rezultatet e pyetjeve dhe analizave. Dokumentacioni i auditimit duhet të mbahet konfidencial dhe duhet të ruhet për një periudhë që përcaktohet nga vetë ISA ose ligji;
- Atëherë kur puna audituese rishikohet nga mbikëqyrësi, shënimet që dalin nga ky rishikim duhet gjithashtu të regjistrohen në dokumentacion;
- Draft raportet dhe raportet finale të auditimit duhet të jenë pjesë e dokumentacionit të auditimit.

MBIKQYRJA DHE RISHIKIMI

Puna e stafit audituesdhet të mbikëqyret në mënyrën e duhur përgjatë auditimit[10] dhe puna e dokumentuar duhet të rishikohet nga një anëtar i lartë i stafit audituesi[11]. Ky i fundit, duhet gjithashtu të ofrojë udhëzimet e nevojshme, trajnimet dhe rolin udhëheqës përgjatë kryerjes së auditimit, i cili do të jetë thelbësor në këtë fushë të re-Auditimi i TI.

RAPORTIMI

Një raport auditimi TI-së duhet të ndjekë paraqitjen e përgjithshme të sistemit të raportimit të ndjekur nga ISA. Raportet e audituesve të TI-së duhet të masin çështjet teknike të raportuara bazuar në nivel të detajuar, e kërkuar kjo nga audienca për të cilat raportet hartohen. Raporti i auditimit të TI-së duhet të pasqyrojë gjetjet në një kohë të kufizuar, duhet të jetë konstruktiv dhe i dobishëm për subjektin nën auditim, po ashtu si edhe kuptimplotë ndaj palëve të tjerë të interesit. Raporti duhet të dorëzohet tek autoritetet e duhura, sipas mandatit të ISA dhe auditimit të TI.

FAZAT E RAPORTIMIT

Ka një sërë mënyrash sesi mund të përmbushen kërkesat e ISSAI, lidhur me fazën e konkluzioneve të procesit të auditimit. Ato varen nga traditat e ISA-ve si dhe kuadrit ligjor. Një nga këto mënyra përbëhet nga tre faza raportimi gjatë procesit të auditimit:

1. Dokumenti i diskutimit

Procesi i raportimit nis me diskutimin e përmbajtjes së draft raportit të auditimit (dokumenti i raportimit) i cili shërben si dokument diskutimi në takimin përmbyllës me entitetin. Kjo lejon që fjalë të gabuara, gabime faktike ose mospërputhje për t'u identifikuar, korrigjuar ose eliminuar. Pasi klienti dhe audituesi kanë diskutuar çështjet në përmbajtje të draftit për diskutim, audituesi kryen rregullimet e nevojshme dhe dërgon tek klienti draft raportin final të auditimit për komente.

2. Draft raporti dhe Letra e menaxhmentit

Draft raporti dhe Letra e menaxhmentit në rastet kur aplikohet, është drafti formal që i dorëzohet subjektit të audituar, në mënyrë që të përgjigjet ndaj verifikimeve të ngritura. Kjo lejon që menaxhmenti të fokusohet drejt gjetjeve, përfundimeve dhe rekomandimeve, të cilat gjenden në draftin formal të cilin e pranojnë. Në këtë pikë, është detyrë e menaxhmentit të subjektit të audituar të shkruajë komentet/përgjigjet zyrtare ndaj audituesve dhe të trajtojë gjetjet.

3. Raporti përfundimtar i auditimit

Pasi janë marrë komentet e subjektit, audituesi përgatit një përgjigje duke treguar pozicionin e auditimit. Kjo arrihet duke vendosur së bashku komentet e audituesit dhe përgjigjet e subjektit në një raport, i cili është Raporti i Auditimit.

[10] *ISSAI 100* paragrafi 39, 41

[11] *ISSAI 100* paragrafi 54.

Në raportimin e parregullsive ose të mospërputhjeve me rregullat ose ligjet, audituesit duhet të tregohen të kujdesshëm të vendosin gjetjet e tyre në perspektivën e duhur. Raportimet e parregullsive mund të përgatiten pavarësisht kualifikimit të opinionit të audituesit.

Për nga natyra e tyre, raportet e auditimit tentojnë të jenë kritikë, por në menyrë që të jenë konstruktive, raportet gjithashtu duhet të theksojnë veprime përmirësuese, si konkluzionet ose rekomandimet[12].

Formulimi i konkluzioneve dhe rekomandimeve

Gjetjet, konkluzionet dhe rekomandimet e auditimit, duhet të bazohen në dëshmi. Në formulimin e konkluzionit ose të raportit, audituesi i TI-së duhet të ketë parasysh materialitetin sipas natyrës së auditimit ose të subjektit të audituar[13].

Audituesit e TI-së duhet të strukturojnë konkluzionet mbi gjetjet e auditimit, bazuar në Objektivin e auditimit. Konkluzionet duhet të jenë të rëndësishme (relevant-të përshtatshme), logjike dhe të paanshme. Heqja e konkuzioneve për shkak të mungesës së kontrolleve dhe rreziqeve, mund të shmanget, kur ato nuk janë të mbështetura nga testimet substanciale.

Audituesit e TI-së duhet t'i raportojnë rekomandimet kur mundësia për përmirësime në operacione dhe performancë është provuar nga gjetjet e raportuara. Audituesit duhet gjithashtu të raportojnë statusin e gjetjeve dhe rekomandimeve të pa zbatuara të rëndësishme, nga auditime të mëparshme që ndikojnë në Objektivin e auditimit të tanishëm. Rekomandimet konstruktive mund të inkurajojnë përmirësime. Rekomandimet janë më konstruktive kur fokusohen drejt zgjidhjes së problemeve të identifikuara, janë specifike dhe të fokusuara drejt veprimeve, janë të drejtuara ndaj palëve që janë autoritet për të vepruar, janë të realizueshme dhe në nivelin praktik, janë me kosto efektive.

Kufizimet e Auditimit të TI

Kufizimet e auditimit të TI-së duhet të pasqyrohen në raport. Kufizimet tipike mund të jenë qasja ndaj të dhënave dhe informacionit, mungesa e dokumentacionit të procesit të kompjuterizimit, duke çuar audituesin e TI-së të improvizojë metoda të veta ttë/hulumtimi dhe analizimi për të nxjerrë konkluzione. Çdo kufizim tjetër i hasur nga audituesi duhet të pasqyrohet në raport në mënyrën e duhur.

Përgjigja e subjektit të audituar

Në rastin e raportit të auditimit të TI-së, është shumë e rëndësishme të merret përgjigje ndaj verifikimeve të auditimit. Audituesit e TI-së duhet të kryejnë takime me menaxhmentin e lartë të subjektit të audituar dhe të dokumentojnë përgjigjen e tyre. Nëse këto përpjekje dështojnë, dëshmitë e mjaftueshme mbi përpjekjet duhet të mbahen dhe të përmenden në raport.

[12] *ISSAI 100 paragraph 55*
[13] *ISSAI 100 paragraph 54*

Referencat:

1. Manuali i Auditimit të TI-së, Vëllimi I, Kontrolli dhe Audituesi i përgjithshëm i Indisë
2. Auditimi i Sistemeve të Informacionit, nga Ron Weber, Impresioni i Katërt, 2011
3. Struktura COBIT, Institucioni i Qeverisjes së TI
4. IDI AfroSAI/Kurs auditimi E-IT
5. ISSAI 100 Parimet themelore të Auditimit të Sektorit Publik
6. ISSAI 200 Parimet themelore të Auditimit Financiar
7. ISSAI 300 Parimet themelore të Auditimit të Performancës
8. ISSAI 400 Parimet themelore të Auditimit të Pajtueshmërisë
9. Weber, Ron. Auditimi i Sistemeve të Informacionit, Impresioni i katërt, 2011

SHTOJCA I

Modeli i matricës se auditimit

Përdorimi i matricës së auditimit

Gjatë fazës së auditimit, është e dobishme të zhvillohet një matricë auditimit që mbulon të gjitha çështjet e lidhura me qëllimin dhe Objektivi i auditimit. Formati tipik i një matrice auditimi, e përdorur gjithashtu në këtë Manual, është si më poshtë:

ZONA/FUSHA E AUDITUESHME	
Objektivi i auditimit:	
Çështja e auditimit:	
Kriteret:	
Informacioni i kërkuar	**Metodat e analizimit**
Konkluzioni i auditimit Të plotësohet nga audituesi:	

Matrica përmbledh të gjithë procesin e auditimit të SI. Audituesit e TI-së duhet të identifikojnë çështjet e auditimit përgjatë fazës së vlerësimit paraprak. Çështjet mund të jenë të lidhura me SI ose me çështje qeverisjeje, të cilat kanë ndikim në sistemet e informacionit të subjektit. Audituesit duhet gjithashtu të identifikojnë kriteret e vlerësimit, të cilat do të maten, në përputhje me objektivat/çështjet e auditimit.

Për të përmbushur kriteret, informacione ose evidenca të përshtatshme duhet të identifikohen dhe mbledhur në një mënyrë që të njëjtat të mund të ruhen për referenca të ardhshme, për mbështetjen e konkluzioneve. Grumbullimi i informacioneve mund të ketë nevojë për mjete dhe teknika specifike. Këto të fundit duhet të identifikohen dhe shfrytëzohen, veçanërisht gjatë fazës së testimit. Metodat e analizimit, janë gjithashtu specifike ndaj mjediseve të SI dhe kanë nevojë të shfrytëzohen për të arritur në konkluzione të qëndrueshme dhe kuptimplota. Kjo temë është trajtuar në kapitullin e testimit substancial nën ekzekutimin e auditimit.

Identifikimi i burimit të informacionit

Burimet karakteristike të informacionit në një organizatë që përdor sisteme TI-së mund të jenë:

a) Diagramet e rrjedhjes (flow diagrams) ku përfshihen diagrami i rrjedhjes së sistemit, diagrami i rrjedhjes së procesit etj.
b) Dokumentacion i zhvillimit të sistemit si për shembull, dokumentacion i specifikimeve të kërkesave të përdoruesit (SKP[14]), specifikimet e kërkesave të sistemit (SKS)

[14]SKP Dokumenti i Specifikimit të Kërkesave të Përdoruesit përmban kërkesa që tregojnë funksionet e organizatës që sistemi TI-së supozohet të kryejë dhe operacionaliteti i dëshiruar i përdoruesit. Kjo është faza ku një përcaktim i plotë dhe i qartë i kërkesave të përdoruesit duhet të specifikohet nga

c) Të dhënat elektronike[15]
d) Informacion tjetër i disponueshëm në subjekt që lidhet me funksionet, sistemet kontrolluese dhe monitoruese etj. Si për shembull formularë, informacion mbi buxhetin, raporte të ndryshme ku përfshihen auditime të kaluara, auditime të jashtme, rishikime të brendshme etj.,
e) Politikat, procedurat dhe udhëzime të tjera dhe
f) Përdoruesit e sistemit

Identifikimi i teknikave dhe mjeteve që grumbullojnë informacionin

Subjektet e audituara do të kenë kombinimin e tyre të pajisjeve harduerike, sistemit operativ, sistemet e menaxhimit të bazave të të dhënave, programet e aplikimit dhe programet e rrjetit (softuer aplikativ dhe të rrjetit) etj. Audituesit e TI-së duhet të jenë në gjendje të grumbullojnë informacion nga këto burime për nxjerrjen e konkluzioneve. Njohja e sistemit TI-së dhe bazës së të dhënave është një hap i rëndësishëm në nxjerrjen e të dhënave.

Audituesit e TI-së duhet të vendosin për përshtatshmërinë e përdorimit të një ose më shumë nga teknikat e mësipërme dhe të sigurijonë vetën e tyre mbi integritetin dhe dobishmërinë e teknikave. Përdorimi i secilës prej teknikave të mësipërme duhet të mos ndikojnë integritetin e sistemit aplikativ dhe të të dhënave të tij në subjektin nën auditim. Teknikat e mbledhjes së të dhënave duhet të bazohen në vlerësime rreziku dhe duhet të kthejnë përfundimet e pritura.

Matricat e sugjeruara të audititmit për fusha të ndryshme të auditimeve të TI-së janë të pasqyruara në Shtojcat II-VIII të këtij Manuali.

përdoruesit. Një specifikim i dobët i kërkesës së përdoruesit mund të çojë në fund të fundit në zhvillimin e një sistemi të mangët. Ky është një pikënisje e mirë për Audituesin e TI-së.

[15] Të dhënat elektronike do të përfshijnë të dhëna të strukturuara ku ato më të zakonshmet janë Sistemet e Menaxhimit të Baza e të Dhënave Relacionale(SMBDR) që janë të aftë të trajtojnë vëllime të mëdha të të dhënave si Oracle, IBM DB2, Microsoft SQL Server, Sybase dhe Teradata.

KAPITULLI 2

Qeverisja e TI

Çfarë është Qeverisja e TI

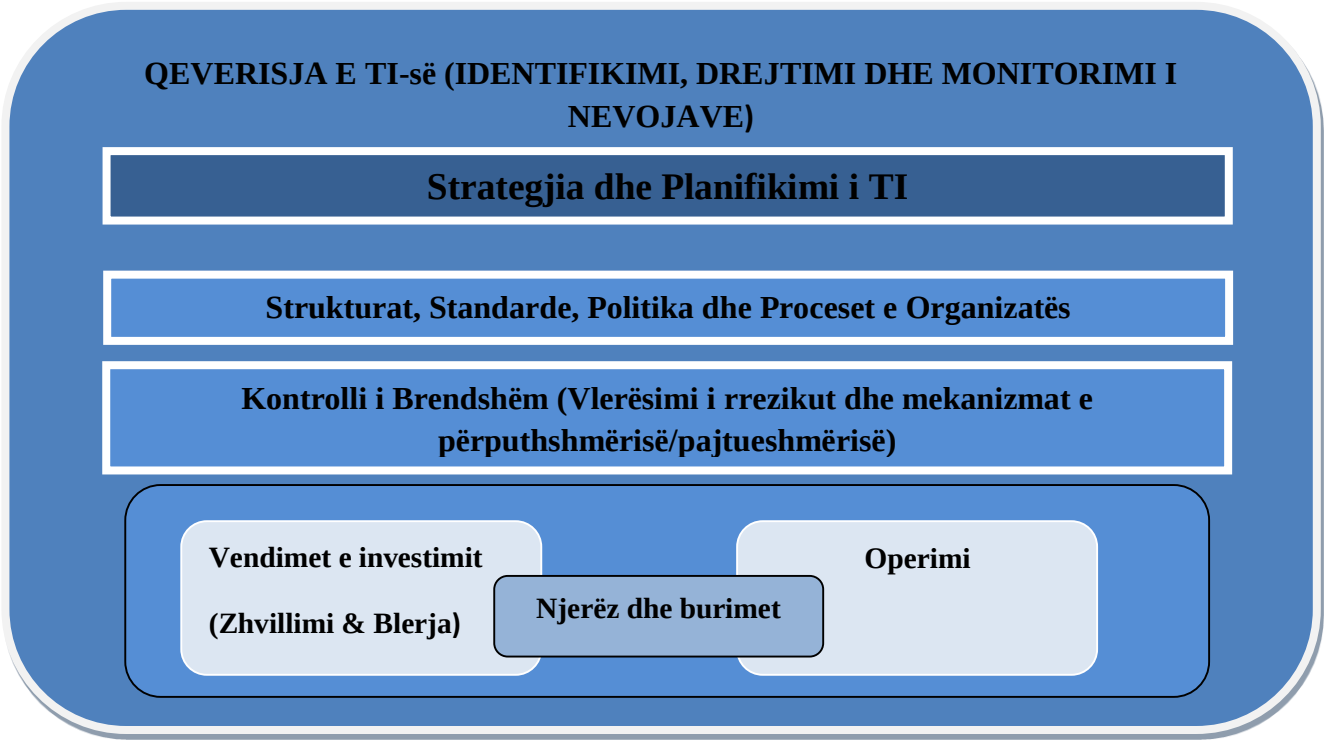
Qeverisja e TI-së mund të përkufizohet si struktura e përgjithshme që udhëheq operacionet e TI-së në një organizatë për të siguruar se përputhen me nevojat e biznesit sot dhe ka plane për nevojat e së ardhmes. Është një pjesë integrale e qeverisjes së organizatës dhe përbëhet nga udhëheqja e organizatës, strukturat dhe proceset institucionale dhe mekanizma të tjerë (raportimi dhe informatat kthyese, zbatimi, burimet etj) që sigurojnë se sistemet e TI-së mbështesin qëllimet dhe strategjinë duke balancuar rreziqet dhe duke menaxhuar në mënyrë efektive burimet.

Qeverisja e TI-së luan një rol kyç në përcaktimin e mjedisit të kontrollit dhe vendos themelet për krijimin e një praktike të mirë në kontrollin e brendshëm si dhe në raportimin në nivelet funksionale për mbikëqyrjen dhe rishikimin menaxherial.

Ka disa lloje standardesh dhe strukturash që përcaktojnë parimet dhe konceptet e Qeverisjes së TI-së dhe sesi një organizatë mund të zgjedhë implementimin e tyre.

Një strukturë e përgjithshme e qeverisjes së TI-së paraqitet në figurën e mëposhtme:

Figura 2.1 Struktura e përgjithshëme e qeverisjes së TI



Identifikimi, Drejtimi dhe Monitorimi i nevojave

Qeverisja e TI-së është një shtesë e qeverisjes së përgjithshme të organizatës. Qeverisja e TI-së duhet të shihet sesi TI-së krijon vlerë që përshtatet me Strategjinë e përgjithshme të Qeverisjes së Korporatës dhe asnjëherë të mos shihet si një disiplinë e veçantë. Duke e trajtuar në këtë mënyrë, të gjithë palët e interesit (stakeholders) duhet të marrin pjesë në procesin e vendimmarrjes. Kjo krijon një pranim të gjerë të përgjegjësisë për sistemet kritike dhe siguron se vendimet mbi TI-në janë marrë dhe drejtuar nga biznesi dhe jo anasjelltas.

Që Qeverisja e TI-së të sigurohet se investimet në TI gjenerojnë vlerë për biznesin dhe se rreziqet e lidhura me TI-në janë të reduktuara, është e rëndësishme që të ekzistojnë struktura organizative me role të mirë-përcaktuara për përgjegjësinë e informacionit, proceseve të biznesit, aplikacioneve dhe infrastrukturës.

Është e rëndësishme që Qeverisja e TI-së të angazhohet në identifikimin e nevojave të reja ose të përditësuara dhe më pas në ofrimin e zgjidhjeve të duhura TI-së për përdoruesit e biznesit. Gjatë zhvillimit ose blerjes së zgjidhjeve të nevojave të biznesit, Qeverisja e TI-së siguron që zgjedhjet e bëra janë të duhurat për biznesin dhe se trajnimi dhe burimet e nevojshme (harduer, vegla, kapaciteti i rrjetit etj) janë të disponueshme për implementimin e zgjidhjeve. Aktivitetet monitoruese mund të zhvillohen nga auditimi i brendshëm ose grupi i sigurimit të cilësisë, i cili do të raportojë periodikisht rezultatet tek menaxhmenti.

Elementet kyçe që përcaktojnë Qeverisjen e TI-së të një organizate përshkruhen më poshtë.

Elementet kyçe të Qeverisjes së TI

a. Strategjia dhe Planifikimi TI

Strategjia e TI-së përfaqëson lidhjen e përbashkët në mes të objektivave të Strategjisë së TI-së dhe atyre të strategjisë së biznesit. Objektivat e strategjisë së TI-së duhet të marrin parasysh nevojat e tashme dhe të ardhshme të biznesit, kapacitetin aktual të TI-së për të ofruar shërbime dhe kërkesat e burimeve[16]. Strategjia duhet të marrë në konsideratë ekzistencën e infrastrukturës dhe arkitekturës së TI-së, investimeve, modelit të ofrimit, burimet duke përfshirë stafin, si dhe paraqitjen e strategjisë që integron këto elemente në një qasje të përbashkët për të mbështetur objektivat e biznesit.

Është e rëndësishme për audituesin e TI-së të rishikojë Strategjinë e TI-së të subjektit për të vlerësuar shtrirjen në të cilën Qeverisja e TI-së ka qënë pjesë e vendimmarrjes së korporatës mbi Strategjinë e TI.

b. Struktura e organizatës, standardet, politikat dhe proceset

Strukturat e organizatës janë një element kyç i qeverisjes së TI-së në artikulimin e roleve të organeve të ndryshme menaxheriale dhe qeverisëse në biznes dhe në vendimmarrje. Ato duhet të caktojnë delegim

[16] ISO 38.500

të qartë për vendimmarrje dhe monitorim të performancës. Strukturat organizative duhet të mbështeten me standardet, politikat dhe procedurat e duhura, të cilat duhet të rrisin kapacitetin e vendimmarrjes.

Strukturat organizative në një subjekt shtetëror janë të influencuara nga **Palët e Interesit** - të gjitha grupet, organizatat, anëtarë të sistemit të cilët ndikojnë ose ndikohen nga veprimet e organizatës-shembuj të të palëve të rëndësishme të interesit përfshijnë Parlamentin dhe/ose njësi qeveritare së bashku me popullin. Strukturat organizative janë të influencuara gjithashtu nga **Përdoruesit** -të jashtëm dhe të brendshëm. Përdoruesit e brendshëm janë ekzekutivët e biznesit, departamentet që zotërojnë proceset e biznesit, si dhe individët brenda kompanisë që bashkëveprojnë me proceset e biznesit. Përdoruesit e jashtëm janë subjektet, individët, publiku që përdor produktet ose shërbimet e ofruara nga një organizatë (për shembull departamentet, qytetarët, etj.). Një tjetër influencë për Strukturat organizative janë **Ofruesit**- një kompani, njësi ose person-si të jashtëm ashtu edhe të brendshëm-që ofrojnë shërbime.

Nevoja për funksionalitetet e TI-së lind nga përdoruesit dhe palët e interesit. Në të gjitha rastet, strukturat, detyrat dhe përgjegjësitë e duhura organizative qeverisëse, kërkohet të mandatohen nga organet qeverisëse, duke ofruar zotërim dhe llogaridhënie të qartë për detyra dhe vendime të rëndësishme. Kjo duhet të përfshijë marrëdhëniet me palët e treta kyçe, si ofruesit e shërbimeve TI.

c. Struktura organizative e TI-së zakonisht përfshin funksionet e mëposhtme:

Komiteti Drejtues TI- kjo është pjesa qendrore e strukturës organizative. Konsiston në anëtarë të menaxhmentit të lartë dhe ka përgjegjësinë e rishikimit, miratimit dhe gjetjes së fondeve për investimet e TI-së. Komiteti Drejtues duhet të ketë rëndësinë e tij në vendimet e biznesit për të cilat teknologjia duhet të ofrohet për të mbështetur investimet e biznesit ashtu si edhe në aprovimin sesi të blihen këto teknologji. Vendimet e investimit që përfshijnë zgjedhjen në mes "ndërto/blej" janë përgjegjësi e Komitetit Drejtues të TI-së, zakonisht pas disa rekomandimeve që vijnë nga grupe ose komitete të tjera.

Së fundmi, Komiteti Drejtues luan një rol kritik në promovimin e blerjeve të nevojshme dhe në ofrimin e mbështetjes menaxheriale për programe që sjellin ndryshime në organizatë.

Në shumë organizata të sektorit publik, funksionet e Komitetit Drejtues të TI-së janë pjesë e funksioneve menaxheriale.

Zyrtar i lartë i informacionit- Chief Information Officer (CIO)-është një autoritet i lartë, përgjegjës për menaxhimin dhe operimin e kapaciteteve të TI-së në organizatë. Në shumë organizata të sektorit publik funksionet e kryera nga CIO mund të ndërmerren nga një grup ose departament i cili ka përgjegjësitë, autoritetin dhe burimet e nevojshme.

d. Standardet, Politikat dhe Proceset

Standartet dhe politikat janë të adoptuara nga organizata dhe të aprovuara nga menaxhmenti i lartë. Politikat vendosin strukturën për operacionet e përditshme në mënyrë që të arrihen qëllimet e vendosura nga organet qeverisëse. Politikat mbështeten nga procedurat dhe proceset, të cilët përcaktojnë sesi do të realizohet dhe kontrollohet puna. Këto qëllime janë vendosur nga menaxhmenti i lartë për përmbushjen e misionit të organizatës dhe në të njëjtën kohë në përputhje me kërkesat ligjore dhe rregullatore.

Politikat dhe procedurat korresponduese duhet të komunikohen në të gjitha nivelet e organizatës në intervale sistematike kohore.

Disa prej politikave kyçe që udhëzojnë Qeverisjen e TI-së përfshijnë:

- **Politikat e Burimeve Njerëzore**

Politikat e Burimeve Njerëzore lidhen me punësimin, trajnimin, ndërprerjen e marrëdhënieve të punës dhe funksione të tjera. Lidhet me detyrat dhe përgjegjësitë e personelit të ndryshëm brenda organizatës ashtu si edhe me aftësitë e nevojshme ose trajnimet që duhet të posedohen për kryerjen e punës. Politikat e Burimeve Njerëzore gjithashtu përcakton rolet, përgjegjësitë si dhe ndarjen e detyrave.

- **Politikat e dokumentimit dhe të ruajtjes së dokumenteve**

Dokumentimi i sistemeve të informacionit, aplikacioneve, detyrat e punës, sistemet e raportimit dhe periodiciteti është një pikë referimi e rëndësishme për lidhjen e operacioneve të TI-së me objektivat e biznesit. Politikat e duhura të ruajtjes së dokumenteve mundësojnë kapjen dhe menaxhimin e ndryshimeve të përsëritura të arkitekturës së informacionit në njësi.

- **Politikat e kontraktimit**

Marrja nga jashtë e teknologjisë së informacionit shpesh ka si qëllim të lejojë menaxhmentin e subjektit të përqendrojnë përpjekjet e tyre në aktivitetet kryesore të biznesit. Nevoja për kontraktimin mundet gjithashtu të lindë nga nevoja për reduktimin e kostove. Një politikë e kontraktimit siguron që propozimet për operacionet e jashtme dhe/ose funksionet, bazën e të dhënave do të zhvillohen dhe zbatohen në një mënyrë të dobishme për organizatën.

- **Politikat e sigurisë së TI**

Këto politika vendosin kërkesat për mbrojtjen e aseteve të informacionit dhe mund TI-së referohen procedurave ose mjeteve të tjera në mënyrën sesi këto do të mbrohen. Politikat duhet të jenë të disponueshme ndaj të gjithë punonjësve përgjegjës për sigurinë e informacionit, përfshirë përdoruesit e sistemeve të biznesit të cilët kanë rol në mbrojtjen e informacionit (personeli regjistrues, të dhënat financiare, etj.).

e. Kontrolli i brendshëm

Kontrolli i brendshëm është procesi i prezantimit dhe zbatimit të një sistemi masash dhe procedurash për të përcaktuar nëse aktivitetet e organizatës janë dhe qëndrojnë në përputhje me planet e aprovuara. Nëse është e nevojshme, masa korrigjuese ndërmerren në mënyrë që objektivat e politikave të realizohen. Kontrolli i brendshëm mban në drejtim sistemin e TI-së. Kontrollet e brendshme përfshijnë menaxhimin e rrezikut, pajtueshmërinë me procedurat dhe instruksionet e brendshme si dhe me legjislacionin dhe rregulloret e jashtme, raportet periodike dhe të qastit të menaxhmentit, kontrollet e progresit dhe të rishikimit të planeve të auditimeve, vlerësimin dhe monitorimin.

Menaxhimi i rrezikut

Menaxhimi i rreziqeve të TI-së duhet të formojë një pjesë integrale të strategjisë dhe politikave të menaxhimit të rrezikut të kompanisë. Menaxhimi i rrezikut përfshin identifikimin e rreziqeve që prekin ekzistencën e aplikacioneve dhe infrastrukturën e TI-së, menaxhimin e vazhdueshëm, përfshirë rishikimin dhe përditësimin vjetor/periodik nga menaxhimi i rreziqeve dhe monitorimin e strategjive reduktuese. Ky seksion trajtohet në kapitullin e Politikave të Sigurisë së TI.

Mekanizmi i pajtueshmërisë

Organizatat duhet të kenë mekanizma pajtueshmërie që sigurojnë se të gjitha politikat dhe procedurat e lidhura me to janë duke u zbatuar. Normalisht, është kultura e organizatës që i bën punonjësit më të ndjeshëm ndaj çështjeve të mos-pajtueshmërisë. Mekanizmat mbështetës të pajtueshmërisë mundet gjithashtu të përfshijnë grupin e sigurimit të cilësisë, stafin e sigurisë, mjetet e automatizuara etj. Një raport i mos-pajtueshmërisë duhet të rishikohet nga menaxhmenti i duhur dhe çështjet e mos-pajtueshmërisë serioze dhe të përsëritura duhet të trajtohen. Menaxhmenti mund të zgjedhë të trajtojë këto çështje me anë të trajnimeve të përsëritura, procedurave të modifikuara, ose edhe procedura ndëshkuese në varësi të natyrës së mospajtueshëmrisë (shkelje e sigurisë, mungesë e trajnimeve të detyrueshme, etj.).

Siguria e pavarur, në formën e auditimeve (ose rishikimeve) të jashtme dhe të brendshme, mund të ofrojë reagime në kohë mbi pajtueshmërinë e TI-së me politikat, standardet, procedurat dhe objektivat e përgjithshme të organizatës. Këto auditime duhet të kryhen në mënyrë të paanshme dhe objektive, në mënyrë që menaxherët janë pajisur me një vlerësim të drejtë të projektit të TI-së që po auditohet.

Vendimet e investimit (Zhvillimi dhe Blerja e zgjidhjeve)

Qeverisja e TI-së duhet tu ofroj përdoruesve të biznesit zgjidhje ndaj kërkesave të tyre të reja ose të modifikuara. Këto mund të arrihen nga Departamenti i TI-së ose duke zhvilluar (ndërtuar) programe ose sisteme të reja ose duke i blerë ato nga tregtarë me kosto efektive. Në mënyrë që të arrihet kjo gjë efektivisht, praktikat më të mira zakonisht kërkojnë një trajtim të disiplinuar ku kërkesat identifikohen, analizohen, prioritizohen dhe aprovohen, si dhe zhvillohet një analizë kosto/përfitim në mes të zgjidhjeve të përzgjedhura për tu selektuar zgjidhja më optimale (për shembull, në të cilën ekuilibrohet kosto me rrezik).

Operacionet e TI

Operacionet e TI-së zakonishtjanë infrastruktura e përditshme e TI-së që ekzekuton dhe mbështet nevojat e biznesit. Operacionet e TI-së të menaxhuara në mënyrën e duhur bëjnë të mundur identifikimin e pengesave dhe planifikojnë ndryshimet në kapacitet (harduer shtesë, ose burime rrjeti), matë performancën për t'u siguruar se përputhet me nevojat e pronarëve të biznesit, si dhe ofron tavolinë ndihmëse (help desk) dhe mbështetje të menaxhimit të incidenteve ndaj përdoruesve të burimeve të TI.

f. Njerëz dhe burime

Rekomandohet që menaxhmenti të sigurohet nëpërmjet vlerësimeve të herë pas hershme se burime të mjaftueshme janë të shpërndara në TI për arritjen e nevojave të organizatës, sipas prioriteteve të aprovuara dhe kufizimeve të buxhetit. Për më tepër, aspekti njerëzor duhet të respektohet nga politikat, praktikat dhe vendimet e TI-së, të cilat duhet të konsiderojnë nevojat aktuale dhe të ardhshme të pjesëmarrësve në proces. Menaxhmenti qeverisës duhet të vlerësojë vazhdimisht nëse burimet përdoren ose jo dhe prioritizohen sipas kërkesave të objektivave të biznesit.

Rreziqet e subjektit nën auditim

Audituesit duhet të kuptojnë dhe vlerësojnë elementet e ndryshme të strukturës së Qeverisjes së TI-së për të përcaktuar nëse vendimet, drejtimet, burimet, menaxhimi dhe monitorimi i TI-së mbështesin strategjitë dhe objektivat e organizatës. Për kryerjen e vlerësimit, audituesi duhet të njohë elementet kyçe të Qeverisjes dhe Menaxhimit të TI-së. Audituesi duhet të jetë i ndërgjegjshëm mbi rreziqet e lidhura me pamjaftueshmërinë e çdo elementi në subjekt.

Secila organizatë ndeshet me sfida të veçanta, për shkak të mjedisit, politikës, çështjeve gjeografike, ekonomike dhe sociale të ndryshme. Edhe pse kjo është një listë jo e plotë, pasojat e pasqyruara më poshtë përfaqësojnë rreziqet e përbashkëta të cilat mund të vijnë nga mungesa e qeverisjes së saktë të TI-së.

Sistemet e TI-së jo efektive, jo efikase ose të papërshtatshme për përdoruesin. Sistemet e administratës publike të cilët kanë si qëllim t'i shërbejnë shoqërisë, biznesit ose të rrisin funksionalitetin e subjekteve qeveritare, janë shpesh jashtëzakonisht të gjëra dhe me zgjidhje komplekse. Ato duhet të dizejnohen në mënyrën e duhur, të ndërtohen në përputhje me nevojat reale, të koordinuara më së miri dhe të ekzekutohen efektivisht. Qeverisja e dobët e TI-së në nivel shtetëror dhe në nivelin e organizatave individuale, mund të jetë një pengesë në marrjen e sistemeve cilësore të TI-së.

Funksionet e TI-së që nuk u shërbejnë nevojave të biznesit: Vlera e ulët e biznesit mund të derivojë nga investimet e mëdha në TI që nuk janë të koordinuara në mënyrë strategjike me burimet dhe objektivat e biznesit. Ky koordinim i dobët strategjik do të thotë që edhe cilësia e ulët e TI-së nuk do të kontribuojë efektivisht dhe në mënyrë efikase për arritjen e objektivave të organizatës. Një mënyrë për koordinim, është angazhimi i përdoruesve dhe palët e interesit të cilët njohin vendimmarrjen e TI-së në biznes.

Kufizimet e rritjes së biznesit: Planifikimi i dobët ose mungesa planifikimit mund të sjellë që rritja e biznesit të kufizohet nga një mungesë e burimeve të TI-së ose përdorim jo efikas i burimeve ekzistuese. Një mënyrë për reduktimin e këtij rreziku, është përditësimi periodik i Strategjisë së TI-së, gjë e cila do të identifikojë burimet dhe planet për arritjen e nevojave të ardhshme të biznesit.

Menaxhim jo efektiv i burimeve: Për arritjen e rezultateve optimale me kosto minimale, një organizatë duhet të menaxhojë burimet e saj të TI-së në mënyrë efektive dhe efikase. Të siguruarit se ekzistojnë burimet e mjaftueshme teknike, harduer, softuer dhe njerëzore të disponueshme për të ofruar shërbime të TI-së, është faktori kryesor në arritjen e vlerës nga investimi në TI. Përcaktimi dhe monitorimi i

përdorimit të burimeve të TI-së, për shembull në një SLA[17], lejon organizatën të njohë objektivisht nëse burimet janë të mjaftueshme për plotësimin e këtyre nevojave.

Vendimmarrje jo e saktë: Strukturat e dobëta të raportimit mund të sjellin vendimmarrje jo të saktë. Kjo prek mundësinë e ofrimit të shërbimit ndaj klientëve. Komitetet Drejtuese dhe grupe të tjerë te organizatës, me anë të përfaqësimit të duhur, ndihmojnë në vendimmarrje që ndikojnë në organizatë.

Dështim i projekteve: Shumë organizata nuk marrin në konsideratë rëndësinë e qeverisjes së TI-së. Ato angazhohen në projektet e TI-së pa një njohje të plotë të kërkesave të organizatës mbi këto projekte dhe sesi këto projekte lidhen me objektivat e biznesit. Kjo gjë haset edhe në blerjen dhe/ose implementimin e aplikacioneve që nuk plotësojnë standardet minimale të sigurisë dhe arkitekturës. Këto projekte mund të bëjnë shpenzime shtesë për të mirëmbajtur dhe administruar sistemet dhe aplikacionet jo standarde. Një SDLC (*system development and life cycle*) i përcaktuar dhe përdorimi i tij në zhvillimin dhe/ose blerje, është një mënyrë për të reduktuar rrezikun e dështimit të projektit.

Varësi ndaj palëve të treta (tregtarëve): Për shkak të mungesës së proceseve që rregullojnë procedurat e blerjes dhe kontraktimit, organizata mund të përballet me një situatë ku varet tërësisht nga një shitës ose kontraktor. Fillimisht, ky është një mjedis me rrezik të lartë sepse nëse shitësi del nga tregu, ose dështon në ofrimin e shërbimeve të kontraktuara, organizata do të jetë në pozicion të vështirë. Ka gjithashtu çështje të tjera, për shembull konfliktet mbi pronën intelektuale, sistemet, bazat e të dhënave. Organizatat që blejnë ose kontraktojnë rregullisht zgjidhje nga tregtarët, do të duhet të kenë politika kontraktimi ose blerjeje, që përcaktojnë çfarë duhet të blihet ose jo.

Mungesë transparence dhe llogaridhënieje: Llogaridhënia dhe transparenca janë dy elementë të rëndësishëm të qeverisjes së mirë. Transparenca është një forcë që, kur aplikohet në mënyrën e duhur, ndihmon në luftën kundër korrupsionit, përmirëson qeverisjen dhe promovon llogaridhënien[18]. Kështu, në mungesë të strukturave, strategjive, procedurave, kontrolleve monitoruese të mjaftueshme organizative, institucioni mund të dështojë të jetë transparentë dhe llogaridhënës.

Mospajtueshmëri me deklarimet ligjore dhe rregullatore Palët e interesit kërkojnë siguri se kompanitë janë në përputhje me ligjet dhe rregullat dhe konform praktikave të mira qeverisëse në mjedisin operues. Përveç kësaj, për shkak të mundësimit nga ana e TI-së të mungesës së lidhjeve në mes të proceseve të biznesit në mes kompanive, ekziston gjithashtu një nevojë në rritje për sigurimin që kontratat të përfshijnë kërkesa të rëndësishme në lidhje me TI-në në fusha si privatësia, konfidencialiteti, pronësia intelektuale dhe siguria (Struktura COBIT)[19]. Politikat e ndryshme që një organizatë ka, si për shembull Siguria e TI-së, Kontraktimi, Burimet Njerëzore etj. duhet të përfshijnë struktura ligjore dhe rregullatore.

Ekspozim i rreziqeve të sigurisë së informacionit: Shumë rreziqe të sigurisë së informacionit mund të lindin nga mungesa e strukturave, proceseve dhe politikave të duhura, si: keqpërdorim i aseteve, zbulim i paautorizuar i informacionit, qasje e paautorizuar, shkatërrim dhe mosgatishmëri e informacionit,

[17] Service level agreement-marrëveshja e nivelit të sherbimit

[18] ISSAI 20, Concepts of accountability and transparency, f.4

[19] Kornizë-dokument i përditësuar kohë-pas kohe. Versioni i fundit është COBIT 2019

keqpërdorim i informacionit, mospajtueshmëri me të dhënat ligjore dhe rregullatore, dështim nga rimëkëmbja prej fatkeqësive. Politikat e sigurisë së TI-së duhet të përcaktojnë asetet e organizatës (të dhënat, pajisjet, proceset e biznesit) që kanë nevojë për mbrojtje dhe të krijojnë lidhje me procedurat, mjetet dhe kontrollin fizik të qasjes që mbrojnë këto asete.

Qeverisja e TI-së vazhdon të jetë një fushë shqetësimi për shumë organizata të sektorit publik. Në të njëjtën kohë, shumë ISA janë gjithnjë e më shumë duke u fokusuar në Qeverisjen e TI-së si pjesë e auditimit të TI-së. Audituesit e TI-së mund të ndihmojnë në Qeverisjen e TI-së duke:

- siguruar që Qeverisja e TI-së është në programin e qeverisjes së përgjithshme të korporatës; dhe
- promovuar strategjitë e Qeverisjes së TI-së.

Matrica e auditimit

Matrica e auditimit në Shtojcën II është një pikë fillimi për audituesit në vlerësimin e kontrolleve reduktuese, të cilat janë vendosur nga organizata, si dhe në menaxhimin e rreziqeve me të cilat ato përballen në qeverisjen e TI-së. Përmblidhen fushat e trajtuara më lart.

Është e rëndësishme të kujtojmë që çështjet e Qeverisjes së TI-së do të jenë pjesë e vlerësimit të përgjithshëm të audituesve në një mjedis të përgjithshëm të organizatës.

Referencat/ lexim të mëtejshëm:

1. Çfarë është Qeverisja e TI-së dhe pse është e rëndësishme për audituesin e SI, WGITA, IntoIT. http://www.intosaiitaudit.org/intoit_articles/25_p30top35.
2. Struktura COBIT, Institucioni i Qeverisjes së TI.
3. Struktura COBIT 5, 2012, Isaca
4. ISO/IEC 38500, Qeverisja e Korporatës mbi Teknologjinë e Informacionit
5. OECD Parimet e Qeverisjes së Korporatës, OECD 1999 dhe 2004
6. Michaels Paul; Anand, Navin; Iyer; Sudha; Çfarë është Qeverisja e TI-së. Bota Kompjuterike, UK, Prill 2012. http://blogs.computerworlduk.
7. http:// www.gao.gov/new.items/d04394g.pdf.

KAPITULLI 3

Zhvillimi dhe blerja

Çfarë është zhvillimi dhe blerja

Me qëllim që të mbështetet strategjia e biznesit, sektoret e TI-së ofrojnë zgjidhje ndaj biznesit dhe përdoruesve të tij. Procesi i zhvillimit, blerjes, ose kontraktimit për një zgjidhje duhet të planifikohet në mënyrë që rreziqet të menaxhohen dhe të maksimizohen mundësitë për sukses. Përveç kësaj, kërkesat për këto zgjidhje duhet të identifikohen, analizohen, dokumentohen dhe prioritizohen. Organizatat mund të kontraktojnë gjithashtu siguri të cilësisë dhe funksione testimi, për të garantuar cilësi të këtyre zgjidhjeve.

Përgjithësisht, zgjidhjet do të ndërtohen ose blihen nga një strukturë ose ekip të projektit. Edhe pse shpesh organizatat mund të mos zyrtarizojnë një projekt, aktivitetet e zakonshme gjithsesi duhet të realizohen.

Zgjidhjet mund të ofrohen ose nëpërmjet zhvillimit të brendshëm ose duke i blerë nga jashtë nëpërmjet blerjes ose kontraktimit. Zakonisht, shfrytëzohet një trajtim i kombinuar i këtyre të fundit.

Sipas Universitetit Carnegie Mellon CMMI® mbi Blerjen, Versioni 1.3, organizatat janë gjithnjë e më shumë duke u shndërruar në blerës të kapaciteteve të nevojshme, meqë produktet dhe shërbimet janë të gatshme dhe më të lira në çmim sesa ato të vetë-ndërtuara. Sidoqoftë, rreziku i blerjes së produkteve që nuk përputhen me objektivat e biznesi, është real. Këto rreziqe duhet të menaxhohen në mënyrë që blerja të plotësojë me sukses objektivat e biznesit. Nëse kryhet në mënyrë të disiplinuar, blerja mund të përmirësojë efikasistetin e operacioneve të organizatës duke forcuar kapacitetet e furnizuesve për të ofruar shpejt dhe me cilësi zgjidhje, në kosto minimale dhe me teknologjinë e duhur.

Blerja e një produkti ose zgjidhjeje, kërkon që organizata të njohë nevojat dhe kërkesat e saj. Procesi i identifikimit të kërkesave duhet të përfshijë të gjithë palët e lidhura, të cilët preken nga proceset e biznesit, përfshirë këtu përdoruesit final dhe stafin teknik, të cilët mund të nevojitet të mirëmbajnë dhe mbështesin sistemin. Në blerjen e shërbimeve (tavolina ndihmëse, automatizim desktopi, etj.) identifikimi i kërkesave duhet të përfshijë departamentin e TI-së, i cili do të bashkëveprojë me ofruesin e shërbimit. Kërkesat duhet të prioritizohen, në mënyrë që nëse ka shkurtime buxheti ose kufizime të kostos, disa të mund të zhvendosen në ndërtime ose blerje të reja të mëvonshme.

