GUID 5100

Udhëzues në Auditimin e Sistemeve të informacionit

Udhëzuesit e INTOSAI-it janë vendosur nga Organizata Ndërkombëtare e Institucioneve Supreme të Auditimit, INTOSAI, si pjese e Kornizës Profesionale të Standarteve INTOSAI

Për më shumë informacion vizitoni www.issai.org

INTOSAI

INTOSAI

1) Miratoi ISSAI 5100 – Udhëzues për auditimin IT, në 2016
2) Rishikoi dhe ri-emëroi GUID 5100 – Udhëzues në Auditimin e Sistemeve të informacionit, në 2019.

Pasqyra e Lëndës

1 Hyrja

1.1 Udhëzuesi 5100 ofron një trajtim gjithëpërfshirës për kryerjen e auditimit të Sistemeve të Informacionit brenda Kornizës Profesionale të Standarteve INTOSAI (IFPP). Ky udhëzues synon të sigurojë bazën për zhvillimin e udhëzuesve të ardhshëm në serinë 5100-5109 në drejtim të auditimit të Sistemeve të Informacionit, brenda Kornizës Profesionale të Standarteve (IFPP).

1.2 Kuadri rregullator i paraqitur në këtë Udhëzues është në përputhje me Parimet Themelore të Auditimit të Sektorit Publik (ISSAI 100), Parimet Themelore të Auditimit Financiar (ISSAI 200), Parimet e Auditimit të Performancës (ISSAI 300) dhe Parimet e Auditimit të Përputhshmërisë (ISSAI).

1.3 Institucionet Supreme të Auditimit (SAI-et) janë të legjitimuara për të audituar qeveritë dhe subjektet objekt auditimi përgjatë mandatit të tyre.[1] Nëpërmjet aktiviteteve të tyre, SAI-t synojnë të promovojnë efikasitetin, përgjegjshmërinë, efektivitetin dhe transparencën e administratës publike.[2]

1.4 Qeveritë dhe subjektet e tjera të sektorit publik kanë adoptuar vazhdimisht risi në Teknologjinë e Informacionit (IT) në sistemet e tyre të informacionit, me qëllim rritjen e efikasitetit dhe efektivitetit në funksionimin e tyre dhe ofrimin e shërbimeve të ndryshme publike. Kjo për shkak se IT-ja ka bërë të mundur kapjen, ruajtjen, përpunimin, marrjen dhe shpërndarjen e informacionit në mënyrë elektronike, gjë që krijon hapësirë të konsiderueshme për të përmirësuar saktësinë, konfidencialitetin dhe matjet e kohës së sistemeve të informacionit. Për më tepër, mënyra e ofrimit të shërbimeve publike po kalon me shpejtësi nga fizike në elektronike, duke kushtëzuar qeveritë që të funksionojnë si platforma dixhitale që ofrojnë shërbime, si dhe infrastrukturë për sisteme të tjera informacioni të drejtuara nga Teknologjia e Informacionit.

1.5 Ky kalim drejt sistemeve të kompjuterizuara të informacionit dhe përpunimit elektronik nga subjektet e audituara në sektorin publik ka shkaktuar një ndryshim të rëndësishëm në mjedisin ku punojnë SAI-et. Shpenzimet e sektorit publik për IT janë në rritje. Ekziston gjithashtu nevoja për të siguruar që kontrollet e brendshme të IT-së për të ruajtur konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave të miratohen nga njësitë e sektorit publik. Prandaj, bëhet e domosdoshme që SAI-t të zhvillojnë kapacitetet e duhura për të kryer një ekzaminim të plotë të kontrolleve që lidhen me sistemet e informacionit.

[1] *INTOSAI-P 1 Deklarata e Limës*
[2] *Rezoluta A/66/209 e Asamblesë së Përgjithshme të Kombeve të Bashkuara*

2 Objektivi i Udhëzuesit

2.1 ISSAI 100, 200, 300 dhe 400 parashtrojnë parimet bazë të auditimit në lidhje me auditimin financiar, auditimin e performancës dhe auditimin e përputhshmërisë. Këto ISSAI lidhen me parimet, procedurat, standardet dhe pritshmëritë e përgjithshme të një audituesi. Ato janë njëlloj të zbatueshme edhe për auditimet e Sistemeve të Informacionit.