Përcaktimet e kërkesave janë vetëm hapi i parë i procesit të blerjes. Blerja ka nevojë për shumë fusha shtesë për tu menaxhuar, për shembull, rreziku, menaxhimi i programeve, testimi, mbikëqyrja e tregtarit si gjatë blerjes ashtu edhe më vonë, nëse ata veprojnë ose mbështesin sistemin, si dhe integrimi i trajnimeve të brendshme së bashku me çështjet e implementimit. Ka praktika të mirë-përcaktuara, që kur adoptohen, rrisin gjasat për sukses në blerjen e produkteve ose shërbimeve.

Elementët kyçe të zhvillimit dhe blerjes

a. Zhvillimi dhe Menaxhimi i Kërkesave

Për çdo projekt të zhvilluar ose të blerë, organizata ka nevojë të dokumentojë kërkesat se çfarë dëshiron dhe të menaxhojë këto kërkesa. Menaxhimi i kërkesave përfshin prioritizimin duke përdorur kritere (për shembull statusi kritik, kosto, kompleksiteti) dhe segmentimin e tyre në faza nëse ato nuk mund të implementohen në sistemin fillestar. Përveç pronarëve të biznesit, procesi i identifikimit të kërkesave duhet të përfshijë përdoruesit, stafin mbështetës, ekspertë të fushës dhe palët tjera të interesit. Kërkesat formojnë bazën e paketës së zgjedhjeve më të mira (kërkesës për propozim) dhe duhet të jenë të qarta dhe koncize. Duke analizuar dhe prioritizuar kërkesat, organizata është në gjendje të marrë vendime mbi koston, në mënyrë që të përcaktojë zgjedhjen më optimale.

b. Menaxhimi dhe Kontrolli i projektit

Menaxhimi i projektit përfshin përcaktimin e planit të projektit dhe aktivitetet e kontrollit. Menaxhimi i projektit përfshin përcaktimin e kostos dhe programin bazë, përcaktimin e programit të projektit, si dhe angazhimin e palëve të interesuara për aktivitetet kryesore. Kontrolli i projektit përfshin mbikëqyrjen dhe raportimin periodik për të ndërmarrë veprime korrigjuese kur performanca e projektit nuk është në përputhje me planin. Për shembull, nëse kostoja e projektit rritet ndjeshëm, organizata mund të vendosë të shkurtojë funksione të caktuara pas konsultimit me palët e interesit. Struktura e menaxhimit të projektit duhet të përshkruhet në Ciklin e Jetës së Zhvillimit të Sistemit të organizatës (SDLC) ose në strategjinë e blerjes. Përgjithësisht përbëhet nga një menaxher projekti, zyrtar rreziku, stafi i sigurimit të cilësisë, stafi i menaxhimit të konfigurimit, personel i grupit të testimit, etj. Plani i projektit shërben si baza udhëzuese për të gjithë aktivitetet. Udhëzimet periodike nga menaxhmenti i lartë, i mbajnë ata të ndërgjegjshëm mbi gjendjen e projektit dhe sesa po menaxhohet rreziku. Përveç kësaj, i lejon ata të masin elemente të tillë si kostoja, programi dhe performanca, pasi është e rrallë që një projekt do të plotësojë të gjithë objektivat në këto fusha.

c. Sigurimi i cilësisë dhe Testimi

Sigurimi i cilësisë ofron ndaj stafit të projektit dhe menaxhmentit depërtim në cilësinë dhe funksionalitetin e produkteve të punës të ndërmjetme/përkohshme dhe përfundimtare. Për të bërë këtë, personeli i angazhuar në sigurimin e cilësisë, sistematikisht vlerëson produktet e punës, për të parë që ato plotësojnë standardet e cilësisë të dokumentuara të organizatës dhe nëse stafi ka ndjekur proceset e nevojshme për zhvillimin e produkteve. Subjektet duhet të sigurohen se produktet e zhvilluara ose të blera përmbushin kërkesat, kriteret e aprovuara (për shembull më pak se një numër i caktuar gabimesh) dhe kanë kaluar në testime me përdoruesit dhe palët e interesuara. Stafi i sigurimit të cilësisë duhet gjithashtu të siguroj se metodologjia e adoptuar dhe e aprovuar është ndjekur. Për shembull, ata duhet të sigurohen se rishikimet (zyrtare dhe jozyrtare) kryhen dhe raportet e nevojshme të gjendjes dërgohen tek menaxhmenti dhe palët e interesuara. Për më tepër, stafi i sigurimit të cilësisë mund të jetë mënyra që menaxhmenti zbaton ose mbledh informacion mbi çështjen nëse ekipi i projektit ka ndjekur paketën e politikave dhe procedurave të brendshme për zbatimin e zhvillimit ose blerjes.

d. Përzgjedhja e kërkesave

Përzgjedhja e kërkesave është procesi i dokumentimit të kërkesave të biznesit dhe mbledhja e materialeve të tjera referuese që do të ndihmojnë shitësin në ofrimin e zgjidhjes së TI-së. Përfshin gjenerimin e paketës e kërkesave dhe vendosjen e tyre për ofertë, marrjen e propozimeve dhe përzgjedhjen në mes të tregtarëve të ndryshëm. Procesi i përzgjedhjes duhet të jetë transparent, objektiv dhe i bazuar në kritere që janë të duhurat për sistemin ose për shërbimet që do blihen. Është e rëndësishme që ekipi i projektit të përfshijë departamentin juridik në këtë proces. Ky departament është i përditësuar me ligjet dhe rregullat dhe mund të ndihmojë në përcaktimin e drejtë të tregtarit dhe do të mund të shkojnë në gjykatë nëse tregtarët e tjerë kontestojnë përzgjedhjen.

e. Menaxhimi i konfigurimit

Menaxhimi i konfigurimit përdoret për të siguruar se mirëmbahet integriteti i dokumenteve, programeve dhe materialeve të tjera përshkruese ose mbështetëse që janë pjesë e sistemit. Ndryshime mbi këto materiale (të quajtura gjithashtu produkte pune) menaxhohen dhe vendosen baza (ose versione) të tilla që organizata është e gatshme të kthehet pas në versione të njohura dhe të testuara. Personeli i menaxhimit të ndryshimit janë gjithashtu të përfshirë në aprovimin ose autorizimin e programeve për tu instaluar në mjedisin produktiv. Zakonisht kjo gjë bëhet pas testimit nga përdoruesi dhe çdo testimi tjetër shtesë, që konfirmon se sistemet e tjerë vazhdojnë të operojnë si më parë në momentin që një sistem i ri ose program është instaluar (testimi i regresit ose testimi i integritetit).

Rreziqet për subjektin nën auditim

Kur një subjekt është duke zhvilluar një program ka një numër të madh rreziqesh dhe sfidash që ato hasin në sigurimin e suksesit të projektit. Disa prej tyre përfshijnë rreziqet e lidhura me aftësitë në fushën e programeve, eksperiencë në testim dhe menaxhim projekti, vlerësime të arsyeshme të kostos dhe përfitimeve dhe të qenurit i gatshëm të monitorojë statusin e projektit.

Përveç kësaj, grumbullimi dhe aprovimi i kërkesave të programit aplikativ ose sistemit duhet të përfshijë përdoruesit dhe audituesit duhet të shohin nëse përdoruesit janë këshilluar në përcaktimin e kërkesave dhe nëse përdoruesit e përfshirë në sigurimin e cilësisë kanë vlerësuar objektivisht cilësinë e sistemit në momentin që po zhvillohet. Ashtu si edhe në blerje, menaxhmenti ka nevojë të informohet periodikisht mbi statusin e projektit dhe duhet të ndërmarrë masa korrigjuese sipas rastit.

Fokusi primar për audituesit në momentin e përballjes me një subjekt që ka ndërmarrë procesin e blerjes së një sistemi, është të përcaktojë nëse ata po menaxhojnë shitësin, nëse marrin raporte periodike mbi statusin dhe nëse kryejnë veprime korrigjuese. Për tu bërë kjo, kontrata duhet të specifikojë ndodhitë kryesore përgjatë zhvillimit ku ekzistojnë rishikime zyrtare dhe raporte të statusit që i ofrojnë subjektit informacion mbi koston, programin dhe performancën. Audituesi duhet të sigurohet se menaxhmenti i subjektit ose personeli i përcaktuar janë duke marrë, rishikuar dhe korrigjuar dhe duke ndërmarrë veprime mbi raportet e statusit dhe aktivitetet e kontratës.

Matrica e auditimit

Çështjet e audituеshme për vlerësimin e strategjive të zhvillimit dhe blerjes të një organizate, janë të pasqyruara në matricën e auditimit në Shtojcën III.

Referencat/ lexim të mëtejshëm

1. http://www.dodig.mil/Audit/pmeguide.html.
2. DCAA Contract Audit Manual, SHBA, 2013 http://www.dcaa.mil/cam.htm.
3. CMMI për Blerjen, Versioni 1.3 http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm.
4. CMMI për Zhvillimin, Versioni 1.3 http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm.
5. ISACA-Zhvillimi i Sistemit & Auditimi i Menaxhimit të Projektit/ Struktura e Sigurimit
6. Struktura Cobit 4.1, 2007[20], Instituti i Qeverisjes TI-së. Blerja dhe Implementimi
7. Cobit 5 Familja e Produktit http://www.isaca.org/COBIT/Pages/Product-Family.aspx.
8. ISO/IEC 12207 Inxhinieria e Sistemeve dhe programeve-Proceset e ciklit të jetës së programeve

[20] COBIT – i përdorur në këtë dokument, referimi i mëtejm në versionin e fundit të COBIT

KAPITULLI 4

Operacionet e TI-së

Çfarë janë operacionet e TI-së

Ndërkohë që ka disa lloje të ndryshme interpretimesh ose përcaktimesh të operacioneve të IT, përgjithësisht përshkruhen si detyrat e përditshme që angazhohen në ekzekutimin dhe mbështetjen e sistemeve të informacionit të një biznesi (puna e serverave, mirëmbajtja, ofrimi i memories së duhur, puna e help desk-tavolinës ndihmëse, etj). Operacionet maten dhe menaxhohen duke përdorur treguesit kryesorë të performancës (Key Performance Inidcator - KPI) të cilët vendosin parametra përkundrejt të cilëve matet efektiviteti i operacioneve. Këto matje, ose ekuivalentë të tyre, dokumentohen dhe rishikohen sistematikisht. Pjesa më e madhe e organizatave i dokumentojnë në formë marrëveshjesh në mes të përdoruesve të biznesit dhe organizimit të TI-së. SLA e brendshme është një formë e kësaj marrëveshjeje, në të cilën këto parametra janë të dokumentuara.

Elementët kyçe të operacioneve të TI-së

Disa nga fushat ose elementët e Operacioneve të TI-së që audituesi duhet të shohë për të përcaktuar nëse subjekti është duke menaxhuar efektivisht operacionet e TI-së, përfshijnë dizajnimin dhe ofrimin e shërbimit, menaxhimin e kapacitetit dhe të shërbimit, procedura të trajtimit të incidenteve për të siguruar vazhdimësinë e operacioneve, si dhe praktika të përfshira në menaxhimin e ndryshimit. Këto dhe fusha të tjera janë të përcaktuara në ITIL[21], një nga strukturat më të mirëpritura për identifikimin, planifikimin, ofrimin dhe mbështetjen e shërbimeve TI-së të biznesit.

Për të përcaktuar nëse subjekti nën auditim është duke gjeneruar efektivisht shërbimet e dokumentuara, audituesi duhet të përdorë SLA-t, të cilat kanë parametra të ndryshëm për shërbime të ndryshme. Mund të ketë raste në organizata të vogla ku në vend të SLA mund të kemi grafikë të dokumentuar, ose ndonjë shkresë tjetër. Pavarësisht se çfarë emërtimi ka, parametrat duhet të jenë të dokumentuara dhe të aprovuara nga biznesi ose grupet e përdoruesve dhe sektori i TI-së.

[21] ITIL, http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

a. Menaxhimi i Vazhdimësisë së Shërbimit të TI-së

Qëllimi i menaxhimit të vazhdimësisë, është të mirëmbahen kërkesat e vazhdimësisë së biznesit. Organizimi i TI-së e përmbush këtë gjë, duke vendosur afate kohore të rimëkëmbjes për elementë të ndryshëm të TI-së që mbështesin proceset e biznesit, bazuar në kërkesat e nevojshme dhe të miratuara. Përveç kësaj, menaxhimi i vazhdimësisë përfshin rishikimin periodik dhe përditësimin e afatit të rimëkëmbjes për të siguruar që ato janë në përputhje me Planet e Vazhdimësisë së Biznesit dhe prioritetet e tij. Kjo fushë është e sqaruar në Kapitullin mbi PVB/PRF.

b. Menaxhimi i Sigurisë së Informacionit

Menaxhimi i sigurisë së informacionit lidhet me menaxhimin e rreziqeve të lidhura me sigurinë, marrjen e masave të duhura dhe sigurinë se informacioni është i disponueshëm, i përdorshëm, i plotë dhe i pa kompromentueshëm. Lidhet gjithashtu me sigurimin se vetëm përdoruesit e autorizuar kanë qasje në informacion dhe se ky i fundit është i mbrojtur në momentet e transferimit midis destinacioneve dhe i besueshëm kur arrin. Kjo fushë është e trajtuar në kapitullin mbi sigurinë e informacionit.

c. Menaxhimi i kapacitetit

Menaxhimi i kapacitetit përfshin menaxhimin e shërbimeve të ndryshme që mbështesin biznesin në atë mënyrë që të përputhen me kërkesat e biznesit ose të përdoruesve. Optimizimi i kapacitetit, disponueshmëria e burimeve, optimizmi i hapësirës ruajtëse dhe shtimi i saj, janë pjesë e menaxhimit të kapacitetit. Për tu menaxhuar kapaciteti, organizimi në TI duhet të masë kushtet aktuale dhe duhet të ndërmarrë masa që lehtësojnë ofrimin e kapacitetit shtesë ndaj përdoruesve, për shembull duke blerë fuqi shtesë procesuese kur kryqëzohen parametra të ndryshëm (për shembull kur shfrytëzimi i kompjuterit është në 75% ose më shumë, për 60% të ditës së punës). Përveç kësaj, për një organizim të TI-së që ofron shërbime ndaj biznesit, menaxhimi i kapacitetit do të jetë efektiv kur punësohet staf i kualifikuar/trajnuar, kur angazhohen burime të mjaftueshme dhe mjetet e duhura për të mundësuar monitorimin e rrjetit dhe funksionet e tavolinës ndihmëse.

d. Menaxhimi i Incidenteve dhe Problemeve

Menaxhimi i incidenteve janë sistemet dhe praktikat e përdorura për të përcaktuar nëse incidentet ose gabimet janë regjistruar, analizuar dhe zgjidhur brenda një afati. Menaxhimi i problemeve ka si qëllim të zgjidhë çështjet nëpërmjet investigimit dhe me analiza të thella, të incidenteve të mëdha ose të përsëritura, për të gjetur shkakun e ndodhjes. Pasi problemi është identifikuar dhe është kryer analiza e gjetjes së shkakut, shndërrohet në gabim të njohur ose jo efikasitet dhe më tej do të zhvillohet një zgjidhje për të trajtuar atë dhe për të parandaluar ndodhjen e incidenteve të ngjashme në të ardhmen. Duhet të vendoset një mekanizëm për zbulimin dhe dokumentimin e kushteve që mund të çojnë në identifikimin e një incidenti. Seksioni i operacioneve të TI-së duhet të ketë procedura të dokumentuara për zbulimin dhe regjistrimin e kushteve të parregullta. Një gjurmë manuale, e kompjuterizuar për softuer të dedikuara të TI-së mund të përdoret për të regjistruar këto kushte. Shembuj të incidenteve mund të përfshijnë si qasjen e paautorizuar të përdoruesve ashtu edhe ndërhyrje (siguri), dështime të rrjetit (operacionale),

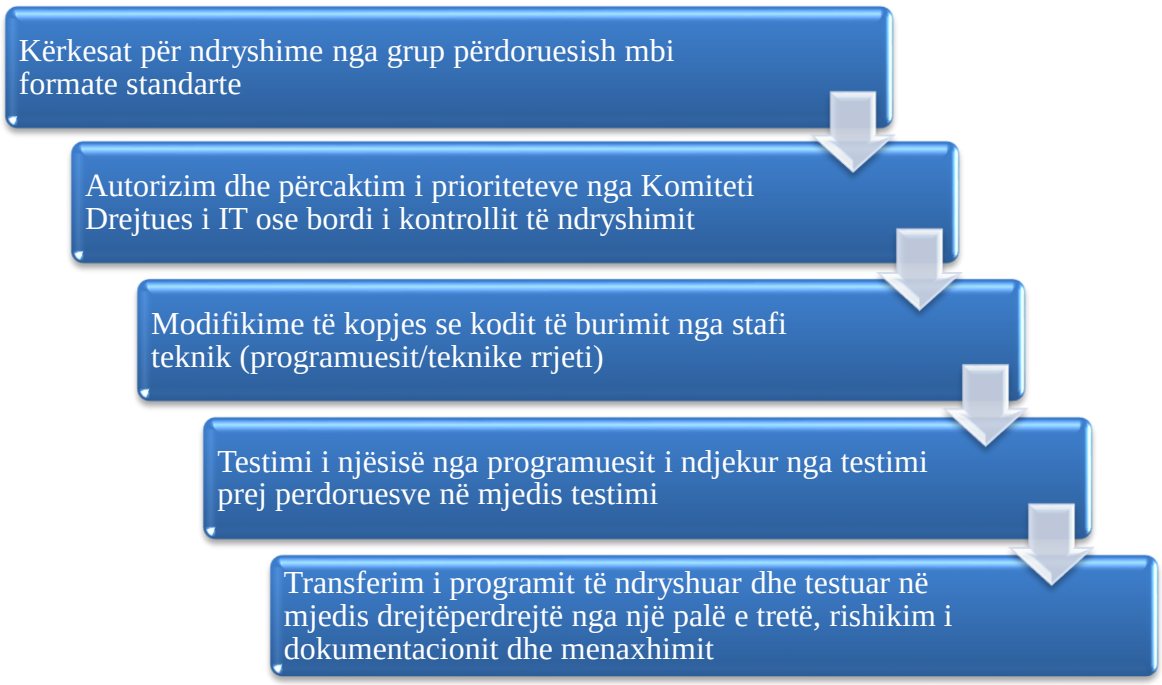
funksionalitet i ulët i programeve (ofrimi i shërbimeve) ose mungesë e aftësive të përdoruesve të fundit (trajnim).

e. Menaxhimi i ndryshimit

Në sektorët/organizatat e TI-së, procesi i menaxhimit të ndryshimit zakonisht përdoret për të menaxhuar dhe kontrolluar ndryshimet në asete, siç janë programi kompjuterik, hardueri dhe dokumentacioni përkatës. Kontrollet e ndryshimit nevojiten për të siguruar se të gjithë konfigurimet e ndryshimeve të sistemeve janë të autorizuara, testuara, dokumentuara dhe kontrolluara në mënyrë që sistemet të vazhdojnë të mbështesin operacionet e biznesit në mënyrën e planifikuar dhe që të ketë gjurmë/regjistrim adekuat të ndryshimeve.

Një ndryshim i paaprovuar ose aksidental mund të ketë rreziqe të ndryshme dhe pasoja financiare për organizatën. Organizatat ndjekin një procedurë të përcaktuar të menaxhimit të ndryshimit, e cila kërkon aprovim nga një bord përpara implementimit në mjedisin operacional. Procesi i menaxhimit të ndryshimit duhet të sigurojë që ndryshimet janë regjistruar, vlerësuar, autorizuar, prioritizuar, planifikuar, testuar, implementuar, dokumentuar dhe rishikuar në pajtim me procedurat e dokumentuara dhe të aprovuara të menaxhimit të ndryshimit.

Ndryshimet mund të nisin për shembull nga ndryshimi i mjedisit të biznesit, ndryshime të modelit të biznesit, nevoja ndërmjet operacioneve ose nga rezultati i analizës së incidenteve/problemeve. Procedurat e kontrollit të ndryshimit duhet të përfshijnë procedura për menaxhimin e autorizimit; testim të plotë dhe autorizim nga menaxhimi i operacioneve përpara përdorimit në mjedis pune, rishikimi i menaxhimit të efekteve të çdo ndryshimi, mirëmbajtje e regjistrimeve të përshtatshme; përgatitja e planeve alternative (në rast se diçka nuk shkon mirë); dhe vendosja e procedurave për kryerjen e ndryshimeve emergjente.



Kostoja e ndryshimit, ndikimi mbi sistemet e TI-së dhe objektivave të biznesit, efekti i mosimplementimit dhe kërkesat e ardhshme të burimeve, janë përcaktime të rëndësishme gjatë autorizimit dhe prioritizimit të ndryshimit.

Ndryshimet emergjente nuk mund të presin të kalojnë përgjatë procedurave të kontrollit të ndryshimit dhe duhet të implementohen me minimumin e vonesave. Koha është e reduktuar për kryerjen dhe testimin e ndryshimit. Kjo krijon rrezik më të lartë të gabimeve të programimit.

Atje ku ekzistojnë procedurat e ndryshimeve emergjente, audituesi duhet të kontrollojë që ato janë të arsyeshme dhe përfshijnë disa forma kontrolli. Këto do të përfshijnë Aprovimin e ndryshimeve emergjente nga anëtar i personelit me autoritetin e duhur, aprovim retrospektiv nga bordi i ndryshimit/pronari i sistemit, testim retrospektiv dhe përditësim i dokumenteve.

f. Marrëveshja e Nivelit të Shërbimit (SLA)

SLA dokumenton parametrat e ndryshëm që sektori i TI-së përdor për të ofruar shërbime ndaj biznesit. Parametrat në SLA përgjithësisht janë të aprovuar nga pronarët e biznesit dhe sektori i TI-së. Audituesi do të përdorë këto parametra për të parë nëse sektori i TI-së është në pajtim me nivelet e shërbimit, nëse pronarët e biznesit janë të kënaqur dhe nëse këta të fundit ndërmarrin masat e nevojshme kur ka devijime nga parametrat e aprovuara. Përgjithësisht, ka gjithashtu një SLA ose formë të ngjashme në mes sektorit të TI-së dhe tregtarëve. Për shembull, një njësi e TI-së mund të ketë disa SLA në mes vetëvetes dhe shitësve të ndryshëm që ofrojnë shërbime. SLA për të cilën po diskutojmë, është SLA e brendshme në mes sektorit të të TI-së dhe klientëve të biznesit brenda organizatës.

Në mes të elementëve të tjerë, SLA përmban treguesit kyç të performancës (KPI[22]) për shërbimet e TI-së. Rishikimi i KPI-ve do të ndihmojë audituesin të bëjë pyetje lidhur me:

- Nëse sistemet po veprojnë sipas marrëveshjeve të dokumentuara
- Nëse ekzistojnë mekanizmat për identifikimin e boshllëqeve në performancë, duke trajtuar boshllëqet e identifikuara dhe ndjekur implementimin e masave korrigjuese të ndërmarra si rezultat i vlerësimit të performancës së subjektit
- Identifikimin e çështjeve të kontrollit në subjektin nën auditim, duke përcaktuar në këtë mënyrë natyrën, periudhën dhe shtrirjen e testimit.

Për shembull, matjet e KPI-ve, përcaktimet korresponduese dhe qëllimet për menaxhimin e ndryshimit janë pasqyruar më poshtë:

Procesi	Qëllimi (Faktori kritik i suksesit)	Treguesi Kyç i Performancës	Arkitektura e Matjes
Menaxhimi i Ndryshimit	Reduktimi i Incidenteve të krijuara nga ndryshimet e paautorizuara	Përqindja e reduktimit në numër incidentesh si rezultat i qasjes së paautorizuar	Të kapura nëpërmjet Menaxhimit të Incidenteve, Menaxhimit të Ndryshimit, të raportuara në bazë mujore

[22] Key Performance Indicators

Mund të ketë raste ku sektori i TI-së ka nënkontraktuar pjesën më të madhe të funksioneve të tyre tek një tregtar. Në këto raste sektori i TI-së është ndërlidhësi në mes të tregtarit dhe përdoruesve, si dhe është përgjegjës për menaxhimin e tregtarit për të siguruar se punohet për arritjen e nevojave të biznesit. Kapitulli mbi Kontraktimet paraqet detaje të këtyre rasteve.

Rreziqet e subjekteve nën auditim

Objektivi kryesor për audituesit është marrëveshja e niveleve të shërbimit. Ajo parashtron parametrat, treguesit e performancës dhe kërkesat ndaj të cilave sektori i TI-së duhet të matet. Nëse ky dokument mungon ose nuk rishikohet zyrtarisht dhe nuk aprovohet nga pronarët e biznesit, atëherë ekziston rreziku që burimet e TI-së të organizatës mund të mos shfrytëzohen në mënyrën më efektive ose efikase. Kur auditohen operacionet e TI-së, audituesi duhet të marrë dokumentin ku pasqyrohen të gjitha qëllimet dhe parametrat teknikë të operacioneve të TI-së, zakonisht SLA.

Në fushën e menaxhimit të ndryshimit, audituesi duhet të kontrollojë nëse ekzistojnë procedura kontrolli të ndryshimit që sigurojnë integritetin e sistemit dhe duhet të sigurojnë gjithashtu se vetëm aplikacionet e aprovuara dhe testuara janë të prezantuara në mjedisin operacional.

Audituesi duhet të jetë i ndërgjegjshëm se si subjekti menaxhon kapacitetin (memoria, CPU, burimet e rrjetit, etj) në mënyrë aktive për t'u përgjigjur përdoruesve, menaxhimin e incidenteve dhe çështje të tjera të sigurisë, në mënyrë që funksionet e biznesit të mos kompromentohen.

Matrica e Auditimit

Matrica e auditimit mund të gjendet në Shtojcën IV.

Referencat/ lexim të mëtejshëm

1. CISA Manuali i rishikimit, ISACA
2. CISA Guida e Zhvillimit të Elementëve, ISACA http://www.isaca.org/Certification/Write-an-Exam-Question/Documents/CISA-Item-Development-Guide.pdf.
3. COBIT 5, 2012
   www.uservices.umn.edu/.../sla/BEST_PRACTICE_Service_Level_Agreement.
4. NIST-Guida e Trajtimit të Incidenteve Siguria e Kompjuterëve
   http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-458050.pdf.
5. ISACA Programi i Sigurimit të Auditimit, Menaxhimi i Ndryshimit
6. ISACA-Programi i Sigurimit të Auditimit, Incidentet e Sigurisë
7. Çfarë është TIIL http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx.

KAPITULLI 5

Nënkontraktimi

Çfarë është nënkontraktimi

Nënkontraktimi është procesi i kontraktimit të një procesi ekzistues të biznesit të cilin organizata më parë e ka realizuar brenda, ose kontraktimi i një funksioni të ri biznesi nga një subjekt i jashtëm. Subjekti i kontraktuar është përgjegjës për ofrimin e shërbimeve të kërkuara me kontratë kundrejt një pagese. Një organizatë mund të zgjedhë të marrë nga jashtë pjesë të përzgjedhura të infrastrukturës së TI-së, shërbimeve ose proceseve. Organizata duhet të ketë politika ose vizion, se çfarë aspektesh ose funksione biznesi (zakonisht të TI-së, por mund të ketë edhe të tjerë) do të marrë nga jashtë dhe cilët funksione do të mbajë brenda ambienteve të saj. Në varësi të emergjencës ose gjendjes kritike të shërbimit të kontraktuar, një organizatë mund të zgjedhë të kryejë kontrolle të forta ose të dobëta zyrtare mbi këto shërbime. Sektoret e TI-së mund të vendosin të kontraktojnë të gjitha ose disa prej operacioneve të tyre sepse kontraktimi ofron avantazhe të ndryshëm që përfshijnë:

- **Fleksibiliteti i punësimit të stafit**

Kontraktimi do të lejojë operacionet që kanë kërkesa sezonale ose periodike të sjellë burime shtesë kur organizata ka nevojë për to dhe t'i lirojë ato kur operacionet sezonale mbarojnë.

- **Zhvillimi i stafit**

Nëse një projekt ka nevojë për aftësi të cilat organizata aktualisht nuk i disponon, ajo mund të vendosë të kontraktojë nga jashtë projektin në vend që të trajnojë stafin e brendshëm, duke kursyer para dhe kohë. Kështu, duke u mbështetur në vendndodhjet fizike dhe ekspertizën teknike të tregtarëve, organizata mund të ketë personel të brendshëm që punon së bashku me stafin e tregtarit për një periudhë kohore duke garantuar një trajnim praktik për stafin e saj.

- **Reduktimi i kostos**

Kontraktimi duhet të rezultojë në reduktim të kostos duke zhvendosur punën dhe kostot të tjera drejt një tregtari që ka kosto pune më të ulët. Sektorët e TI-së konsiderojnë që t'i i kontraktojnë detyrat të cilat janë më të kushtueshme se sa të realizohen brenda kompanisë. Një shembull i këtyre detyrave do të ishe një detyrë lidhur me programet e cila kërkon trajnim të specializuar. Organizatat të cilat nuk kanë staf të kualifikuar për të përmbushur këto detyra, mund të përfitojnë financiarisht duke i kontraktuar nga jashtë këto detyra. Kontraktimi i operacioneve jo kryesore, ndihmon gjithashtu organizatën të përqendrohet në biznesin qendror dhe të ofrojë rezultate në mënyrë efikase.

- **Ekspertët e kontraktuar**

Kontraktimi i mundëson organizatës të ketë ekspertë të kontraktuar duke pritur të ndihmojnë në çështjet ekzistuese ose emergjente. Subjekti ka mundësi të përgjigjet shpejt ndaj ndryshimeve sipas nevojave të biznesit (misione të reja ose shtim funksionesh) me ndihmën e ekspertëve.

- Shembuj të kontraktimeve

Sipas dokumenteve mbi kontraktimin të ISACA, organizatat mund të kontraktojnë fusha të ndryshme të biznesit dhe të infrastrukturës së TI-së. Disa prej tyre përfshijnë:

- Infrastrukturen e operimit, që mund të përfshijë të dhënat qendrore dhe proceset lidhur me to
- Procesimin e aplikacioneve, të zhvilluara brenda organizatës, nga një ofrues shërbimi
- Zhvillimin e sistemeve ose mirëmbajtje e aplikacioneve
- Instalimin, mirëmbajtjen dhe menaxhimin e kompjuterëve desktop dhe rrjeteve të lidhura me to

Një zhvillim i fundit i kontraktimit është Cloud Computing. Në këtë rast organizata kontrakton procesimin e të dhënave në kompjutera të zotëruara nga tregtarët. Fillimisht tregtari mban pajisjet ndërkohë që subjekti nën auditim ende ka kontrollin mbi aplikacionet dhe të dhënat. Kontraktimi gjithashtu mund të përfshijë shfrytëzimin e kompjuterave për tu ruajtur, backup (të dhëna rezervë) dhe për të ofruar qasje online të të dhënave të organizatës. Organizata do të ketë nevojë të ketë qasje të fuqishme në internet nëse do që përdoruesit ose personeli të ketë qasje të drejtpërdrejtë ndaj të dhënave ose proceseve që përpunojnë ato. Në mjedisin aktual, të dhënat ose aplikacionet, janë gjithashtu të disponueshme nga platforma mobile/portabël (laptop me Wi-Fi ose karta celulare, smart phone dhe tableta).

Shembuj të cloud computing përfshijnë aplikacione e-mail të bazuara në rrjet online si dhe aplikacione të zakonshme biznesi që qasen online nëpërmjet shfletuesve dhe jo nëpërmjet kompjuterëve lokalë.

Elementet kryesore të kontraktimit

a. Politikat e kontraktimit

Organizatat duhet të kenë disa politika të cilat përcaktojnë se cilat funksione mund të kontraktohen dhe cilat funksione duhet të zhvillohen në ambientet e organizatës. Zakonisht, organizatat kontraktojnë operacione rutinore të TI-së, mirëmbajtje e madje edhe platforma harduerësh desktop. Kontraktimi i burimeve njerëzore dhe regjistrat e personelit janë mbajtur në funksione të ambienteve të organizatës, pasi kërkojnë monitorim të afërt dhe janë subjekt i kërkesave të privatësisë dhe sigurisë.

Audituesi duhet të fillojë duke rishikuar politikat dhe procedurat e kontraktimit të subjektit nën auditim. Në organizatat e mëdha, të cilat kanë të nënkontratkuara sasi të mëdha të operacioneve të tyre të biznesit, është e rëndësishme që ato të kenë politika të miratuara kontraktimi përfshirë këtu edhe proceset e mirë përcaktimit të kërkesave. Organizatat më të vogla mund të mos kenë politika formale, por ato duhet të ndjekin procedura efikase dhe transparente të përzgjedhjes së kërkesave.

b. Përzgjedhja e kërkesave

Ky proces është aktiviteti i dokumentimit të kërkesave të sistemit dhe mbledhja e materialeve të tjera që do të ndihmojnë tregtarin në ndërtimin e sistemit. Përfshin gjenerimin e paketës së kërkesave dhe vendosjen e tyre në ofertë, marrjen e propozimeve dhe kryerjen e përzgjedhjes në mes të tregtarëve të

ndryshëm. Procesi i përzgjedhjes duhet të jetë transparent dhe objektivë, si dhe i bazuar mbi kriteret e duhura për sistemin ose shërbimet për të cilat ato kërkohen.

c. Menaxhimi i tregtarit/kontratës

Menaxhimi i shitësit është një element thelbësor i kontraktimit për të siguruar që shërbimet ofrohen në bazë të pritjeve të klientit. Organizata nën auditim duhet të ketë procese për të garantuar ndjekjen periodike të gjendjes së projektit, cilësisë së shërbimit, dëshmi të testimit të produkteve përpara prezantimit të tyre në mjedisin operacional, etj. Përveç kësaj, si pjesë e procesit monitorues të tregtarit, organizata nën auditim mundet gjithashtu të auditojë procesin e brendshëm të sigurimit të cilësisë të tregtarit për tu siguruar se personeli i kompanisë tregtare është duke ndjekur politikat e aprovuara të kontraktimit dhe planet për të gjithë punën e tyre.

Audituesi do të duhet të rishikojë nëse organizata ka përcaktuar kërkesat e tij për funksionin e kontraktuar përpara përzgjedhjes së tregtarit (kërkesat specifike dhe parametrat operacionalë janë në kontratë dhe në SLA), nëse organizata është duke monitoruar plotësimin e kërkesave nga tregtari të pasqyruara këto në SLA (nëpërmjet raporteve të statusit), nëse organizata ka ndërmarrë masa në momentet kur tregtari nuk ka plotësuar parametrat e përshkruara në SLA (masa korrigjuese ose penalitete me pagesë).

d. SLA

SLA është një marrëveshje e dokumentuar midis organizatës dhe tregtarit prej të cilit është marrë shërbimi dhe është një dokument kyç për menaxhimin e tregtarit. SLA duhet të përcaktojë shërbimet që tregtari duhet të kryejë ashtu si edhe parametrat teknikë për ato shërbime, meqë është një marrëveshje ligjërisht e detyrueshme midis tregtarit dhe organizatës.

Fushat karakteristike të trajtuara në SLA janë:

- Llojet e shërbimeve që tregtari do të kryejë;
- Shpërndarja e përgjegjësive në mes të organizatës dhe tregtarit;
- Shërbimet që do të maten, periudha e matjes, afati, vendi dhe afatet e raportimit (rangu i defekteve, koha e përgjigjes, orët e personelit të tavolinë ndihmëse, etj);
- Koha për implementimin e funksionaliteteve të reja, niveli i ripunimeve;
- Lloji i dokumenteve të nevojshme për aplikacionet e zhvilluara nga tregtarët;
- Vendndodhja ku shërbimet do të kryhen;
- Frekuenca e backup, parametrat e rimëkëmbjes së të dhënave;
- Metodat dhe formatet e ndërprerjes dhe ofrimit të të dhënave;
- Klauzolat e nxitjes dhe penaliteteve.

Shkurtimisht, shumica e artikujve që janë kritik për organizatën duhet të vendosen në këto marrëveshje. Audituesi i TI-së duhet të pyesë për SLA ose dokument tjetër (kontratë ose marrëveshje formale) ku këto parametra janë të dokumentuara dhe të sigurohet se raportimi nga tregtari mbi parametra të ndryshëm, përmbush kërkesat ose që organizata ka ndërmarrë masa korrigjuese për të trajtuar mangësitë.

e. Realizimi i përfitimit

Përgjithësisht, subjektet e audituara kontraktojnë për të reduktuar kostot. Këto arrihen kur kostoja e ofrimit të këtyre shërbimeve janë më të ulëta nga një tregtar sesa shfrytëzimi i punës ose infrastrukturës në ambientet e organizatës. Sa herë që të mundet organizata duhet të përpiqet të përcaktojë nëse kursimet e projektuara janë duke u grumbulluar. Kjo shërben si një nga pikat për të vendosur nëse të vazhdojë ose të ndalojë me kapacitetet e kontraktuara.

f. Siguria

Ndërkohë që ka të nënkontraktuar bazat e të dhënave dhe administrimin e saj, sektori i TI-së duhet të vlerësojë nëse tregtari ka praktika të fuqishme dhe të mjaftueshme të sigurisë dhe nëse tregtari mund të përmbushë kërkesat e sigurisë. Pjesa më e madhe e sektorëve të TI-së i gjejnë praktikat e sigurisë së tregtarëve impresionuese (shpesh tejkalojnë praktikat e tyre të brendshme), rreziku i thyerjeve të sigurisë ose i pronës intelektuale është rritur nga fakti se të dhënat janë nënkontraktuar. Çështjet e privatësisë duhet të theksohen. Çështje të tjera të sigurisë do të përfshijnë keqmenaxhimin ose zbulimin e të dhënave sensitive, qasjen e paautorizuar tek të dhënat dhe aplikacionet si dhe plani i rimëkëmbjes nga fatkeqësitë. Edhe pse këto çështje rrallë përbëjnë pengesë për burimet e jashtme, kërkesat duhet të dokumentohen.

Rreziqe e organizatës nën auditim

1. Mbajtja e njohurive të biznesit dhe pronësia e proceseve të biznesit

Ekziston një rrezik i brendshëm i humbjes së njohurive të biznesit i cili qëndron brenda zhvilluesve të aplikacioneve. Nëse tregtari, për arsye të ndryshme, nuk ka mundësi të ofrojë shërbime, sektori i TI-së duhet të jetë gati ta rimarrin si detyrë. Po ashtu, pasi zhvillimi i aplikacionit do të ndodhte jashtë organizatës, organizata gjithashtu rrezikon të dështoj ose të humbasë pronësinë e procesit të biznesit, e cila mund të pretendohet nga ofruesi i shërbimit si pronë e tyre intelektuale. Organizatat duhet të trajtojnë këtë çështje në momentin e nënshkrimit të kontratës dhe të sigurohen se zotërojnë dokumentacionin e plotë të procesit të zhvillimit të sistemit ashtu si edhe të dizajnit të sistemit. Kjo do të ndihmojë organizatën të ndërrojë ofruesit e shërbimeve, nëse do të ishte e nevojshme.

2. Tregtari dështon të gjenerojë produkt

Ndonjëherë një tregtar mund të dështojë të prodhojë produkt në kohë ose produkti duhet të mos përdoret për shkak të mungesës së funksionalitetit të tij. Nëse procesi i dokumentimit të kërkesave nuk është implementuar në mënyrën e duhur, atëherë ekziston një rrezik i lartë i mundësisë që sistemi ose shërbimet e blera të mos përmbushin kërkesat e përdoruesve, të jenë nën standarde, të kushtojnë më shumë, të kërkojnë më shumë burime për tu mirëmbajtur dhe për të operuar ose të kenë cilësi aq të dobët sa do të kenë nevojë për zëvendësim në të ardhmen. Një kontratë e varfër, sistem me të meta nga zgjedhja e tregtarit, faza/momente të paqarta dhe/ose kushte të pafavorshme tregu, janë disa nga arsyet e dështimit të tregtarit.

Sektoret e TI-së duhet të kenë plane emergjente për një ngjarje të tillë. Kur marrim në konsideratë marrjen e burimeve nga jashtë, sektoret e TI-së duhet të vlerësojnë ndërlikimet e dështimit të tregtarit

(për shembull, a ka dështimi ndërlikime të rëndësishme për biznesin). Disponueshmëria e dokumentacionit të detajuar mbi dizajnin e sistemit dhe zhvillimit të tij, do të ndihmojë që organizata të sigurohet për vazhdimësinë e biznesit nëpërmjet një ofruesi tjetër të shërbimit.

3. Shtrirja e fushëveprimit

Të gjitha kontratat e marrjes së burimeve të jashtme, përmbajnë kritere dhe supozime. Nëse puna aktuale ndryshon nga vlerësimet, klienti do të paguajë diferencën. Ky fakt i thjeshtë është bërë pengesë për sektorët e TI-së që habiten me mos fiksimin e çmimit ose që tregtari pret të paguhet për pagesë shtesë për shkak të ndryshimeve të fushëveprimit. Pjesa më e madhe e projekteve ndryshojnë me 10%-15% përgjatë ciklit të zhvillimit.

4. Qarkullimi i personelit kyç

Rritja e shpejtë në mes të tregtarëve të jashtëm, ka krijuar një treg dinamik të forcës punëtore. Personeli kyç zakonisht është në kërkim të projekteve të reja, të projekteve me profil të lartë ose edhe nën rrezikun e rekrutimit nga tregtarë të rinj. Ndërkohë që tregtarët shpesh do të citojnë statistika që shfaqen relativisht të ulëta, statistikat më të rëndësishme për tu menaxhuar janë qarkullimet e personelit kyç. Nivelet më të zakonshme të qarkullimit janë të rangut 15%-20% dhe krijimi i termave kontraktual rreth këtyre niveleve është një kërkesë e arsyeshme.

5. Rreziqet e jashtme

Kontraktimi i ofruesve të shërbimeve jashtë shtetit është një formë e zakonshme e burimeve të jashtme, veçanërisht në një mjedis cloud. Në këto raste, rreziqet e kontraktimit do të përfshinin rregullat e jashtme mbi ruajtjen e informacionit dhe transferimi mund të kufizojë se çfarë mund të ruhet dhe si mund të procesohet, të dhënat mund të përdoren nga zbatimi i ligjit të shtetit të huaj pa dijeninë e organizatës, standardet e privatësisë dhe sigurisë mund të mos jenë gjithnjë proporcionale dhe mosmarrëveshjet për shkak të juridiksioneve të ndryshme ligjore nuk mund të shmangen plotësisht.

Matrica e Auditimit

Matricën e auditimit për këtë seksion mund ta gjeni në Shtojcën V.

Referencat/ lexim të mëtejshëm

1. Dean Davison, 10 Rreziqet më ta larta të Nënkontraktimit, 2003 http://www.zdnet.com/news/top-10-risks-of-offshore-outsourcing/299274
2. Programi i Auditimit/ Sigurisë së Mjedisit të Kontraktimit të TI-së, 2009, ISACA http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx
3. Qeverisja e Kontraktimit, ISACA

http://www.isaca.org/Knowledge-Center/Research/Documents/Outsourcing.pdf

4. Udhëzime mbi marrëveshjen e shërbimeve: Elementet kryesore Sekretariati Kanadez i Bordit të Thesarit www.tbs-sct.gc.ca
5. NIST SP 500-292, NIST Arkitektura Referuese e Cloud Computing
6. NIST SP 800-144, Udhëzime mbi Sigurinë dhe Privatësinë në Cloud Computing Shtetëror

KAPITULLI 6

Plani i vazhdimësisë së biznesit (PVB) dhe plani i rimëkëmbjes nga fatkeqësia (PRF)

Çfarë është PVB dhe PRF

Organizatat qeveritare gjithnjë e më shumë mbështeten në disponueshmërinë dhe funksionimin korrekt të sistemeve të tyre kompjuterike për të përmbushur detyrimet e tyre ligjore. Sistemet kompjuterike luajnë rol të rëndësishëm në aktivitete të tilla të shumëllojshme, siç është vlerësimi dhe vjelja/mbledhja e taksave dhe të hyrave nga dogana; pagesa e pensioneve shtetërore dhe përfitimeve të sigurimeve shoqërore; si dhe përpunimin e statistikave kombëtare (lindje, vdekje, krime, sëmundje, etj). Në fakt, shumë aktivitete nuk mund të kryhen në mënyrë efektive - apo fare, pa mbështetje në kompjuterë.

Mungesa e energjisë elektrike, veprimet industriale, zjarri dhe dëmtimet e ndryshme mund të kenë efekte shkatërruese në sistemet kompjuterike. Mund të nevojiten shumë javë të tëra që një organizatë të rifillojë operacionet efektive të biznesit nëse nuk ka një plan të zbatueshëm të vazhdimësisë së biznesit.

Termat si Plani i Vazhdimësisë së Biznesit dhe Plani i Rimëkëmbjes nga fatkeqësitë shpesh përdoren si sinonime, por në fakt janë dy terme të ndryshme por plotësuese për njëra tjetrën. Të dyja janë të rëndësishme për audituesin e TI-së, sepse të dyja së bashku sigurojnë që organizata të jetë në gjendje të operojë me kapacitete të përcaktuara pas një ndërprerje të shkaktuar nga natyra ose njeriu. Të dy këto terme janë shpjeguar më poshtë:

- **Planifikimi i vazhdimësisë së biznesit (PVB)** është proces gjatë së cilës një organizatë planifikon dhe teston rimëkëmbjen e proceseve të biznesit (veprimtarisë) pas një ndërprerjeje. Ky proces përshkruan se si një organizatë do të vazhdojë të funksionojë në kushte të pafavorshme që mund të shfaqen (për shembull, fatkeqësi natyrore ose fatkeqësi të tjera).

- **Planifikimi i rimëkëmbjes nga fatëkeqësitë (PRF)** është proces i planifikimit dhe testimit të rimëkëmbjes së infrastrukturës së teknologjisë informative pas një fatëkeqësie natyrore ose ngjashëm. Është nën-grup i planifikimit të vazhdimësisë së biznesit. PVB vlen për funksionet e biznesit organizativ ndërsa PRF për burimet e TI-së që mbështesin funksionet e biznesit.

Në esencë, PVB adreson aftësinë e një organizate për të vazhduar funksionimin në momentin që operacionet normale të ndërpriten. Ky plan përfshin politikat, procedurat dhe praktikat që lejojnë një organizatë të rimëkëmbet dhe të rifillojë proceset kritike manuale dhe të automatizuara të misionit pas fatëkeqësisë ose krizes. Përveç theksimit të praktikave që duhet të ndiqen në rast të një ndërprerje, disa PVB përfshijnë edhe komponentë të tjerë, siç janë rimëkëmbja nga fatëkeqësitë, reagim emergjent, rimëkëmbja e përdoruesit dhe aktivitetet e menjëhershme dhe të menaxhimit të krizave. Si e tillë, në këto organizata, vazhdimësia e biznesit shihet si term gjithëpërfshirës që përfshin si rimëkëmbjen nga fatëkeqësitë por edhe rifillimin e aktiviteteve të biznesit.

Sidoqoftë, qoftë si pjesë e PVB ose një dokumenti të veçantë, PRF-të duhet të përcaktojnë burimet, veprimet, detyrat dhe të dhënat e nevojshme për të menaxhuar procesin e rimëkëmbjes së një organizate në rast të ndërprerjes së biznesit (veprimtarisë). Ky plan duhet të ndihmojë organizatën kur të

rifunksionalizojë proceset e ndikuara të biznesit (veprimtarisë), duke përshkruar hapat specifikë që organizata duhet të ndërmarrë në rrugën e saj drejt rimëkëmbjes. Në mënyrë të veçantë, PRF përdoret për përgatitjen dhe planifikimin e avancuar të nevojshëm për të minimizuar dëmet nga fatëkeqësitë si dhe për të siguruar disponueshmërinë e sistemeve të informacionit e që janë kritike për organizatën. Sa i përket TI-së, PRF-të adresojnë rimëkëmbjen e pasurive kritike të teknologjisë, përfshirë sistemet, aplikacionet, bazat e të dhënave, pajisjet e ruajtjes dhe burimet e tjera të rrjetit.[23]

Elementet kryesore të PVB dhe PRF

Audituesi i TI-së detyrohet të vlerësojë programet e menaxhimit të vazhdimësisë së organizatës, e që përfshin vlerësimin e planeve të tij të rimëkëmbjes nga fatkeqësitë dhe vazhdimësisë së biznesit (veprimtarisë) dhe sistemeve të menaxhimit të krizave. Për ta bërë këtë, audituesit duhet të kuptojnë se çka përfshihet në zhvillimin e një strategjie të menaxhimit të vazhdimësisë së biznesit (veprimtarisë) dhe hapat që duhet të ndërmarrin për të vlerësuar efektivitetin e programeve ekzistuese që përfshijnë vazhdimësinë e nevojshme të biznesit, rimëkëmbjen nga fatëkeqësitë dhe përpjekjet për menaxhimin e krizave.

Një planifikim efektiv i vazhdimësisë ka disa faza të zakonshme që vlejnë për të gjitha sistemet e informacionit. Hapat e përgjithshëm në proces janë[24]:

1. Politika dhe plani i vazhdimësisë së biznesit
2. Organizimi i funksionit të vazhdimësisë së biznesit
3. Vlerësimi i Ndikimit të Biznesit (VNB) dhe Menaxhimi i Rrezikut
4. Kontrollet parandaluese përfshirë kontrollet e mjedisit
5. Plani i Rimëkëmbjes nga Fatkeqësitë
6. Dokumentimi i planit të vazhdimësisë së biznesit
7. Planifikimi i testimit dhe trajnimeve
8. Siguria gjatë zbatimit të PVB/PRF
9. Kopje rezervë (back-up) dhe rimëkëmbja nga fatëkeqësitë për shërbimet e jashtme (të kontraktuara.

Këto hapa përfaqësojnë elementët kryesorë në aftësinë e planifikimit gjithëpërfshirës të biznesit. Elementet janë shpjeguar si më poshtë:

a. Politika, Plani dhe Organizimi i vazhdimësisë së biznesit

Planifikimi efektiv i vazhdimësisë fillon me krijimin e një politike të vazhdimësisë së biznesit të një organizate. Ekipi i menaxhimit të vazhdimësisë së biznesit[25] që përfaqëson të gjitha funksionet e përshtatshme të biznesit gjithashtu luan një rol të rëndësishëm në suksesin e organizatës në planin e vazhdimësisë së biznesit. Deklarata e politikave të planifikimit të biznesit të vazhdimit duhet të

[23] Roli i Auditorit IT në Menaxhimin e Vazhdimësisë së Biznesit, Botimi IIA http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management

[24] Publikimi Special NIST 800-34, Udhëzuesi i Planifikimit të Emergjencave për Sistemet Federale të Informacionit, ofron udhëzime mbi proceset e planifikimit të emergjencave

[25] Shpjegohet në pjesën në vazhdim

përcaktojë objektivat e përgjithshëm të vazhdimësisë së organizatës dhe të krijojë kornizën organizative dhe përgjegjësitë për planifikimin e vazhdimësisë.

b. Krijimi i funksionit të vazhdimësisë së biznesit

Për të qenë i suksesshëm, ekipi menaxhues për vazhdimësi të biznesit duhet të jetë i organizuar në drejtim të përfaqësimit të të gjitha funksioneve të përshtatshme të biznesit. Menaxhmenti i lartë dhe zyrtarët tjerë të lidhur duhet të mbështesin një program vazhdimësie dhe të shoqërohen me proces të hartimit të politikave. Rolet dhe përgjegjësitë në ekip duhet të identifikohen dhe përcaktohen qartë.

c. Vlerësimi i Ndikimit në Biznes dhe Menaxhimi i Rrezikut

i. Vlerësimi i kritikalitetit dhe ndjeshmërisë së operacioneve të kompjuterizuara dhe identifikimi i burimeve mbështetëse

Në çdo organizatë, vazhdimësia e operacioneve të caktuara është më e rëndësishme se sa operacionet tjera dhe nuk është e kushtueshme për të siguruar të njëjtin nivel vazhdimësie për të gjitha operacionet. Për këtë arsye, është e rëndësishme që organizata të përcaktojë se cilat janë më kritike dhe cilat burime janë të nevojshme për t'i rikuperuar dhe mbështetur ato. Kjo realizohet duke kryer një vlerësim të rrezikut, duke identifikuar kërcënime të mundshme dhe ndikimet e tyre në informacionin e organizatës dhe burimet e lidhura, përfshirë të dhënat dhe programin aplikativ dhe operacionet. Vlerësimi i rrezikut dhe ndikimit duhet të përfshijë të gjitha fushat funksionale. Një vendim mbi rrezikun e mbetur duhet të merret në përputhje me rrethanat kur ndikimi i një kërcënimi të mundshëm është minimal ose sistemet e kontrollit janë adekuate për të identifikuar raste të tilla në kohë.

ii. Identifikimi dhe prioritizimi i të dhënave dhe operacioneve kritike

Kritikaliteti dhe ndjeshmëria e të dhënave dhe operacioneve të ndryshme duhet të përcaktohet dhet'ijepet prioritet bazuar në kategorizimet e sigurisë dhe vlerësim të përgjithshëm të rrezikut të operacioneve të organizatës. Një vlerësim i tillë i rrezikut duhet të shërbejë si bazë për planin e sigurisë së një organizate. Faktorët që duhet të merren parasysh përfshijnë rëndësinë dhe ndjeshmërinë e të dhënave dhe aseteve të tjera të organizatës si dhe koston e mos rivendosjes së shpejtë të të dhënave ose operacioneve. Për shembull, një ndërprerje njëditore e sistemeve kryesore të mbledhjes së taksave ose tarifave ose humbja e të dhënave që ndëridhen me to mund ta ngadalësojnë ose ndalojnë ndjeshëm mbledhjen e të hyrave, të zvogëlojnë kontrollet mbi miliona dollarë në arkëtime dhe të zvogëlojnë besimin e publikut. Në një rast tjetër, një sistem që monitoron aftësimin e punonjësve mund të jetë jashtë shërbimit për muaj të tërë, por pa pasoja të rënda.

Në përgjithësi, të dhënat kritike dhe operacionet duhet të identifikohen dhe renditen nga personeli i përfshirë në veprimtarinë ose programet e organizatës. Është rëndësishme që të merret miratimi/aprovimi i menaxhmentit të lartë me përcaktime të tilla, përfshirë edhe pajtueshmërinë nga grupet e ndikuara.

Listimi i prioriteve të burimeve kritike të informacionit dhe operacioneve duhet të rishikohet në mënyrë periodike për të përcaktuar nëse kushtet aktuale reflektohen në të. Shqyrtime të tilla duhet të ndodhin sa

herë që ka ndryshime të rëndësishme në mision dhe operacione të organizatës ose në vendndodhjen apo edhe dizajnin e sistemeve që mbështesin këto operacione.

iii. Identifikimi i burimeve që mbështesin operacionet kritike

Pasi të përcaktohen të dhënat kritike dhe operacionet, duhet të identifikohen burimet minimale të nevojshme për t'i mbështetur ato si dhe të analizohen rolet e tyre. Burimet që duhen marrë parasysh përfshijnë burimet e kompjuterit, siç janë hardueri, softueri dhe dosjet (fajllat); rrjetet, përfshirë komponentë të tillë si ruterat dhe muret mbrojtëse (Firewall); furnizimet, përfshirë stokun e letrës dhe format e para-shtypura; shërbimet telekomunikuese; dhe çdo burim tjetër që është i nevojshëm për operacione, siç janë njerëzit, objektet dhe furnizimet e zyrës, si dhe regjistrimet jo të kompjuterizuara.

Për shkak se burimet thelbësore ka gjasa të mbahen ose menaxhohen nga grupe të ndryshme brenda një organizate, është e rëndësishme që programi dhe stafi mbështetës i sigurisë së informacionit të punojnë së bashku për të identifikuar burimet e nevojshme për operacione kritike.

iv. Vendosja e prioriteteve për procesim të urgjencës

Me identifikimin dhe prioritizimin e funksioneve kritike, organizata duhet të hartojë një plan për rivendosjen e operacioneve kritike. Plani duhet të përcaktojë qartë renditjen në të cilën duhet të kthehen aspektet e ndryshme të procesimit, kush është përgjegjës dhe çfarë pajisje ndihmëse ose burime të tjera do të nevojiten. Një plan i kthimit i zhvilluar me kujdes mund të ndihmojë punonjësit të fillojnë menjëherë procesin e kthimit (restore) dhe të shfrytëzojnë burimet e kufizuara kompjuterike gjatë një urgjence në mënyrë sa më efikase. Që të dy, si përdoruesit e sistemit ashtu dhe stafi i ndihmës për sigurinë e informacionit duhet të përfshihen në përcaktimin e prioriteteve për procesim të urgjencës.

v. Parandalimi dhe minimizimi i dëmtimit dhe ndërprerjes së mundshme

Ekzistojnë një numër hapash që një organizatë duhet të ndërmarrë për të parandaluar ose minimizuar dëmtimin e operacioneve të automatizuara që mund të ndodhin shkaku i një ngjarje të papritur. Këto mund të kategorizohen si:

- Dyfishim ose kopje rezervë (back-up) i skedarëve të të dhënave (data files), programeve kompjuterike dhe dokumenteve kritike në vende tjera; dhe/ose aranzhimi i hapisërave të largëta për kopje rezervë që mund të përdoren nëse objektet e zakonshme të organizatës dëmtohen aq sa nuk mund të përdoren.
- Vendosja e sistemit të informacionit me aftësi të rimëkëmbjes dhe rikonstruksionit mënyrë që sistemi i informacionit të rimëkëmbet dhe rikonstruktohet në gjendjen e tij origjinale pas ndërprerjejes ose dështimit.
- Instalimi i kontrolleve mjedisore, siç janë sistemet kundër zjarrit ose furnizimi me energji elektrike rezervë.
- Sigurimi që personeli dhe përdoruesit e tjerë të sistemit të kuptojnë përgjegjësitë e tyre gjatë emergjencave.
- Mirëmbajtja efektive e harduerit, administrimi i problemeve dhe menaxhimi i ndryshimeve.

vi. Zbatimi i procedurave për kopjen rezervë (back-up) të të dhënave dhe programit

Kopjimi i skedarëve (fajllave) dhe softuerëve në mënyrë rutinore dhe ruajtja e këtyre skedarëve në një vend të sigurt, në distancë, janë zakonisht veprime me kosto më efektive që një organizatë mund të ndërmarrë për të lehtësuar ndërprerjen e shërbimit. Megjithëse pajisjet shpesh mund të zëvendësohen lehtësisht, kostoja mund të jetë e rëndësishme dhe rikonstruimi i skedarëve të të dhënave të kompjuterizuara dhe zëvendësimi i softverit mund të jetë jashtëzakonisht i kushtueshëm dhe kërkon shumë kohë. Në të vërtetë, skedarët e të dhënave jo gjithmonë mund të rikonstruktohen. Përveç kostove të drejtpërdrejta të rikonstruimit të skedarëve dhe marrjes së softuerëve, ndërprerjet e shërbimit mund të çojnë në humbje të konsiderueshme financiare.

vii. Trajnimi

Stafi duhet të trajnohet dhe të jetë i vetëdijshëm për përgjegjësitë e tyre në parandalimin, zbutjen dhe përgjigjen ndaj situatave emergjente. Për shembull, stafi ndihmës për sigurinë e informacionit duhet të ndjekë trajnime periodike për procedurat në rast të incidenteve nga zjarri, uji dhe aktivizimi i alarmit, si dhe për përgjegjësitë e tyre për fillimin dhe drejtimin e vendndodhjes alternative të përpunimit të të dhënave. Gjithashtu, nëse përdoruesit e jashtëm janë kritikë për operacionet e organizatës, ata duhet të informohen për hapat që duhet të ndërmerren si rezultat i një emergjence.

viii. Planet për mirëmbajtjen e pajisjeve, menaxhimin e problemeve dhe menaxhimin e ndryshimeve

Ndërprerjet e papritura të shërbimit mund të ndodhin nga dështimet e pajisjeve harduerike ose nga ndërrimi i pajisjeve pa njoftim të duhur paraprak për përdoruesit e sistemit. Për të parandaluar dukuri të tilla kërkohet të ketë një program efektiv për mirëmbajtje, menaxhim të problemeve dhe menaxhim të ndryshimit për pajisjet harduerike.

d. Kontrollet parandaluese dhe mjedisore

Kontrollet mjedisore parandalojnë ose lehtësojnë dëmtimin e mundshëm të objekteve dhe ndërprerjet në shërbim. Shembuj të kontrolleve mjedisore përfshijnë:

- aparate zjarri dhe sistemet kundër përhapjes së zjarrit;
- alarmet për zjarr;
- detektorët për tym;
- detektorët për uji;
- ndriçim emergjent;
- hapësirë në sistemet e ftohjes së ajrit;
- furnizime rezervë me energji elektrike;
- ekzistimi i valvulave të mbylljes dhe procedurave për çdo linjë hidraulike të ndërtesave që mund të rrezikojnë hapësirat për procesim;
- objektet e përpunimit të ndërtuara me materiale rezistente ndaj zjarrit dhe të dizajnuara për të zvogëluar përhapjen e zjarrit;

- politika që ndalojnë ngrënien, pirjen e lëngjeve të ndryshme dhe duhanit brenda ambienteve kompjuterike.

Kontrollet mjedisore mund të zvogëlojnë humbjet nga disa ndërprerje siç janë zjarret ose parandalojnë incidentet duke i detektuar problemet e mundshme në fillim, siç janë rrjedhjet e ujit ose tymi, në mënyrë që ato të mund të rregullohen. Gjithashtu, furnizimet me energji të pandërprerë ose rezervë mund të mbajnë strukturën si duhet përmes një ndërprerjeje të shkurtër të energjisë ose të mundësojnë kohë të mjaftueshme për të kopjuar të dhënat dhe për të kryer procedurat e rregullta të mbylljes gjatë ndërprerjeve të zgjatura të energjisë.

e. Plani i Rimëkëmbjes nga Fatkeqësitë

Plani i rimëkëmbjes nga fatkeqësitë duhet të hartohet në mënyrë që të bëhet rivendosja e aplikacioneve kritike; kjo përfshin aranzhime për hapësirat alternative të procesimit në rast se objektet kryesore dëmtohen dukshëm ose janë të pa qasshme. Politikat dhe procedurat e nivelit të organizatës përcaktojnë procesin e planifikimit të rimëkëmbjes dhe kërkesat e dokumentacionit. Për më tepër, një plan i gjerë i organizatës duhet të identifikojë sistemet kritike, aplikacionet dhe planet vartëse ose të ndërlidhura. Është e rëndësishme që këto plane të dokumentohen në mënyrë të qartë, t'i komunikohen stafit i cili ndikohet nga këto dhe të azhurnohen për të pasqyruar operacionet aktuale.

i. Dokumentimi i planit aktual të rimëkëmbjes

Planet e rimëkëmbjes nga fatkeqësitë duhet të dokumentohen, të bien dakord nga departamentet e sigurisë dhe ai i biznesit (veprimtarisë) dhe t'i komunikohen stafit që ndikohet nga to. Plani duhet të pasqyrojë rreziqet dhe prioritetet operative që janë identifikuar nga organizata. Duhet të jetë i dizajnuar ashtu që kostot e planifikimit të rimëkëmbjes të mos tejkalojnë kostot e shoqëruara me rreziqet që plani ka për qëllim të zvogëlojë. Plani gjithashtu duhet të jetë i detajuar dhe i dokumentuar sa duhet që suksesi i tij të mos varet nga njohuria ose ekspertiza e një ose dy individëve.

Kopje të shumta të planit të vazhdimësisë duhet të jenë në dispozicion, ku disa prej tyre ruhen edhe jashtë objektit për të siguruar që ato nuk do të shkatërrohen nga të njëjtat ngjarje që i bënë këto hapësira brenda objektit kryesor të mos jenë në dispozicion.

ii. Aranzhimet për vendndodhjen alternative

Në varësi të asaj se sa nevojitet vazhdimësia e shërbimit, zgjedhjet për vendet ose objektet alternative do të shkojnë nga një vend i pajisur i gatshëm për shërbim të menjëhershëm të back-up, i referuar si një “Hot site (vend i nxehtë)”, në një vend tjetër i cili nuk është edhe i pajisur dhe duhet kohë për t'u përgatitur për operacione, e të cilave i referohemi si “cold site (vend i ftohtë)”. Për më tepër, me furnizuesit mund të aranzhojmë lloje të ndryshme të shërbimeve. Këto përfshijnë marrëveshjet me furnizuesit e pajisjeve kompjuterike dhe shërbimeve telekomunikuese, si dhe me furnizuesit tjerë të biznesit dhe furnizimeve të tjera të zyrës.

f. Testimi

i. Testimi periodik i planit të vazhdimësisë

Testimi i planeve të vazhdimësisë është thelbësor për të përcaktuar nëse ato do të funksionojnë siç synohet në rast të një situatë emergjente. Testimi duhet të zbulojë dobësi të rëndësishme në plane, të tilla si hapësirat për kopjet rezervë (back-up) që nuk mund të kopjojnë në mënyrë të duhur operacionet kritike siç parashikohej. Përmes procesit të testimit, këto plane duhet të përmirësohen në mënyrë thelbësore.

Frekuenca e testimit të planit të vazhdimësisë duhet të ndryshojë në varësi të asaj sa kritike janë operacionet e organizatës. Në përgjithësi, planet e vazhdimësisë për funksione shumë kritike duhet të testohen plotësisht rreth një apo dy herë në vit, sa herë që bëhen ndryshime të rëndësishme në plan, ose kur të ndodhin lëvizjet të stafit kryesor. Është e rëndësishme që Menaxhmenti i lartë të vlerësojë rreziqet e problemeve të planit të vazhdimësisë dhe të hartojë dhe dokumentojë politika për shpeshtësinë dhe shtrirjen e këtij testimi.

ii. Përditësimi i planit të vazhdimësisë bazuar në rezultatet e testimit

Rezultatet e testit të vazhdimësisë japin një masë të rëndësishme të realizueshmërisë së planit të vazhdimësisë. Si e tillë, ato duhet të raportohen te menaxhmenti i lartë në mënyrë që të përcaktohet nevoja për modifikim dhe testim shtesë dhe kështu që menaxhmenti i lartë të jetë i vetëdijshëm për rreziqet e vazhdimit të operacioneve me një plan të papërshtatshëm të vazhdimësisë.

g. Siguria

Siguria e burimeve dhe operacioneve duhet të inkorporohet në planin e vazhdimësisë së biznesit (veprimtarisë) pasi të dhënat kritike, aplikacioni softuerik, operacionet dhe burimet mund të kompromentohen lehtë gjatë çfarëdo ndodhie të fatkeqësisë ose aktiviteti të menaxhimit të vazhdimësisë së biznesit. Për shembull, gjatë kopjimit të të dhënave, mungesa e sigurisë mund të çojë në krijimin e kopjeve të dyfishta (duplicate copies) dhe rrjedhjen e të dhënave të rëndësishme. Në të njëjtën kohë, mund të ndodhë që të dhënat që janë bërë kopje rezervë (back-up) të kompromentohen gjatë procesit të “backup” (të dhënat kopjohen nga serveri i transaksioneve në të dhënat që ruhen në një server rezervë).

h. Kopje rezervë (back-up) dhe rikuperim i të dhënave për shërbimet e jashtme (të kontraktuara)

Shumë organizata i transferojnë të gjitha ose një pjesë të veprimtarisë së tyre një ofruesi të shërbimit. Meqenëse funksionimi ditor dhe kontrollet e përditshme do të kryheshin nga ofruesi i shërbimit, është thelbësore për organizatën që të sigurojë që plani i vazhdimësisë së biznesit dhe rimëkëmbjes nga fatkeqësitë të përfshihet në kontratë. Organizata gjithashtu do të duhet të monitorojë që vazhdimësia e biznesit dhe gatishmëria e rimëkëmbjes nga fatkeqësitë sigurohen nga ofruesi i shërbimit. Kjo do të përfshijë edhe gatishmërinë për ofruesin e shërbimit për siguri. Organizata mund të ketë nevojë të sigurojë edhe atë që ofruesi i shërbimit të ruajë konfidencialitetin e të dhënave në një aplikacion softuerik që mirëmbahet nga ofruesi i shërbimit. Pronësia e procesit të biznesit duhet të ruhet nga organizata. Organizata duhet të ketë edhe një plan të vazhdimësisë për të siguruar edhe vazhdimësinë e ofruesit të shërbimit për veprimtarinë e tyre ose të marrë përsipër këtë nga një kompani tjetër.

RREZIQET PËR ENTITETIN E AUDITUAR

Shërbimet ose produktet kritike janë ato që duhet të dorëzohen për të siguruar mbijetesën, për të shmangur shkaktimin e humbjes dhe përmbushjen e detyrimeve ligjore ose të tjera të një organizate. PVB/PRF është proces proaktiv i planifikimit që siguron se proceset e biznesit (veprimtarisë) dhe Infrastruktura e TI-së brenda një organizate të jenë në gjendje të mbështesin nevojat e misionit pas një fatkeqësie ose ndërhyrjeje tjetër. Agjencitë qeveritare shërbejnë për shumë nevoja kritike për misionin (pagesa për qytetarë, ofrimin e kujdesit shëndetësor, arsim, mbrojtje dhe shërbime të tjera ku qytetarët mbështeten). Nëse këto shërbime ndërpriten për periudha të gjata kohore, kjo mund të çojë në humbje financiare dhe humbje të tjera. Audituesit duhet të sigurojnë që të gjitha agjencitë qeveritare kanë proces të PVB/PRF i cili siguron se agjencia është në gjendje të vazhdojë t'u shërbejë qytetarëve.

Gjatë vlerësimit nëse proceset e PVB/PRF janë në gjendje të garantojnë dhe mbrojnë besueshmërinë dhe vazhdimësinë e Infrastrukturës së TI-së dhe procesit të biznesit (veprimtarisë), ekzistojnë disa rreziqe të auditimit, në të cilat audituesit mund të përqendrohen gjatë vlerësimit të efektivitetit të një vazhdimësie biznesi (veprimtarie) dhe planit të rimëkëmbjes nga fatkeqësitë. Këto përfshijnë zhvillimin e planeve të rimëkëmbjes nga fatkeqësitë dhe planeve të vazhdimësisë së biznesit për të mbuluar të gjitha fushat funksionale kritike. Nëse rimëkëmbja nga fatkeqësitë të një fushe kritike funksionale rrezikohet, do të rrezikohet vazhdimësia e biznesit (veprimtarisë). Nëse rolet dhe përgjegjësitë nuk janë të qarta dhe nuk janë kuptuar nga personeli përkatës, edhe plani i mirë i vazhdimësisë gjithashtu mund të bëhet joefektiv.

Procedura e vlerësimit të ndikimit të biznesit (veprimtarisë), kontrollet parandaluese dhe mjedisore, dokumentacioni, testimi i planit të vazhdimësisë dhe trajnimi i personelit përkatës të mbështesin zbatimin efektiv të planit të vazhdimësisë së biznesit (veprimtarisë) së organizatës. Siguria e pamjaftueshme në zbatimin e planit të vazhdimësisë së biznesit dhe planit të rimëkëmbjes nga fatkeqësitë paraqesin rrezikun e humbjes së të dhënave, humbjen e kohës së vlefshme dhe kostot tjera për shkak të rimëkëmbjes joefektive në rast të një fatkeqësie.

Shërbimet e jashtme (të kontraktuara) paraqesin një fushë të veçantë rreziku kur PVB dhe PRF nuk janë plotësisht nën kontrollin e organizatës. Ekzistojnë rreziqe të sigurisë së të dhënave, humbjes së të dhënave, trajtimit të paautorizuar dhe rrjedhjeve të të dhënave që duhen adresuar. Vazhdimësia e funksionit përmes ofruesit të shërbimit të jashtëm paraqet rrezik në vetvete qoftë përmes humbjes së njohurive për biznesin (veprimtarinë), pronësinë e procesit dhe si rrjedhojë pamundësinë për të ndryshuar ofruesin e shërbimit në rast të performancës së mangët dhe në raste të tjera mbylljen ose marrjen e shërbimit nga entitetet e tjera.

Matrica e Auditimit

Matrica e auditimit për këtë pjesë mund të gjendet në Shtojcën VI.

Referencat:

1. Manuali i Auditimit të Sistemeve Federale të Informacionit në GAO (FISCAM)
2. Korniza COBIT 4.1, 2007, Instituti i Qeverisjes së TI-së
3. Udhëzuesi i Planifikimit të Emergjencave NIST për Sistemet Federale të Informacionit, Publikimi Special 800-34
4. Roli i audituesit të TI-së në menaxhimin e vazhdimësisë së biznesit, auditori i brendshëm, janar, botim i vitit 2008.

KAPITULLI 7

Siguria e informacionit

Çfarë është siguria e sistemit të informacionit

Siguria e Informacionit mund të përcaktohet si mundësia e një sistemi për të mbrojtur informacionin dhe burimet e sistemit në pajtim me termat e konfidencialitetit dhe integritetit. Mbrojtja e informacionit dhe sistemeve të inforamcionit ndaj qasjes ose modifikimeve të paautorizuara të informatës kryhet në ruajtje, procesim ose transferim. Siguria e informacionit përfshin ata parametra të nevojshëm për tu identifikuar, dokumentuar dhe numëruar të tillë si kërcënime. Siguria e informacionit lejon një organizatë të mbrojë Infrastrukturën e Sistemit të Informacionit nga përdoruesit e paautorizuar. Siguria e informacionit përbëhet nga siguria e kompjuterit dhe siguria e komunikimit.

Një aspekt themelor i qeverisjes së TI-së është siguria e informacionit për të siguruar **disponueshmërinë**, **konfidencialitetin** dhe **integritetin**- mbi të cilat çdo gjë tjetër mbështetet. Siguria e informacionit duhet të jetë shumë domethënëse për organizatën. Është rojtari i aseteve të informacionit të kompanisë. Kjo lidhet me atë që programi i sigurisë së informacionit të mbrojë të dhënat organizative duke bërë të mundur që ndërmarrja të ndjekë objektivat e saj të biznesit dhe të tolerojë një nivel të pranueshëm rreziku në këtë veprim. Garantimi i informacionit ndaj atyre që duhet ta kenë është aq e rëndësishme sa mbrojtja e tij ndaj atyre që s'duhet ta kenë. Siguria duhet të jetë në funksion të biznesit dhe duhet të mbështesë objektivat e tij dhe jo t'i shërbejë vetvetes.

Domosdoshmëria e Sigurisë së Informacionit

Siguria e Informacionit është bërë gjithnjë e më shumë e rëndësishme për institucionet qeveritare, kjo si pasojë rritjes së kompleksitetit të kontrollit të qasjes dhe ruajtjes së konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave nga ndërlidhja e rrjeteve publike me ato private dhe nga shkëmbimi (sharing) i burimeve të informacionit.

Sistemet e informacionit janë bashkime komplekse të teknologjisë, proceseve dhe njerëzve që funksionojnë së bashku për të rregulluar procesimin, ruajtjen dhe transferimin e informacionit për të mbështetur misionin e organizatës dhe funksionet e biznesit. Prandaj, çdo organizatë e ka si detyrim ndërtimin e programit të sigurisë së informacionit.

Objektivi i një programi të sigurisë së sistemit të informacionit është të mbrojë informacionin e organizatës duke reduktuar rrezikun e humbjes së konfidencialitetit, integritetit dhe disponueshmërisë të atij informacioni në një nivel të pranueshëm. Nëse organizata nuk ka një garanci të sigurisë së informacionit, atëherë do të ndeshet me rreziqet dhe kërcënimet e mundshme ndaj operacioneve të organizatës, me arritjen e objektivave të përgjithshëm dhe me ndikimin në besueshmërinë ndaj organizatës.

Me rritjen e potencialit, kompleksitetit dhe rolit të Teknologjisë së Informacionit, Siguria e Informacionit bëhet një çështje e rëndësishme për auditimet e TI-së. Është faktor kritik për aktivitetet e organizatës, sepse dobësitë e sigurisë së informacionit mund të shkaktojnë dëme të ndryshme:

- **Ligjore**- abuzime me kërkesat ligjore dhe rregullatore.
- **Reputacioni**- dëme ndaj pozicionit të organizatës, duke shkaktuar thyerje të besimit, ose duke dëmtuar imazhin e qeverisë ose shtetit.
- **Financiar**- për shembull gjobat, kompensimet, shitje të reduktuara, etj.
- **Produktivitetit**- reduktimi i efektivitetit dhe/ose efikasistetit të projektit, programit ose të gjithë shërbimit të ofruar nga organizata.
- **Cenueshmëri**- sistemet dhe të dhënat e qasshme në një mënyrë të paautorizuar janë të prirur për infektimin nga malware[26] dhe të hapur për ndërhyrje të tjera.

Këto dëme mund të shkaktohen nga:

- Thyerje të sigurisë, të zbuluara ose jo
- Lidhje të paautorizuara me ndërtesa (remote site) të largëta
- Ekspozim i informacionit- zbulimi i aseteve të korporatës dhe informacionit të ndjeshëm ndaj palëve të paautorizuara.

Formimi i Kulturës së Sigurisë së Informacionit

Përcaktues për suksesin e programeve të sigurisë së informacionit në një organizatë, është krijimi i kulturës së organizatës e cila trajton çështjet e sigurisë. Për të trajtuar në mënyrë të njëtrajtshme këto dhe çështje të tjera në një organizatë të madhe, duhet të ndiqet një model biznesi i sigurisë së informacionit[27]. Elementët përfshijnë:

Krijimin e ndërgjegjësimit ndaj sigurisë: konsiston (qëndron/përbëhet) në aktivitete të ndërgjegjësimit mbi sigurinë e informacionit dhe sesioneve të edukimit për punonjësit. Këto sesione janë mundësi të mira të fillohet me prezantimin e përgjegjësive të tyre mbi sigurinë e informacionit. Funksioni i burimeve njerëzore mund të jetë përgjegjës për trajnimin fillestar të ndërgjegjësimit të punonjësve të rinj. Trajnimi duhet të zhvillohet gjatë punësimit të tyre dhe deri në shkëputje te marrëdhënies se punes duhet gjithnjë të promovohet ndërgjegjësimi i sigurisë.

Kërkimi për angazhimin e menaxhmentit: angazhimi i menaxhmentit është një element unik në formimin e kulturës së sigurisë së informacionit. Angazhimi shfaqet jo vetëm në përgatitjen e dokumentacionit zyrtar të politikave të sigurisë së informacionit, por edhe në përfshirjen aktive dhe pranisë së tyre në organizatë. Nëse menaxhmenti nuk mbështet programin e sigurisë së informacionit, mund të dekurajojë ndjenjën e përgjegjësisë dhe obligimit të punonjësve dhe cdo iniciativë tjetër me programin. Në këtë mënyrë, është esenciale për menaxhmentin të pranojë pronësinë mbi sigurinë e informacionit dhe të mbështesë plotësisht programin.

[26] Malware është çdo softuer i krijuar qëllimisht për të shkaktuar dëme në një kompjuter, server, klient ose rrjet kompjuteri

[27] ISACA Business Model for Information Security, 2010

Ndërtimi i një koordinimi të fortë duke vendosur grupe ndër-funksionale (cross-function): Siguria e informacionit përfshin shumë aspekte të organizatës, të cilat kërkojnë koordinim. Kështu që duhet marrë në konsideratë ngritja e grupeve me funksione të kryqëzuara/ndër-funksionale. Përdorimi i këtyre grupeve inkurajon komunikimin, bashkëveprimin dhe redukton izolimin në departamente dhe dyfishimin e përpjekjeve.

Ndërtimi i kulturës së sigurisë së informacionit, është një pjesë integrale e implementimit të qeverisjes brenda sektorit të SI dhe karakterizohet nga tipare të ndryshme të cilat janë:

- **Lidhja në mes të sigurisë së informacionit dhe objektivave të biznesit:** Është e nevojshme lidhja në mes të sigurisë së informacionit dhe objektivave të biznesit, gjë e cila mundëson dhe mbështet objektivat e biznesit. Programi i sigurisë së informacionit është në pajtim me organizatën dhe kërkon kontrolle të sigurisë së informacioni për të qenë praktik dhe për të ofruar reduktim real dhe të matshëm të rrezikut.
- **Vlerësimi i rrezikut:** Aplikimi i sigurisë së informacionit duhet të plotësohet përmes vlerësimit të rrezikut, për të përcaktuar formën e kontrollit të domosdoshëm. Shpesh vlerësimi i rrezikut injorohet, i cili mund të rezultojë në zvogëlimin e nivelit të mbrojtjes së infrastrukturës dhe informacionit të ndjeshëm, apo në disa raste edhe mbrojtje më të lartë të panevojshme. Aplikimi i vlerësimit të rrezikut do të ndihmojë menaxhmentin të përzgjedhë kontrollet e duhura për të reduktuar rrezikun efektivisht.

  Procesi i vlerësimit të rrezikut përfshin identifikimin dhe analizën e:

  - të gjitha aseteve dhe proceseve të lidhura me sistemin;
  - kërcënimet e mundshme që mund të ndikojnë konfidencialitetin, integritetin ose disponueshmërinë e sistemit;
  - dobësitë e sistemit dhe kërcënimet e shoqëruara;
  - ndikimet dhe rreziqet e mundshme nga aktivitetet kërcënuese;
  - kërkesat e mbrojtjes për reduktimin e rreziqeve;
  - përzgjedhje e masave të duhura të sigurisë dhe analiza e marrëdhënieve me rrezikun.

- **Balanca në mes të organizatës, njerëzve, proceseve dhe teknologjisë:** Siguria efektive e informacionit kërkon mbështetje organizative, staf kompetent, procese efikase dhe përzgjedhje të përshtatshme të teknologjisë. Secili element ndërvepron me një tjetër në zonë tjetër, ndikon dhe mbështet elementët e tjerë, shpesh në mënyra komplekse, në mënyrë që të arrihet një balancë në mes tyre. Nëse një prej elementeve është jo efikas, siguria e informacionit reduktohet.

Elementet kyçe për Sigurinë e Informacionit

a. Mjedisi i sigurisë së informacionit

Për të mbështetur implementimin e suksesshëm të Sigurisë efektive të Informacionit, ekzistojnë disa elemente thelbësore për tu arritur:

- **Konfidencialiteti** është mbajtja (preserving) i kufizimeve të autorizuara mbi qasjen dhe zbulimin e informacionit, përfshirë mjetet e mbrojtjes së privatësisë personale dhe pronësisë së informacionit. Aspektet e konfidencialitetit janë shumë të rëndësishme sepse përmbajnë çështje të privatësisë që duhet të parashikohen. Për të mirëmbajtur në mënyrë konstante, sistemi duhet të sigurohet se çdo individ ka të drejtën e kontrollit se çfarë informacioni grumbullohet mbi ta, si përdoret, kush e përdor, kush e mirëmban dhe për çfarë qëllimi përdoret.
- **Integriteti** është ruajtja e informacionit kundrejt modifikimeve ose shkatërrimit, të cilat përfshijnë sigurimin e informacionit nga mosnjohja dhe autenticiteti. Për të certifikuar integritetin e informacionit, nevojitet një mekanizëm autenticiteti për të siguruar se përdoruesit janë personat që pretendojnë se janë. Ndërkohë procesi i sigurimit të informacionit të krijuar ose të transmetuar ka nevojë të arrijë kërkesat e mosnjohjes.
- **Disponueshmëria** është sigurimi se të gjitha sistemet e informacionit përfshirë pajisjet, rrjetet e komunikimit, programet aplikative dhe të dhënat që ato mbajnë, do të jenë të gatshme për përdoruesit në kohën e nevojshme për kryerjen e aktiviteteve të biznesit. Duhet gjithashtu të sigurohet afati dhe besueshmëria e qasjes dhe përdorimit të informacionit. Sidoqoftë, plotësimi i parimeve të sigurisë mbi përdorimin e pajisjeve kompjuterike, rrjeteve të komunikimit, programeve aplikativë dhe qasjes në të dhëna do të kërkojë politikat të kontrollit të qasjes. Qëllimi i kontrollit të qasjes është që të sigurojë që përdoruesit të kenë qasje vetëm në ato burime dhe shërbime të cilave u takojnë të drejtat dhe që përdoruesve të kualifikuar nuk u mohohet qasja në shërbime që ata pritet në mënyrë të ligjshme TI-së kenë.

Siguria e informacionit lidhet me minimizimin e ekspozimit, bazuar në menaxhimin e rrezikut, në të gjitha fushat e Qeverisjes së TI-së. Mos implementimi dhe mungesa e monitorimit të procesit të reduktimit të rrezikut në një fushë mund të shkaktojë dëme në të gjithë organizatën. Edhe kur është e ditur se menaxhimi efektiv i rreziqeve të sigurisë së informacionit është esencial për sigurinë e organizatës, këto rreziqe shpesh kapërcehen ose masat paraprake të sigurisë janë të papërditësuara në përgjigje të kushteve të ndryshueshme.

Diskutimi i Sigurisë së Informacionit në organizatë mbulon dymbëdhjetë fusha, të cilat janë:

b. Vlerësimi i rrezikut

Vlerësimi i rrezikut është procesi i identifikimit, analizës dhe vlerësimit të rreziqeve në infrastrukturën e Sigurisë së TI-së. Është procesi i vlerësimit të rreziqeve të lidhura me sigurinë dhe kërcënimet e jashtme ndaj subjektit, aseteve dhe personelit të tij.

c. Politikat e sigurisë

Politikat e sigurisë së organizatës janë grupi i ligjeve, rregullave dhe praktikave që rregullojnë sesi një organizatë menaxhon, mbron dhe shpërndan burimet për të arritur objektivat specifikë të sigurisë. Këto ligje, rregulla dhe praktika duhet të identifikojnë kriteret për autoritetin përkatës të individëve dhe mund të specifikojnë kushtet nën të cilat këta individë janë të lejuar të ushtrojnë autoritetin e tyre. Më qartë, këto ligje, rregulla dhe praktika duhet të ofrojnë ndaj individëve aftësi të arsyeshme për të përcaktuar nëse veprimet e tyre bien ndesh ose përputhen me politikat.

Një formë e rekomanduar e politikave të sigurisë të TI-së jepet më poshtë:

Elementet e një Politike të Sigurisë së TI-së	○ Përkufizim i sigurisë së informacionit- objektivat dhe qëllimi (përfshirë konfidencialiteti i të dhënave)
	○ Parimet, standardet dhe kërkesat e detajuara të pajtueshmërisë ○ Personeli i departamentit të TI-së duhet të mos ketë përgjegjësi operacionale ose të kontabilitetit
	○ Përkufizim të përgjegjësive të përgjithshme dhe specifike për të gjitha aspektet e sigurisë së informacionit
	○ Përdorimi i aseteve të informacionit dhe qasjes në email, Internet
	○ Mënyra dhe metodat e qasjes
	○ Procedurat e backup-it
	○ Elemente të trajnimit dhe të edukimit mbi sigurinë
	○ Procesi për raportimin e incidenteve të dyshimta të sigurisë
	○ Planet e vazhdueshmërisë së biznesit
	○ Procedurat e trajtimit të programeve me ndikim negativ
	○ Metodat e komunikimit me stafin mbi politikat dhe procedurat e përshtatura për sigurinë e SI

d. Organizimi i sigurisë së TI-së

Organizimi i sigurisë së TI-së përfshin implementimin e politikave të sigurisë në subjekt. Kjo mund të jetë puna e dhënë ndaj një njësie ose individi, i cili punon në strukturën e TI-së për të blerë mjetet e përshtatshme dhe për të implementuar proceset e duhura të cilat zbatojnë politikat e sigurisë. Ata janë gjithashtu përgjegjës për ofrimin e trajnimeve fillestare dhe rifreskuese ndaj stafit dhe për adresimin e incidenteve të sigurisë. Ekziston gjithashtu nevoja për sigurimin e mbrojtjes së të dhënave të organizatës që transferohen jashtë njësisë. Audituesi duhet të shohë nëse subjekti ka aftësi të implementojë kërkesat e sigurisë së TI-së, siç janë të dokumentuara nga organizata.

e. Menaxhimi i komunikimeve dhe operacioneve

Subjekti duhet të mbajë gjurmë mbi proceset dhe procedurat që përdor për operacionet e tij të biznesit. Kjo gjë përfshin një grup të procedurave dhe proceseve organizative që sigurojnë përpunim korrekt të të dhënave në organizatë. Gjithashtu përfshin procedurat e dokumentimit mbi të dhënat, kanalet e komunikimit, procedurat e emergjencave, regjistrimin e sigurtë në rrjet dhe procedurat e backup-it.

f. Menaxhimi i aseteve

Menaxhimi i aseteve i referohet çdo elementi të afërt të sistemit që ka vlerë për subjektin apo grupin që monitorohet apo mirëmbahet. Menaxhimi i aseteve është një proces sistematik i operimit, mirëmbajtjes, zhvillimit dhe rregullimit të efektivitetit të kostos së aseteve.

Për Teknologjinë e Informacionit, menaxhimi i aseteve përfshin mirëmbajtjen e një inventari të saktë të pajisjeve TI-së, duke ditur se licencat janë për pajisjet përkatëse, mirëmbajtjen dhe mbrojtjen (kyçjen, dhomat e kontrolluara, etj.) e pajisjeve. Menaxhimi i aseteve të TI-së përfshin gjithashtu menaxhimin e programeve dhe dokumentacionin e proceseve që janë të vlefshme për subjektin.

Për një subjekt shtetëror menaxhimi i aseteve të TI-së është shumë i rëndësishëm në mjedisin aktual fiskal, pasi kufizimet financiare mund të mos lejojnë zëvendësimin e aseteve të vjedhura ose të humbura në mënyrën më të arsyeshme. Për më tepër, organizata mund të jetë në rrezik nëse ata nuk kanë një inventar të plotë të pasurive të tyre kur ata kanë nevojë për përditësime softuerike për të përmbushur nevojat e ardhshme të biznesit.

g. Siguria e burimeve njerëzore

Punonjësit që merren me të dhënat personale në një organizatë kanë nevojë për trajnime të përshtatshme të ndërgjegjësimit dhe përditësime të rregullta në përpjekje për të ruajtur të dhënat që atyre u janë besuar. Detyra dhe përgjegjësitë përkatëse të caktuara për çdo pozicion pune, kanë nevojë të përcaktohen dhe dokumentohen në pajtim me politikat e sigurisë së organizatës. Të dhënat e institucionit duhet të ruhen nga qasjet e paautorizuara, zbulimi, modifikimi, ndërprerja dhe ndërveprimi. Menaxhimi i sigurisë së burimeve njerëzore dhe rreziqeve të privatësisë është i nevojshëm përgjatë të gjitha fazave të punësimit në një organizatë. Tre fushat e Sigurisë së Burimeve Njerëzore janë:

- **Para-punësimi:** Kjo fazë përfshin përcaktimin e roleve dhe përgjegjësive të vendit të punës, përcaktimin e qasjes së duhur në informacione të ndjeshme për vendin e punës dhe përcaktimin e thellësisë së niveleve të kontrollimit të kandidatit - të gjitha në pajtim me politikën e sigurisë së TI-së të kompanisë. Përgjatë kësaj faze, duhet të vendosen gjithashtu edhe kushtet e kontratës.
- **Përgjatë punësimit:** Punonjësit me qasje në informacionin sensitiv në një organizatë duhet të marrin njoftime periodike mbi përgjegjësitë e tyre si dhe të ndjekin trajnime periodike të ndërgjegjësimit mbi sigurinë për të siguruar njohjen e tyre me kërcënimet aktuale dhe me praktikat korresponduese të sigurisë për të reduktuar këto rreziqe.
- **Shkëputja apo ndryshimi i marrëdhënieve të punësimit:** Për të parandaluar qasje në informacionin sensitiv, qasjet duhet të ndërpriten menjëherë. Kjo përfshin kthimin e çdo aseti në organizatë, aset i cili mbahej nga punonjësi.

Duhet të ekzistoj një program i ndërgjegjësimit mbi sigurinë, duke i kujtuar të gjithë stafit mbi rreziqet e mundshme dhe ekspozimin dhe përgjegjësitë e tyre si kujdestarë të informacionit të organizatës.

h. Siguria fizike dhe mjedisore

Siguria fizike përshkruan masat që janë hartuar për të mohuar qasjen e personelit të paautorizuar (përfshirë sulmet ose ndërhyrjet aksidentale) nga hyrja e paautorizuar në ndërtesë, objekte, burime ose informacionin e ruajtur; dhe udhëzime mbi mënyrën sesi duhet të hartohen strukturat që t'i rezistojnë akteve me ndikim të keq. Siguria fizike mund të jetë aq e thjeshtë sa një derë e mbyllur ose aq e përpunuar sa shtresa të shumta të pengesave, roje të armatosura të sigurisë dhe vendosja e rrethojës.

Siguria fizike lidhet së pari me kufizimin e qasjes fizike për persona të paautorizuar (zakonisht quhen ndërhyrës) ndaj objekteve në kontroll, edhe pse ka shumë raste kur masat e sigurisë fizike janë të vlefshme (për shembull, qasje e limituar ndaj objekteve dhe/ose aseteve specifike, kontrolleve mjedisore për të reduktuar incidentet fizike të tilla si zjarre dhe rrjedhje).

Siguria shoqërohet me kosto dhe në realitet, nuk mund të jetë kurrë perfekte ose e plotë me fjalë të tjera, siguria mund të reduktojë por nuk mund të eliminojë totalisht rreziqet. Duke qenë se kontrollet nuk janë perfekte, siguria e fuqishme fizike aplikon parimin e mbrojtjes në thellësi duke përdorur kombinime të përshtatshme të kontrolleve plotësues dhe bllokues. Për shembull, kontrollet e qasjes fizike për mbrojtjen e objekteve përgjithësisht kanë për qëllim të:

- ndalojnë ndërhyrësit e mundshëm (p.sh. shenjat paralajmëruese dhe shënjuesit e perimetrit);
- dallojnë personat e autorizuar nga ata të paautorizuar (p.sh. duke përdorur karta/çelësa);
- vonojnë/shpërqendrojnë ose idealisht parandalojnë përpjekjet për ndërhyrje (p.sh. mure të fortë, kyçe dyersh dhe roje);
- zbulojnë ndërhyrjet dhe monitorojnë/regjistrojnë ndërhyrësit (p.sh. alarmet e ndërhyrjes dhe sistemet e video vezhgimit);
- nxisin reagimet e duhura ndaj incidenteve (p.sh. rojet e sigurisë dhe policia).

i. Kontrolli i qasjes

Kontrolli i qasjes i referohet ushtrimit të kontrollit mbi ata që mund të ndërveprojnë me burimet. Shpesh por jo gjithnjë, kjo përfshin një autoritet, i cili kryen kontrollin. Burimi mund të jetë një ndërtesë, grup ndërtesash, ose një sistem i TI-së i bazuar në kompjuter. Kontrolli i qasjes-mund të jetë fizik ose logjik, në realitet, është një fenomen i përditshëm. Një kyçje në derën e makinës është një formë e thjeshtë e kontrollit të qasjes. Një PIN në një sistem ATM në një bankë është një mjet tjetër i kontrollit të qasjes ashtu si edhe pajisjet biometrike. Posedimi i kontrollit të qasjes është i rëndësisë së parë kur personat kërkojnë një informacion ose pajisje të rëndësishme, konfidenciale ose sensitive.

Në një mjedis shtetëror, kontrolli i qasjes është i rëndësishëm sepse shumë subjekte publike përpunojnë të dhëna sensitive dhe çështjet e privatësisë limitojnë se cilët persona duhet të shohin pjesë të ndryshme të informacionit. Kontrolli i qasjes siguron se vetëm përdoruesit me kredencialet e duhura kanë qasje në të dhënat sensitive.

j. Blerja, Zhvillimi dhe mirëmbajta e sistemeve të TI-së

Cikli i jetës së zhvillimit të sistemit (SDLC), ose procesi i zhvillimit të softuerit në inxhinierinë e sistemeve, sistemet e TI-së dhe inxhinieria softuerike, është një proces i krijimit ose alternimit të sistemeve të TI-së, dhe modeleve e metodologjive që përdorin njerëzit për zhvillimin e këtyre sistemeve. Në inxhinierinë softuerike, koncepti i SDLC lidhet me shumë lloje të metodologjive të zhvillimit të programeve. Këto metodologji formojnë strukturën për planifikimin dhe kontrollin e krijimit të sistemit të TI-së ose të procesit të zhvillimit të sistemit.

Mirëmbajtja e një sistemi të TI-së gjatë ciklit të tij të jetës përfshin ndryshime dhe azhurnime në sistem si rezultat i kërkesave të reja, rregullimi i gabimeve të sistemit dhe përmirësimet e bëra si rezultat i ndërfaqeve të reja.

Zhvillimi i sistemit përfshin ndryshimet dhe zhvillimet përpara ndarjes ose largimit të sistemit. Mirëmbajtja e sistemit është një aspekt i rëndësishëm i SDLC. Me ndërrimin e pozicionit të punës së punonjësve kryesorë në organizatë, ndryshime të reja do të implementohen, të cilat do të kërkojnë sistem.

k. Menaxhimi i incidenteve të sigurisë së TI-së

Në fushat e sigurisë kompjuterike dhe në teknologjinë e informacionit, menaxhimi i incidenteve të sigurisë së TI-së përfshin monitorimin dhe zbulimin e ngjarjeve të sigurisë në një kompjuter ose rrjet kompjuterash, si dhe ekzekutimin e reagimit të përshtatshëm ndaj këtyre ndodhive. Menaxhimi i incidenteve të sigurisë së TI-së është një formë e specializuar në menaxhimin e incidenteve.

l. Menaxhimi i vazhdimësisë së biznesit

Planifikimi i vazhdimësisë së biznesit është procesi që një organizatë përdor për të planifikuar dhe testuar rimëkëmbjen e proceseve të biznesit pas një ndërprerjeje. Përshkruan gjithashtu sesi një organizatë do të vazhdojë funksionin e saj nën kushte të pafavorshme që mund të lindin (për shembull katastrofa natyrore ose të tjera).

m. Përputhshmëria

Audituesi i TI-së duhet të rishikojë dhe të vlerësojë pajtueshmërinë në të gjitha kërkesat e jashtme dhe të brendshme (ligjore, cilësia e mjedisit dhe e informacionit, sigurinë).

Rreziqet e subjektit nën auditim

Politikat, procedurat e sigurisë së TI-së, dhe zbatimi i tyre mundëson që një organizatë të mbrojë infrastrukturën e saj të TI-së nga përdoruesit e paautorizuar. Politikat e sigurisë së TI-së për një organizatë shpalosin kërkesat e nivelit të lartë për organizatën dhe punonjësit e saj, në mënyrë që të ndiqet ruajtja e aseteve kritike. Ofron gjithashtu trajnim të stafit mbi sigurinë dhe siguron se ndiqen procedurat e vendosura për qasjen dhe kontrollin e të dhënave. Përveç kësaj, politikat e sigurisë së SI i referohen ligjeve dhe rregullave të tjera që organizata duhet të ndjek. Ekzistojnë gjithashtu shumë pengesa që organizatat hasin në lidhje me implementimin e sigurisë efektive të informacionit. Në

mungesë të një qeverisje efektive për të trajtuar këto pengesa, siguria e TI-së do të ketë një rrezik të lartë të dështimit në arritjen e objektivave të organizatës.

Çdo organizatë has në sfidat e veta unike, për sa kohë që mjedisi i tyre, politikat, pozicioni gjeografik, ekonomik dhe social ndryshon. Çdo njëri prej këtyre elementëve mund të paraqesë një pengesë në ofrimin e qeverisjes efektive të TI-së dhe është përgjegjësia e audituesit të TI-së që të theksojë rreziqet e sigurisë së informacionit në vëmendje të menaxhimit.

Më poshtë listohen disa prej rreziqeve të rëndësishëm në një organizatë:

- zbulimi i paautorizuar i informacionit;
- modifikim ose shkatërrim i paautorizuar i informacionit;
- sulme të sigurisë së SI;
- dëmtim të infrastrukturës së SI;
- ndërprerje të qasjes ose përdorimit të informacionit ose të sistemit të informacionit;
- ndërprerje të përpunimit të sistemit të informacionit;
- vjedhja e të dhënave ose informacionit.

Duke parë për ekspozimin ndaj rreziqeve të subjektit nën auditim, vëmendje e veçantë duhet t'i kushtohet fushave të mëposhtme:

- Strategjive të sigurisë së informacionit të cilat nuk janë në pajtim me kërkesat e TI-së ose të biznesit;
- Politikat që nuk aplikohen në mënyrë uniforme;
- Mospajtueshmërinë me kërkesat e jashtme dhe të brendshme;
- Siguria e informacionit që nuk është përfshirë në mirëmbajtjen e portofoleve të projekteve dhe në proceset e zhvillimit;
- Dizajni i arkitekturës që rezulton në zgjidhje joefektive, joefikase ose të gabuara të sigurisë së informacionit;
- Masa jo të përshtatshme të sigurisë fizike dhe të menaxhimit të aseteve;
- Konfigurim jo adekuat i pajisjeve kompjuterike ose i programeve aplikativë;
- Organizim i pamjaftueshëm i proceseve të sigurisë së informacionit dhe strukturë e papërcaktuar ose konfuze e përgjegjësive të SI;
- Zgjidhje jo të përshtatshme të burimeve njerëzore;
- Përdorimi joefektiv i burimeve financiare të alokuara për sigurinë e informacionit, strukturën e vlerës së sigurisë së informacionit (kost-benefiti) që nuk përputhet me nevojat ose qëllimet e biznesit;
- Siguria e informacionit e pamonitoruar ose e monitoruar jo efektivisht.

Audituesi duhet të fillojë duke vlerësuar saktësinë e metodave të vlerësimit të rrezikut dhe të marrë në konsideratë çështjet e auditimit të lidhura me implementimin e sigurisë së informacionit. Matrica e auditimit do të ndihmojë audituesin të ngrisë pyetjet e auditimit, kriteret për vlerësim, dokumentet e

kërkuara dhe analizat teknike që mund të përdoren. Në fund, audituesi mund të zhvillojë një program të detajuar të auditimit në përputhje me nevojat dhe zhvillimet përgjatë fushës së punës së auditimit.

Gjatë kryerjes së auditimit të sigurisë së informacionit, audituesi duhet të adresojë çështjet që lidhen me dymbëdhjetë fushat në sigurinë e informacionit.

Matrica e auditimit

Matrica e auditimit për këtë seksion mund të gjendet në Shtojcën VII.

Referencat/ lexim të mëtejshëm

1. ISISA 5310 Metodologjia e Rishikimit të Sigurisë së Sistemeve të Informacionit
2. ISO 27000 Sistemi i Menaxhimit të Sigurisë së Informacionit
3. ISO 27005 Menaxhimi i Rrezikut të Sigurisë së Informacionit
4. Struktura e Rrezikut TI-së ISACA
5. COBIT 4.1, 2007, Instituti i Qeverisjes TI
6. COBIT 5, 2012, Isaca
7. ISACA ITAF-Një strukturë profesionale për garantimin e TI-së, SHBA, 2008
8. ISACA Auditimi i Sigurisë së Informacionit/Programi i Garancisë, 2010
9. ISACA Auditimi i Menaxhimit të Rrezikut TI/Programi i Garancisë, 2012
10. COSO Struktura e Menaxhimit të Rrezikut të Kompanisë

KAPITULLI 8

Kontrollet e aplikacioneve

Çfarë janë kontrollet e aplikacioneve

Një aplikacion është një program specifik që përdoret për të kryer mbështetur një proces të caktuar biznesi. Mund të përfshijë procedura si manuale ashtu edhe të kompjuterizuara për origjinën e transaksionit, procesimin e të dhënave, mbajtjen e shënimeve dhe përgatitjen e raportit. Çdo subjekt ka një numër aplikacionesh që ekzekutohen që radhiten për nga madhësia në korporata të mëdha-sisteme gjithëpërfshirëse që mund të qasen nga çdo punonjës, në kompani të vogla ku aplikacionet mund të qasen nga vetëm një punonjës. Programi aplikativ mund të jetë një sistem pagesash, një sistem faturimi, një sistem inventarizimi ose, edhe një planifikim i burimeve të ndërmarrjes – enterprise resource planing ERP- i integruar.

Një rishikim i kontrolleve të aplikacioneve i mundëson audituesit t'i ofrojë menaxhmentit një vlerësim të pavarur të eficencës dhe efektivitetit të ndërtimit dhe operimit të kontrolleve të brendshme dhe procedurave operuese të lidhura me automatizimin e proceseve të biznesit, si dhe në identifikimin e aplikacioneve të lidhura me çështje që kërkojnë vëmendje.

Përsa kohë kontrollet e brendshme janë të lidhur ngushtë me transaksione individuale, është më e thjeshtë të shihet se përse testimi i kontrolleve do t'i ofrojë audituesit një garanci mbi saktësinë e funksionaliteteve specifike. Për shembull, testimi i kontrolleve në një aplikacion pagesash, do të ofronte siguri mbi shumën e paguar në llogarinë e klientit. Nuk do të ishte e dukshme që testimi i kontrolleve të përgjithshme të TI-së së klientit (për shembull, procedurat e kontrollit) do të ofronin nivel të përafërt sigurie mbi të njëjtat deklarime të llogarive.

Në varësi të objektivave specifike të auditimit, rishikimi i aplikacioneve mund të ketë qasje të ndryshme. Kështu që mënyra që kontrollet duhet të testohen, mund të ndryshojnë nga një auditim në tjetrin. Për shembull, rishikimi i kontrolleve mund të përqendrohet në pajtueshmërinë ligjore dhe me standartet, në mënyrë që pika kryesore të jetë verifikimi nëse kontrollet e aplikacioneve ndihmojnë në adresimin e këtyre çështjeve. Nga një këndvështrim tjetër, rishikimi i aplikacioneve mund të jetë pjesë e auditimit të performancës, kështu që është e rëndësishme të shihet sesi rregullat e biznesit përkthehen në aplikacion. Gjatë analizës së sigurisë së informacionit, fokusi mund të jetë në kontrollet e aplikacioneve, përgjegjëse për sigurimin e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave.

Hapat që duhet të ndiqen në kryerjen e një rishikimi të kontrolleve të aplikacioneve, mund të përfshijnë një cikël aktivitetesh. Edhe pse mund të jetë interesantë të fillohet nga perspektiva e biznesit, është e rëndësishme të përmendet se nuk ekziston një renditje strikte e këtyre hapave. Disa prej tyre janë përmendur më poshtë dhe janë përshkruar shkurtimisht në seksionet që vijojnë.

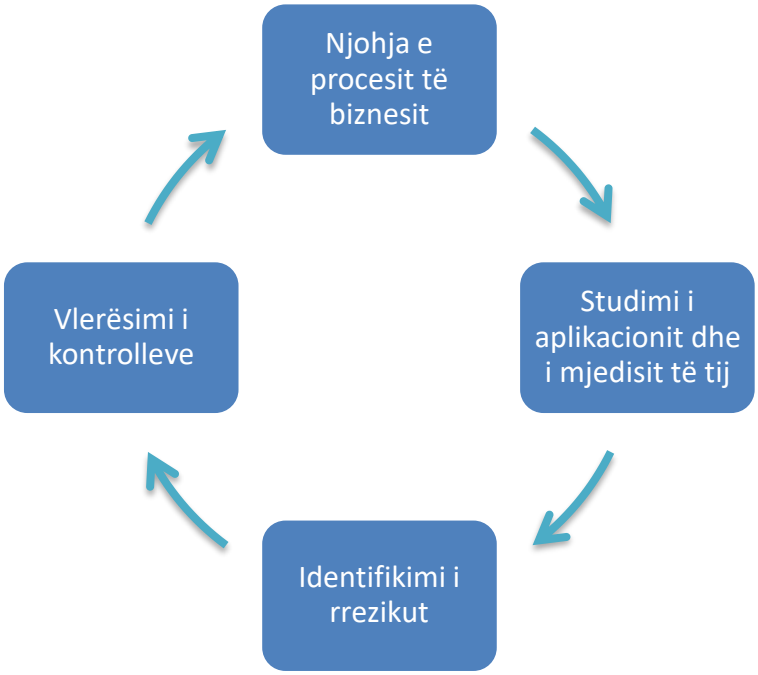


Figura 8.1 Cikli i rishikimit të aplikacionit

- **Njohja e procesit të biznesit:** përpara hulumtimit në çështje teknike lidhur me aplikacionet, do të ishte e dobishme të konsideronim një rishikim të proceseve të automatizuara nga aplikacionet-rregullat e tij, rrjedhjen e informacionit, detyrat dhe kërkesat lidhur me pajtueshmërinë. Të kuptuarit e biznesit themelor është një hap i rëndësishëm për të mundësuar të verifikohet konsistenca e kontrolleve të aplikacionit dhe proceset e automatizuara. Shtrirja e këtij hapi do të ndryshoj sipas objektivave të auditimit. Zakonisht bëhet përmes studimit të procedurave operative/të punës, grafikut të rrjedhës së procesit të organizatës ose materialit tjetër referencë. Ekipi i auditimit gjithashtu mund të ketë nevojë të takojë dhe intervistojë menaxherët e biznesit, drejtuesit e TI-së dhe përdoruesit kryesorë të aplikacionit.
- **Studimi i aplikacionit dhe mjedisit të tij:** studioni dizajnimin dhe sjelljen e aplikacionit ose duke rishikuar dokumentacionin (diagramat organizative, diagramat e rrjedhjes së të dhënave, manualet e përdorimit) ose duke intervistuar personelin kryesor. Studioni funksionet kyçe të programeve në punë duke observuar dhe bashkëpunuar me personelin operues gjatë punës. Gjatë diskutimeve, kryhet një kontrollë fizike e proceseve dhe aplikacioneve të biznesit nga hyrja burimore drejt përfundimit dhe barazimit për të parë sesi proceset rrjedhin dhe observohet çdo aktivitet manual të lidhur me to që mund të veproj si kontrollë plotësuese. Të diskutohet me menaxherët, operatorët dhe zhvilluesit, si dhe të mbahet dokumentacion mbi infrastrukturën teknike: sistemin operativ, mjedisin e rrjetave, sistemin e menaxhimit të bazës së të dhënave, bashkëveprimi me aplikacionet e tjera, burimet e brendshme ose të jashtme, hyrja e batch-it/koha reale/ procesimi online i transaksioneve. Kjo gjë jep një tregues sesi infrastruktura teknike ndikon mbi aplikacion.
- **Identifikimi i rrezikut:** më së shumti të identifikohen rreziqet e lidhura me aktivitetet/funksionet e biznesit që ofrohen nga aplikacionet (çfarë mund të shkojë keq?) dhe të shihet sesi këto rreziqe

menaxhohen nga programet (çfarë e kontrollon?). Ndonjëherë, një vlerësim i rrezikut të procesit të biznesit mund të jetë i disponueshëm (mund të ishte bërë nga një auditim i mëparshëm, auditim i brendshëm ose nga menaxhmenti) dhe audituesi mund të përfitonte nga përdorimi i tij pasi të vlerësonte besimin e vlerësimit ekzistues të rrezikut.

- **Vlerësimi i kontrolleve:** pas njohjes së mjedisit (të biznesit dhe teknik) që rrethon aplikacionet, audituesi do të jetë më i qartë rreth vlerësimit të kontrolleve të përdorura për adresimin e rreziqeve ekzistues. Audituesi duhet të përdorë gjykimin në vlerësimin e kontrolleve të aplikacioneve dhe duhet të tregojë kujdes në lënien e rekomandimeve për përmirësime. Vlerësimi do të përfshijë vlerësimin e llojeve të ndryshme të kontrolleve të aplikacioneve, të cilat do të përshkruhen në seksionet e mëposhtme.

Elementet kryesore të kontrolleve të aplikacioneve

Kontrollet e aplikaciove janë kontrolle specifike të veçanta për çdo aplikacion kompjuterik. Kur proceset e biznesit janë të automatizuara në aplikacione të TI-së, rregullat e biznesit ndërtohen gjithashtu në aplikacion në formën e kontrolleve të aplikacioneve. Ato aplikohen në segmente të aplikacioneve dhe lidhen me transaksionet dhe të dhënat e qëndrueshme. Ndërkohë që kontrollet e përgjithshme të TI-së në një subjekt vendosin tonin për mjedisin e përgjithshëm të kontrollit për sistemet e informacionit, kontrollet e aplikacioneve janë ndërtuar në aplikacione specifike për të siguruar dhe mbrojtur saktësinë, integritetin, realizueshmërinë dhe konfidencialitetin e informacionit. Ato sigurojnë inicimin e transaksioneve të autorizuara në mënyrën e duhur, procesimin e të dhënave të vlefshme, regjistrimin e plotë dhe raportimin e saktë.

Ilustrim

Në një aplikacion pagese online (shihni figurën e mëposhtme), një kusht hyrës mund të jetë data e skadencës së kartës së kreditit e cila duhet të jetë pas datës së transaksionit. Një tjetër mund të jetë që numri i kartës të jetë i vlefshëm dhe të korrespondojë si me emrin e kartëmbajtësit ashtu edhe me shifrën e verifikimit të kartës (numri CVV). Tjetër mund të jetë që detajet në momentin e transferimit në rrjet të jenë të koduara. Kontrollet e ndërtuara në aplikacion do të sigurojnë që këto kushte të jenë të pathyeshme, duke siguruar vlefshmërinë e transaksioneve.

Figura 8.2: Shembull i Kontrolleve të Aplikacionit

Kontrollet e aplikacioneve përfshijnë procedura manuale të cilat operojnë ngushtë me aplikacionin. Këto kontrolle nuk ndërtohen në aplikacionet specifike, por gjithashtu rrethojnë proceset e biznesit. Për shembull, një nëpunës për regjistrimin e të dhënave mund të kërkojë që një formë e futjes së të dhënave të nënshkruhet (miratohet) përpara se të futet në sistem. Kombinimi i kontrollit manual dhe të automatizuar shpesh është rezultat i konsiderimit të kostove dhe kontrolleve në fazën e ndërtimit të një aplikacioni.

Një aplikacion mund të ndahet në dy segmente: **hyrja** e të dhënave (origjinimi/fillimi dhe hyrja e të dhënave); **përpunimi** i transaksioneve; **dalja** e të dhënave (shpërndarja e rezultateve) dhe siguria (gjurmimi, komunikimet, ruajtja). Kontrollet në një aplikacion ndërtohen në përputhje me kontrollet që kërkojnë kufizim të qasjes ndaj aplikacionit dhe dosjeve.

Edhe pse nuk është reale sigurimi i hapave të testimit të detajuar dhe kontrolleve për çdo ndryshim të mundshëm të një aplikacioni, një auditues i TI-së duhet të ketë njohuri mbi konceptet e kontrollit që janë të përbashkët për të gjithë aplikacionet. Mund të përdoret për të gjeneruar mendime dhe ide lidhur me hapa specifikë auditimi ndaj aplikacionit nën auditim.

Figura 8.3: Kontrollet e Aplikacionit "Elementet Kryesore"

Disa prej elementëve më të zakonshëm të kontrollit janë pasqyruar në tabelën e mëposhtme:

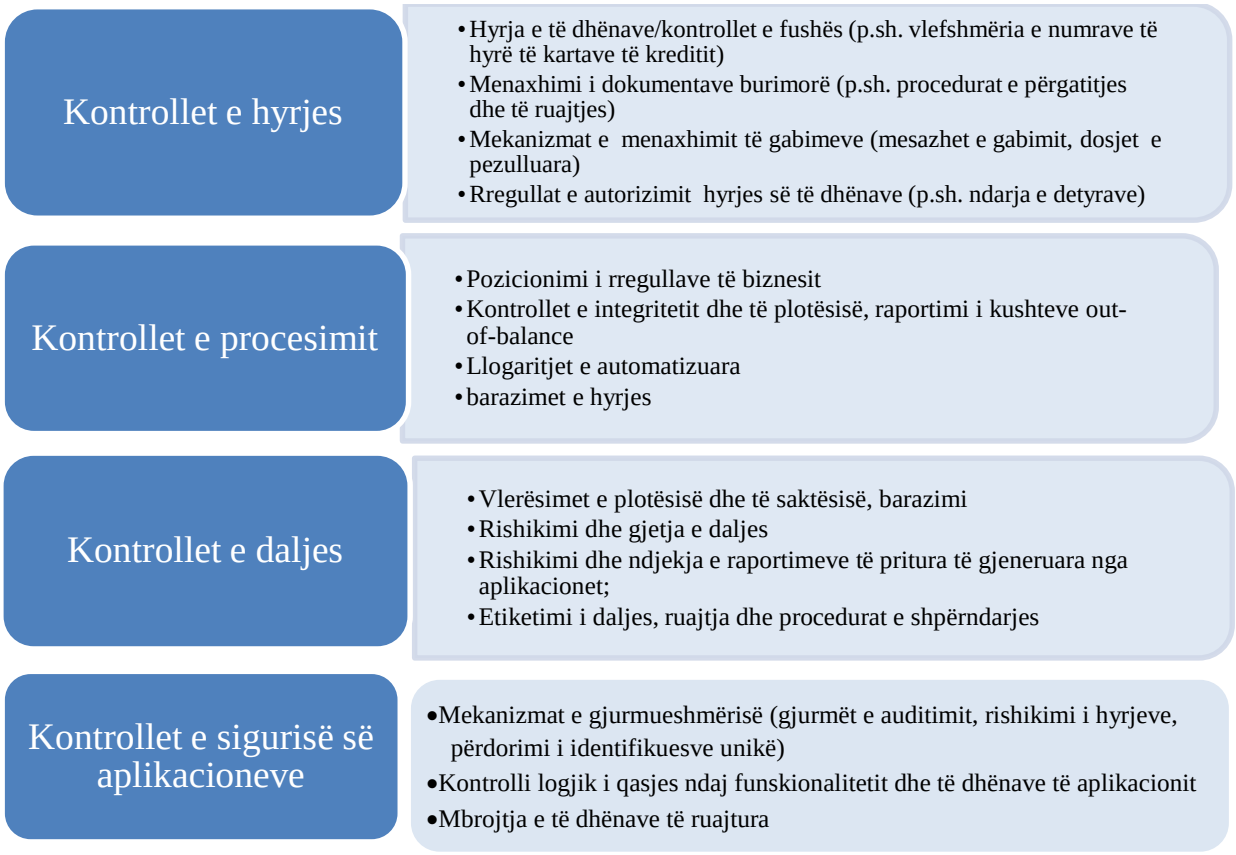


Figura 8.4: Disa shembuj të kontrolleve të aplikacioneve

a. Kontrollet e hyrjes

Objektivat e kontrolleve të hyrjes janë kërkimi për vlefshmërinë dhe origjinalitetin e veprimeve të përgatitjes së të dhënave burimore, autorizimit dhe hyrjes në mënyrë që të dhëna të sakta, të besueshme dhe të plota, të pranohen nga aplikacioni brenda kohës së caktuar.

Një pjesë e konsiderueshme e këtyre masave janë ndërtuar në fazën e zhvillimit të një aplikacioni gjatë fazave të zhvillimit të sistemeve pasi janë formuluar rregullat e biznesit sipas specifikimeve të kërkesave. Ndërkohë që futja e të dhënave mund të jetë manuale ose nëpërmjet ndërfaqes së sistemit, gabime dhe mosveprime mund të minimizohen nëpërmjet formës së mirëndërtuar të hyrjes, ndarjes së duhur të detyrave lidhur me origjinalitetin dhe aprovimin e dokumentave të hyrjes, si dhe vendosjes së autenticitetit të përshtatshëm, kontrolleve të saktësisë dhe plotësisë (me opsione në menu ose mesazhe interaktivë).

Elementët e kontrolleve të hyrjes	Përshkrimi
Kontrolle të hyrjes së të dhënave (vlefshmëri, plotësi, kontrolle të dyfishimeve)	Kontrolle të automatizuara të vlefshmërisë mbi të dhënat e futura (P.sh. data e udhëtimit bie jashtë periudhës së prenotimit); kontrolle të plotësisë për tu siguruar se i gjithë informacioni kyç i transaksioneve është futur (P.sh. data e udhëtimit, emrat e pasagjerëve, numrat e identitetit janë fushat e kërkuara); kontrolle të dyfishimeve krahasojnë transaksionet me ato të postuara më parë (P.sh. kontrolle kundrejt faturave të dyfishuara)
Menaxhimi i dokumentave burimore	Dokumentimi i procedurave të përgatitjes së dokumentave burimorë; logimi i këtyre dokumentave (gjurmueshmëria); numërimi i tyre; procedurat e mbajtjes/ruajtjes së dokumetnave.
Procedurat e menaxhimit të gabimeve	Procedura për trajtimin e hyrjeve jo të lejueshme (P.sh. mesazhe gabimi, masa shtesë korrigjuese, dritare që mundësojnë ri-futjen, përdorimi i dosjeve të pezulluara).
Autorizimi i hyrjeve	Procedura manuale/autorizim në nivel mbikëqyrjeje të të dhënave në formularin e hyrjes së tyre. P.sh. autorizimi i faturës së detajeve të futura nga mbikëqyrësi përpara regjistrimit nga nëpunësi i regjistrimit së të dhënave për procesim në aplikacionet doganore

b. Kontrollet e procesimit/përpunimit

Objektivi i matjeve të kontrolleve të procesimit është kërkimi për mbrojtjen e integritetit, vlefshmërisë dhe besueshmërisë së të dhënave, si dhe mbrojtja e tyre kundrejt gabimeve në procesim gjatë ciklit të përpunimit të transaksionit-nga momenti i marrjes së të dhënës nga nënsistemi i hyrjes deri në momentin që e dhëna dërgohet në bazën e të dhënave, në komunikim ose në nënsistemin e daljes. Ato gjithashtu sigurojnë që e dhëna e vlefshme përpunohet vetëm një herë dhe se zbulimi i transaksioneve të gabuara nuk ndërpret përpunimin e transaksioneve të sakta. Për më tepër, ato kërkojnë të rrisin besueshmërinë e programeve aplikativë që ekzekutojnë instruksione për arritjen e kërkesave specifike të përdoruesve.

Procedurat e kontrollit përfshijnë vendosjen dhe zbatimin e mekanizmave për autorizimin e inicimit të përpunimit të transaksionit dhe për garantimin se vetëm aplikacionet dhe mjetet e duhura dhe të autorizuara janë duke u përdorur. Rregullisht verifikohet se përpunimi është kryer plotësisht dhe në mënyrë të përshtatshme me kontrollet e automatizuara.

Llojet e kontrollit mund të përfshijnë kontrollimin e gabimeve në sekuencat dhe dyfishimet, numërimin e transaksioneve/regjistrimeve, kontrollet e integritetit referencial, totalet e kontrollit dhe hash-it, kontrollet e sferës dhe rrjedhjen e amortizuar. Në sistemet në kohë reale, disa prej kontrolleve kompensues do të ishin një për një kontrollimi, grumbullimi historik, përjashtimi dhe raportimi i llogarive të pezulluara.

c. Kontrollet e daljes

Objektivat e kontrolleve të daljes janë matjet të ndërtuara brenda aplikacionit për tu siguruar se dalja e transaksionit është i plotë, i saktë dhe i shpërndarë në mënyrë korrekte. Ato gjithashtu kanë për qëllim mbrojtjen e të dhënave të përpunuara nga një aplikacion kundrejt modifikimeve dhe shpërndarjeve të paautorizuara.

Proceset e kontrollit përfshijnë përcaktimin e qartë të daljes, raportet e dëshiruara në fazën e ndërtimit të sistemit dhe në fazën e zhvillimit të tij, dokumentimin e saktë të logjikës së nxjerrjes së raportit, kontrollet e hyrjes së kufizuar për mbrojtje të të dhënave, rishikim të daljes, barazimin dhe rishikimin.

d. Kontrollet e sigurisë së aplikacionit

Siguria e aplikacionit lidhet me ruajtjen e konfidencialitetit, integritetit dhe disponueshmërisë së informacionit në elementet e aplikacionit. Për qëllimet e një auditimi, është e rëndësishme të kuptohen bashkëvepruesit, p.sh. burimet e ndryshme të të dhënave në hyrje dhe dalje të aplikacionit si dhe mënyra e ruajtjes së të dhënave.

Pjesa më e madhe e aplikacioneve qasen nëpërmjet ID individuale të përdoruesve dhe fjalëkalimeve të aplikacionit. Sidoqoftë, forma të ndryshme të qasjes, si mekanizma të qasjes së njëhershme, janë bërë më të popullarizuara, duke pasur parasysh madhësinë e aplikacioneve të përdorura në një mjedis të korporatës. Një auditues mund të ketë nevojë të rishikojë politikën dhe procedurat e subjektit për lejimin dhe ndalimin e qasjes së përdoruesit në mënyrë që të kuptojë shkallën në të cilën rregullat e qasjes janë përfshirë në secilën shtresë të aplikacionit dhe për të siguruar që aplikacioni të ketë kontrolle rreth sigurimit të qasjes.

Për të kuptuar procedurat e kontrollit të sigurisë së aplikacionit, audituesit do t'i nevojitet të kuptojë aktorët, detyrat dhe përgjegjësitë e përfshira në aplikacion, si admnistratorët, përdoruesit e priveligjjuar, përdoruesit e zakonshëm, etj. Ndërtimi i modulit të kontrollit të qasjes logjike mund të jetë i llojeve të ndryshme. Shumica e programeve do të kontrollonin kombinimin e ID dhe fjalëkalimit të përdoruesit për të lejuar qasjen. Qasja mund të kontrollohet për secilin modul, opsion të menu-së, ose çdo ndarje kontrollohet nëpërmjet objekteve dhe detyrave. Audituesi i TI-së duhet të rishikojë ndërtimin e modulit të kontrollit të qasjes, duke patur parasysh gjendjen kritike të funksioneve/veprimeve të disponueshme. Për më tepër, është e domosdoshme të njihet mekanizmi i përdorur për sigurimin e autorësisë dhe gjurmueshmërisë së transaksioneve, po ashtu, edhe për mbrojtjen e të dhënave të ruajtura nga aplikacioni.

Më poshtë jepet një listë shembujsh të çështjeve të auditueshme në lidhje me kontrollet e sigurisë së aplikacionit

- Gjurmueshmëria e transaksioneve: gjurmimi i transaksioneve; përdorimi i ID unike të përdoruesve; raportimi dhe monitorimi i gjurmëve; në mënyrë ideale regjistri i auditimit duhet të regjistrojë cilat rekorde ose fusha u ndryshuan, kur ato u ndryshuan, çka është ndryshuar dhe kush e bëri ndryshimin.

- Llogaritë e përdoruesve, menaxhimi i të drejtave dhe fjalëkalimeve: përdorimi i llogarive për vizitorë (guest), test dhe të përgjithshëm; llogaritë e priviliegjuara dhe të administratorit përdorin kontrolle kompensuese; procedura për lejimin dhe anulimin e qasjes; procedura të ndërprerjes së punës dhe të largimit të qasjes; adoptimi i parimit më pak privilegje; qasja e ekipit të TI/zhvillimit në bazat e të dhënave në ambiente produktive; procedura formale për aprovimin dhe lejimin e qasjes; përdorimi i fjalëkalimeve të fuqishme; zbatimi i ndryshimeve sistematike; kodimi i fjalëkalimit, etj.
- Mbrojtja e të dhënave të qëndrueshme dhe masterfile[28]: kontrolle për të siguruar se ndryshimet ndaj të dhënave të qëndrueshme janë të autorizuara; përdoruesit mbeten përgjegjës për çdo ndryshim të bërë; të dhënat e qëndrueshme janë të përditësuara dhe të sakta dhe se integriteti i masterfile ruhet. Shembuj të të dhënave të qëndrueshme: detajet e furnizuesit dhe klientit (emri, adresa, telefoni, numri i llogarisë); normat e inflacionit; të dhëna të administrimit të sistemit, siç janë skedarët e fjalëkalimeve dhe lejet e kontrollit të qasjes etj.
- Detyrat konfliktuese dhe adoptimi i ndarjes së detyrave: detyra të ndryshme për përdorues; të drejta të qasjes të disponueshme për çdo profil përdoruesi; ndarje detyrash.

Rreziqet e subjektit nën auditim

Pasojat e dështimeve të kontrolleve të aplikacionit zakonisht do të varen nga natyra e aplikacionit të biznesit. Rreziqet mund të variojnë nga mospërmbushja e kërkesave të përdoruesit në shkatërrime të mëdha dhe humbje jetësh. Për shembull, organizata mund të humbasë aksione në treg nëse shërbimi shndërrohet në të padisponueshëm; organizata mund të humbasë para nëse sistemet e shitjeve online nuk arrijnë të regjistrojnë porositë online; besueshmëria e qytetarëve në shërbimet qeveritare mund të ulet; mungesa e pajtueshmërisë me standartet ligjore mund të sjellë përballje në gjyq; energjia elektrike mund të mos arrijë shtëpitë e njerëzve; llogaritë bankare mund të jenë të ekspozuara ndaj mashtrimit, etj.

Në mënyrë të veçantë, rreziqet e rëndësishme që mund të ndodhin në mungesë të kontrolleve të duhur të hyrjes janë rreziku i përpunimit të gabuar ose mashtrues dhe aplikacioni nuk do të arrijë të realizojë objektivat e biznesit. Të dhënat e përpunuara nga aplikacioni mund të jenë jo të sakta dhe mund të ofrohet rezultati i pasaktë. Për më tepër, edhe në prani të kontrolleve të tilla, mund të ndodhë të anashkalohen në situata të caktuara. Në këtë rast, duhet të ketë kontrolle kompensuese të tilla si gjurmët dhe rregullat e autorizimit, përndryshe anashkalimi i privilegjit mund të keqpërdoret dhe të çojë në të dhëna jo konsistente për t'u futur në aplikacion.

Procedurat për menaxhimin e dokumenteve burimorë dhe autorizimin e të dhënave të futura, janë gjithashtu të rëndësishme si kontrolle hyrëse. Në mungesë të menaxhimit jo të plotë të dokumenteve burimorë, mund të mos jetë e mundur të ndiqet informacioni burimor i cili ka hyrë në sistem pajtueshmëria ligjore mund të mos arrihet dhe politikat parandaluese mund të shkelen, të dhëna jo të besueshme mund të hyjnë në aplikacion. Në anën tjetër, në mungesë të kontrolleve të autorizimit, të dhëna të paautorizuara mund të sjellin gabime ose mashtrime.

[28] Fajlli kryesor

Në përgjithësi, dështimi në kontrollet e procesimit mund të sjellë gabim të përpunimit dhe dështim në arritjen e qëllimeve të biznesit për aplikacionin. Ato dalin për shkak të planifikimit të pasaktë të rregullave të biznesit, testimit të pamjaftueshëm të kodit të programit ose kontrollit jo adekuat të versioneve të ndryshme të programeve për të rikthyer integritetin e përpunimit pas shfaqjes së një problemi ose ndërprerjes së papritur. Në mungesë të praktikave të nevojshme të kontrollit të përpunimit, mund të përsëriten transaksione të gabuara që ndikojnë në objektivat dhe mbarëvajtjen biznesit.

Me sistemet e përpunimit në kohë reale, krahasohen disa nga masat e kontrollit të tilla si barazimi i totalit të hyrjeve dhe atyre të daljeve për të konstatuar tërësinë e informacionit, për ruajtjen e origjinës së disa të dhënave për gjurmë auditimi, nuk ekzistojnë. Sidoqoftë, sistemet në kohë reale mund të kenë kontrolle të tjerë kompensues brenda aplikacionit, si bashkëveprimi i plotësisë së të dhënave, kërkesat e vlefshmërisë, gjurmimi i përpjekjeve të qasjes, etj.

Mungesa e kontrolleve të duhura të daljes sjell rreziqe të mosautorizimit të fshirjes/modifikimit të të dhënave, krijimin e raporteve të gabuara të menaxhimit dhe thyerje të besueshmërisë së të dhënave. Gjithashtu, rezultatet e gjenerimit të një dalje të gabuar do të varen shumë nga mënyra e përdorimit të informacionit nga biznesi.

Në kontekst të sigurisë së aplikacionit, jo efikasiteti i mekanizmave të gjurmimit mund ta bëjë të pamundur gjurmimin e sjelljeve jo të duhura të autorëve specifik. Gjithashtu, ndërgjegjësimi i përdoruesit mbi ekzistencën e procedurave të rishikimit të gjurmimit dhe mekanizmave të raportimit, mund të zvogëlojë rrezikun e keqpërdorimit të sistemeve të informacionit. Gabimet në të dhënat e qëndrueshme kanë një ndikim largpamës ndaj aplikacionit, për shkak se këto të dhëna mund të përdoren për një sasi të madhe të transaksioneve të aplikacionit.

Aktualisht, rreziku i mostrajtimit të saktë të sigurisë së informacionit shkon përtej kësaj. Mund të sjellë pasoja të ndryshme: humbje të të ardhurave, ndërprerje shërbimi, humbje besueshmërie, ndërprerje biznesi, keqpërdorim informacioni, pasoja ligjore, çështje gjyqësore, abuzim me pronën intelektuale, etj. Këto rreziqe dhe kontrollet e zvogëlimit, trajtohen më me detaje në Kapitullin e Sigurisë së Informacionit.

Matrica e Auditimit

Kjo matricë gjendet në Shtojcën VIII.

Referencat

1. Auditimi i TI-së ISACA dhe Udhëzimi i Sigurisë G38, Kontrollet e Qasjes
2. Manuali i Auditimit TI-së Vëllimi I, ISA i Indisë
3. Auditimi i IT: Përdorimi i Kontrolleve për Mbrojtjen e Aseteve të Informacionit,- Botimi i Dytë nga Chris Davis, Mike Schiller dhe Kevin Wheeler McGraw-Hill/Osborne
4. Singleton, Tommie W. Auditimi i aplikacioneve-Pjesa e dytë, ISACA journal, Vëllimi i IV, 2012

KAPITULLI 9

Çështje të tjera me interes

Ky seksion paraqet një përmbledhje të disa çështjeve lidhur me Auditimin e TI-së, të cilat audituesi mund t'i hasë gjatë kryerjes së auditimit. Ekzistojnë një sasi e madhe e fushave të zhvilluara në TI të cilat mund të kthehen në subjekt të audituesheme. Për këtë, audituesi duhet të jetë i ndërgjegjëshëm për ekzistencën e këtyre fushave dhe të jetë i aftë të ecë përpara në auditim me këto tipe subjektesh.

Ueb-faqe/Portale

Ueb-faqet janë sisteme informacioni të vendosura në internet ose edhe në intranete të cilët garantojnë shërbim dhe përmbajtje si tekst, fotografi, video, audio, etj. Një portal uebi organizon informacionin nga burime të ndryshme në mënyrë uniforme duke garantuar pamje dhe ndjesi të qëndrueshme. Përgjithësisht, portalet e uebit ofrojnë shërbime si makinë kërkimi, lajme, informacion, qasje në sisteme, baza të dhënash dhe zbavitje. Shembuj të portaleve publikë të uebit: AOL, Google, Yahoo, India.com.

Fusha të audituesheme

- Përvoja e përdoruesit;
- Siguria, privatësia;
- Koha e përgjigjes;
- Çështje të lidhura me kontraktimin e jashtëm.

Referencat/ lexim të mëtejshëm

11. http://en.wikipedia.org/wiki/Web_site
12. http://en.wikipedia.org/wiki/Web_portal
13. Kenyon, Geoff. Kontrollet e Auditimit të http://www.seomoz.org/blog/how-to-do-a-site-audit
14. Jones, Harrison. Si të:Udhëzues- për Kryerjen e Auditimit të Website-tit 2011, http://www.techipedia.com/2011/website-audit-guide/

Kompjuterika mobile

Ekziston një përpjekje e shtuar në ofrimin e shërbimeve tek publiku nëpërmjet të gjitha kanaleve të ndryshme të TI-së. Kjo i referohet përdorimit të teknologjive të komunikimit, komunikimet pa tel (wireless) për të garantuar aplikacionet dhe informacionin. Në ditët e sotme, shumë aplikacione ofrohen në mjediset e telefonisë. Celularët, tabletat, rrjetet wi-fi, TV-të dhe një sasi e madhe e pajisjeve dhe mjeteve elektronike ofrojnë informacion. Kompjuterika mobile mund të shihet si një pikë qasje e TI-së (kompjuter, laptop, etj), por ato kanë disa fusha specifike auditimi që mund të jenë të rëndësishme.

Fushat e audituesshme

- Siguria, privatësia, kodimi i rrjeteve wireless;
- Përvoja e përdoruesit;
- Politika specifike lidhur me kompjuterikën mobile në organizatë;
- Rreziqet e përdorimit të pajisjeve personale për tu qasur në të dhëna dhe shërbime të kompanisë;
- Rreziqet e qasjes së paautorizuar ndaj të dhënave që janë në pajisje;
- Rreziqet e rritura të dëmit ose vjedhjes së pajisjeve të kompanisë.

Referencat/lexim të mëtejshëm

1. ISACA Udhëzues të Audimit i TI-së dhe i Sigurisë G27-Kompjuterika Mobile http://www.isaca.org/Knowledge-Center/Standards
2. Auditimi i Sigurisë së Kompjuterizimit të Telefonisë/Programi i Sigurisë, ISACA http://www.isaca.org/audit programs

Auditimi i Forenzik (ose Forenzika Kompjuterike)

Auditimi i forenzik është ai lloj auditimi i cili kryhet për të ekzaminuar mediat dixhitale mbi provat referuar një hetimi ose mosmarrëveshje. Mbrojtja e provave është analiza më e rëndësishme e forenzikës kompjuterike. Përfshinë qasjen, mjetet dhe teknikat e ekzaminimit të informacionit dixhital për identifikimin, ruajtjen, rimëkëmbjen, analizimin dhe paraqitjen e fakteve dhe mendimeve mbi informacionin e ruajtur.

Është më së shumti e lidhur me hetimin e krimit në mënyrë që të ndihmojë zbatimin e ligjit dhe të garantojë prova të forta në seanca gjyqësore. Forenzika kompjuterike është aplikuar në një numër të lartë të fushave, por jo i kufizuar, në mashtrim, spiunazh, vrasje, kërcënime, keqpërdorime të kompjuterave, abuzime me teknologjitë, shpifjet, emaile me qëllime të këqija, rrjedhje informacioni, vjedhje e pronës intelektuale, pornografi, pirateri dhe transferta të paligjshme të parave.

Fushat e audituesshme

Disiplina përfshin teknika dhe parime të ngjashme me rimëkëmbjen e të dhënave, por me udhëzime dhe praktika shtesë të ndërtuara për të krijuar gjurmë ligjore të auditimit.

- Ruajtja e provave (të dhëna, qasje, gjurmë) për analiza;
- Kapja dhe ruajtja e të dhënave sa më afër thyerjes (shkeljes) së ligjit që është e mundur;
- Standartet e grumbullimit të të dhënave për përdorim të mundshëm të zbatimit të ligjit;
- Procesi i kapjes së të dhënave minimale invazive pa ndërprerjen e operacioneve të biznesit;
- Identifikim i sulmuesve nëse është e mundur.

Referencat/ lexim të mëtejshëm

1. ISACA Udhëzues të Audimit të IT dhe të Sigurisë G27-Kompjuterika Mobile http://www.isaca.org/Knowledge-Center/Standards
2. Ekzaminimi i mjekësisë ligjore të të dhënave dixhitale: Një udhëzues për zbatimin e ligjit http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
3. Hetimi i Skemës së Krimit Elektronik: Një Udhëzues i Praktikës së Mirë për Provat Elektronike të Bazuara në Kompjuter http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf
4. Kompjuterizimi i Mjekësisë Ligjore. Wikipedia http://en.wikipedia.org/wiki/Computer_forensics

Qeveri elektronike, Qeverisje elektronike dhe Qeverisje mobile (eGov, e-Gov dhe m-Gov)

Zhvillimi i teknologjisë së informacionit ka ndryshuar në mënyrë depërtuese mbi atë sesi qeveritë ofrojnë shërbime ndaj qytetarëve të tyre. Ndërkohë që teknologjia shpërndahet në mes popullatës, qeveritë janë të ndërgjegjshme ndaj qasjeve të reja për ofrimin e informacionit dhe aplikacioneve për përfitim të publikut. Qeveritë elektronike, qeverisjet elektronike (të njohura si eGov ose e-gov) dhe qeverisjet mobile janë disa nga fushat që trajtohen në këtë subjekt. Këto koncepte janë të lidhura, edhe pse jo sinomime në mënyrë perfekte.

Fushat e auditimit

Për qëllime auditimi, audituesi duhet të jetë vigjilent/i vetëdishëm që qeverive përgjithësisht iu kërkohet të ofrojnë shërbime në mënyrë efektive, efikase dhe ekonomike. Shpesh, ofrimi i shërbimeve elektronike mundëson zgjidhjen më të zgjuar me kosto të arsyeshme.

Në perspektivën e auditimit, auditimi i sistemeve të informacionit ose të proceseve të biznesit të përfshira në një strategji e-gov ose m-gov, nuk ndryshon nga auditimet tradicionale të TI-së. Audituesi mund të ketë nevojë të shikojë disa politika shtesë dhe mekanizma zbatimi (për shembull, një politikë organizative për kompjuterikën mobile, programin e enkriptimit, duke kufizuar përdorimin e telefonit inteligjent personal, etj.).

Referencat/ lexim të mëtejshëm

1. Qeverisja elektronike. Wikipedia;
2. http://en.wikipedia.org/wiki/E-Governance;
3. Qeverisja telefonike. Ministria e Komunikacionit dhe Teknologjisë së Informacionit. Qeveria Indiane;
4. http://mgov.gov.in/msdpbasic.jsp;
5. Studim mbi E-Qeverisje Kombet e Bashkuara;
6. http://www2.unpan.org/egovkb/global_reports/10report.htm;

Tregtia elektronike (E-commerce)

Tregtia elektronike i referohet çdo lloj transaksioni të biznesit ose shitjeve të bëra nëpërmjet rrjeteve. Ajo përfshin, por nuk kufizohet në shitjen dhe tregtimin e informacionit, mallrave dhe shërbimeve.

Edhe pse e-commerce në përditshmëri i referohet vetëm tregtimit të mallrave dhe shërbimeve në Internet, aktivitete më të gjëra ekonomie janë të përfshira. E-commerce lidhet me biznes-konsumator dhe biznes-biznes ashtu si edhe transaksione të brendshme organizative që mbështesin këto aktivitete.

Një tërësi teknologjish dhe procesesh biznesi janë sot të lidhura me E-commerce si: portalet, transfertat elektronike të fondeve, bankingu online, menaxhimi i zinxhirit të furnizimit, marketingu, blerja online, tregtia mobile, menaxhimi i inventarëve, etj.

Fushat e auditimit

Ekzistojnë aspekte të ndryshme të cilat janë kritike për një sistem e-commerce. Disa prej tyre duhet të merren paraysh në momentin e përzgjedhjes së objektivave të auditimit, p.sh.:

- disponueshmëria;
- siguria e transaksioneve;
- përshkallëzimi i zgjidhjes;
- përvoja e përdoruesit shumë e rëndësishme;
- proceset e biznesit të kryera si pasojë e strategjisë e-commerce.

Me shumë mundësi, proceset e biznesit të kryera nëpërmjet strategjive të e-commerce kërkojnë mekanizma të fuqishëm sigurie, në mënyrë që të garantojnë kryesisht integritetin, besueshmërinë dhe origjinalitetin e transaksioneve online. Kështu, një grup procesesh dhe teknologjish të quajtura Infrastruktura më çelës publik (Public-Key Infrastructure – PKI), hyjnë në skenë.

PKI përbëhet nga një sërë algoritme standarde kriptografike dhe teknikat për të i mundësuar përdoruesve të komunikojnë në mënyrë të sigurt në rrjetet jo të sigurta publike për të siguruar që informacioni i komunikohet marrësit të synuar. Pa këtë teknologji, e-commerce që ne njohim do të ishte e pamundur.

Në mënyrë që të auditohen sistemet e-commerce, shpesh audituesit duhet të kenë njohuri mbi elementet kryesore të infrastrukturës PKI:

- Çelësat privatë dhe publikë;
- Mekanizmat e nënshkrimit dixhital;
- Çertifikatat dixhitale;
- Autoritetet e regjistrimit dhe të certifikimit;
- Algoritmat kriptografik.

Ndërkohë që audituesi nuk ka nevojë të jetë ekspert në këto fusha, ata duhet të kenë njohuri të standardeve gjerësisht të pranuara dhe nëse organizata i ka adoptuar ato.

Referencat/ lexim të mëtejshëm

1. E-Commerce. Encyclopedia Britannica. http://www.britannica.com/EBchecked/topic/183748/e-commerce
2. E-Commerce dhe Auditimi i Infrastrukturës Kyçe Publike/Program i Sigurisë. Isaca http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/E-commerce-and-Public-Key-Infrastructure-PKI-Audit-Assurance-Program.aspx
3. Gjurmët e Auditimit në Mjedisin e E-commerce http://www.isaca.org/Journal/Past-Issues/2002/Volume-5/Pages/Audit-Trails-in-an-E-commerce-Environment.aspx

Shtojca II. Matrica e sugjeruar e auditimit mbi Qeverisjen e TI-së

<table>
<tr><th colspan="2">2.1.Identifikimi, Drejtimi dhe Monitorimi i kërkesave të biznesit</th></tr>
<tr><td colspan="2">Objektivi i auditimit:

Vlerësimi nëse menaxhmenti i organizatës drejton, vlerëson dhe monitoron efektivisht përdorimin e TI-së në organizatë, me qëllim të përmbushjes së misionit të organizatës.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr.1: Përcaktimi i kërkesave të TI-së

Si i identifikon dhe aprovon organizata kërkesat e biznesit dhe të TI-së?</td></tr>
<tr><td colspan="2">Kriteret: Organizata ka një plan sesi të identifikojë kërkesat e reja të biznesit ose nevojat e TI-së dhe Komiteti Drejtues, i cili aprovon kërkesat, ka informacion të mjaftueshëm për vendimarrje.</td></tr>
<tr><td>Informacioni i kërkuar

Procesi i menaxhimit të kërkesave

Prosesverbalet e Komitetit Drejtues

Statuti dhe parimet e operimit të Komitetit Drejtues, përfshirë kufijtë e aprovimit dhe refuzimit

Listë me kërkesat e aprovuara dhe të refuzuara</td><td>Metodat e analizimit

Rishikim i dokumentave për tu siguruar që kërkesat e reja të biznesit janë identifikuar dhe analizuar në përputhje me prosesin e menaxhimit të kërkesave të organizatës.

Rishikimi i kërkesave të aprovuara ose refuzuara për tu siguruar se ato janë në përputhje me parimet e pranuara të operimit.

Intervistimi i menaxhmentit ose personave të tjerë përgjegjës për aprovimin e projekteve për tu siguruar se merren parasysh kapacitetet, aftësitë, burimet dhe trajnimi i TI-së në organizatë, si dhe aftësia e përdoruesve për të shfrytëzuar mjetet, metodat dhe procedurat e reja.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 2: Menaxhmenti

Si drejton dhe monitoron menaxhmenti performancën e objektivave të biznesit dhe të TI-së mbi baza periodike?</td></tr>
<tr><td colspan="2">Kriteret: Matjet e performancës janë të vendosura dhe komiteti drejtues (ose ekuivalenti) kryen rishikime dhe mbledhje periodike, si dhe ndërmerr veprimet e duhura, ose ekziston një sistem raportimi i cili informon menaxhmentin mbi gjendjen e masave kryesore të performancës.</td></tr>
<tr><td>Informacioni i kërkuar

Matjet e perfomancës për biznesin dhe TI</td><td>Metodat e analizimit

Rishikimi i mostrave të vendimeve të menaxhmentit apo memot për tu siguruar se ato janë të qarta, të argumentuara mirë dhe të kuptueshme.</td></tr>
</table>

Raporte të rregullta mbi gjendjen e projektit Procesverbale nga rishikime periodike Listë e elementëve të veprimit dhe gjendjes së tyre	Rishikim i masave të performancës për tu siguruar se mbulojnë si sistemet e biznesit ashtu edhe ato të TI. Rishikim i raporteve të gjendjes së projekteve (ose dokumentacion tjetër që ka gjendjen e projektit (procesverbale mbledhjesh, emaile, etj.)) për tu siguruar që përmbajnë kostot, programin dhe treguesit e performancës dhe devijimet nga plani. Rishikim i menaxhimit të elementëve të veprimit për tu siguruara se janë të përcaktuara dhe të gjurmuar për mbyllje dhe mësimet e marra.
Çështja e auditimit nr. 3: Investimet e TI-së Si i menaxhon organizata investimet në TI?	
Kriteret: Organizatat duhet të menaxhojnë projektet dhe investimet e tyre të TI-së, me qëllim maksimizimi të përfitimeve dhe konsiderimin e elementëve, të tillë si rrezikun, kapacitetet dhe prioritarizimi në mes investimeve konkuruese.	
Informacioni i kërkuar	**Metodat e analizimit**
Planet dhe procedurat e menaxhimit të investimeve Portfoli i projekteve të TI Raporte titpikë të analizave të kost-benefiteve Listë e projekteve të aprovuara dhe të refuzuara ose të shtyra Raporte të gjendjes së projektit për projekte të aprovuara Raporte të vlerësimit të post projekteve	Intervistimi i menaxhimit për të përcaktuara procedurat e menaxhimit të investimeve të organizatës. Rishikim i portfolios për të vlerësuar nëse projektet janë prioritarizuara në përputhje me kriteret e aprovuara. Rishikimi i raporteve të gjendjes për të parë nëse ofrohet gjurmimi i programit dhe i kostove Rishikimi i raporteve të analizave të kost-benefiteve për të vlerësuar që ato janë të plota, pasqyrojnë kushtet aktuale dhe nuk tejkalojnë përfitimet, kuptojnë kostos ose programin (shfrytëzojnë shërbime të specializuara të ekonomistëve ose ekspertë të kostove sipas nevojës). Në rast të projekteve me probleme, përcktohen nëse metodologjitë e tyre janë të përshtatshme për projektin dhe janë të mirë aplikuara, si dhe nëse është përfshirë pyetësori QA (pyetje-përgjigje) përgjatë ciklit të jetës. Intervistimi i menaxhmentit për të përcaktuar nëse çdo projekt është ndalur për shkak të mosarritjes së përfitimeve dhe performancës.

	Intervistimi i menaxhmentit për të përcaktuar nëse organizata merr vendime mbi ndërtimin apo blerjen e zgjidhjeve (për shembull, bazuar në kapacitet, aftësi, kosto, rrezik, etj).
Konkluzionet e auditimit:	Të plotësohen nga audituesi

2.2.Strategjia e TI	
Objektivi i auditimit: Konfirmimi nëse ekziston një strategji TI-së, e cila përfshin plan të TI-së dhe proceset për zhvillimin, aprovimin dhe zbatimin dhe mirëmbajtjen e strategjisë, e cila është e lidhur me strategjinë dhe objektivat e organizatës. Rreziqet dhe burimet gjatë përmbushjes së objektivave të TI-së janë të menaxhuara efektivisht.	
Çështja e auditimit nr. 4: **Cilësia e strategjisë së TI-së** A ka organizata një strategji TI-së që shërben për të udhëzuar funksionet e TI-së?	
Kriteret: Ekziston një plan në nivel strategjik i TI-së, i cili përkthen objektivat e biznesit në qëllime dhe kërkesa të TI-së, adreson burimet e nevojshme për të mbështetur biznesin, rishikohet dhe azhurnohet sistematikisht.	
Informacioni i kërkuar Plani strategjik i TI-së, dokument ekuivalent Procesverbale nga mbledhjet e Komitetit Drejtues të organizatës	**Metodat e analizimit** Rishikim i dokumentave. Intervistimi i pronarëve të biznesit për të përcaktuar nëse nevojat e tyre janë arritur nga sektori i TI. Rishikimi i procesverbaleve të mbledhjeve të Komitetit Drejtues të organizatës për tu siguruar se pronarë e biznesit janë të përfaqësuar dhe se vendimet e strategjisë së TI-së janë marrë në nivel të Komiteti Drejtues. Rishikimi i Strategjisë së TI-së ose intervistimi i menaxhmentit për të përcaktuar kërkesar për burime, si janë përcaktuar dhe aprovuar, kush aprovon blerjet e duhura të mjeteve dhe burimeve të tjera (stafin, kontraktorët, aftësimi përmes trajnimeve, etj).
Çështja e auditimit nr. 5: Menaxhimi i rrezikut Si i menaxhon organizata rreziqet e saj?	

Kriteret: Organizata ka politika dhe plane të menaxhimit të rrezikut, si dhe ka përcaktuar burimet e mjaftueshme për të identifikuar dhe menaxhuar rreziqet.	
Informacioni i kërkuar	**Metodat e analizimit**
Plani i menaxhimit të rrezikut Lista e strategjive të rreziqeve dhe zvogëlimit të tyre (përfshirë TI) Procesverbalet e vlerësimeve periodike të rrezikut ose dokumenta të tjerë ekuivalentë	Rishikim i planit të menaxhimit të rrezikut ose dokumentave të tjerë për tu siguruar se përgjegjësitë e menaxhimit të rrezikut janë të qarta dhe të mirëpërcaktuara. Rishikim i dokumentave për të përcaktuar nëse rreziqet e TI-së janë pjesë e rrezikut të përgjithshëm qeverisës dhe kornizës së pajtueshmërisë. Rishikim i procesverbaleve të mbledhjeve për tu siguruar se rreziqet e reja janë të përfshira dhe të analizuara në mënyrë të përshtatshme . Intervisitimi i prsonelit përgjegjës për menaxhimin e rrezikut për të përcaktuar nëse rreziqet që duhen reduktuar kanë vlerësime të sakta të kostove dhe burimet janë shpërndarë. Intervistimi i menaxhmentit ose rishikimi i procesverbaleve për të përcaktuar nëse lidershipi është në dijeni të rreziqeve TI-së dhe rreziqeve të tjera, si dhe nëse moritonon gjendjen e tyre mbi baza periodike.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

2.3.Struktura organizative, politikat dhe procedurat
Objektivi i auditimit: Garantimi se ekzistojnë strukturat organizative, politikat dhe proçedurat që mundësojnë organizatën të arrijë mandatin për qëllimet e biznesit.
Çështja e auditimit nr. 6: Struktura organizative e TI-së A mundëson struktura e organizative e TI-së në arritjen e qëllimeve të TI-së dhe nevojat e biznesit?
Kriteret: Sektori i TI-së është pozicionuar në një nivel të kënaqshëm brenda organizatës, rolet dhe përgjegjësitë janë të përcaktuara qartë, përfshirë ato të CIO-s (ose personit ekuivalent).

Informacioni i kërkuar	Metodat e analizimit
Struktura e përgjithshëm i organizatës Struktura e sektorit të TI-së	Rishikim i strukturës së organizatës për të përcaktuar nëse sektori i TI-së është pozicionuar në një nivel strategjik (për shembull si një CIO që raporton ose është anëtar në Komitetin Drejtues). Rishikim i strukturës organizative të TI-së për të përcaktuar nëse është i përcaktuar për të mbështetur bizneset (ka tavolonën ndihmëse, manaxherët e bazave të të dhënave, personelin e mirëmbajtjes ose kontraktorët që ndihmojnë dhe lehtësojnë operacionet e TI).
Çështja e auditimit nr. 7: Politikat dhe procedurat A ka aprovuar organizata dhe a është duke përdorur politikat dhe procedurat për të udhëzuar operacionet e biznesit dhe operacionet e TI-së?	
Kriteret: Organizata dokumenton, aprovon dhe komunikon politikat dhe procedurat e duhura për të udhëzuar operacionet e biznesit dhe të TI-së, me qëllim të arritjes të mandatit të saj.	
Informacioni i kërkuar	**Metodat e analizimit**
Politikat organizative lidhur me: Burimet njerëzore, përfshirë politikat e rekrutimit dhe ndërprerjes, ruajtja e dokumentave, kontraktimi, zhvillimi i programeve dhe/ose blerja, etj. Procedurat për zgjedhjen e fushave të politikave Email-at ose mënyra të tjera me anë të të cilave politikat komunikohen te përdoruesit e duhur dhe tek palët e interesit Raportet e sigurimit të cilësisë për menaxhmentin mbi politika dhe procedura	Rishikim i politikave për tu siguraur se janë të aprovuara dhe aktuale. Për shembull, rishikimi i poltikave të Burimeve Njerëzore për të përcaktuar se kërkesat për aftësi janë të përcaktuara dhe trajnimi është identifikuar për stafin e ri dhe të vjetër. Rishikimi i materialeve të trajnimit fillestar dhe të rifreskimit ose procese të tjera të brendshme përmes të cilave këto politika dhe procedura komunikohen brenda organizatës. Intervista me pjesëmarrësit e sigurimit të cilësisë ose një grupi tjetër që është përgjegjës për zbatimin e politikave për të parë sesi sigurohet pajtueshmëri. Intervisa me grupin e sigurimit të cilësisë ose stafin e pajtueshmërisë për të përcaktuar sesi dhe kur ata raportojnë rezultatet e tyre në menaxhimin e lartë. Intervista me personelin përgjegjës për pajtueshmërinë e politikave dhe procedurave për të përcaktuar sesa shpesh ata raportojnë rezultatet tek menaxhmenti i lartë dhe sesi ata kërkojnë (marrjen e informatave të)e mospajtueshmërisë mbi baza anonime ose të pavarura. Intervista me menaxherët dhe përdoruesit për të kuptuar perceptimin dhe sjelljen e tyre në politikat dhe procedurat e analizuara. Në rast të

pajtueshmërinë dhe çështje të tjera Ndryshime të kërkuara të politikave dhe/ose rishikime dhe rezultate periodike	opinionit të shpeshtë: "Procedurat janë komplekse" pyesni sesi mund dhe çfarë mund të përmirësohet. Rishikim i historisë së kontrollit të ndryshimit të politikave për të përcaktuar se politikat janë të përditësuara periodikisht ose kur nevojiten. Rishikim i raporteve të sigurimit të cilësisë për t'u siguruara se ato përmbajnë çështje të përshtatshme të politikave dhe procedurave të pajtueshmërisë. Rishikim i email-eve ose mekanizmave të tjerë (posta fizike, trajnim, etj) për tu siguruara se politikat janë shpërndarë tek përdoruesit e duhur dhe tek palët e interesuara në momentin e përditësimit të tyre ose mbi baza nevoje. Rishikim i politikave për të përcaktuar përshtatshmërinë duke parë për (si shembull): • Qëllimi dhe mandati i politikave. • Përcaktimin e detyrave dhe përgjegjësive. • Burimet dhe mjetet e nevojshme. • Lidhja me procedurat. • Rregullat për të trajtuar mospajtueshmërisë.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

2.4.Njerëzit dhe Burimet	
Objektivi i auditimit: Punësimi i personelit të kualifikuar dhe të trajnuar dhe ofrimi i qasjeve ndaj burimeve të përshtatshme që mundësojnë organizatës arritjen e qëllimeve të biznesit.	
Çështja e Auditimit nr. 8: Burimet njerëzore dhe logjistika Si e trajton organizata arritjen e kërkesave aktuale dhe të ardhshme në njerëz dhe burime?	
Kriteret: Organizata duhet të ketë një plan për arritjen e kërkesave aktuale dhe të ardhshme për plotësimin e nevojave të biznesit.	
Informacioni i kërkuar	**Metodat e analizimit:**

Politikat organizative lidhur me: Burimet njerëzore & Trajnimet Strategjia TI-së ose Plani Strategjik Planet e Punësimit & Trajnimit	Rishikim i politikave për t'u siguruara se ato janë aktuale dhe të aprovuara. Rishikimi i politikave për t'u siguruar se ato kanë nevojë për grupe të ndryshëm (TI, sigurim cilësie, përdorues biznesi) për të identifikuar nevojat aktuale dhe të ardhshme mbi personelin dhe burimet. Rishikim i planeve të punësimit dhe të trajnimit për t'u siguruara se ato reflektojnë nevojat e identifikuara. Për shembull rishikim i politikave të të Burimeve Njerëzore për të përcaktuar nëse janë identifikuar kërkesat për aftësitë, si dhe nëse janë identifikuar trajnimet për stafin e ri dhe ekzistues. Intervista me Burimet Njerëzore ose menaxherët e biznesit për t'u vlerësuar se si ata sigurohen që pozicionet kritike plotësohen gjatë pushimeve ose mungesave të gjata. Rishikimi i materialeve fillestare dhe të rifreskuara të trajnimit ose proceset e tjera të brendshme përmes të cilave këto politika dhe procedura komunikohen brenda organizatës. Rishikim i planit Strategjik të TI-së për tu siguruar se përmban kërkesa për njerëz dhe burime për nevoja aktuale dhe të ardhshme.
Konkluzioni i audituesit: Të plotësohet nga audituesi.	

2.5.Vlerësimi i rrezikut dhe mekanizmat e pajtueshmërisë
Çështja e auditimit nr. 9: Mekanizmat Në cilën mënyrë organizata sigurohet se posedon mekanizma të përshtatshëm dhe funksionalë të pajtueshmërisë për të siguruar se të gjithë politikat dhe procedurat janë duke u ndjekur?
Kriteret: Organizata posedon mekanizma (nëpërmjet grupit të sigurimit të cilësisë, ose kontrolle, etj.) me anë të të cilëve siguron se janë duke u ndjekur të gjitha politikat dhe procedurat.

Informacioni i kërkuar	**Metodat e analizimit**
Politika dhe procedura organizative (Siguria, SDLC, Trajnime, etj.) Struktura organizative Plani i sgurimit të cilësisë Raportet prej grupit të pajtueshmërisë ose grupeve të tjera Procesverbalet e Komitetit Drejtues	Përzgjedhja e një mostre procedurash ose politikash organizative për të vlerësuar pajtueshmërinë. Intervista me menaxhmentin për të përcaktuara se cilët janë përgjegjës për sigurimin e pajtueshmërisë të politikave dhe procedurave të lidhura me to (të përzgjedhura nga grupi i auditimit). Intervista me personat ose grupin përgjegjës për pajtueshmërinë, në mënyrë që të përcaktohet se si i kryejnë ata detyrat tyre. Rishikim i procesverbaleve të Komitetit Drejtues për të parë nesë çështjet me nivel të lartë të pajtueshmërisë janë diskutuar. Intervista me autorët për të përcaktuar arsyet që kanë sjellë ndryshimin e politikave ose procedurave ekzistuese. Rishikim i çështjeve dhe zgjidhjeve të mospërputhjeve. Rishikim i mekanizmave të trajnimit ose të tjerë (emaile, memo, njoftime) për të parë nëse adresohen çështjet e mospajtueshmërisë.
Konkluzioni i auditimit: Të plotësohet nga audituesi	
Shiko Shtojcën III dhe IV respektivisht për matricat e auditimit mbi Zhvillimin dhe Blerjet si dhe mbi Operacionet TI	

Shtojca III. Matrica e sugjeruar e auditimit mbi Zhvillimin dhe Blerjet

<table>
<tr><th colspan="2">3.1.Zhvillimi dhe menaxhimi i kërkesave</th></tr>
<tr><td colspan="2">Objektivi i auditimit:

Vlerësimi sesi organizata identifikon, prioritarizon dhe menaxhon kërkesar për sistemet e TI-së.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 1: Identifikimi i kërkesave të përdoruesve për Sistemet e TI-së

Si identifikon organizata kërkesat e përdoruesit për Sistemet e TI-së?</td></tr>
<tr><td colspan="2">Kriteret: Organizata ka plane ose procedura sesi të mbledhë, të rishikojë dhe të kategorizojë kërkesat për funksionalitete të reja ose të shtuara.</td></tr>
<tr><td>Informacioni i kërkuar

Plani ose procedura e menaxhimit të kërkesave

Mostrat nga kërkesat e dorëzuara prej përdoruesve

Mostrat e rishikimit fillestar</td><td>Metodat e analizimit

Rishikim i planit ose procedurave të menaxhimit të kërkesave për të siguruar se përdoruesit, palët e interesit, ose të tjerë, janë të përfshirë në identifikimin e kërkesave.

Në një zhvillim të madh të përmirësimit të funksionalitetit, konsultimi i përdoruesit dhe zhvillimi i prototipit mund të zbatohen paralelisht. Shkëmbimi i informacionit në mes pronarëve të procesit të biznesit dhe organizatës shitës / TI-së duhet të merret në konsideratë.

Rishikim i mostrave të kërkesave për t’u siguruar se ekziston një rishikim fillestar dhe se kërkesat e ngjashme ose të dyfishuara janë grupuar.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 2: Analiza, përparësia dhe menaxhimi i kërkesave të përdoruesve

Si analizon, prioritarizon dhe menaxhon organizata kërkesat e përdoruesve?</td></tr>
<tr><td colspan="2">Kriteret: Organizata analizon, prioritarizon dhe menaxho kërkesat për t’u siguruar se nevojat e përdoruesve janë plotësuar në mënyrë optimale dhe me kosto efektive.</td></tr>
<tr><td>Informacioni i kërkuar

Lista me kërkesat

Mostrimi i analizave të kërkesave

Matrica e gjurmueshmërisë së kërkesave</td><td>Metodat e analizimit

Rishikim i kërkesave për të përcaktuar se ato përmbajnë autorin, datën, prioritetin, koston, rrezikun dhe elementë të tjerë.

Rishikim i analizave të kërkesave ose të komenteve mbi to prej pronarëve të biznesit ose prej palëve të interesit, për të përcaktuar se të gjitha pikëpamjet janë përmbledhur për të kryer një analizë të plotë (pranim, diferencim, refuzim, etj.).</td></tr>
</table>

Kriteret për prioritarizimin e kërkesave	Rishikimi i matricës së gjurmueshmërisë për të përcaktuar se kërkesat e aprovuara u caktohen projekteve të zhvillimit ose përvetësimit dhe gjurmohen në përfundim kur implementohen. Rishikim i kritereve për prioritarizimin e kërkesave për të vlerësuar nëse ato përmbajnë elemente lidhur me kostot, nevojat e biznesit, çështjet emergjente dhe kapacitetet e reja.
Konkluzioni i audituesit: Të plotësohet nga audituesi	

3.2.Menaxhimi dhe Kontrolli i projektit	
Objektivi i auditimit: Vlerësimi sesi organizata menaxhon dhe kontrollon zhvillimin ose blerjen e projekteve të aprovuara për TI-në.	
Çështja e auditimit nr. 3: Plani për zhvillimin ose blerjen e projekteve të TI-së Si planifikon organizata zhvillimin ose blerjen e projekteve TI?	
Kriteret: Organizata ka një plan menaxhimi projektesh ose ekuivalent me të për çdo projekt të aprovuar, i cili udhëzon ekzekutimin e projektit	
Informacioni i kërkuar	**Metodat e analizimit**
Plan menaxhimi të projekteve ose ekuivalent me të	Rishikim i planit të menaxhimit të projektit për t'u siguruar se ai përmban përshkrimin, qëllimin, koston, shtrirjen kohore, rreziqet, strukturën menaxheriale dhe identifikimin e palëve të interesit (të brendshëm ose të jashtëm) për projektin. Rishikim i planit për tu siguruar se është i aprovuar nga menaxhmenti i lartë dhe përmban komente prej palëve të interesit. Rishikim i strukturës organizative të projektit për të përcaktuar detyrat e individëve përgjegjës për sigurimin e cilësisë ose testimin, zhvillimin dhe instalimin e sistemit në infrastrukturën e TI-së, të organizatës, grupin mbështetës, etj. Për projektet e furnizuara/të blera sigurohuni se plani liston se cilët do të jenë përgjegjës për mbikëqyrjen e përgjithshme dhe rishikoni çdo material të sjellë prej tyre për aprovim.

	Intervista me menaxherët e projektit për të përcaktuar cila metodë SDLC është duke u përdorur në zhvillimin e projektit.
Çështja e auditimit nr. 4: Kontrolla e projekteve të TI-së Si kontrollon organizata projektet e TI-së?	
Kriteret: Organizata kontrollon dhe përcjell projektet për tu siguruar në arritjen e kërkesave mbi koston, shtrirjen kohore dhe performancën e tyre.	
Informacioni i kërkuar Kostot e projektit dhe bazat e shtrirjes kohore Raportet e statusit të projektit Raportet e statusit të kontraktorëve, SLA Rezultatet e rishikimeve Planet e veprimit	**Metoda e analizimit** Krahasoni koston e projektit dhe bazën e shtrirjes kohore me raportet e statusit për të vlerësuar shmangiet, nëse ka. Intervista me menaxherë e projektit/rishikim i raporteve për të përcaktuar nëse janë ndërmarrë veprimet e përshtatshme korrigjuese ndaj shmangieve të mëdha. Intervista me grupin e menaxhimit të projektit dhe rishikim i procesverbaleve të mbledhjeve me kontraktorin për të vlerësuar frekuencën dhe efektivitetin e monitorimit të aktiviteteve të projektit të furnizuar. Rishikim i SLA së kontraktorit ose kontratave të tjera për tu siguruar se janë duke u ndjekur kushtet e kontratës, për shembull shihni për rishikimet periodike të kontraktori, dorëzimi i raporteve të statusit, përcjellja e planeve të veprimit, aktivitetet referuar rreziqeve në lidhje me kontratën. Intervista me punonjësit e hartimit të kontratës në organizatë për të përcaktuar sesi ata menaxhojnë kontraktorin nëse nuk posedon SLA.
Çështja e auditimi nr. 5: Menaxhimi i rrezikut në lidhje me projektet e TI-së Si menaxhohen rreziqet e lidhura me projektin?	
Kriteret: Aktivitetet e menaxhimit të projektit përfshijnë menaxhimin e rreziqeve të lidhura me projektin dhe ndërmarrjen e aktiviteteve të përshtatshme të reduktimit të tyre.	

Informacioni i kërkuar	Metodat e analizimit
Plani i menaxhimit të projektit ose ekuivalent me të Plani i menaxhimit të rrezikut të projektit Lista e rreziqeve, detyrat dhe përgjegjësitë për menaxhimin e rreziqeve Procesverbalet e mbledhjeve në të cilat diskutohen rreziqet e projektit	Rishikim i planit të menaxhimit të projektit ose planit të menaxhimit të rreziqeve për të përcaktuar nëse rreziqet janë identifikuar për këtë projekt, rreziqet janë kategorizuar dhe i janë caktuar individëve ose grupeve të ndryshme për t'u monitoruar ose reduktuar sipas mënyrave më të përshtatshme. Rishikim i planit të menaxhimit të rreziqeve ose intervista e menaxherëve të projektit për të përcaktuar nëse ata janë duke ndjekur politikat organizative në menaxhimin e rreziqeve të tyre. Rishikim i procesverbaleve të mbledhjeve për tu siguruar se rreziqet diskutohen periodikisht dhe se ato përcjellën; rreziqet e reja në rast se identifikohen, hyjnë në regjistrin e rreziqeve ose në momentin që grupi i plotë i rreziqeve të projektit dokumentohet.
Konkluzioni i auditimit: Të plotësohet prej audituesit.	

3.3.Sigurimi dhe Testimi i Cilësisë	
Objektivi i auditimit: Vlerësimi sesi organizata siguron se projektet TI-së arrijnë qëllimet e tyre nëpërmjet zhvillimit ose blerjes	
Çështja e auditimit nr. 6: Organizimi i sigurimit të cilësisë A ka organizata një strukturë sigurimi të cilësisë dhe a janë përcaktuar detyrat dhe përgjegjësitë?	
Kriteret: Një procedurë për kryerjen e aktiviteteve të sigurimit të cilësisë.	
Informacioni i kërkuar	**Metodat e analizimit**
Politikat ose planet e sigurimit të cilësisë Procedurat e sigurimit të cilësisë Detyrat dhe përgjegjësitë e grupit ose individëve të sigurimit të cilësisë	Rishikim i politikave ose planeve të sigurimit të cilësisë për të përcaktuar se cili grup ose individ është përgjegjës për kryerjen e aktiviteteve të sigurimit të cilësisë për projektin (për shembull, grupi i sigurimit të cilësisë duhet të rishikojë dokumentet për tu siguruar se ato reflektojnë kërkesat, rishikon manualet e përdorimit për tu siguruar se janë të qarta dhe nuk përmbajnë elemente ose hapa të munguar).

Raportet e sigurimit të cilësisë Projekti i përshtatur SDLC	Rishikim i procedurave të sigurimit të cilësisë ose intervistë e personelit të sigurimit të cilësisë për të përcaktuar se çfarë aktivitetesh ata kryejnë. Rishikim i raporteve të strukturës së sigurimit të cilësisë për të përcaktuar se çfarë ata verifikojnë (nëse grupi i projektit është duke ndjekur planin e menaxhimit të projektit, etj.) ndaj kujt raportohen çështjet.
Çështja e auditmit nr. 7: Planifikimi dhe testimi i sistemeve të TI-së Si e planifikon dhe kryen organizata testimin e sistemeve TI?	
Kriteret: Organizata kryen testimet mbi sistemet TI-së dhe bazuar mbi rezultatet pranon ose refuzon sistemin.	
Informacioni i kërkuar	**Metodat e analizimit**
Plani i testimit Programi i testimit Rezultatet e testimit Kriteret e pranimit ose refuzimit	Rishikim i planeve të testimit. Krahasimi i kostove të projektit dhe programin me raportet e statusit të projektit për të vlerësuar shmangiet, nëse ka. Intervista me menaxherët e projektit/ rishikim i raporteve për të përcaktuar nëse janë ndërmarrë veprimet e përshtatshme korrigjuese për shmangiet e mëdha. Intervistim i grupit të menaxhimit të projektit dhe rishikim i procesverbaleve të mbledhjeve me kontraktorët për të vlerësuar frekuencën dhe efektivitetin e monitorimit të aktiviteteve të projektit të kontraktuar. Rishikim i SLA-s ose kontratë tjetër për tu siguruar se janë duke u ndjekur kushtet e kontratës, për shembull shihni për rishikime periodike të kontraktorëve, dorëzimi i raporteve të statusit, përcjellja e planeve të veprimit, kryerja e aktiviteteve të menaxhimit në pajtim me kontratën. Intervista me punonjësit e hartimit të kontratë në organizatë për të përcaktuar sesi ata menaxhojnë kontraktorin nëse nuk ekziston SLA.
Konkluzioni i auditimit: Të plotësohet prej audituesit.	

3.4.Dokumentimi i kërkesave

Objektivat e auditmit:

Vlerësimi sesi organizata siguron se aktivitetet e dokumentimit të kërkesave (grup detyrash si dokumentimi i nevojave, inkuadrim i kërkesave për propozime (KPP), vlerësimi i propozimeve, kryerja e qartësimeve përpara ofertës, dizajni dhe tenderimi, vlerësimi, etj. që sjellin fitimin e një kontrate) kryhen në pajtim me planin e dokumentimit të kërkesave ose procedurave të ngjashme.

Çështja e auditimit nr. 8: Plani ose procedura e dokumentimit të kërkesave

Cili është plani ose procedura për kryerjen e aktiviteteve të dokumentimit të kërkesave?

Kriteret: Aktivitetet e dokumentimit të kërkesave përfshirë përzgjedhjen e furnizuesve (tregtarëve operatorëve ekonomik), kryhen në pajtim me planin e dokumentimit të kërkesave të organizatës

Informacioni i kërkuar	**Metoda e analizimit**
Plani ose procedura e dokumentimit të kërkesave Paketa e dokumentimit të kërkesave Rishikim i kërkesave prej përdoruesve Rishikim i paketës së kërkesave të dokumentuara prej përdoruesve Ligjet në fuqi që udhëheqin kryerjen e dokumentimit të kërkesave	Rishikim i planit të dokumentimit të kërkesave për tu siguruar se ai mbulon fusha si përfshirja e përdoruesit, vendosje e ofertave në baza konkurrencë, kryerja e kërkimeve në treg përpara kontratës dhe se përzgjedhja e furnizuesit/operatorit ekonomik bazohet në kritere objektive. Intervista me personelin kryesor të kontratës për të vlerësuar sesi ata sigurojnë se paketa e dokumentimit të kërkesave është e plotë (për shembull duke marrë përdorues, palë të interesuara, ekspertë për rishikim të saj). Intervista me përdorues ose pronarët të biznesit për tu siguruar se ata janë këshilluar gjatë gjenerimit të kërkesave ose që kanë aprovuar kërkesat teknike të listës së dokumentuar dhe/ose paketës në tender. Intervista me punonjësit e hartimit të kontratës për të vlerësuar sesi ata sigurojnë se procesi i dokumentimit të kërkesave ndjek ligjet dhe rregullat në fuqi.

Çështja e auditimit nr. 9: Përzgjedhja e furnizuesve/operatorëve ekonomik

Cilat kritere përdor organizata në përzgjedhjen e furnizuesve/operatorëve ekonomik?

Kriteret: Organizata përdor kritere objektive dhe të publikuara për përzgjedhjen e çdo furnizuesi.

Informacioni i kërkuar	Metodat e analizimit
Kriteret e përzgjedhjes së furnizuesve Matrica e pikëzimit/vlerësimit të furnizuesve ose ekuivalente me të	Rishikim i kritereve të përzgjedhjes së furnizuesve për tu siguruar se ato reflektojnë qëllimin e kërkesave të dokumentuara (për shembull, në një kontratë softueri, përzgjedhja e furnizuesit nuk duhet të përmbajë parametra jo kritikë për organizatën). Intervista me palët kryesore të interesit për të vlerësuar nëse ata janë dakord me kriteret e përzgjedhura. Rishikim i matricës së pikëzimit/vlerësimit të furnizuesve ose element tjetër ekuivalent për të konfirmuar se është në përputhje me kriteret e përzgjedhura.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

3.5.Menaxhimi i konfigurimit	
Objektivat auditimit: Vlerësimi sesi organizata menaxhon konfigurimin e produkteve të punës të lidhura me zhvillimin dhe blerjen.	
Çështja e auditimit nr. 10: Politika për menaxhimin e konfigurimit Cilat politika përdor organizata për menaxhimin e konfigurimit?	
Kriteret: Aktivitetet e menaxhimit të konfigurimit kryhen në pajtim me politikat ose procedurat organizative.	
Informacioni i kërkuar	**Modelet e analizimit**
Politika ose procedura të menaxhimit të konfigurimit ose ekuivalente me to	Rishikim i politikave të menaxhimit të konfigurimit mbi përshtatshmërinë, duke kontrolluar (si shembull): Qëllimin dhe mandatin e politikave; Përcaktimin e detyrave dhe përgjegjësive; Burimet dhe mjetet e nevojshme; Lidhja me procedurat; Rregullat për trajtimin e mos pajtueshmërive.

	Intervista me personelin përgjegjës për menaxhimin e konfigurimit nëse nuk ekzistojnë politika, për të vlerësuar sesi ata sigurojnë se detyrat e tyre kryhen njëtrajtësisht në emër të organizatës.
Çështja e auditimit nr. 11: Përgjegjësia për autorizimin e ndryshimeve Cili grup ose individ është përgjegjës për autorizimin e ndryshimeve dhe për instalimin final në mjedisin e prodhimit?	
Kriteret: Vetëm ndryshimet e autorizuara dhe të aprovuara do të prezantohen në mjedisin prodhimit.	
Informacioni i kërkuar Grup ose individ përgjegjës për autorizimin e ndryshimeve Procesi për aprovimin, prezantimi i ndryshimeve të aprovuara dhe të testuara në mjedisin e prodhimit	**Metodat e analizimit** Sigurimi se ekziston grupi për autorizimin e ndryshimeve ndaj produkteve të punës. Grupi mund të jetë bordi i kontrollit të ndryshimeve ose ekuivalent me të, i cili rishikon dhe aprovon ndryshimet. Intervista me personelin përgjegjës për autorizimin e prezantimit të programeve të reja në mjedisin e prodhimit për tu siguruara se programi është testuar (përfshi testimin regresiv me programet e tjera nëse është e nevojshme), plotëson kriteret e pranimit, ka dokumentacion të përshtatshëm dhe përfshinë trajnim për përdoruesit (nëse është e nevojshme) përpara prezantimin në biznes. Intervista me personelin përgjegjës për autorizimin e ndryshimeve në sistemin e prodhimit për të verifikuar sesi ata kontrollojnë dhe parandalojnë ndryshimet e paautorizuara në sistem (për shembull, duke kontrolluar qasjen në sistemin e prodhimit, ndarjen e mjedisit të prodhimit nga ai i zhvillimit, etj.).
Konkluzioni i auditimit: Të plotësohet nga audituesi	

Shtojca IV. Matrica e sugjeruar e auditimit mbi Operacionet e TI-së

<table>
<tr><th colspan="2">4.1.Menaxhimi i shërbimit</th></tr>
<tr><td colspan="2">Objektivi i auditimit:

Vlerësimi nëse struktura e TI-së monitoron në mënyrë aktive operacione e TI-së kundrejt marrëveshjeve SLA ose kontratave të tjera.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 1: Parametrat kryesorë

Cilat matje bazë të shërbimit mbulohen prej SLA-s së brendshme në mes të biznesit dhe strukturës së TI?</td></tr>
<tr><td colspan="2">Kriteret: Praktikat më të mira të SLA, alokimi i përgjegjësive në mes të pronarëve të proceseve të biznesit dhe grupit mbështetës të TI-së, objektivat e dokumentuar të rrjetit të menaxhimit të biznesit, ofrimet dhe matjet e shërbimit, përcaktimi i llojeve të problemeve, përgjegjësitë e tavolinës ndihmëse.</td></tr>
<tr><td>Informacioni i kërkuar

SLA-t e brendshme të subjektit në mes të pronarëve të biznesit dhe strukturës së TI

-Përgjegjësitë e tavolinës ndihmëse

-Raportet e gjeneruara të shërbimeve

-Koha e përgjigjes së përdoruesit/aplikacionit</td><td>Metodat e analizimit

Rishikim i SLA për të verifikuar nëse përmban elementët e përshtatshëm- objektivat e detajuar dhe të matshëm në nivel shërbimi, sistemet dhe shërbimet e mbuluara, cilësia e shërbimit, shërbimet që nuk mbulohen, mbështetja në nivel aplikacioni dhe trajtimi i problemeve, disponueshmëria e sistemit, orët e tavolinës ndihmëse, koha e përgjigjes dhe e zgjidhjes në varësi të llojit të klasifikimit të problemit, listës së problemeve, shtrirja kohore e mirëmbajtjes, etj.

Kontrolli nëse praktikat e backup-it dhe të rimëkëmbjes janë të qëndrueshme me standardet e Planit të Vazhdimësisë së Biznesit.

Kontrolli nëse pronarët e proceseve të biznesit kanë nënshkruar marrëveshjen.

Intervista e një mostre përdoruesish për të kuptuar ndërgjegjësimin.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 2: Pajtueshmëria

Cilat janë mekanizmat ekzistues që sigurojnë se SLA respektohet në mënyrë të vazhdueshme??</td></tr>
<tr><td colspan="2">Kriteret: SLA e implementuar, e monitoruar dhe e ndryshuar sipas nevojës.</td></tr>
</table>

Informacioni i kërkuar	**Metodat e analizimit**
Parametrat e SLA Periudha e raportimit; Diagrame apo grafikë që tregojnë suksesin ose dështimin sesi janë arritur këto marrëveshje përgjatë kohës; Dokumentet e takimeve periodike që rishikojnë analizën bazës fillestare dhe trendëve Parametrat operacional-normat e defekteve, kërkesat në tavolinën ndihmëse, gjurmë të tjera komunikimi, koha e përgjigjes, koha e implementimit të funksionaliteteve të reja, dokumentimi i ndryshimeve, vendndodhjet e shërbimeve; Klauzolat e nxitjes dhe të penaliteteve (veçanërisht e rëndësishme nëse shërbimet e mbështjetjes së TI-së janë të kontraktuara).	Rishikim i raporteve që struktura e TI-së gjeneron mbi baza ditore ose mbi çdo interval tjetër. Kontrolli nëse këto tregues janë duke u monitoruar nëpërmjet raporteve ose grafikëve etj. Rishikim i raporteve për të ekzaminuar se cilat matje janë matur dhe raportuar tek menaxhmenti periodikisht. Rishikim i dokumentave për të verifikuar nëse raportet e aktivitetit të tavolinës ndihmëse janë konsideruar prej menaxhmentit dhe janë krahasuar me kërkesat e zgjidhura, çështjet kritike janë evidentuar për vendimet e blerjes dhe për rishikim periodik të vetë SLA-s. Intervistim i personelit të strukturës së TI-së dhe ekzaminim i mbikqyrjes së personelit të tavolinës ndihmëse, monitorimi i veglave të përdorura, prioritizimi i detyrave mbështetëse, grumbullimi i bazave mbi rrjetin dhe aplikacionet, të dhënat mbi kohën e përgjigjes, frekuenca e backup-eve, testimi i të dhënave backup për të verifikuar pajtueshmërinë me kërkesat e SLA. Kontrolli nëse veprimet janë ndërmarrë nga njësia e TI-së, ose në rast të grupit mbështetës të kontraktuar-nga menaxhmenti i organizatës-nëse parametrat janë ose jo në pajtim me kërkesat e SLA.
Çështja e auditimit nr. 3: Efektiviteti A siguron menaxhmenti i shërbimeve të TI-së plotësimin e kërkesave të përdoruesve të biznesit dhe a ndihmon në arritjen e objektivave të biznesit të organizatës?	
Kriteret: Arritja e matjeve të performancës që janë në lidhje me nevojat dhe qëllimet e biznesit.	

Informacioni i kërkuar	**Metodat e analizimit**
Raportet e tavolinës ndihmëse, procesverbalet e mbledhjeve në mes të palëve të interesit të biznesit dhe strukturës së TI-së; Pikat e axhendës për ciklin e rishikimeve të SLA-s.	Intervista me një mostër të përdoruesve të biznesit (në nivele të ndryshme ose kryerja e sondazheve të plotësimit të kërkesave mbi cilësinë e shërbimeve nga grupi i tavolinës ndihmëse dhe grupi mbështetës i TI-së. Rishikim i raporteve të tavolinës ndihmëse për të verifikuar nëse janë parandaluar një sasi domethënëse e çështjeve kritike të shërbimeve përpara se të raportohen nga përdoruesit. Kontrolli nëse koha e zgjidhjes për çështjet e raportuara është me e vogël se parametrat e vendosur në SLA. Kontrolli nëse parametrat e SLA-s rishikohen periodikisht nga menaxhmenti dhe nëse ekzaminohen çështjet e cilësisë se shërbimeve.
Konkluzioni i auditimit:	Të plotësohet nga audituesi

4.2. Menaxhimi i kapaciteteve	
Objektivi i auditimit: Vlerësimi nëse struktura e TI-së siguron se kapaciteti i sistemit dhe performanca e tij arrin nevojat aktuale dhe të ardhshme të biznesit.	
Çështja e auditimit nr. 4: Aprovimi i parametrave A ekziston një marrëveshje e dokumentuar në mes të biznesit dhe strukturës së TI-së, e cila përdoret si bazë për përzgjedhjen e parametrave operacionale për operacionet e TI?	
Kriteret: Qeverisja TI-së - përcjellja dhe monitorimi i implementimit të strategjisë sa i përket treguesve të matshëm.	
Informacioni i kërkuar	**Metodat e analizimit**
SLA e brendshme, ose forma të tjera marrëveshjeje Parametrat operacional të TI-së - disponueshmëria e burimeve të përpunimit, koha mesatare e hyrjes në	Rishikimi i marrëveshjes ose udhëzimit operativ që përdor grupi i TI-së. Siguria që është rishikuar dhe nënshkruar nga përdoruesit përkatës të biznesit ose menaxhmentit i lartë ekzekutiv. Krahasimi i parametrave bazë të performancës (disponueshmëria e burimeve në rrjet, koha e përgjigjes së pritësit) të vendosura nga struktura e TI-së me udhëzimet operacionale të vendosura nga pronarët

sistem, përqindja e jo produktivitetit, koha mesatare e përgjigjes së sistemit, etj..	e proceseve të biznesit, për të verifikuar se struktura e TI-së ndjek udhëzimet operacionale.
Çështja e auditimit nr. 5: Monitorimi A grumbullon dhe rishikon organizata të dhënat e performancës së sistemit mbi baza reale/periodike për ndërlidhje më të mirë me nevojat e biznesit?	
Kriteret: Praktikat më të mira nga administratorët e sistemit/rrjetit, përfshirë rreshtimin e bazës së performancës, mbledhjen e informacionit për trafikun dhe konfigurimin, disponueshmërinë e burimeve të sistemit, vëzhgimin e statistikave dhe tendencave të trafikut, analizat nëse dhe përdorimin e mjeteve për të identifikuar shkaqet e përkeqësimit të performancës.	
Informacioni i kërkuar Raporte, plane veprimi, koha e përgjigjes së tavolinës ndihmëse dhe matje të tjera	**Metodat e analizimit** Përdorimi i çështjes së pajtueshmërisë në matricën e SLA. Kushtoni vëmendje të veçantë ndaj gjithë elementeve që kanë ndikim në kapacitet, p.sh. krahasimi i matjeve të kapacitetit aktual me kërkesat e SLA, etj.
Çështja e auditimit nr. 6: Performanca e analizës së të dhënave A janë analizuar dhe rregulluar të dhënat e performancës për përfitimet e efikasitetit dhe shmangien e kufizimeve të kapaciteteve ?Nëse nevojitet, a ka planifikuar struktura e TI-së blerjen e burimeve shtesë për arritjen e qëllimeve të biznesit? A punëson, trajnon ose kontrakton personel struktura e TI-së me ndryshimin e nevojave të biznesit?	
Kriteret: Parametrat e vendosur në marrëveshje/udhëzime. Praktikat më të mira në akordimin e performancës (memoria, optimizmi i kohës së përgjigjes së rrjetit, sistemi operativ, hyrja/dalja; skemë efikase e dizajnit të bazës së të dhënave, detyrat e planifikuara në përputhje me prioritetin dhe burimet e kërkesave, procedurat e rritjes ose të akordimit të vendosura për të menaxhuar çështjet e kapacitetit mbi baza emergjente dhe afatgjata.	
Informacioni i kërkuar Raporte, veprime, raporte të statusit, grafikë/diagrame të matjeve të performancës	**Metodat e analizimit** Rishikim i raporteve që struktura e TI-së gjeneron mbi baza ditore apo periudha tjera kohore dhe më gjatë, verifikimi për të parë nëse ata gjenerojnë dhe analizojnë e trendin e të dhënave, identifikojnë pengesat për të parë veprimet, raportimi për çështjet e kapacitetit. Krahasim me kërkesat e SLA.

Procesverbale të takimeve me temë të TI-së në nivel organizativ	Krahasim i modeleve te raporteve/trendëve për të verifikuar veprimet procedurale të ndërmarra në përgjigje të raporteve. Rishikim i procesverbaleve të takimeve dhe verifikimi nëse çështjet e personelit të TI-së, problemet e kapaciteti dhe nevoja të tjera burimore diskutohen dhe theksohen në kohën e duhur.
Konkluzioni i auditimit:	Të plotësohet nga audituesi

4.3. Menaxhimi i problemeve dhe incidenteve	
Objektivi i auditimit: Vlerësimi i efektivitetit të menaxhimit të politikave dhe procedurave të menaxhimit të problemeve dhe incidenteve të organizatës.	
Çështja e auditimit nr. 7: Ndërgjegjësimi ndaj politikave A ekzistojnë dokumente të politikave të përgjigjes ndaj incidenteve dhe a janë të ndërgjegjshëm përdoruesit ndaj tyre?	
Kriteret: Praktikat më të mira në përgjigjet ndaj incidenteve	
Informacioni i kërkuar Politikat e organizatës për përgjigjen ndaj incidenteve Udhëzime për komunikimin me palët e jashtme në rast të incidenteve	**Metodat e analizimit** Rishikim i politikave për të verifikuar nëse përmbajnë fazat e duhura: përgatitja, zbulimi dhe analizat, kontrollimin dhe eliminimin, aktivitetet pas incidentit. A ndikon lloji i incidentit në madhësinë ose nivelin e incidentit? Verifikimi nëse politikat caktojnë përgjegjësitë, qëllimin dhe kërkesat e raportimit. Rishikim i procedurave aktuale nëpërmjet të cilave përdoruesit e biznesit janë në njohje të politikave; dhe natyrën e komunikimit në mes grupit të përgjigjes ndaj incidentit dhe palëve të interesit ndaj biznesit. Intervista me një mostër përdoruesish të biznesit në organizatë për të marrë siguri rreth ndërgjegjësimit mbi planet e reagimit ndaj incidenteve.

<table>
<tr><td colspan="2">Çështja e auditimit nr. 8: Përcaktimi i aftësive dhe burimeve

A ekziston një grup i aftë për reagimin ndaj incidenteve duke pasur mjetet e duhura, burimet dhe mbështetjen e menaxhmentit të lartë në trajtimin e incidentve?</td></tr>
<tr><td colspan="2">Kritere: Praktikat më të mira në përgjigjen ndaj incidenteve, udhëzimet NIST (udhëzime për mbrojtjen e infrastrukturës teknologjike), të përshkruara si në SLA.</td></tr>
<tr><td>Informacioni i kërkuar

Politikat dhe planet e përgjigjes ndaj incidenteve

Strukturë e grupit të përgjigjes ndaj incidenteve, përbërja dhe ekspertiza e tyre

SLA

Trajnime të ndërgjegjësimit për përgjigjes ndaj incidentit, strategji të përditësuar për aftësitë e stafit të grupit për përgjigje ndaj e incidenteve;

Lista e veglave të gjurmimit dhe të aplikacioneve të përdorura në monitorimin e rrjetit dhe në përdorimin e tij</td><td>Metodat e analizimit

Verifikimi nëse grupi ka një statut të investigimit të incidenteve.

Verifikimi për ekspertizë në rrjete, sisteme operative dhe sigurinë të anëtarëve të grupit dhe sesi ata e kryejnë punën e tyre.

Rishikim i procedurave të tavolinës ndihmëse për të kontrolluar nëse procedurat e përshkallëzimit përcaktohen për incidente të cilat nuk mund të zgjidhen menjëherë në përputhje me kategorizimin e rreziqeve të përcaktuar në SLA.

Rishikim se cilat veprime janë ndërmarrë për zgjidhjen e incidenteve të mëparshme.

Rishikim i raporteve të çështjeve për të kontrolluar nëse personeli i duhur është përfshirë në investigimin e incidenteve.

Kontrolli se cilat mjete të menaxhimit të incidenteve janë përdorur -a janë të lidhura me nevojat e biznesit?

Verifikimi nëse organizata ka zhvilluar standarde dhe procedura të gjurmimit për tu siguruar se informacioni adekuat mblidhet nga gjurmët dhe programet e sigurisë dhe se të dhënat rishikohen periodikisht.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 9: Efektiviteti në përgjigjje

A rezulton strategjia e përgjigjes ndaj incidenteve në përgjigje efektive ndaj incidenteve?</td></tr>
<tr><td colspan="2">Kritere: Praktikat më të mira të përgjigjes ndaj incidenteve (COBIT, ITIL)</td></tr>
</table>

Informacioni i kërkuar	Metodat e analizimit
Planet e veprimit në përgjigje ndaj incidenteve, format e gjurmëve, etj. Trajnime periodike mbi ndërgjegjësimin ndaj sigurisë Procedurat e trajtimit të incidenteve- udhëzime mbi prioritizimin e incidenteve Raportet e çështjeve dhe veprimet e ndërmarra	Verifikim nëse një prioritet i përgjigjes/trajtimit të incidentit është caktuar për çdo aset ose shërbim. Verifikimi nëse procedurat parashikojnë kapjen dhe analizën e të dhënave të paqëndrueshme dhe statike në kohën e duhur.. Verifikim nëse grupi i përgjigjes ndaj incidenteve ndërgjegjëson periodikisht përdoruesit rreth politikave dhe procedurave në lidhje me përdorimin e duhur të rrjetit, sistemeve, mediumeve të jashtme dhe aplikacioneve. Rishikimi dokumentet për të parë nëse aktivitetet pas incidenteve, siç është trajnimi rifreskues, u është dhënë grupeve të përdoruesve për të shmangur përsëritjen e kushtueshme të incidenteve të rëndësishme. Verifikimi nëse është identifikuar burimi i incidentit. Observim për veprimet e ndërmarra. (Ndryshimi i procedurave, vërejtjet, trajnimet, etj.) Kontrolli nëse grupi i përgjigjes ndaj incidenteve regjistron të gjitha incidentet e zgjidhura në detaje dhe rishikon informacion për përditësim të mundshëm në bazën e njohurive.
Konkluzioni i auditimit:	Të plotësohet nga audituesi

4.4.Menaxhimi i ndryshimit
Objektivi i auditimit: Vlerësimi nëse institucioni ka implementuar një procedurë të standardizuar për kontrollin e të gjitha ndryshimeve në sistemet dhe aplikacionet kryesore të TI-së.
Çështja e auditimit nr. 10: Politikat A ka organizata një politik të aprovuar për menaxhimin e ndryshimeve, e cila përmban kontrollet e përshtatshme përgjatë ciklit të ndryshimit?
Kriteret: Praktikat më të mira në kontrollin e ndryshimeve: Kërkesë për ndryshim - vërtetimi - pranimi - prioritizimi - ndryshimi i dizajnit - testimi i ndryshimit - implementimi – dokumentimi.

Informacioni i kërkuar	Metodat e analizimit
Politikat dhe procedurat e menaxhimit të ndryshimit, diagramet e rrjedhjes së proceseve Statuti i bordit të kontrollit t ndryshimit; Periudha e rishikimit të politikave Dokumentacioni i ndryshimit:-Kërkesa për ndryshim, Procedurat e testimit të kontrollit të ndryshimit, plani i sigurimit të cilësisë, planet dhe procedurat e testimit Raportet dhe gjurmët e programit të menaxhimit të ndryshimit Procesverbalet e takimeve të bordit të kontrollit të ndryshimeve Raportet përmbledhës të menaxhimit të ndryshimit të marrë parasysh nga menaxhmenti	Referojuni kërkesave të përgjithshme për politikat dhe procedurat në seksionin *Qeverisja TI-së.* Rishikim i politikave të menaxhimit të ndryshimit për të verifikuar nëse procedurat për nisjen, rishikimin dhe aprovimin e ndryshimit janë shtrirë dhe pozicionuar sipas përgjegjësive dhe detyrave. Rishikoni statutin e bordit kontrollues të ndryshimit për të identifikuar ndarjen e përgjegjësive dhe niveleve të përgjegjësisë. Intervista me personelin, observim i praktikave aktuale dhe rishikim i dokumenteve për të siguruar se procedurat e menaxhimit të ndryshimit janë ndjekur: Kërkoni që të shihni një ndryshim, gjurmoni ndryshimin në mjedisin operacional, shihni procedurat e nevojshme-p.sh. a është ndjekur menaxhimi i rishikimi dhe prioritizimit , shihni për aprovim dhe dokumentim. Shihni nëse sigurimi i brendshëm i cilësisë ka bërë një vlerësim. Rishikoni nëse rishikimi adekuat i gjurmëve dhe raporteve është bërë nga menaxhmenti ku përdoret një softuer i menaxhimit të ndryshimit Sigurohuni se qasja në librarinë aplikacioneve (p.sh. source code, konfigurimet) është i limituar për stafin dhe se struktura e TI-së parandalon ndryshimet e paautorizuara në mjedisin operacional. Rishikoni dokumentet, vëzhgoni praktikat për të siguruar që përdoruesit e biznesit janë të përfshirë gjatë testimit të ndryshimeve për të siguruar korrektësi Sigurohuni se ndryshimet në softuer janë të përshtatshme dhe të aprovuara këto nga palët përkatëse të biznesit para se të kalojnë në ambient produktiv.
Çështja e auditimit nr. 11: Procedurat e tërheqjes Si siguron struktura e TI-së që organizata mund të kthehet përsëri në një version të mëparshëm nëse është e nevojshme?	
Kriteret: Praktikat më të mira të menaxhimit të ndryshimit- dokumentacion mbi procedurat dhe përgjegjësitë për rikuperimin e zonave të prekura për shkak të ndikimit të padëshiruar të ndryshimit.	

Informacioni i kërkuar	Metodat e analizimit
Procedurat e menaxhimit të ndryshimit Dokumentacion mbi testimet dhe implementimet e ndryshimeve Dokumentim të rikthimit dhe gjurmë të ndryshimeve në konfigurim Procedurat e backup-it dhe të rivendosjes.	Rishikim i dokumentacionit, intervista me përdoruesit e biznesit për të gjetur nëse ndikime të paqëllimshme të ndryshimeve/përmirësimeve në funksionalitete janë adresuar me prioritet, në përputhje me interesat e biznesit.
Çështja e auditimit nr. 12: Ndryshimet emergjente A janë kontrolluar ndryshimet emergjente në mënyrë të duhur kur procedurat e menaxhimit të ndryshimit për përcaktimin, autorizimin, testimin dhe dokumentimin e ndryshimeve nuk mund të ndiqen?	
Kriteret: Organizata duhet të ketë të vendosura procedura për ndryshimet emergjente.	
Informacioni i kërkuar	**Metodat e analizimit**
Procedurat e kontrollit të ndryshimeve emergjente Dokumentim të ndryshimeve emergjente që janë kryer gjatë periudhës së audituar.	Rishikim të procedurave të menaxhimit të ndryshimeve për të identifikuar nëse përmbajnë një seksion të dedikuar dhe një set procedurash për të kontrolluar ndryshimet emergjente në sistem. Kërkoni një shembull të ndryshimeve emergjente. Bëni krahasime me procedurat e dokumentuara. Shihni për çfarë është bërë testimi përpara prezantimit në ambientin produktiv. Nëse nuk ekzistojnë procedura të dokumentuara, pyesni sesi ata kanë ditur se çfarë të bëjnë dhe kush i aprovon ato ndryshime. Ekzaminoni nëse ndryshimet emergjente janë aprovuar nga anëtarët e duhur përpara zhvendosjes në ambient produktiv.
Çështja e auditimit nr. 13: Dokumentimi dhe mbyllja e ndryshimeve A janë ndjekur proceset e duhura për përditësimin e sistemeve dhe dokumentacionin e përdoruesit pas implementimit të një ndryshimi?	

Kriteret: Praktikat më të mira të menaxhimit të ndryshimit (p.sh. Cobit, ITIL mbi mbështetjen e shërbimit).	
Informacioni i kërkuar Dokumentim të proceseve të funksionaliteteve të prekura nga ndryshimet; Procedurat e vendosura për dokumentim.	**Metodat e analizimit** Rishikim të dokumenteve për tu siguruar për gjithëpërfshirje dhe qëndrueshmëri të ndryshimeve të implementuara. A kanë ndjekur procedurat operacionale, informacionet e konfigurimit, dokumentimi i aplikacionit, ndihma dhe materialet e trajnimit dhe të njëjtat konsiderohen të jenë pjesë integrale e ndryshimit Ekzaminim nëse ekziston një periudhë e përshtatshme ruajtjeje për dokumentacionin e ndryshimit dhe sistemin para dhe pas ndryshimit dhe dokumentacionin e përdoruesit. Ekzaminim nëse ekzistojnë mekanizmat për përditësimin e proceseve të biznesit për ndryshime në harduer ose softuer për tu siguruar se përdoren funksionalitetet e reja dhe ato të përmirësuara.
Konkluzioni i auditimit:	Të plotësohet nga audituesi

Shtojca V. Matrica e sugjeruar e auditimit mbi kontraktimin

5.1.Politikat e kontraktimit	
Objektivi i auditimit: Vlerësimi nëse subjekti posedon politika të përshtatshme të kontraktimi?	
Çështja e auditimit nr. 1: Elementet kyçe të politikës së kontraktimit A posedon subjekti politika të kontraktimit?	
Kriteret: Politikat organizative mbi kontraktimin.	
Informacioni i kërkuar	**Metodat e analizimit**
Dokumentet e politikave; Proceset e aprovuara për kontraktimin e funksioneve/shërbimeve; Listë me funksionet/shërbimet e kontraktuara; Listë me funksionet/shërbimet të kontraktuara pjesërisht; Mënyra e shërbimit të ofruesi i shërbimit; Analiza e kost-benefiteve për shërbimet/funksionet e kontraktuara Listë e ofruesve të shërbimeve të kontraktuara me vendndodhjet e tyre; Dokumentet lidhur me aprovimin e shërbimeve/funksioneve të kontraktuara	Rishikim i politikave për tu siguruar nëse është aprovuar Rishikim të politikave për të kontrolluar (për shembull) nëse përmban informacion rreth aseteve të organizatës që mund të kontraktohen ose jo, nëse identifikon listën e shërbimeve/funksioneve që mund të kontraktohen. Rishikim të dokumenteve të aprovimit të blerjes ose të kontraktimit për tu siguruar nëse menaxhmenti i lartë është përfshirë në aprovim. Rishikim të dokumenteve për të vlerësuar se organizata ka identifikuar rreziqet e lidhura me mënyrat e ndryshme të kontraktimit dhe vendndodhjes së ofruesve të shërbimit. Rishikim të dokumenteve për të verifikuar nëse organizata ka siguruar vazhdimësinë e biznesit, të drejtat e të dhënave, sigurinë, zotërimin dhe kostot janë shpërndarë sipas marrëveshjes që mbulon blerjen. Rishikim të dokumenteve për të vlerësuar se politikat përfshijnë identifikimin e parametrave të monitorimit për funksionet e kontraktuara.

Strategjia për të siguruar vazhdimësinë në rast të marrjes së shërbimit nga një organizatë tjetër; Informacion rreth marrjes së një ofruesi të shërbimi Dokumentet/raportet e monitorimit	
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.2.Dokumentimi i kërkesave	
Objektivi i auditimit: Vlerësimi nëse organizata posedon politika për mënyrën e menaxhimit të dokumentimit të kërkesave.	
Çështja e auditimit nr. 2: Politika dhe procesi i kërkesës - A ka organizata politika mbi blerjen? - A ka organizata një proces të përcaktuar për identifikimin dhe përzgjedhjen e ofruesve të shërbimit? - A ka organizata një proces për sigurimin e përfshirjes së kërkesave të përdoruesve në Kërkesat e Nivelit të Shërbimit/ kërkesat kontraktuale? - Vendimet që merren a janë në nivelet e përshtatshme?	
Kriteret: Dispozitat e politikave të organizatës mbi kontraktimin dhe politikave të prokurimeve të shërbimeve të TI-së që lidhen me dokumentimin e kërkesave.	
Informacioni i kërkuar	**Metodat e analizimit**
Politikat e blerjes ose ekuivalente me to	Rishikim i dokumenteve për të verifikuar nëse organizata ka politika mbi dokumentimin e kërkesave ose blerjes.
Lista e ligjeve që rregullojnë blerjen dhe kontraktimin	Rishikim të politikave për të siguruar se përmban dispozita për kërkesat e të dhënave nga nënkontraktorët nëse kontraktori kryesor ka kërkuar përfshirjen e nënkontraktorëve si pjesë të propozimit.
Përzgjedhje e proceseve për identifikimin dhe zgjedhjen e ofruesve të shërbimeve	Rishikim të dokumenteve për të vlerësuar se politikat mbi dokumentimin e kërkesave janë në pajtim me ligjet mbi prokurimin dhe blerjen (rishikim se i referohet për të ofruar lidhje me ligjet dhe rregullat e aplikuara).

Lista e funksioneve/shërbimeve të kontraktuara Kërkesat e përdoruesve për shërbimet e kontraktuara Kontrata/Marrëveshja në nivel shërbimi Dokumentet lidhur me aprovimin për përzgjedhjen e ofruesit të shërbimit	Rishikim të procesit të përzgjedhjes për pajtueshmëri ndaj politikave për çdo kontratë të zgjedhur ose për shërbim të kontraktuar (rishikim nëse procesi i përzgjedhjes është transparent, ka kritere objektive, komisioni i përzgjedhjes është i përbërë nga personel që kupton kërkesat, është i përfaqësuar nga personel të kontraktuar dhe ligjor dhe këshillohet me përdoruesit). Sigurohuni se kërkesat kontraktuale janë aprovuar nga përdoruesit dhe nga palët e interesit. Zhvilloni takime me zyrën kontraktuese për të siguruar që një nivel i duhur i menaxhmentit - ka aprovuar kontratën dhe dokumentimin e kërkesave.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.3.Monitorimi i furnizuesit ose kontraktorit	
Objektivi i auditimit: Vlerësimi nëse organizata menaxhon kontraktorin ose furnitorin dhe ndërmerr veprimet e duhura nëse performanca ose cilësia shmanget nga bazat e vendosura.	
Çështja e auditimit nr. 3:Monitorimi i ofruesit të shërbimit - A ekziston një kontratë me ofruesin e shërbimit? - A janë identifikuar nivelet e shërbimi dhe a janë aprovuar nëpërmjet një marrëveshjeje në nivel shërbimi? - A ekziston një marrëveshje monitorimi për ofruesin e shërbimit? - A janë siguruar nivelet e shërbimit nëpërmjet kësaj marrëveshjeje? - A ndërmerren veprimet e duhura në rast se nuk arrihen dispozitat e marrëveshjes?	
Kriteret: Dispozitat/parametrat e përcaktuar në Marrëveshjen në Nivel Shërbimi dhe veprimet për përcjelljen të tyre nga organizata.	
Informacioni i kërkuar	**Metodat e analizimit**
Kontrata /Marrëveshja në nivel të Shërbimit	Rishikim të dokumenteve për të vlerësuar nëse është vendosur marrëveshja në nivel shërbimesh.
Oraret e aprovuara, bazat, kostot dhe parametrat e tjerë	Rishikim të raporteve të monitorimit të dorëzuara nga kontraktori për tu siguruar se ato përmbajnë elementë që janë në kontratë ose në SLA

teknikë që përcaktojnë produktin ose shërbimin që është blerë/kontraktuar Dokumentet e monitorimit/raportet/ procesverbalet e takimeve të rishikimeve të kryera, veprimet e ndërmarra, drejtimet e furnitorit; Vlerësimi i ndikimeve të devijimeve; Veprimet ose drejtimet e furnitorit; Raportet e veprimeve të ndërmarra mbi devijimet nga nivelet e shërbimeve.	(marrëveshja në nivel shërbimi), elementë si kosto, orari, performanca, rreziku, statusi, çështjet dhe situata e veprimeve ose detyrave të mëparshme). Rishikim të raporteve të monitorimit për të identifikuar mangësitë e shërbimit/ devijimet si dhe vlerësim të ndikimit për shkak të këtyre mangësive /devijimeve. Rishikimi i njoftimeve dhe raporteve të ndërmarra për veprimet e ndërmarra për të qenë në përpjesëtim me ndikimin në biznes dhe dispozitat kontraktuale.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.4.E drejta në të dhëna
Objektivi i auditimit: Vlerësimi nëse kërkesat për mbrojtjen e të dhënave të organizatës janë identifikuar dhe nëse ato janë pjesë e kërkesave kontraktuale.
Çështja e auditimit nr. 4: Mbrojtja dhe menaxhimi i të dhënave - A janë përfshirë mbrojtja e të dhënave dhe të drejtat e qasjes në kontratën e shërbimit? - A janë përcaktuar në mënyrë të përshtatshme të dhënat për të mbuluar të dhënat e transaksioneve ashtu si edhe programet që mbështesin të dhënat, në varësi të rastit? - A ekziston një mekanizëm që siguron se kërkesat për mbrojtjen e të dhënave dhe për sigurinë ashtu si SLA është adaptuar dhe implementuar nga ofruesi i shërbimit?
Kriteret: Kërkesat për mbrojtjen e të dhënave të organizatës dhe për të drejtat e qasjes janë përcjellë te kontraktori në formën e duhur.

Informacioni i kërkuar	Metodat e analizimit
Kërkesat për Mbrojtjen e të Dhënave të Organizatës dhe kërkesat për të drejtat e qasjes Përcaktim i të dhënave (për mbrojtje dhe të drejtë në qasje) Kontrata me ofruesin e shërbimit Lista e regjistrave të qasjes së të dhënave nga ofruesi i shërbimeve Raportet nga auditimet e jashtme ose vetë-vlerësimet së bashku me rekomandimet dhe përcjellja e tyre; Raporte monitorimi Korrespondenca me ofruesin e shërbimit Raportet e trajtimit të incidenteve Marrëveshje e mosdhënies së informacioneve me kontraktorin	Rishikimi i dokumentit mbi përshtatshmërinë e mbrojtjes së të dhënave dhe kërkesat e të drejtave të qasjes/përkufizimi i të dhënave Rishikimi i dokumentit të kontratës me ofruesin e shërbimit për të kontrolluar përfshirjen e kërkesave për Mbrojtjen e të Dhënave dhe të drejtat e qasjes.. Rishikim të dokumenteve, raporteve të auditimeve të jashtëm / vetëvlerësimeve. Rishikimi i dokumentit të raporteve të monitorimit, korrespodencës dhe raporteve të trajtimit të incidenteve për të vlerësuar aktivitetet vijuese nga organizata.. Rishikimi i marrëveshjes për mos-dhënien e informacioneve për të verifikuar nëse të gjitha informacionet përkatëse janë të mbuluara. Verifikimi nëse shpalosja e informacionit nga kontraktori është e autorizuar.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.5.Ofruesit e shërbimeve jashtë shtetit

Objektivi i auditimit:

Përcaktimi nëse organizata ka strategji mbi shërbimet e kontraktuara në ofruesit jashtë shtetit.

Çështja e auditimit nr. 5: Menaxhimi i tregtarit jashtë shtetit Vlerësimi nëse organizata njeh çështjet e përfshira në kontraktimin e subjekteve të huaja gjatë kontraktimit të ofruesve të shërbimit jashtë shtetit.	
Kriteret: Dispozitat e politikave të kontraktimit të lidhura me kontraktimin e subjekteve jashtë shtetit. Ligjet e rregullimit të biznesit me subjekte jashtë shtetit.	
Informacioni i kërkuar	**Metodat e analizimit**
Lista e ligjeve dhe rregullave lidhur me shërbimet e kontraktuara	Rishikim të dokumenteve për të vlerësuar nëse organizata ka identifikuar rreziqet e lidhur me kontraktimin e subjekteve jashtë shtetit
Informacion mbi çdo lloj prezence të ofruesve të shërbimeve	Rishikim i dokumenteve për të vlerësuar analizat e kost-benefiteve të cilat adresojnë rreziqet e lidhura me kontraktimin e subjekteve jashtë shtetit.
Listë e ligjeve dhe rregullave që rregullojnë shërbimet e kontraktura në shtetin përkatës të ofruesit jashtë shtetit	Rishikim të dokumenteve për të vlerësuar se kontrolle të mëparshme janë kryer ndaj ofruesit të shërbimeve në mënyrë të përshtatshme.
Lista e zyrave të jashtme në organizatë	Rishikim të dokumenteve për të vlerësuar se ekziston një sistem i fuqishëm për të siguruar performancën e SLA dhe kontratës.
Marrëveshje bilaterale në mes vendit të organizatës dhe ofruesit të shërbimeve që lehtësojnë marrëveshjet e jashtme	Rishikim i dokumenteve për të vlerësuar se çdo devijim nga SLA dhe kontrata ndiqet në mënyrë të menjëhershme për të minimizuara humbjet në organizatë.
Raporte mbi performancën e ofruesit të shërbimit në ofrimin në kohë dhe në cilësi	
Analiza kost-benefit të ofruesve vendas dhe të huaj	
Kontrata dhe SLA	

Informacion mbi situatën financiare të furnitorëve Lista e devijimeve nga SLA dhe kontrata Raporte monitorimi dhe ndjekje mbi veprimet e ndërmarra ndaj devijimeve të ofruesve të shërbimit	
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.6.Mbajtja e njohurive të biznesit / Pronësia e proceseve të biznesit	
Objektivi i auditimit: Vlerësimi nëse organizata mban njohuritë e biznesit dhe pronësinë e proceseve të biznesit	
Çështja e auditimit nr. 6: Politika mbi pronësinë e njohurive dhe proceseve të biznesit - A është përcaktuar dhe dokumentuar mirë pronësia e proceseve të biznesit? - A sigurohet që humbja e njohurive të biznesit për shkak të kontraktimit të mos ndodhë? A ka kapacitete për zhvillimin e shërbimeve të kontraktuara në organizatë? - A sigurohet vazhdimësia e biznesit nëse tregtari nuk ka mundësi të ofrojë në një pikë në të ardhmen këto shërbime?	
Kriteret: Organizatat mbajnë njohuritë e biznesit dhe janë në gjendje të vazhdojnë operacionet brenda funksionit kritik nëse kontraktorët ose shitësit nuk janë në gjendje të ofrojnë shërbimin. Mbajtja e pronësisë së proceseve të biznesit Mbajtja e njohurive të biznesit Performanca vazhdimësisë së biznesit në raport të dështimit të ofruesit të shërbimit për ta bërë më këtë shërbim në të ardhmen.	
Informacioni i kërkuar	**Metodat e analizimit**
Identifikim të proceseve të biznesit, si dhe të aftësive kritike të nevojshme që duhet të mbesin brenda	Rishikim të dokumenteve për të vlerësuar nëse pronësia e proceseve, e të dhënave dhe e programit aplikativ mbahet nga organizata nëpërmjet dispozitave të përshtatshme në kontratë. Rishikim të dokumentave për të vlerësuar nëse njohuritë e biznesit në kushtet e të dhënave, programit aplikativ, ndërtimit të sistemit janë të

Dokumentim të proceseve të biznesit Dokument të detajuar të ndërtimit të sistemit të shërbimit të kontraktuar Lista e personelit të trajnuar në proceset e biznesit, ndërtimin e sistemit, të dhënat, programet aplikative. Raporte të incidenteve /korrespondenca lidhur me ndërprerjen e shërbimit/ mosmarrëveshje me ofruesin e shërbimit, përfshirë ato me pronarin e sistemit/të dhënave. Procesverbale të takimeve me kontraktorin	mirë-dokumentuara dhe nëse personeli është i rifreskuar më këto periodikisht nëpërmjet trajnimeve, etj. Rishikim të dokumenteve për të vlerësuar nëse personeli i organizatës është i përfshirë në çdo përditësim të sistemit të kryer nga subjekti i kontraktuar dhe nëse dokumentacioni i përditësimit të sistemit ofrohet në organizatë. Rishikim të dokumenteve për të vlerësuar nëse ekzistojnë incidente ose ndërprerje me ofruesin e shërbimit referuar pronësisë së sistemit dhe të dhënave. Rishikim të procesverbaleve të mbajtura gjatë takimeve me kontraktorët për tu siguruar nëse ekzistojnë nivele të larta rreziku, të cilat menaxhohen dhe gjurmohen për të siguruar vazhdimësinë e operacioneve.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.7.Kontrolli dhe menaxhimi i kostos

Objektivi i auditimit:

Vlerësimi nëse organizata ka siguruar kostot më ekonomike nëpërmjet ciklit të jetës së kontratës së kontraktuar.

Çështja e auditimit nr. 7: Vlerësimi i kostos dhe benefitit

- A janë identifikuar të gjitha kostot e kontraktimit (përfshirë ato të së ardhmes)?
- A janë kryer analizat kost-benefit për alternativën më të mirë të zgjedhur?
- A ka përgjegjësi specifike për organizatën në burimet e jashtme dhe a kanë ato elemente/ndikime kritike të kostove të ndërtuara brenda? (A ngarkohen kosto të tjera ose përshkallëzuese ndaj subjektit?

Kriteret: Analiza kost-benefit është reale dhe është baza në të cilën menaxhohet dhe kontrollohet programi.	
Informacioni i kërkuar	**Metodat e analizimit**
Analizat fillestare kost-benefit Kostot e vlerësuara të kontratës me burimet e jashtme Procesi i përzgjedhjes së ofruesit të shërbimit kundrejt kosotos së një elementi. Dokumentet të aprovimit të procesit lidhur me përzgjedhjen. Elemente të kostove tjera të përshkallëzuara nga ofruesi i shërbimeve SLA dhe kontrata Raporte monitorimi në raport të funksioneve të veçanta/aktiviteteve për të cilat kostot alternative/të përshkallëzuara janë matur. Dokumentet e veprimit mbi kërkesat për kosto alternative/të përshkallëzuara nga ofruesi i shërbimit	Rishikim të dokumenteve për të vlerësuar nëse të gjitha kostot janë identifikuar nga organizata, rishikuar dhe aprovuar nga palët e interesit. Rishikim të dokumenteve në procesin e aprovimit dhe përzgjedhjes. Rishikim të dokumenteve për të vlerësuar nëse të gjitha kostot janë reflektuar në kontratë dhe nëse ekzistojnë kosto të tjera të fshehura, përfshirë kosto të ardhshme. Rishikim të të gjitha kostove për të verifikuar nëse janë subjekt i analizave përpara angazhimit. Rishikim dhe krahasim të kostove të vlerësuara me shpenzimet aktuale në kontratë. Rishikim të shpenzimeve në buxhet. Rishikim të performancës së ofruesit të shërbimit mbi aktivitetin/funksionin specifik për të cilin janë evidentuar ndryshime në kosto nëpërmjet raporteve të monitorimit dhe vlerësimi i nevojës për ndryshim. Rishikim të veprimeve nga organizata në kostot shtesë/të përshkallëzuara nga ofruesi i shërbimeve.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.8.Marrëveshja në Nivel Shërbimi (SLA)

Ovjektivi i auditimit: Vlerësimi nëse subjekti ka zhvilluar një marrëveshje të detajuar në nivel shërbimi së bashku me të gjitha kërkesat dhe nëse aktivisht monitoron tregtarit kundrejt marrëveshjes.

Çështja e auditimit nr. 8: Përshtatshmëria/Adekuatshmëria e SLA

- A ekziston një marrëveshje në nivel shërbimi në mes të organizatës dhe ofruesit të shërbimit?
- A është e mjaftueshme marrëveshja e detajuar për të identifikuar të gjitha detyrat dhe përgjegjësitë në mes të organizatës dhe ofruesit të shërbimit?
- A është implemntuar në mënyrë të përshtatshme marrëveshja?
- A posedon organizata një mekanizëm për monitorimin e implementimit të marrëveshjes në nivel shërbimi?
- A ekziston një mekanizëm për adresimin e pritshmërive të marrëveshjes?

Kriteret: Marrëveshja në nivel shërbimi është baza për monitorimin dhe kontrollin e kontraktorit ose furnitorit kundrejt specifikimeve teknike.

Informacioni i kërkuar	**Metodat e analizimit**
SLA ose kontrata	Rishikim të dokumentacionit për të vlerësuar se të gjitha kërkesat e përdoruesve janë përkthyer në kërkesat e nivelet e shërbimit.
Kërkesat teknike (lista e shërbimeve që do të kryhen nga ofruesi i shërbimit)	Rishikim të dokumenteve për të vlerësuar se detyrat dhe përgjegjësitë e organizatës dhe të tregtarit janë identifikuar dhe janë implementuar.
Lista e përgjegjësive të organizatës dhe të ofruesit të shërbimit	Rishikim të dokumenteve për të vlerësuar nëse parametrat për nivelet e performancës janë identifikuar qartësisht dhe nëse janë përfshirë në marrëveshjen në nivel shërbimi.
Bazat për shërbimet që do të maten, periudha e matjes, kohëzgjatja, vendndodhja dhe periudha e raportimit (normat e defekteve, koha e përgjigjes, orët e tavolinës ndihmëse, etj.)	Rishikim të dokumenteve për të vlerësuar nëse mekanizmi i monitorimit të nivelit të shërbimit është vendosur dhe është aprovuar nga organizata dhe ofruesi i shërbimit. Rishikim të raporteve të statusit të tregtarit për të vlerësuar nëse parametrat në SLA raportohen nga kontraktori dhe rishikohen nga personeli i duhur në organizatë.
Raportet periodike të statusit të performancës së tregtarit	Vlerësim të pajtueshmërisë së parametrave teknikë të SLA. Verifikim të veprimeve të ndërmarrë nga organizata për devijimet nga SLA.

Konkluzioni i auditimit: Të plotësohet nga audituesi

5.9.Siguria

Objektivi i auditimit:

Vlerësime nëse kërkesat e sigurisë janë adresuar në prokurim dhe janë në përputhje me to.

Çështja e auditimit nr. 9: Përgjigja ndaj kërkesave të sigurisë

- A janë identifikuar kërkesat e sigurisë nga organizata referuar shërbimeve të jashtme?
- A ekziston mekanizëm që siguron se kërkesat e sigurisë janë adresuar nga ofruesi i shërbimit?
- A posedon organizata një mekanizëm për monitorimin e pajtueshmërisë së kërkesave të sigurisë nga ofruesi i shërbimit?

Kriteret: Kërkesat e sigurisë së organizatës janë theksuar nga kontraktori në mënyrë të përshtatshme.

Informacioni i kërkuar	**Metodat e analizimit**
Politikat e sigurisë së organizatës	Rishikim të dokumenteve për të vlerësuar se kërkesat e sigurisë janë identifikuar prej organizatës dhe janë hartuar në kontratë ose në SLA.
Kontrata e kontraktimit (shërbimeve të jashtme)	Verifikim nëse organizatës ka një inventar të të dhënave, të programeve aplikativë.
SLA	Verifikim nëse organizata monitoron/ është e ndërgjegjshme për statusin e të dhënave, programeve aplikativë dhe pajisjeve, nëse ato janë ruajtur gjatë procesit të backup-it dhe gjatë procesit të rimëkëmbjes, të kryera këto nga ofruesi i shërbimit.
Inventar i të dhënave, programe aplikative dhe pajisjeve me ofruesin e shërbimit	Verifikim nëse organizata ka siguri mbi autorizimin e ndryshimeve në të dhëna, programe aplikativë dhe pajisje kompjuterike.
Inventar të dosjeve backup të të dhënave dhe programeve aplikativë me ofruesin e shërbimit	Verifikim nëse organizata ka siguri mbi autorizimin e qasjes në të dhëna, programe aplikativë dhe pajisjet kompjuterike në vendndodhjen e kontraktorit nëpërmjet studimit të gjurmëve të qasjes (fizike dhe logjik).
Gjurmë të kontrollit të qasjes së të dhënave, programeve aplikativë, ashtu si edhe pajisjet kompjuterike në vendndodhjen e kontraktorit	Verifikim nëse organizata ka siguri mbi mekanizmat e sigurisë të vendosura nga ofruesi i shërbimit.
Plani i sigurisë për ndërtesën ku ndodhen backup (të dhënat rezervë)	Verifikim nëse organizata merr raporte të rregullta dhe akte mbi informacionin e raporteve të monitorimit.

dhe qendrën për rikthim nga fatkeqësitë Raportet e monitorimit referuar çështjeve të sigurisë Korrespondenca në mes të organizatës dhe ofruesit të shërbimit referuar çështjeve të sigurisë	
Konkluzioni i auditimit: Të plotësohet nga audituesi	

5.10. Backup (PVB) dhe rimëkëmbja nga fatkeqësitë (PRFPRF) për shërbimet e kontraktuara	
Objektivi i auditimit: Vlerësimi nëse shërbimet e /kontraktuara i përmbahen planeve të rimëkëmbjes nga fatkeqësitë dhe të backup-it siç kërkohen në kontratë ose në SLA.	
Çështja e auditimit nr. 10: Procedurat e Backup-it dhe të rikthimit A plotëson furnitori kërkesat e kontratës ose të SLA për PVBdhe PRF?	
Kriteret: Marrëveshje ose kontratë mbi nivelin e shërbimit për PVB dhe PRF të tregtarit.	
Informacioni i kërkuar Kontrata ose SLA Auditimi i Brendshëm ose certifikim i jashtëm për gatishmërinë e PVB dhe PRF të tregtarit Raporte periodike mbi PVB/PRF si dhe testimet ose përditësimet e tyre	**Metodat e analizimit** Rishikim të kontratave ose SLA për tu siguruar se tregtarit i është kërkuar të siguroj PVB dhe PRF mbi të dhënat e prokuruara/kontraktuara, aplikacionet dhe shërbimet. Rishikim të kontratës ose SLA-së për tu siguruar se tregtari ofron raporte të audituesve të pavarur që konfirmojnë se ekzistojnë aktivitetet PVB/PRF dhe se tregtari i teston ato periodikisht. Rishikim të raporteve të dorëzuara nga tregtari për tu siguruar se testimi është kryer në përputhje me kushtet e kontratës dhe të SLA-së. Rishikim të raporteve periodike për tu siguruar se procedurat janë përditësuar sipas nevojave.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

Shtojca VI. Matrica e sugjeruar e auditimit mbi PVB//PRF

6.1.Politikat e Vazhdimësisë së Biznesit	
Objektivi i auditimit: Vlerësimi nëse ekzistojnë politika efektive mbi vazhdimësinë e biznesit në organizatë.	
Çështja e auditimit nr. 1: Politikat organizative mbi vazhdimësinë e biznesit A posedon organizata plan dhe procedura të qëndrueshme për vazhdimësinë e biznesit?	
Kriteret: Politikat organizative mbi vazhdimësinë e biznesit, të cilat përmbajnë detyrat dhe përgjegjësitë, qëllimin, kriteret e alokimit të burimeve/parimet, kërkesat për trajnim, orar të mirëmbajtjMees, orarin e testimeve, planet backup, si dhe nivele e aprovimit. Alternative: Organizata ka plan dhe politika të publikuara të qëndrueshme të cilat mbulojnë të gjitha fushat e operacioneve dhe identifikon qartësisht kërkesat për trajnim dhe oraret e testimit.	
Informacioni i kërkuar	**Metodat e analizimit**
Dokument i Politikave të Vazhdimësisë së Biznesit Dokument i Politikave të TI-së Procesi i aprovimit për adaptimin e objektivave të politikës së biznesit Korrespondenca dhe procesverbalet e mbledhjeve lidhur me vazhdimësinë e biznesit	Rishikim të dokumenteve për të vlerësuar nëse politikat janë konsistonte me politikat e përgjithshme të TI-së në organizatë. Rishikim të dokumenteve për të vlerësuar se politikat adresojnë kërkesat për vazhdimësi biznesi duke përcaktuar objektivat e qëndrueshëm të organizatës, strukturën organizative dhe përgjegjësitë për planifikim emergjent. Rishikim se intervista me personelin për të përcaktuar sesa shpesh përditësohen politikat nëse ndryshojnë kushtet. Rishikim të politikave për të përcaktuar se nga kush janë aprovuar dhe kur është shpërndarë për herë të fundit/ Intervista me një mostër përdoruesish të biznesit për të vlerësuar nëse politikat janë komunikuar mjaftueshëm në organizatë.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

6.2.Struktura e Funksionit të Vazhdimësisë së Biznesit
Objektivi i auditimit: Vlerësimi nëse ekziston grupi i përshtatshëm i vazhdimësisë së biznesit.

Çështja e auditimit nr. 2: Funksioni i vazhdimësisë së biznesit A ekziston një grup ose funksion për vazhdimësinë e biznesit?	
Kriteret: Mbulim i të gjitha fushave kritike të organizatës në grup. Kërkesat për detyrat dhe përgjegjësitë për anëtarët e grupit.	
Informacioni i kërkuar Struktura organizative Struktura organizative e grupit të vazhdimësisë së biznesit Përshkrim të detyrave/ përgjegjësive të anëtarëve të grupit të vazhdimësisë së biznesit Procesverbale të korrespondencës/takimeve mbi temat e vazhdimësisë së biznesit Plan i vazhdimësisë së biznesit	**Metodat e analizimit** Rishikim të dokumenteve/intervistë me stafin përgjegjës për të vlerësuar të gjitha fushat kritike të organizatës të cilat duhet të përfaqësohen në grupin e vazhdimësisë së biznesit. Rishikim të dokumenteve për të vlerësuar se ekzistojnë pronësi dhe detyra mbi përgjegjësitë e vazhdimësisë së biznesit në menaxhmentin e lartë. Për shembull, nëse menaxhmenti ka identifikuar nivelin dhe emergjencën e rimëkëmbjes dhe nëse është reflektuar kjo në politika. Rishikim të dokumenteve për të vlerësuar se të gjithë departamentet kritikë kanë përcaktuar anëtarë në grupin për rimëkëmbje nga fatkeqësitë së bashku me detyrat e mirë-përcaktuara. Intervista me një mostër të personelit në grupin e vazhdimësisë së biznesit/ ose ekuivalent, për të vlerësuar nëse ata janë të ndërgjegjshëm për rolin e tyre në vazhdimësinë e biznesit për secilën njësi/departament kritik të biznesit.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

6.3.Vlerësimi i ndikimit në biznes
Objektivi i auditimit: Verifikimi nëse vlerësimi i ndikimit në biznes dhe vlerësimi i rrezikut kanë përfunduar dhe ekziston një sistem i menaxhimit të rrezikut..
Çështja e auditimit nr. 3: Vlerësimi i rrezikut A janë realizuar analiza e ndikimit në biznesit dhe vlerësimet e rrezikut dhe a janë identifikuar dhe priorizuar të dhënat kritike, programet aplikative, operacionet dhe burimet?

Kriteret: Kuadri/struktura e menaxhimit të rrezikut të organizatës apo ekuivalente.

Politikat e vazhdimësisë së biznesit apo ekuivalente.

Përfundimi i vlerësimit të ndikimit në biznes dhe identifikim i të dhënave kritike, programit aplikativ, operacioneve dhe burimeve.

Informacioni i kërkuar	**Metodat e analizimit**
Raporte të vlerësimit të rreziqeve	Rishikim të dokumenteve për të verifikuar se vlerësimet e rreziqe janë kryer, kërcënimet e mundshme dhe ndikimet e tyre janë identifikuar.
Raporte të vlerësimeve të ndikimit në biznes	Rishikim të dokumenteve për të vlerësuar se të gjitha fushat funksionale janë marrë parasysh në vlerësimin e rreziqeve dhe të ndikimit në biznes.
Listë e të dhënave, të programeve aplikativë, të burimeve, operacioneve kritike për çdo funksion	Rishikim të dokumenteve për të vlerësuar se vendimet për reduktimin e rreziqeve janë marrë në nivelet e përshtatshme.
Listë e rreziqeve ekzistente	Rishikim të dokumenteve për të vlerësuar nëse organizata posedon RTO (Objektiva për Kohën e Rimëkëmbjes) dhe RPO (Objektivat për Pikat e Rimëkëmbjes) për çdo aplikacion kritik.
Raporte të rishikimeve të rreziqeve dhe të vlerësimit të ndikimeve në biznes	Rishikim të dokumenteve për të vlerësuar se RTO dhe RPO janë praktike dhe të arsyeshme për çdo aplikacion.
Politika/struktura të vlerësimit të rrezikut të organizatës	Rishikim të dokumenteve për të vlerësuar angazhimin e menaxhmentit të lartë.
Procesverbalet e takimeve mbi vlerësimet e rreziqeve dhe të ndikimeve në biznes	Rishikim të dokumenteve për të vlerësuar se palët e interesit janë të përfshira në identifikimin e rreziqeve dhe në vlerësimin e ndikimeve.

Çështja e auditimit nr. 4: Menaxhimi i rrezikut

A ekziston procesi i menaxhmit të rreziqeve dhe a janë vendosur prioritetet e përpunimit të emergjencave?

Kriteret: Mbulim i proceseve të menaxhimit të rrezikut nëpërmjet vlerësimit të rreziqeve dhe vlerësimit të ndikimeve në biznes.

Rreziqet dhe emergjencat janë adresuar me përpikëmëri sipas parametrave të vendosur nga organizata.

Informacioni i kërkuar	Metodat e analizimit
Dokument i procesit të menaxhimit të rrezikut	Rishikim të dokumenteve për të vlerësuar se procesi i menaxhimit të rrezikut adreson të gjitha pikat me përparësi të lartë..
Raportet e vlerësimit të rrezikut dhe të ndikimit në biznes	Intervista dhe rishikime dokumentesh për të vlerësuar se i gjithë personeli i përfshirë, si dhe menaxhmenti i lartë është i ndërgjegjshëm për detyrat dhe përgjegjësitë.
Listë e të gjithë personelit të përfshirë, anëtarë të grupit të PVB së bashku me detyrat dhe përgjegjësitë	Rishikim të dokumenteve për të vlerësuar nëse rreziqet ekzistente nuk kanë ndikim material në biznes.
Lista e artikujve të prioritizuar për proceset emergjente	Rishikim të dokumenteve dhe observim të tyre për të vlerësuar se çështjet emergjente janë trajtuar në mënyrë të përshtatshme. Rishikim të dokumenteve për të vlerësuar ndikimin e emergjencave.
Liste e rreziqeve të mbetura të identifikuara Listë e rasteve të proceseve emergjente të kërkuara Raportet e proceseve/përgjigjeve emergjente	Rishikim të procesverbaleve të takimeve, ose të listës së rreziqeve për të përcaktuar nëse rreziqet janë caktuar, aktivitetet e reduktimit janë përcaktuar dhe se rreziqet janë përcjellë periodikisht dhe statusi i tyre është përditësuar.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

6.4.Plani i rimëkëmbjes nga fatkeqësitë

Objektivi i auditimit:

Vlerësimi nëse Plani i Vazhdimësisë së Biznesit përfshin plane për backup dhe për rimëkëmbje për pajisjet kompjuterike, të dhënat, programet aplikativë dhe për qendrën e të dhënave dhe a është implementuar siç duhet?

Çështja e auditimit nr. 5: Procedurat e backup-it

A janë ndarë dhe implementuar në mënyrë efektive procedurat për backup-in e të dhënave dhe të programeve?

<table>
<tr><td colspan="2">Kriteret: Vendosja e pikave kritike të aplikacioneve dhe funksioneve për Vlerësimin e Ndikimit në Biznes të organizatës

Perioda e përcaktuar i backup-eve

Planet e dokumentuara të backup-it dhe të rimëkëmbjes</td></tr>
<tr><td>Informacioni i kërkuar

Planet dhe procedurat e backup-it për pajisjet kompjuterike, të dhënat dhe programet aplikative

Regjistrimet e backup-it si dhe versioneve të tij

Detyrat dhe përgjegjësitë për backup

Lista e vendndodhjeve të ruajtjes dhe periodiciteti

Periudha e ruajtjes

Marrëveshje e sigurisë për ndërtesën e backup-it

Regjistrat e trajnimit për personelin përgjegjës

Vlerësimi i ndikimeve të personelit përgjegjës

Raport mbi aktivitetet e rimëkëmbjes nga fatkeqësitë</td><td>Metodat e analizimit

Rishikim të dokumenteve për të vlerësuar se planet backup përfshijnë të gjithë pajisjet, të dhënat, programet aplikative kritike.

Rishikim të dokumenteve për të vlerësuar se janë hartuar procedurat e backup-it.

Rishikim të dokumenteve për të vlerësuar se plani i backup-it është implementuar në mënyrën e duhur.

Analiza e regjistrave për të vlerësuar se backup-i është ndërmarrë në afatet e duhura dhe se ruhet për kohën e specifikuar.

Verifikim nëse është i disponueshëm versioni i duhur i backup-it.

Rishikim të dokumenteve për të vlerësuar saktësinë e vendndodhjes së backup-it dhe mënyrën e transportit të backup.

Verifikim se siguria, fizike ose logjike, është e përshtatshme për ndërtesën e backup-it.

Rishikim të dokumenteve për të vlerësuar se procedurat e backup-it janë implementuar duke minimizuar humbje në kohë dhe në burime.

Rishikim të dokumenteve për të vlerësuar se procedurat e rimëkëmbjes janë ndarë dhe janë përfshirë në parametrat e rifillimit të sistemit, në instalimin e përditësimeve të programeve, vendosjen e parametrave të konfigurimit, disponueshmërinë e dokumentacionit të sistemit dhe të procedurave të operimit, ri-instalimin e programeve aplikative dhe të sistemit, disponueshmërinë e backup-eve të fundit, testimin e sistemit.

Rishikim të dokumenteve për të vlerësuar se procedurat e rimëkëmbjes janë implementuar me minimizim të humbjeve në kohë dhe në burime.

Rishikim të dokumenteve për të vlerësuar se personeli përgjegjës është trajnuar mbi procedurat e backup-it dhe të rimëkëmbjes.</td></tr>
<tr><td colspan="2">Konkluzioni i auditimit: Të plotësohet nga audituesi</td></tr>
</table>

6.5.Kontrolli i mjedisit

Objektivi i auditimit:

Vlerësimi nëse organizata posedon një kontroll të përshtatshëm të mjedisit në ndërtesat e backup-it.

Çështja e auditimit nr. 6: Mekanizmat e Kontrollit

Mekanizamt e kontrollit të mjedisit janë të ndarë dhe të vendosur në ndërtesat e bcakup-it.

Kriteret: Parametrat e kontrollit të mjedisit në mekanizmat e kontrollit të mjedisit.

Informacioni i kërkuar	**Metodat e analizimit**
Programi i kontrollit të mjedisit Listë e rreziqeve të mundshëm mjedisore të identifikuar gjatë vlerësimit të rrezikut së bashku me vendodhjet (dokument i vlerësimit të rrezikut) Listë e hapave të ndërmarrë referuar reduktimit të rreziqeve mjedisore	Rishikim të dokumenteve dhe verifikim të tyre për të vlerësuar se: - Ekziston një burim i pandërprerë i energjisë; - Ekziston sistem për mbrojtjen ndaj zjarrit; - Lagështira, temperatura dhe tensioni janë të kontrolluara; dhe të mbajtura brenda limiteve; - Ekziston sistem i mbrojtjes nga përmbytjet; - Kontrollet mjedisorë janë sipas rregulloreve; - Masat e kontrollit mjedisor janë të njohura dhe të zbatuara nga i gjithë stafi i lidhur me to;

Konkluzioni i auditimit: Të plotësohet nga audituesi

6.6.Dokumentimi

Objektivi i auditimit: Plani i vazhdimësisë së biznesit është i dokumentuar në mënyrë të duhur për të kryer përkohësisht aktivitete efektive të biznesit dhe procedurave të rimëkëmbjes pas një ndërprerjeje të biznesit.

Çështja e auditimit nr. 7: Plane të dokumentuara për backup dhe procedura të rimëkëmbjes, rolet dhe përgjegjësitë

A ka organizata një plan të dokumentuar të rimëkëmbjes nga fatkeqësitë që është i disponueshëm për backup dhe rikthim?

Kriteret: Disponueshmëria dhe saktësia e planit të vazhdueshmërisë së biznesit dhe planit të rimëkëmbjes nga fatkeqësitë.	
Informacioni i kërkuar	**Metodat e analizimit**
Plani i vazhdimësisë së biznesit	Rishikim të dokumenteve për të vlerësuar saktësinë e planit të vazhdueshmërisë së biznesit.
Plani i rimëkëmbjes nga fatkeqësitë	Rishikim të dokumenteve për të vlerësuar saktësinë e planit të rimëkëmbjes nga fatkeqësitë.
Versioni i planit të vazhdimësisë së biznesit dhe i rimëkëmbjes nga fatkeqësitë	Verifikim nëse versioni më i fundit i dokumenteve të planeve të vazhdueshmërisë dhe të rimëkëmbjes janë komunikuar tek personat e duhur.
Lista e shpërndarjes së planeve të vazhdimësisë së biznesit dhe rimëkëmbjes nga fatkeqësitë për të gjitha palët e interesit	Përcaktoni nëse dokumentet e planeve të rimëkëmbjes dhe të vazhdueshmërisë janë të disponueshme jashtë institucionit në rast të fatkeqësive. Intervista me një mostër punonjësish për të vlerësuar nëse procedurat e rimëkëmbjes janë të qarta dhe të kuptuara.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

6.7.Testim i PVB/PRF
Objektivi i auditimit: Vlerësimi nëse procedurat e rimëkëmbjes nga fatkeqësitë dhe procedurat të vazhdimësisë së biznesit janë testuar.
Çështja e auditimit nr. 8: Testimi A ka testuar organizata procedurat e saj të vazhdimësisë së biznesit dhe rimëkëmbje nga fatkeqësitë dhe çfarë ndryshimesh janë kryer si rezultat i testimeve?
Kriteret: Organizata duhet të testojë procedurat e saj të dokumentuara të PVB dhe PRF nëpërmjet përpjekjeve dhe imitimeve për tu siguruar se punohet në kushte aktuale. Personeli i përfshirë në vazhdimësinë e biznesit duhet të jetë i ndërgjegjshëm për detyrat e tij.

Informacioni i kërkuar	Metodat e analizimit
Procedurat e BC& DR dhe Procedurat e Testimit Listë e artikujve për të cilat duhet të testohen planet e rimëkëmbjes dhe të vazhdimësisë Frekuenca e testimeve të planeve Lista e testeve të kryera Lista e kritereve si RTO dhe RPO, etj. Lista e metodave të përdorura të testimit Rezultatet e testimit dhe veprimet e ndërmarra ose rekomandimet e tyre Planet e ndjekjes, të bazuara mbi rezultatet e testimit	Rishikim të dokumenteve për të vlerësuar nëse të gjitha elementet e duhura janë përfshirë në testim. Rishikim të dokumenteve për të vlerësuar nëse testimet janë kryer në intervale të duhura të kohës. Rishikim të dokumenteve për të vlerësuar se testimet janë kryer kundrejt kritereve të identifikuara. Rishikim të dokumenteve për të vlerësuar se testimet janë kryer kundrejt metodave të testimit. Rishikim të dokumenteve për të vlerësuar se rekomandimet janë përçuar në autoritetet e duhura për përcjellje. Rishikim të dokumenteve për të vlerësuar se rekomandimet e testimeve janë ndjekur në mënyrën e duhur dhe se plani i vazhdimësisë së biznesit ose plani i rimëkëmbjes nga fatkeqësitë janë përditësuar në mënyrë të duhur.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

6.8.Siguria

Objektivi i auditimit:

Vlerësimi nëse plani i vazhdimësisë së biznesit dhe plani i rimëkëmbjes nga fatkeqësitë sigurojnë sigurinë e të dhënave, programeve aplikative, pajisjes kompjuterike dhe qendrës së të dhënave.

Çështja e auditimit nr. 9: Efikasiteti i Indikatorëve të Sigurisë

Vlerësimi nëse të dhënat, programet aplikative, pajisjet kompjuterike dhe qendra e të dhënave janë siguruar përgjatë procedurave të backup-it dhe të rimëkëmbjes.

Kriteret: Bazat e sigurisë për organizatën si procedurat e përcaktuara në politikën e sigurisë së TI-së dhe planet për rimëkëmbje nga fatkeqësitë.	
Informacioni i kërkuar	**Metodat e analizimit**
Inventar i të dhënave, programeve dhe pajisjeve harduerike Inventar të të dhënave backup dhe të programeve aplikative Gjurmët e kontrollit të qasjes së të dhënave, programeve aplikative dhe pajisjeve harduerike Planet e sigurisë për ndërtesën e backup-it dhe të rimëkëmbjes	Verifikimi nëse numri dhe statusi i të dhënave, i programeve dhe i pajisjeve është ruajtur gjatë procesit të backup-it dhe të rimëkëmbjes. Verifikimi nëse të dhënat, programet dhe pajisjet nuk i janë nënshtruar ndryshimeve gjatë procesit të backup-it dhe të rimëkëmbjes nëpërmjet një studimi të kontrollit të numrit total të regjistrave dhe madhësisë së dosjeve lidhur me të dhënat dhe programet aplikative. Verifikimi nëse kanë ndodhur thyerje të sigurisë nëpërmjet ekzaminimit të regjistrave të kontrolleve të qasjes (fizik ose logjik).
Konkluzioni i auditimit: Të plotësohet nga audituesi	

6.9.Backup dhe rimëkëmbja nga fatkeqësitë për shërbimet e kontraktuara
Objektivi i auditimit: Vlerësimi nëse shërbimet e kontraktuara janë në përputhje me planet e vazhdimësisë së biznesit dhe të rimëkëmbjes nga fatkeqësitë.
Çështja e auditimit nr. 10: Ofruesi i shërbimit të jashtëm siguron BCP dhe DRP Përcaktimi nëse ofruesi i shërbimit të kontraktuar siguron së do të adaptojë planin e vazhdimësisë së biznesit dhe planin e rimëkëmbjes nga fatkeqësitë.
Kriteret: Bazat e sigurisë për organizatën si procedurat e përcaktuara në politikën e sigurisë së TI-së dhe planet për rimëkëmbje nga fatkeqësitë..

Informacioni i kërkuar	**Metodat e analizimit**
Inventar i të dhënave, të programeve aplikative, të pajisjeve harduerike të organizatës me subjektin e kontraktuar Inventar të të dhënave dhe programeve aplikative backup të organizatës me subjektin e kontraktuar Gjurmët e kontrollit të qasjes së të dhënave, të programeve aplikative dhe të pajisjeve harduerike me subjektin e kontraktuar Rezultatet e testimit të planit të rimëkëmbjes dhe të vazhdimësisë së biznesit në subjektin e kontraktuar Plani i sigurisë për ndërtesën e backup-it dhe të rimëkëmbjes në subjektin e kontraktuar Strategjia për sigurimin e vazhdimësisë në rast të blerjes së ofruesit të shërbimit nga një organizatë tjetër Informacion në çdo blerje të ofruesve të shërbimit nga organizatë të tjera	Verifikim nëse organizata ekzaminon nëse numri dhe statusi i të dhënave, programeve aplikative dhe i pajisjeve është ruajtur gjatë backup-it dhe gjatë rimëkëmbjes në subjektin e kontraktuar. Observim nëse organizata verifikon se të dhënat, programet aplikative dhe pajisjet harduerike i janë nënshtruar ndryshimeve gjatë procesit të backup-it dhe të rimëkëmbjes nëpërmjet studimit të kontrolleve të numrit total të rekordeve dhe madhësisë së dosjeve të lidhura me të dhënat dhe programet e kontraktuara nga subjekti. Observim nëse organizata verifikon se testimi i backup-it dhe i rimëkëmbjes është siguruar nga subjekti i kontraktuar. Observim nëse organizata është e ndërgjegjshme për rreziqe e lidhura me mundësinë e blerjes së subjektit të kontraktuar nga një subjekt tjetër. Verifikim nëse organizata ka siguruar se vazhdimësia e biznesit është e pasqyruar në marrëveshjen e shërbimit.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

Shtojca VII. Matrica e sugjeruar e auditimit mbi Sigurinë e Informacionit

<table>
<tr><th colspan="2">7.1.Vlerësimi i rrezikut</th></tr>
<tr><td colspan="2">Objektivi i auditimit:

Të sigurohet se të gjithë rreziqet e lidhur më sigurinë e informacionit janë identifikuar dhe se ekziston një strategji e përshtatshme për reduktimin e rrezikut.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 1: Mekanizmat e vlerësimit

A ka organizata një mekanizëm efektiv dhe të mirë dokumentuar të vlerësimit të rrezikut të sigurisë së informacionit?</td></tr>
<tr><td colspan="2">Kriteret: Organizata është e përgatitur për të menaxhuar të gjitha rreziqet kritike (politika të brendshme, procedura dhe rregulla).</td></tr>
<tr><td>Informacioni i kërkuar

Politikat e sigurisë së Sistemeve të Informacionit

Procedurat formale për menaxhimin e rreziqeve

Dokumentimi i konfigurimit të sistemit</td><td>Metodat e analizimit

Analizë e politikave të menaxhimit të rrezikut, dokumentet e vlerësimit të rrezikut dhe intervista me menaxhmentin e lartë dhe ata në nivel operacionale për:
- të kuptuar rolin e vërtetë të organizatës në procedurat e vlerësimit të rrezikut
- të identifikuar personat e përfshirë në vlerësimin e rreziqeve
- të gjetur kostot e mekanizmave operacional
- të verifikuar nëse vlerësimi i rrezikut është kryer dhe dokumentuar rregullisht ose kurdoherë që ndryshojnë kushtet
- të kontrolluar nëse konfigurimi aktual i sistemit është dokumentuar, duke përfshirë lidhjet me sistemet e tjera
- të kontrolluar nëse dokumentacioni përmban përshkrime të rreziqeve kryesore për bizneset e sistemeve të organizatës dhe për infrastrukturën?

Në rast të mungesës së procedurave dhe dokumenteve formale në vlerësimin e rrezikut, mos nënvlerësoni kontrollet të cilat janë vendosur në procedurat operacionale të organizatës-verifikoni nëse mekanizmat kompensues janë efektiv.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 2: Mbulimi

A mbulon të gjitha rreziqet e brendshme dhe të jashtme vlerësimi i rrezikut? A maten efektet dhe ndikimet e mundshme të dëmtimeve në sigurinë e informacionit?</td></tr>
</table>

Kriteret: Të gjithë rreziqet domethënës janë identifikuar dhe matur në mënyrën e duhur (praktikat më të mira në vlerësimin e rrezikut).	
Informacioni i kërkuar Vlerësimi i dokumentuar i rreziqeve Regjistri i rreziqeve Raportet e trajtimit të incidenteve	**Metodat e analizimit** Rishikim i dokumenteve për të kontrolluar nëse vlerësimi i rrezikut i kryer nga organizata bazohet në informacion të mjaftueshëm dhe të përgjithshëm. Kontrolloni nëse të dhënat dhe raportet janë ruajtur nga sistemi i menaxhimit të incidenteve të organizatës. (I mbështesni analizat tuaja me rezultate të metodave të analizimit në operacionet e TI-së të përqendruara në sistemet e menaxhimit të incidenteve veçanërisht nëse informacioni i trajtimit të incidenteve të sigurisë formon një sistem të shkëputur nga sistemi i përgjithshëm i menaxhimit të incidenteve.) **Testi 1 i vlefshmërisë:** Gjurmët e auditimit të sigurisë: Përcaktoni nëse gjurmët e auditimit të sigurisë kapin identifikimin e përdoruesit (ID), llojin e ngjarjes, datën dhe orën, suksesin ose dështimin e treguesit, origjinën e ngjarjes, si dhe identitetin ose emrin e objektit të prekur. Intervistoni personelin përkatës për të verifikuar nëse ekziston një rivlerësim standard i rrezikut kurdoherë që organizata planifikon të qarkullojë sisteme të reja informacioni, të zgjerohet, ose të sjellë versione të reja. Kontrolloni ndërtimin e vlerësimit të rrezikut për plotësi, relevancë, kohëzgjatje dhe matje. Kontrolloni nëse elementë ndërveprues të infrastrukturës janë konsideruar gjatë caktimit të kategorive të rrezikut. Verifikoni dokumentet për të parë nëse janë kryer analizat e ndikimit në biznes për elementët e informacionit kritik të shndërruar në të padisponueshëm, të manipuluar, i kompromentuar ose i humbur. Rishikoni raportet e kthimit të përgjigjes dhe dokumentet/regjistrat e hershëm të rreziqeve për të ekzaminuar nëse metodologjia e vlerësimit të rrezikut ka qenë efektive në të shkuarën.
Çështja e auditimit nr. 3: Reduktimi Rreziqet e rëndësishme a reduktohen në mënyrë efektive dhe efikase?	
Kriteret: Ekzistojnë praktika të përshtatshme të reduktimit të rrezikut	

Informacioni i kërkuar	Metodat e analizimit
Raportet e trajtimit të problemeve/ incidenteve Raporte periodike të aktivitetit	Rishikimi i raporteve të trajtimit të incidenteve dhe kontrollimi nëse ishin krijuar procedurat e duhura për të parandaluar, zbuluar dhe kontrolluar rreziqet e sigurisë të identifikuara në dokumentin e vlerësimit të rrezikut. Në organizatat që nuk përdorin një mekanizëm për vlerësimin e rrezikut, përcaktoni çfarë elemente kontrolli tjetër ekziston. Analizoni nëse kanë ndodhur incidente të mëdha të sigurisë në lidhje me rreziqet të cilat mund të ishin reduktuar më mirë me anën e mekanizmave të reduktimit të rrezikut, kundrejt kontrolleve kompensues ekzistues. Merrni parasysh që raportet e problemeve/incidenteve mund të jenë të paplotë në disa raste. Megjithatë, ngjarjet e rëndësishme mund të reflektohen direkt ose indirekt në dokumente të tjerë, si p.sh. raportet e aktivitetit vjetor ose raporte të tjerë periodik.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

7.2.Politikat e sigurisë së informacionit

Objektivi i auditimit:

Vlerësimi nëse ekziston një drejtim strategjik i përshtatshëm dhe një mbështetje për sigurinë e informacionit në termat e politikave të sigurisë, mbulimin e saj, ndërgjeshmëria në nivel organizativ dhe pajtueshmëria.

Çështja e auditimit nr. 4: Politikat e sigurisë së informacionit

A posedon organizata Politika të Sigurisë së Informacionit? A është e mirë implementuar dhe e dokumentuar? A formon ajo një plan të qëndrueshëm dhe të fuqishëm të sigurisë së TI?

Kriteret: Politikat e sigurisë së informacionit mbulojnë të gjithë rreziqet operacional dhe ka mundësi të mbrojë në mënyrë të arsyeshme të gjithë asetet e informacioneve kritike kundrejt humbjeve, dëmtimit dhe abuzimit. (Ref. ISO 27000 Sistemi i menaxhimit të sigurisë së informacionit dhe politika të tjera të brendshme, procedura ose rregulla të aplikueshme).

Informacioni i kërkuar	Metodat e analizimit
Strategjia e TI	Kontrolloni dokumentet për të verifikuar nëse Stretegjia e TI-së adreson në mënyrë të përshtatshme rolin kritik të sigurisë së informacionit. Gjithashtu referojuni përdorimit të matricës së

Akte ligjore që përcaktojnë kërkesat e sigurisë së informacionit Politikat e shkruara dhe formale të sigurisë së informacionit Struktura organizative dhe përshkrimet e punës Marrëveshje kontraktuale me palët e jashtme Plani i sigurisë së TI	*Qeverisjes TI-së* dhe matricës së *Strategjisë TI-së.* Në mungesë të strategjisë së shkruar të TI-së, intervistoni menaxhmentin e lartë, atë të mesëm dhe personelin për të parë se çfarë njohje kanë ata mbi rolin strategjik të sigurisë së informacionit. Vlerësoni pajtueshmërinë e strategjisë së TI-së dhe të politikave të sigurisë së informacionit. Krahasoni qëllimet e politikave dhe procedurave të sigurisë për të përcaktuar efektivitetin e integritetit të kërkesave të sigurisë së informacionit në planin e sigurisë së TI-së (grafik, strukturë, manual, etj.). Verifikoni nëse rishikohet rregullisht në nivelet e duhura menaxheriale. Ekzaminoni mbulimin e planit të sigurisë së TI-së dhe kontrolloni nëse merr në konsideratë planet taktikë të TI-së, klasifikimin e të dhënave, standardet teknologjike, politikat e kontrollit dhe menaxhimin e rrezikut. Kontrolloni nëse plani i sigurisë së TI-së identifikon: detyrat dhe përgjegjësitë (bordit, menaxhmentit ekzekutiv, menaxhmentit të linjës, personelit dhe të gjithë përdoruesve të infrastrukturës TI-së së organizatës), kërkesat e stafit, ndërgjegjësimi dhe trajnimi mbi sigurinë, zbatimin e praktikave, nevoja për investime në burimet e kërkuara të sigurisë. Rishikoni dhe analizoni diagramin për të verifikuar se i referohet një apetiti të rrezikut organizativ të lidhur me sigurinë e informacionit dhe se ky diagram përfshin qartazi qëllimin dhe objektivat e funksionit të menaxhimit të sigurisë. Kontrolloni raportet e incidenteve të sigurisë dhe dokumentet e ndjekjes së tyre për të gjetur se çfarë veprimesh janë ndërmarrë në rastet kur individët kanë abuzuar me politikat e sigurisë. Kontrolloni raportet e sigurisë për të identifikuat numrin e abuzimeve me sigurinë e informacionit nga punonjësit ose palët e jashtme në një periudhë të caktuar për të vlerësuar efektivitetin e politikave.
Çështja e auditimit nr. 5: Konfidencialiteti A ka hartuar organizata kërkesa konfidencialiteti ose marrëveshje *moszbulimi* që reflektojnë përshtatshmërisht nevojën për mbrojtjen e informacionit? A sigurojnë politikat informacionin në marrëdhëniet e organizatës me palët e jashtme?	

Kriteret: Politikat e sigurisë së informacionit janë të afta të mbrojnë të gjithë informacionin konfidencial lidhur me palët e brendshme dhe të jashtme.	
Informacioni i kërkuar Rregullat e brendshëm dhe të jashtme lidhur me informacionin e klasifikuar dhe konfidencial P.sh. çështjet e moszbulimit për punonjësit Marrëveshjet kontraktuale me palët e jashtme Politikat e sigurisë së informacionit Plani i sigurisë së TI	**Metodat e analizimit** Kontrolloni vlerësimet e procedurave të ndërmarra nga organizata për pajtueshmëri me kërkesat konfidenciale. Në rastet kur çështjet e thyerjes së konfidencialitetit janë strikte ndaj procedurave të veçanta ligjore dhe ndaj subjekteve të veçanta, opinionin tuaj bazojeni në raportet e tyre dhe në rekomandimet e menaxhmentit të organizatës-nëse është e nevojshme. Rishikoni marrëveshjet kontraktuale me palët e jashtme ose kontraktorët. A përfshijnë ata dhënien ose kërkesën e qasjes, përpunimit, komunikimit ose menaxhimit të aseteve të informacionit të organizatës? Kontrolloni nëse kushtet dhe detyrimet kontraktuale përcaktojnë limitet e sigurisë dhe detyrimet e saj, të cilat kontrollojnë sesi kontraktori do të përdorë asetet e organizatës, qasjen e sistemeve të informacioni dhe shërbimet e tij. Kontrolloni nëse kanë ndodhur shkelje të sigurisë së informacionit nga kontraktorët. Kontrolloni veprimet e ndërmarra nga menaxhmenti.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

7.3.Struktura e sigurisë së TI-së	
Objektivi i auditimit: Sigurimi i operimit të sigurt të pajisjeve përpunuese të TI-së.	
Çështja e auditimit nr. 6: Struktura A ka subjekti një strukturë të qartë të sigurisë së TI? A janë përcaktuar detyrat dhe përgjegjësitë referuar politikave të sigurisë së informacionit?	
Kriteret: Detyra dhe përgjegjësi të qarta të TI-së lidhur me Politikat e Sigurisë së Informacionit (referuar ISO 27000).	
Informacioni i kërkuar	**Metodat e analizimit**

Struktura, sektori organizativ i TI Rregullat e brendshme të lidhura me sigurinë e SI Përshkrimet e punës Procesverbalet e mbledhjeve të grupeve përkatëse	Përcaktoni nëse janë mirë përcaktuar përgjegjësitë për sigurinë e TI. Kontrolloni nëse ekziston një proces për prioritizimin e iniciativave të propozuara të sigurisë, përfshirë nivelet e kërkuara të politikave, standardeve dhe procedurave. Kontrolloni sesi menaxhmenti i lartë mban një nivel të përshtatshëm të interesit në sigurinë e informacionit në organizatë.
Çështja e auditimit nr. 7: Koordinimi Si i koordinon organizata aktivitetet e sigurisë së informacionit nga pjesë të ndryshme të organizatës?	
Kriteret: Jo konflikte përgjegjësish ose jo-harmoni në aktivitetet e sigurisë së informacionit.	
Informacioni i kërkuar	**Metodat e analizimit**
Kërkesat ligjore lidhur më informacionin e klasifikuar Struktura organizative Rregullat e brendshme lidhur me sigurinë e informacionit Procesverbale të takimeve të komiteteve të sigurisë së TI Raporte të dështimeve	Kontrollimi i dokumenteve, observim i praktikave dhe intervista me personelin për të verifikuar nëse ekzistojnë konflikte të brendshme, tejkalime, hapësira në mes të procedurave të sigurisë të ndjekura nga punonjësit në departamente/njësi të ndryshme. Kontroll i procedurave operacionale për të identifikuar nëse informacioni transmetohet në palët e jashtme jashtë kontrollit të punonjësve përgjegjës. Kontroll nëse menaxherët e nivelit të lartë janë në dijeni të problemeve të koordinimit dhe nëse ata mbikëqyrin aktivitetet e inspektimit dhe të koordinimit. Rishikoni proceset për të kontrolluar nëse ka ndonjë procedurë të caktuar për menaxhmentin që të autorizojë objektet e reja të përpunimit të informacionit.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

7.4.Menaxhimi i komunikimeve dhe operacioneve
Objektivi i auditimit: Sigurimi se komunikimi i brendshëm dhe i jashtëm janë të sigurt.

Çështja e auditimit nr. 8: Politikat dhe procedurat A janë politikat dhe procedurat për komunikimet e brendshme dhe të jashtme të përshtatshme të sigurta dhe efikase?	
Kriteret: Politikat dhe procedurat formojnë një mjedis të qëndrueshëm menaxheria për komunikimet e brendshme dhe të jashtme. (Ref. ISO-27002, S15-IT control (Satandardet e ISACA-s), COBIT)	
Informacioni i kërkuar	**Metodat e analizimit**
Politikat formale dhe të shkruara për komunikimet dhe operacionet e TI Dokumentacioni për procedurat operacionale	Kontrollimi nëse politikat dhe procedurat e organizatës përshtaten me komunikimin me qytetarët, me mediat dhe me organizatat e jashtme. Verifikim sesi organizata dokumenton procedurat e veta dhe sesi i bën të disponueshme për të gjithë përdoruesit. Intervista me një mostër përdoruesish të niveleve të ndryshme për të ekzaminuar nëse të gjitha procedurat për trajtimin e të dhënave janë të njohura nga punonjësit. Kontrollimi sesa shpesh rishikohen dhe përditësohen procedurat e trajtimit të të dhënave dhe komunikimeve.
Çështja e auditimit nr. 9: Kontrolli i rrjetit Si menaxhon dhe kontrollon organizata informacionin në rrjet?	
Kriteret: Operacionet e rrjetit menaxhohen dhe kryhen në mënyrë të sigurt dhe efektive. (ref. ISO 270002, S15-IT Control (Standardet e ISACA-s), COBIT).	
Informacioni i kërkuar	**Metodat e analizimit**
Politikat e kufizimit të informacionit Regjistrat/gjurmët e administratorit të rrjetit Rezultatet e analizave të gjurmëve Raportet e testimit të pranimit të përdoruesit SLA	Kontrollimi se çfarë mjetesh përdoren për monitorimin dhe analizën e rrjetit. Verifikim nëse përdoruesit dhe sistemet e TI-së të subjektit janë të mbrojtur kundrejt sulmeve. Kontrollimi nëse konfigurimet e Sistemit të Zbulimit të Ndërhyrjeve dhe gjurmëve analizohen nga personeli i duhur për të ofruar sigurinë e informacionit nga sulmet dhe ndërhyrjet keqdashëse. Verifikoni nëse sulmet (ato efektive dhe jo-efektive) janë analizuar dhe raportuar. Kontrolloni statistikat për sulmet keqdashëse. Investigoni sesi organizata ofron lëvizje të sigurt të transaksioneve nëpërmjet rrjeteve publike. P.sh. Qarkullimi/ Njoftimi i procedurave operuese ndaj përdoruesve të tregtisë elektronike/ transaksionet online.

Informacioni publik ose i gjetur ne faqet e internetit	Rishikim të politikave për të verifikuar nëse lëvizja e të dhënave jashtë organizatës kërkon një formatim të koduar përpara transmetimit. Investogoni nëse politikat e sigurisë së informacionit kanë implementuar në përputhje me klasifikimin e të dhënave sensitive të organizatës. Nëpërmjet investigimit, përcaktoni nëse klientët përdorin kodimin për përpunimin e informacionit sensitiv. Nëse po, kryeni një testim vlefshmërie. **<u>Kontrolli i testimit të procedurave të vlefshmërisë</u>** **Testi i vlefshmërisë nr. 1:** Efektiviteti i operimit të kontrolleve të kodimit: Përcaktoni: - ekzistencën e proceseve për ciklin e menaxhmentit kryesor - ndërhyrjet kryesore - ndarjet e detyrave për kujdestarët kryesorë
Çështja e auditimit nr. 10: Menaxhimi i konfigurimit A janë nën kontrollin e përshtatshëm të konfigurimit rregullimet/aplikacionet e TI?	
Kriteret: Sistem të qartë dhe të mirë-menaxhuar që mbështet Sigurinë e Informacionit në komunikim dhe në operacione.	
Informacioni i kërkuar Politikat dhe procedurat referuar çështjeve të konfigurimit në fushën e operacioneve Lista/libraria e konfigurimeve	**Metodat e analizimit** Rishikimi i matricave të detyrave për të përcaktuar se cilët janë përgjegjës për administrimin e konfigurimit dhe cili është qëllimi për kontrollin e konfigurimit në operacione. Kontrolloni sesi regjistrohet, kontrollohet dhe përditësohet. Verifikoni nëse kanë ndodhur probleme në të shkuarën për shkak të pasaktësive në konfigurim. Nëse po, intervistoni menaxherët për të kontrolluar se çfarë procedurash janë implementuar ndaj ndryshimeve në konfigurim.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

7.5.Menaxhimi i aseteve

Objektivi i auditimit:

Inkurajimi i mbrojtjes së duhur të aseteve të TI.

Çështja e auditimit nr. 11: Menaxhimi i aseteve

A ka organizata ndonjë sistem të përshtatshëm të menaxhimit të aseteve i cili mbështet Sigurinë e Informacionit?

Kriteret: Sigurimi i mbrojtjes së përshtatshme të Sigurisë së Informacionit (ref. ISO 27000 Sistemi i menaxhimit të sigurisë së informacionit, COBIT dhe politika të tjera të brendshme, procedura ose rregulla të aplikuara)

Informacioni i kërkuar	**Metodat e analizimit**
Politikat e menaxhimit të aseteve Klasifikim të aseteve Klasifikim të informacionit Procedurat e asgjësimit të aseteve Raportet e auditimit financiar (nëse ato i referohen aseteve dhe inventarëve)	Rishikim të politikave për të kontrolluar nëse ekzistojnë politika të pranueshme përdorimi për programet dhe pajisjet kompjuterike TI-së (shembull, laptop-ët mund të përdoren për përdorim personal nëse nuk interferon me biznesin.) Kontrolloni nëse baza e të dhënave është e përditësuar. Kontrolloni regjistrimet e inventarit për të verifikuar nëse asetet janë kategorizuar në terma të vlerës, sensitivitetit ose kategorive të tjera. Procedurat e rishikimit për asgjësimin e pasurive dhe nivelin e mbikëqyrjes të mandatuar. Kontrolloni kërkesat për autorizim për çdo zhvendosje ose ripërdorim të pajisjeve. Intervistoni personelin dhe kontrolloni dispozitat që sigurojnë se të dhënat janë fshirë përpara zhvendosjes ose ripërdorimit të pajisjeve.

Konkluzioni i auditimit: Të plotësohet nga audituesi

7.6.Siguria e burimeve njerëzore

Objektivi i auditimit:

Sigurimi se të gjithë punonjësit (përfshirë të kontraktuarit ose përdoruesit e të dhënave sensitive) janë të kualifikuar për mirëmbajtjen e të dhënave dhe njohin detyrat dhe përgjegjësitë e tyre dhe se qasja ndërpritet sapo ndërpritet kontrata e punësimit/kontraktimit.

Çështja e auditimit nr. 12: Ndërgjegjësimi dhe përgjegjshmëria e punonjësve A janë të ndërgjegjshëm punonjësit mbi detyrat dhe përgjegjësitë referuar detyrave dhe përgjegjësive mbi sigurinë?	
Kriteret: Personeli që prej rekrutimit e deri në shkëputjen e marrëdhënieve të punës, ruajnë Sigurinë e Informacionit. Dobësitë në qasjen profesionale të personelit, rrezikojnë sigurinë e informacionit të organizatës.	
Informacioni i kërkuar	**Metodat e analizimit**
Politikat e burimeve njerëzore dhe procedurat e rekrutimit Politikat e sigurisë së informacionit dhe procedurat përkatëse Standardet e kompetencave për personelin TI Raportet e vlerësimit të individëve Raportet e incidenteve ndaj sigurisë (përfshirë abuzimet me kodin e etikës ose të sjelljes) Fushata të ndërgjegjësimit ndaj sigurisë Detyrat dhe përgjegjësitë e menaxhimit të përdoruesve	Inspektimi i dokumentacionit të punësimit për një mostër përfaqësuesish të personelit të TI-së që të vlerësohet nëse verifikime e historikut kanë përfunduar dhe janë vlerësuar. Inspektim i kritereve të përzgjedhura për performancën e kontrollove të historikut. Detyra për çdo pozicion duhet të jetë e qartë. Aktivitetet mbikëqyrëse duhet të ekzekutohen për kontrollin e pajtueshmërisë ndaj politikave dhe procedurave menaxheriale, kodit të etikës dhe praktikave profesionale. Kontrolloni nëse detyrat të cilat janë kritike për Sigurinë e Informacionit janë të mirë përcaktuara dhe të dokumentuara. Punonjësit dhe palët e interesit, të cilëve u janë ngarkuar këto detyra, duhet të njohin përgjegjësitë e tyre referuar mbrojtjes së aseteve të informacionit të organizatës, përfshirë të dhënat elektronike, infrastrukturën e SI, dokumentet, etj. Rishikim për përcaktim të përshtatshëm të detyrave kritike, për të cilat kërkohen kontrolle të sigurisë. Kjo duhet të aplikohet ndaj punonjësve, kontraktorëve dhe shitësve. Kontrolle për ndarje të detyrave në mes të menaxhmentit dhe operacioneve të sigurisë së TI. Kontrolloni nëse politikat e pozicionimit të personelit të TI-së, transferimi dhe qarkullimi, ashtu si edhe shkëputja e marrëdhënieve të punës është e qartë për të reduktuar pavarësinë e individëve. Verifikoni se cilët mekanizma përdoren për transferimin e njohurive.
Çështja e auditimit nr. 13: Trajnimi A thellohen detyrat e personelit në Sigurinë e Informacionit nëpërmjet trajnimeve efektive?	

Kriteret: Trajnime, të cilat ofrojnë aftësitë dhe njohuritë e duhura ndaj punonjësve, roli i të cilëve në organizatë është domethënës për Sigurinë e Informacionit.	
Informacioni i kërkuar Programet e trajnimit Rezultatet e testimeve përfundimtare Vlerësimi i efektivitetit të trajnimeve	**Metodat e analizimit** Vlerësimi i proceseve të matjes së efektivitetit të trajnimeve, nëse ka, për të konfirmuar se janë përfshirë trajnimet kritike të sigurisë së TI-së dhe kërkesat e ndërgjegjshmërisë. Inspektoni përmbajtjen e programeve të trajnimeve mbi sigurinë e TI-së për plotësi dhe përshtatshmëri. Inspektoni mekanizmat e dorëzimit për të përcaktuar nëse informacioni dorëzohet tek të gjithë përdoruesit e burimeve të TI-së, përfshirë këshilluesit, kontraktorët, si dhe punonjësit e përkohshëm dhe nëse është e aplikueshme klientët dhe furnitorët. Inspektoni përmbajtjen e programeve të trajnimit për të përcaktuar nëse strukturat e brendshme të kontrollit dhe kërkesat e sigurisë janë përfshirë, bazuar në politikat e sigurisë së organizatës (p.sh. ndikimi i mospërputhjes me kërkesat e sigurisë, përdorimin e përshtatshëm të burimeve të organizatës, trajtimin e incidenteve, përgjegjësinë e punonjësve për sigurinë e informacionit). Inspektoni dhe konfirmoni nëse materialet e trajnimit dhe programet rishikohen rregullisht. Inspektoni politikat për të përcaktuar kërkesat për trajnim. Konfirmoni se politikat e kërkesave për trajnim sigurojnë se këto kërkesa reflektohen në programet e trajnimeve dhe të ndërgjegjësimit.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

7.7.Siguria fizike
Objektivi i auditimit: Parandalimin e vjedhjes ose të dëmtimit të pajisjeve kompjuterike, qasjeve të paautorizuar, kopjimit ose shikimit të informacionit sensitiv.
Çështja e auditimit nr. 14: Siguria e objekteve A janë ndërtesat e organizatës të siguruara kundrejt rreziqevee fizike dhe mjedisore?

Kriteret: Ofrimi i sigurisë fizike dhe ambientale është në përputhje me kërkesat për siguri dhe me klasifikimin e sensitivitetit të aseteve të TI-së.	
Informacioni i kërkuar	**Metodat e analizimit**
Diagrama e rrjetit Plani i sigurisë së ndërtesave Raporte periodike mbi testimin fizik Raporte prej shërbimeve të lidhura	Analizoni se cilët janë kontrollet primare të sigurisë fizike të organizatës. Kontrolloni nëse përshtaten me analizat e përditësuara të rrezikut. Rishikoni masat e parandalimit të dëmtimeve fizike për elementët kyç të infrastrukturës së TI-së. Verifikoni nëse ekzistojnë kontrollet mjedisore (fikset e zjarrit, alarmet, sistemet e energjisë, etj). Verifikoni nëse rekomandimet nga shërbimet e lidhura janë implementuar (parandalimi i fatkeqësive, e zjarreve, inspektimi i ambienteve). (Për sigurinë e lidhur me fatkeqësitë, referojuni seksionit PVB dhe PRF në Manual).
Çështja e auditimit nr. 15: Qasja fizike Si siguron organizata se vetëm personat e autorizuar mund të kenë qasje në ndërtesa?	
Kriteret: Sigurohuni se masat organizative dhe fizike sigurojnë parandalimin e qasjeve të paautorizuara.	
Informacioni i kërkuar	**Metodat e analizimit**
Paraqitja e instalimit të pajisjeve harduerike të` TI-së Plani i sigurisë së ndërtesës Konfigurimi i pajisjeve Raportet periodike të testimit fizik Raportet e incidenteve	Rishikim të instruksioneve të sigurisë, diagramës së rrjetit dhe dokumenteve të lidhur me to, si dhe kontrolloni sesi kontrollon organizata qasjen në zonat sensitive. Rishikoni dhe observoni trafikun hyrës/dalës dhe si punon sistemi i sigurisë fizike. Përcaktoni se çfarë mjetesh përdoren. Rishikoni politikat dhe procedurat përsa kohë ato lidhen me sigurinë e ndërtesave dhe përcaktoni sesi këto procedura llogariten për identifikim dhe autenticitet të përshtatshëm.

	Kontrolloni se cilët persona mbajnë dhe kontrollojnë vendndodhjet e kontrolleve të qasjes. Gjeni nëse niveli i menaxhimit është i mjaftueshëm për Sigurinë e Informacionit. Gjeni nëse qasja ndaj zonave të sigurta/ dhomave të sigurisë/ vendndodhjeve të serverave, janë të kufizuara. Përzgjidhni një mostër përdoruesish/ punonjësish dhe përcaktoni nëse qasja e tyre në këto objekte është e saktë, e bazuar në përgjegjësitë e punës. Verifikoni nëse incidentet raportohen në sistemin e menaxhimit të incidenteve/problemeve. Kërkoni nëse ato analizohen dhe prej tyre nxirren mësime.
Çështja e auditimit nr. 16: Mbrojtja nga ndërhyrjet Si zbulon dhe i trajton organizata ndërhyrjet?	
Kriteret: Sigurimi se ndërhyrjet zbulohen dhe trajtohen (Politika të brendshme të sigurisë).	
Informacioni i kërkuar	**Metodat e analizimit**
Plani i sigurisë së ndërtesës Konfigurimi i pajisjeve kompjuterike Raportet e incidenteve	Inspektoni se si siguria e organizatës e di se ka ndodhur një ndërhyrje për të siguruar lokacionet Kontrolloni instruksionet për të gjetur procesin për trajtimin e ndërhyrjeve ndaj një hapësire ose ndërtese të sigurtë. Kontrolloni raportet e incidenteve për të identifikuar nëse ndërhyrjet zbulohen herët. Kontrolloni nëse organizata ka një politikë të qartë ose të pastër për parandalimin e qasjeve të paautorizuara.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

7.8.Kontrollet e qasjes

Objektivi i auditimit:

Të sigurohet se vetëm përdoruesit e autorizuar ndaj informacioneve kanë qasje.

Çështja e auditimit nr. 17: Politikat e qasjes A ka organizata politika të qarta dhe efikase mbi kontrollet e qasjes?	
Kriteret: Politikat e qasjes japin një bazë për kontrollin e ndërhyrjes ndaj informacioneve.	
Informacioni i kërkuar	**Metodat e analizimit**
Politikat dhe procedurat e qasjes Lista e përdoruesve Lista/matrica e qasjes	Analiza e politikave dhe procedurave për të siguruar se detyrat e punonjësve dhe përgjegjësitë e tyre janë të ndara në mënyrë që të reduktohen mundësitë për qasjen e paautorizuar. **<u>Testi i vlefshmërisë:</u>** Efektiviteti i operimit të qasjes së autorizuar të përdoruesit ndaj LAN (jo testim i ndarë i qasjeve të përdoruesve ndaj aplikacioneve). Përzgjidhni një mostër përdoruesish dhe llogari të sistemit për të përcaktuar ekzistencën e elementëve të mëposhtëm (mund të përdoret program i kontrollit të qasjes): - Detyra/përgjegjësi të mirë përcaktuara dhe të pozicionuara në funksionet e punës. - Justifikimi i biznesit për qasje. - Autorizimi i pronarit të të dhënave dhe i menaxhmentit (nënshkrim/ aprovim i shkruar). - Justifikimi i biznesit/rrezikut dhe aprovimi i menaxhmentit për kërkesat jo standarde. - Kërkesat për qasje janë konform funksionit/detyrës së punës dhe ndarjes së nevojshme të detyrave.
Çështja e auditimit nr. 18: Menaxhimi i privilegjeve A është efektivi dhe i sigurtë procesi për ofrimin dhe anulimin e kontrollit të qasjes ndaj punonjësve dhe kontraktorëve?	
Kriteret: Funskioni i Sigurisë së Informacionit monitoron efektivitetin e kontrollit të operacioneve të menaxhimit të llogarive të përdoruesve në kohë dhe raporton efikasitetin dhe efektivitetin e operimit.	
Informacioni i kërkuar	**Metodat e analizimit**
Procedurat e kontrollit të qasjes Mostër të punonjësve të transferuar dhe të pushuar nga puna	Kontroll të procedurave për të përcaktuar sesa shpesh qasjet dhe privilegjet e përdoruesve rishikohen. Kontrolloni sesi privilegjet e dhëna ndaj përdoruesve janë konfirmuar (Shembujt përfshijnë marrjen në pyetje të mbikëqyrësit, zonën menaxheriale, grupe të ndryshme, etj.)

	Intervista me mostër përdoruesish dhe kontroll të instruksioneve për të verifikuar sesi informohen përdoruesit mbi përgjegjësitë e tyre në mbrojtjen e informacionit sensitiv ose të aseteve, nëse u është dhënë qasje përkatëse. Përcaktoni nëse praktikat e sigurisë së organizatës kërkojnë përdorues dhe procese të sistemit që të jenë unifikisht të identifikueshëm dhe sistemet të konfigurohen për të zbatuar autenticitetin përpara dhënies së qasjes dhe se mekanizma të tilla kontrolli shfrytëzohen në të gjithë përdoruesit dhe në qasjen logjike të tyre, në proceset e sistemit dhe në burimet e TI. Analizoni më tepër se privilegjet në fjalëkalimet. p.sh. si kontrollohet se një përdorues ka qasje dhe privilegjet e mjaftueshme për të kërkuar një burim? (Shembujt përfshijnë qasjen në vendndodhje të sigurta, njohjen e shenjave të gishtërinjve, etj). **Testi i vlefshmërisë nr. 1:** Efektiviteti i operimit të transferimit dhe të pushimit nga puna: Merrni nga burimet njerëzore një mostër të transferimeve dhe të pushimit ose dorëheqjes nga puna të punonjësve dhe nëpërmjet rishikimit të profileve të llogarive në sistem të tyre dhe/ose nëpërmjet CAAT (p.sh. ACL, IDEA) përcaktoni nëse qasja ka qenë e përshtatshme dhe e anuluar në kohë. **Testi i vlefshmërisë nr. 2:** Menaxhimi i fjalëkalimeve: Verifikoni nëse janë përcaktuar kërkesat për cilësinë e fjalëkalimeve dhe zbatohen nga sistemi i menaxhimit të rrjetit dhe/ose sistemit të operimit bazuar në politikat e kërkesave lokale/organizative ose nga praktikat më të mira.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

Blerja, zhvillimi dhe mirëmbajtja e sistemeve TI-së ndodhet në SHTOJCËN III
Menaxhimi i vazhdimësisë së biznesit ndodhet në SHTOJCËN VI

Shtojca VIII. Matrica e sugjeruar e auditimit mbi Kontrollet e Aplikacioneve

<table>
<tr><th colspan="2">8.1.Kontrollet e hyrjes</th></tr>
<tr><td colspan="2">Objektivi i auditimit:

Vlerësimi nëse të dhënat e vlefshme janë future në bazën e të dhënave në aplikacion nga personeli i autorizuar.</td></tr>
<tr><td colspan="2">Çështja e auditimit nr. 1: Vlefshmëria e të dhënave hyrëse

A ka aplikacioni kontrolle të përshtatshme për vlefshmërinë e të dhënave hyrëse?</td></tr>
<tr><td colspan="2">Kriteret: Rregullat e vlefshmërisë janë të mirë-hartuara, të dokumentuara dhe të zbatuara në ndërveprimin e hyrjeve (inputit); të dhëna jo të vlefshme refuzohen në mënyrën e duhur nga aplikacioni; kriteret e vlefshmërisë përditësohen në mënyrën e duhur dhe të autorizuar; ekzistojnë kontrolle gjithëpërfshirëse si rregulla regjistrimi dhe autorizimi në rast të mundësisë së kontrolleve thelbësorë të hyrjes</td></tr>
<tr><td>Informacioni i kërkuar

Kërkesat dhe rregullat e biznesit

Llojet e të dhënave hyrëse

Kërkesat ligjore dhe të jashtme

Struktura e ndërveprimit të të dhënave me aplikacione të tjera

Diagramat e rrjedhës së sistemit

Manualet e përdorimit

Rregullat e vlefshmërisë</td><td>Metodat e analizimit

Analizoni rregullat, kërkesat, dokumentacionin e aplikacioneve dhe inspektoni pronarin e proceseve të biznesit për të përcaktuar se cilat rregulla të vlefshmërisë duhet të sigurohen në procesin e biznesit që po vlerësohet. Kontrolloni nëse rregullat e vlefshmërisë janë të mirë hartuara dhe të dokumentuara. Verifikoni nëse kontrollet e vlefshmërisë për të dhënat hyrëse janë në zbatim: observim të përdoruesve të aplikacioneve në veprime reale, ekzekutimi i aplikacionit në mjedis testimi dhe testimi i ndërveprimeve të ndryshme për të dhënat e hyra; analizim të regjistrave të të dhënave të ruajtura në bazën e të dhënave nëpërmjet përdorimit të CAAT-s.

Merrni përshkrimin funksional për secilën klasë të informacionit të hyrjes dhe dizajnit për regjistrimin e të dhënave të transaksionit. Inspektoni funksionalitetin dhe modelin për praninë e kontrolleve në kohë, të plotë dhe mesazheve të gabimit. Nëse është e mundur, vëzhgoni regjistrimin e të dhënave të transaksionit.

Vlerësoni nëse kriteret dhe parametrat e vlefshmërisë në të dhënat hyrëse korrespondojnë me rregullat e biznesit dhe zbatojnë refuzimin e llojeve të të dhënave që nuk përshtaten. Në rast të sistemeve të përpunimit online, verifikoni se të dhënat jo të vlefshme janë refuzuar ose janë rregulluar në hyrje dhe se janë kryer kontrolle të llogaritjeve logjike. Operacionet e bazës së të dhënave (si *, =, ose, select) duhet të mos lejohen si të dhëna të vlefshme përhyrje, pasi ato mund të</td></tr>
</table>

	ndërhyjnë ose mund të korrigjojnë informacionin në bazën e të dhënave. Inspektoni menaxherët mbi rishikimin periodik të kritereve dhe parametrave të vlefshmërisë së të dhënave hyrëse, nëse ato konfirmohen dhe autorizohen në mënyrën e duhur. Siguria duhet të ruhet nëpërmjet rishikimit të dokumentacionit, analizave të kodimit dhe intervistave. Inspektoni dhe kontrolloni dokumentacionin në mënyrë që të verifikohet mundësia e mbizotërimit të vlefshmërisë dhe kontrolleve të të dhënave hyrëse. Verifikoni nëse veprimet mbizotëruese regjistrohen dhe rishikohen përshtatshmërisht. Kontrolloni nëse është i kufizuar kompetenca për mbizotërim vetëm për personelin mbikëqyrës dhe është i limituar në numër situatash. Inspektoni korrigjimet e gabimeve, mbizotërimin e hyrjeve dhe dokumente të tjera për të verifikuar se janë ndjekur procedurat. Përcaktoni se cilat ndërveprime ekzistojnë me aplikacionin. Këto ndërveprime duhet të janë në një formë të transmetimit në kohë reale ose periodike të të dhënave nëpërmjet proceseve të paketave. Rishikoni diagramat e rrjedhjes së proceseve dhe të kodit të sistemit dhe intervistoni zhvilluesit e sistemeve ose administratorët për të marrë informacion mbi ndërveprimet dhe kontrollet mbi to. P.sh. Totalet e kontrolleve mbi transmisionin e ndërveprimeve (p.sh. ngatërresa pa kuptim, si shuma e numrave të llogarive ose numrat e punonjësve në një dosje të zhvendosur, numrat e regjistrave) duhet të gjenerohen dhe përdoren nga sistemi për të përcaktuar nëse transmetimi i kryer është plotësuar përshtatshmërisht.
Çështja e auditimit nr. 2: Menaxhimi i dokumenteve burimore, mbledhja dhe futja e të dhënave A është i përshtatshëm menaxhimi i dokumenteve burimorë dhe i mbledhjes së të dhënave?	
Kriteret: Procedurat e përgatitjes së të dhënave janë dokumentuar dhe njohur nga përdoruesit; ekziston një regjistrim i përshtatshëm i dokumenteve burimorë, ekziston një caktim i numrave unikë dhe sekuencialë për çdo transaksion; dokumentet burimoreorigjinale ,bëhen për një kohë të caktuar me politika dhe dispozita ligjore.	
Informacioni i kërkuar	**Metodat e analizimit**
Klasat/Kategoritë e dokumenteve burimorë	Inspektoni dhe observoni krijimin dhe dokumentimin e procedurave të përgatitjes së të dhënave, inspektoni dhe konfirmoni nëse procedurat

Kriteret e subjektit për kohështrirje, plotësi dhe saktësi të dokumenteve burimorë Procedurat e përgatitjes së të dhënave Ndërveprimet e të dhënave me aplikacione të tjera Politikat e ruajtjes së dokumenteve Diagrama të rrjedhjes së sistemeve	janë mirëkuptuar dhe nëse janë përdorur kanalet e përshtatshme të komunikimit. Vlerësoni nëse grupi i përpunimit të të dhënave ose ekuivalent me të, mban një regjistër të të gjithë dokumenteve burimorë të departamenteve si dhe formatin e tyre final. Verifikoni ekzistencën e një sistemi të barazimit të regjistrave me grupet e përdoruesve të departamenteve. Verifikoni se të gjithë dokumentet burimorë përfshijnë elementë standard, përmban dokumentacion të përshtatshëm (p.sh. kohështrirje, kodet e hyrjes të paracaktuara, vlerat e qenësishme) dhe janë të autorizuara nga menaxhmenti. Inspektoni nëse janë numëruar më parë dokumentet burimorë kritikë dhe sesi janë identifikuar numrat jashtë sekuencës, gjithashtu si janë marrë parasysh ato. Identifikoni dhe rishikoni numrat jashtë sekuence, boshllëqet dhe dyfishimet duke përdorur mjete të automatizuar (CAAT-s). Verifikoni nëse ekziston një caktim unik dhe numra sekuencial për çdo transaksion që parandalon dyfishimin. Intervistoni personelin përgjegjës mbi politikat e ruajtjes. Verifikoni sesi këto politika zbatohen. Një mostër i regjistrave të sistemit duhet të kontrollohet kundrejt dokumenteve burimorë.
Çështja e auditimit nr. 3: Procedurat për trajtimin e gabimeve A përmban aplikacioni procedura të përshtatshme për trajtimin e gabimeve?	
Kriteret: Ekziston një sistem i qartë dhe kompakt për trajtimin e gabimeve duke komunikuar problemet në mënyrë që të ndërmerren veprime korrigjuese për çdo lloj gabimi. Gabimet mund të korrigjohen përshtatshmërisht përpara përpunimit të transaksioneve. Regjistrimet rishikohen periodikisht dhe ndërmerren veprimet e nevojshme korrigjuese.	
Informacioni i kërkuar	**Metodat e analizimit**
Llojet e gabimeve dhe mesazheve Procedurat e rishikimit të regjistrimeve	Diskutoni trajtimin e gabimeve të aplikacioneve me zhvilluesin e tij ose administratorin. Verifikoni dhe konfirmoni nëse ekzistojnë politika dhe procedura për trajtimin e transaksioneve që dështojnë në kontrollet e modifikimit dhe vlefshmërisë. Verifikoni nëse sistemi ofron mesazhe për çdo lloj gabimi (në nivel fushe ose transaksioni), mesazhe të cilat mund të mos përputhen me vlefshmërinë ose modifikimin.

Politikat dhe procedurat për trajtimin e të dhënave të refuzuara Procedurat e rishikimit të dosjeve në pezullim	Verifikoni sesi sillet aplikacioni nëse të dhënat refuzohen nga kontrollet në hyrje. Kontrolloni nëse elementet e të dhënave regjistrohen ose nëse shkruhen automatikisht në një dosje pezullimi. Kontrolloni nëse dosja e pezullurruar(e automatizuar) përmban kode që tregojnë llojin e gabimit, datën dhe kohën e hyrjes dhe identifikoni personin që i ka futur të dhënat. Vlerësoni nëse ekzistojnë procedurat për rishikimin dhe korrigjimin e të dhënave në dosjen e pezullimit përpara ripërpunimit të tyre. Vlerësoni nëse ekziston një procedurë përshkallëzimi kur normat e gabimit janë tepër të larta dhe kur ndërmerren veprime korrigjuese. Intervistoni menaxherët mbi ekzistencën e procedurave të rishikimit periodik të regjistrimeve. Verifikoni nëse procedurat përfshijnë nisjen e masave korrigjuese. Mbani evidenca dokumente fizike ose dixhitale që regjistrimet rishikohen periodikisht.
Çështja e auditimit nr. 4: Menaxhimi i futjes së të dhënave në aplikacion Si menaxhohet autorizimi i futjes së të dhënave në aplikacion?	
Kriteret: Janë vendosur nivelet e autorizimit të transaksioneve dhe zbatohen nëpërmjet kontrolleve të ndryshëm; ekziston ndarje e saktë e detyrave për futjen e të dhënave; ekzistojnë kontrolle kompensues për rastet në të cilat ndarja e detyrave nuk është e mundur.	
Informacioni i kërkuar	**Metodat e analizimit**
Kërkesat e pajtueshmërisë ligjore dhe të jashtme Kërkesat dhe rregullat e biznesit Manualet e përdorimit	Inspektoni dhe konfirmoni nëse dizajnimi i sistemit ofron listë të autorizuar për përdorim. Verifikoni, nëpërmjet inspektimit të listës së autorizimit, se nivelet e autorizimit janë të mirë përcaktuara për çdo grup transaksionesh. Vlerësoni nëse rregullat e autorizimit për futjen e të dhënave, modifikimin, pranimin, refuzimin dhe abuzimin me to, janë të mirë hartuara dhe përcaktuara. Observoni se nivelet e autorizimi janë të mirë aplikuara në aplikacionet që ekzekutohen në mjedisin testues. Verifikoni, nëpërmjet përdorimit të CAAT-s ose moduleve të auditimit, se regjistrat e autorizimit prezente në bazën e të dhënave janë në pajtim me rregullat e përcaktuara të autorizimit. Përcaktoni nëse tabela e ndarjes së detyrave ekziston dhe rishikoni për ndarje të përshtatshme të detyrave kryesore/funksioneve të punës si dhe transaksioneve të lejuara dhe më pas shikoni në listën e përdoruesve dhe në listën e privilegjeve të qasjeve të përdoruesve. Vlerësoni nëse ndarja e detyrave siguron se personi për futjen e të

	dhënave nuk është gjithashtu përgjegjës për verifikimin e dokumenteve. Verifikoni adoptimin e kontrolleve kompensues në rastet në të cilat ndarja e detyrave nuk është e realizueshme.
Konkluzioni i auditimit: Të plotësohet nga audituesi	

8.2.Kontrollet e përpunimit	
Objektivi i auditimit: Vlerësimi nëse aplikacioni siguron integritetin, vlefshmërinë dhe besueshmërinë e të dhënave gjatë ciklit të përpunimit të transaksionit.	
Çështja e auditimit nr. 5: Hartëzimi i rregullave dhe kërkesave të proceseve të biznesit A janë mirë-pozicionuar rregullat dhe kërkesat e proceseve të biznesit në aplikacion?	
Kriteret: Transaksionet e aplikacionit ekzekutohen në përputhje me sjelljen e pritur.	
Informacioni i kërkuar Dokumentimin e aplikacionit Rregullat dhe kërkesat e biznesit Diagramin i rrjedhjes së të dhënave Kodi iburimor	**Metodat e analizimit** Identifikoni programet e ekzekutueshme në aplikacion nëpërmjet një studimi të diagramit të rrjedhjes së të dhënave dhe i gruponi ato me rregullat e përcaktuara dhe të hartuara të proceseve të biznesit. Rishikoni dokumentimin e aplikacionit për të verifikuar se është i pranueshëm dhe i përshtatshëm për detyrat. Nëse është e nevojshme për transaksionet kritike, rishikoni kodin për të konfirmuar se kontrollet në veglat dhe aplikacionet operojnë sipas dizajnimit të tyre. Ripërpunoni një mostër për të verifikuar se veglat e automatizuara operojnë në përputhje me qëllimin. Për transaksionet kritike, vendosni një sistem testimi që operon si sistemi i prodhimit/live. Procesoni transaksionet në sistemin test për të siguruar se transaksionet e vlefshme përpunohen përshtatshmërisht dhe në kohë.
Çështja e auditimit nr. 6: Kontrollet e aplikacioneve A sigurojnë kontrollet e aplikacionit integritetin dhe plotësinë e transaksioneve të tij?	

Kriteret: Aplikacioni identifikon në mënyrë korrekte gabimet në transaksione. Integriteti i të dhënave ruhet edhe gjatë ndërprerjeve të rastësishme në përpunimin e transaksioneve. Ekziston një mekanizëm i përshtatshëm për trajtimin e gabimeve në përpunim, rishikim dhe qartësim të dosjeve në pezullim.

Informacioni i kërkuar	**Metodat e analizimit**
Dokumentimi i dizajnimit të aplikacionit Rregullat dhe kërkesat e biznesit Raportet jashtë Bilancit Barazimet Procedurat e rishikimit të raporteve Dosjet në pezullim	Vlerësoni nëse aplikacioni përmban kontrolle të sakta të vlefshmërisë për të siguruar integritetin e përpunimit. Inspektoni funksionalitetin dhe dizajnimin për praninë e sekuencave dhe gabimeve në dyfishim, kontrolle të integritetit. Inspektoni barazimet dhe dokumente të tjerë për të verifikuar nëse numërimet e hyrjeve janë koherente me numërimet e daljeve për tu siguruar rreth përpunimit të të dhënave. Përcjellni transaksionet nëpërmjet procesit për të verifikuar se barazimi përcakton efektivisht nëse dosjet totale korrespondojnë me kushtet jashtë bilancit të raportuar. Inspektoni nëse dosjet e kontrolleve janë përdorur për të regjistruar numërimet e transaksioneve dhe vlerat monetare dhe se këto vlera janë krahasuara pas postimit. Verifikoni se raportet gjenerohen duke identifikuar kushtet jashtë bilancit dhe se raportet rishikohen, aprovohen dhe shpërndahen në personelin e duhur. Merrni një mostër të transaksioneve hyrëse të të dhënave. Përdorni analiza të përshtatshme të automatizuara dhe mjete kërkimi për të identifikuar rastet kur gabimet janë identifikuar dhe raste të tjera ku nuk janë identifikuar. Inspektoni dhe konfirmoni se janë përdorur mjetet, aty kur është e mundur, për të automatizuar ruajtjen e integritetit të të dhënave gjatë ndërprerjeve të rastësishme në përpunimin e të dhënave. Inspektoni gjurmët e auditimit dhe dokumente të tjerë, plane, politika dhe procedura për të verifikuar se kapacitetet e sistemit janë dizenjuar efektivisht për të ruajtur automatikisht integritetin e të dhënave. Inspektoni përshkrimin funksional dhe informacionin e dizajnit për futjen e të dhënave të transaksioneve për të verifikuar nëse transaksionet që nuk funksionojnë në rutinat e vlefshmërisë janë postuar në skedarë të pezullimit. Verifikoni që skedarët e pezullimit janë prodhuar në mënyrë korrekte dhe të vazhdueshme dhe se përdoruesit janë informuar për transaksionet e postuara për llogari të pezullimit. Për një mostër të

	sistemeve të transaksioneve, verifikoni që llogaritë e pezullimit dhe skedarët e pezullimit për transaksione që nuk funksionojnë në rutinat e vlefshmërisë përmbajnë vetëm gabime të fundit. Konfirmoni që transaksionet më të vjetra të dështuara janë korrigjuar siç duhet.
Konkluzioni i auditimit:	Të plotësohet nga audituesi

8.3.Kontrollet e të dhënave dalëse	
Objektivi i auditimit: Vlerësoni nëse aplikacioni siguron se informacioni dalës është i plotë dhe i saktë përpara përdorimit të mëtejshëm dhe se ruhet në mënyrën e duhur.	
Çështja e auditimit nr. 7: Vlerësimi i aplikacionit A përmban aplikacioni kontrolle që sigurojnë plotësinë dhe saktësinë e rezultateve?	
Kriteret: Janë hartuar procedurat për të siguruar se plotësia dhe saktësia rezultateve të aplikacioneve është vlerësuar përpara përdorimit të rezultatit nga përpunimi i mëtejshëm, përfshirë përpunimi i përdoruesve final; mundësohet gjurmimi i rezultatit të aplikacionit; rezultati rishikohet për arsyeshmëri dhe saktësi; kontrollet e plotësisë dhe të saktësisë janë efektive.	
Informacioni i kërkuar Kontrollet e plotësisë dhe saktësisë Metodat për balancimin dhe barazimin Listë të rezultateve elektronike/raporteve Mostër të rezultatit të përzgjedhur	**Metodat e analizimit** Mbani një listë të rezultatit elektronik që ripërdoret në aplikacionet e përdoruesve finalë. Verifikoni nëse dalja e rrzultatit elektronik testohet për plotësi dhe saktësi përpara ripërdorimit të tij. Ekzaminoni balancimin dhe barazimin e rezultatit të vendosur në metodat e dokumentuara. Përzgjidhni një mostër të rezultait elektronik dhe gjurmoni dokumentet e përzgjedhur nëpërmjet një procesi për të siguruar se plotësia dhe saktësia verifikohet përpara kryerjes së operacioneve të tjera. Rikryeni testime plotësie dhe saktësie për të vlerësuar nëse ato janë efektive. Ekzaminoni nëse çdo produkt dalës përmban emër dhe numër të programit të përpunimit; titull ose përshkrim; periudha e mbuluar e përpunimit; emri i përdoruesit dhe i vendndodhjes; data dhe ora e përgatitjes; klasifikimi i sigurisë.

	Përzgjidhni një mostër të raporteve dalëse dhe testoni arsyeshmërinë dhe saktësinë e rezulttit. Verifikoni nëse janë regjistruar siç duhet gabimet potenciale.
Çështja e auditimit nr. 8: Të dhënat e daljes të mbrojtura siç duhet A është e organizuar në mënyrën e duhur ruajtja e rezultatit të të dhënave?	
Kriteret: Dalja trajtohet në përputhje me klasifikimin e konfidencialitetit të aplikuar; shpërndarja e daljes/raporteve, është e mirë kontrolluar.	
Informacioni i kërkuar Procedurat e trajtimit dhe ruajtjes së rezultatit Politikat e klasifikimit të informacionit	**Metodat e analizimit** Rishikim i procedurave të trajtimit dhe të ruajtjes së rezultatit mbi sigurinë dhe privatësinë. Vlerësimi nëse procedurat janë përcaktuar për të reflektuar regjistrimet e kërkuara të gabimeve të mundshme dhe të zgjidhjes së tyre përpara shpërndarjes së raporteve. Ekzaminimi i sistemit të barazimit të totaleve të kontrolleve të daljes me totalet e kontrolleve të hyrjes përpara gjenerimit të raporteve të integritetit të të dhënave. Kontrolli nëse ekzistojnë procedura të dokumentuara për etiketimin e rezultatit sensitiv të aplikacionit dhe aty ku kërkohet, dërgimi i rezultatit sensitiv/ndjeshëm në pajisjen dalëse me qasje të kontrollit special . Rishikim i mënyrës së shpërndarjes të informacionit sensitiv dhe verifikimi nëse mekanizmat zbatojnë kufizimin e të drejtave të qasjes.
Konkluzioni i auditimit:	Të plotësohet nga audituesi

8.4.Kontrollet e sigurisë së aplikacionit
Objektivi i auditimit: Vlerësimi nëse informacioni i aplikacionit është i sigurtë kundrejt keqpërdorimeve.
Çështja e auditimit nr. 9: Mekanizmat e gjurmueshmërisë A janë të mjaftueshme mekanizmat e gjurmimit aplikacionit për qëllimin e tij?
Kriteret: Ekzistojnë gjurmë të mjaftueshme auditimit që kapin modifikimet, regjistrimet e autorizuara të transaksioneve kritike; gjurmët e auditimit rishikohen periodikisht për të monitoruar

aktivitetet jonormale; gjurmët e auditimit mirëmbahen dhe ruhen në mënyrën e duhur; numra unikë dhe sekuencialë, ose identifikues janë përcaktuar për çdo transaksion.

Informacioni i kërkuar	**Metodat e analizimit**
Struktura e gjurmëve të auditimit dhe dokumentimi i tyre Politikat e shkeljeve Procedurat e rishikimit Bllok-skemat e sistemit	Mbajtja e dokumentacionit dhe vlerësimi i dizajnimit, zbatimit, qasjes dhe rishikimit të gjurmëve të auditimit. Inspektimi i strukturës së gjurmëve të auditimit dhe dokumenteve të tjerë për të verifikuar nëse këto gjurmë janë dizajnuar efektivisht. Hetimi se cilët janë personat e autorizuar për shfuqizimin ose fshirjen e gjurmëve të auditimit. Inspektimi i gjurmëve të auditimit, ose dokumenteve të tjerë, planeve, politikave dhe procedurave për të verifikuar se rregullimet, transaksionet me vlerë të lartë janë të mirë hartuara për tu rishikuar në detaje. Inspektimi i gjurmës së auditimit, transaksioneve, rishikimeve dhe dokumenteve të tjerë; gjurmoni transaksionet nëpërmjet procesit; nëse është e mundur përdorni evidenca të automatizuara, përfshirë të dhëna mostër, të përmbledhura në modulet e auditimit ose në CAAT, për të verifikuar se rishikimi dhe mirëmbajtja periodike e gjurmëve të auditimit zbulon aktivitete jonormale dhe se rishikimet e mbikëqyrjeve janë efektive. Inspektimi i mënyrës sesi qasja ndaj gjurmëve të auditimit është e kufizuar. Ekzaminimi i të drejtave të qasjes dhe regjistrimeve të qasjes ndaj dosjeve të gjurmëve të auditimit. Verifikimi nëse vetëm personat e autorizuar kanë qasje në gjurmët e auditimit. Vlerësimi nëse këto gjurmë janë të mbrojtura kundrejt modifikimeve. Verifikoni, nëse është e mundur, duke përdorur mbledhje automatike të evidencave, se identifikues unikë janë caktuar për çdo transaksion.

Çështja e auditimit nr. 10: Të dhënat e aplikacionit të mbrojtura siç duhet

A mbrohen në mënyrën e duhur të dhënat e aplikacionit?

Për kontrolle të qasjes logjike dhe fizike referojuni Shtojcës VII mbi Sigurinë e Informacionit. Për planifikimin e rimëkëmbjes nga fatkeqësitë referojuni Shtojcës VI mbi PVB/PRF.

Anëtarët e grupit të projektit të Manualit të IDI-WGITA

1. **Mr. Madhav S Panwar**
   Teknolog i nivelit të lartë (Drejtor), Zyra e Llogaridhënies Qeveritare në SHBA

2. **Mr. Pawel Banas**
   Këshilltar i Presidentit të Zyrës Supreme të Auditimit të Polonisë (NIK)

3. **Mr. Neelesh Kumar Sah**
   Kontabilist i përgjithshëm, Zyra e Kontrollorit dhe Auditorit të Përgjtihshëm të Indisë

4. **Mr. Anindya Dasgupta**
   Drejtor, Zyra e Kontrollorit dhe Auditorit të Përgjtihshëm të Indisë

5. **Mr. Marcio Rodrigo Braz**
   Auditues, Gjykata Braziljane e Llogarive (Tribunl de Contas Uniåo)

6. **Ms Shefali S Andaleeb**
   Assistent Drejtor i përgjithshëm, IntoISA Development Initiative (IDI)

7. **Mr. Novis Pramantya Budi**
   Zëvendës Drejtor, Bordi Auditues i Republikës së Indonezisë

8. **Ms Ria Anugriani**
   Zëvendës Drejtor, Bordi Auditues i Republikës së Indonezisë

Anëtarët e grupit të punues nga ZKA për përshtatjen e Manualit

1. **Vlora Spanca**
   Ndihmës i Auditorit të Përgjithshëm

2. **Samir Zymberi**
   Drejtor i Departamentit të Auditimit për Performancë dhe Teknologji të Informacionit

3. **Shqipe Mujku,**
   Auditore Seniore e Teknologjisë së Informacionit

4. **Arberore Sheremeti**
   Auditore Seniore e Teknologjisë së Informacionit

5. **Armend Salihu**
   Auditor i Teknologjisë së Informacionit

6. **Poliksena Berisha**
   Auditore e Teknologjisë së Informacionit

Zyra Kombëtare e Auditimit
Lagjja Arbëria
Rr. Ahmet Krasniqi, 210
10000, Prishtinë
Republika e Kosovës
www.zka-rks.org