2.2 Objektivi i këtij Udhëzuesi është të ofrojë udhëzime për audituesit se si të kryejnë auditime të performancës dhe/ose të përputhshmërisë në lidhje me natyrën specifike të Sistemeve të Informacionit ose ku auditimi i sistemeve të informacionit mund të jetë pjesë e një angazhimi më të madh auditues që mund të jetë financiar, përputhshmërie ose performance.

2.3 Përmbajtja e këtij Udhëzuesi zbatohet nga audituesit gjatë planifikimit, terrenit, raportimit dhe zbatimit të rekomandimeve[3] si faza të procesit të auditimit.

[3] *ISSAI 100*

3 Përkufizime

3.1 **Sistemet e Informacionit:** Sistemet e Informacionit mund të përkufizohen si një kombinim i aktiviteteve strategjike, menaxheriale dhe operacionale që përfshijnë mbledhjen, përpunimin, ruajtjen, shpërndarjen dhe përdorimin e informacionit dhe teknologjive të lidhura me të. Kompleksiteti i një sistemi të tillë informacioni mund të variojë nga një libër i thjeshtë në të cilin shënimet për pranimin dhe pagesën e parave mbahen manualisht, deri te një sistem më kompleks i drejtuar nga IT-ja, siç është sistemi për vlerësimin e taksave, në të cilin të gjitha proceset - mbledhja e të dhënave (p.sh. deklaratat tatimore të paraqitura përmes portalit në internet), ruajtja në serverë, përpunimi i vlerësimit (bazuar në programimin duke përdorur rregullat tatimore) dhe komunikimi i kërkesës tatimore, rimbursimi dhe njohja (në kohë reale ose në intervale të përcaktuara) - janë të automatizuara. Teknologjia e Informacionit përfshin hardware, software, komunikimin dhe lehtësira të tjera të përdorura për të kaluar, ruajtur, përpunuar, transmetuar dhe nxjerrë të dhëna të formateve të cfarëdoshme.

3.2 Auditimi i Sistemeve të Informacionit mund të përkufizohet si ekzaminimi i kontrolleve që lidhen me sistemet e informacionit të drejtuara nga IT-ja, me qëllim identifikimin e rasteve të devijimit nga kriteret, të cilat nga ana tjetër janë identifikuar bazuar në llojin e auditimit - d.m.th. Auditim Financiar, Auditim Përputhshmërie apo Auditim Performance.

4 Qëllimi

4.1 Ky Udhëzues mund të përdoret nga audituesit për të kryer auditime të performancës dhe/ose të përputhshmërisë për natyrën specifike të Sistemeve të Informacionit, si dhe kur auditimi i sistemeve të informacionit është pjesë e një auditimi që mund të jetë Financiar, Përputhshmërie dhe/ose Performance.

4.2. Ky udhëzues ofron udhëzime të mëtejshme se si çdo auditim i Sistemeve të Informacionit mund të adresohet duke përdorur auditimin financiar/performancën/përputhshmërinë dhe nuk përmban ndonjë kërkesë të mëtejshme për realizimin e auditimit.

5 Planifikimi i Auditimit të Sistemeve të Informacionit

5.1 SAI-t mund të adoptojnë planifikimin e auditimit të bazuar në risk për auditimet e sistemeve të informacionit, në përputhje me procedrën e përshkruar sipas ISSAI 100, ISSAI 200 (Auditimi Financiar), ISSAI 300 (Auditimi i Performancës) dhe ISSAI 400 (Auditimi i Përputhshmërisë), në varësi të objektivave të llojit të auditimit.

5.2 Puna e auditimit të sistemeve të informacionit do të përcaktohet nga objektivi dhe qëllimi i auditimit. Shembujt mund të përfshijnë:

1) Të vlerësojë kontrollet e përgjithshme (procedura manuale ose të automatizuara)[4] dhe ***kontrollet e aplikacionit***[5] të cilat kanë ndikim në besueshmërinë e të dhënave nga sistemet e informacionit, që nga ana e tyre kanë ndikim në pasqyrat financiare të subjektit të audituar.
2) Të marrë siguri lidhur me përputhshmërinë e proceseve të sistemeve të informacionit me ligjet, politikat dhe standardet e zbatueshme për subjektin e audituar.
3) Të marrë sigurinë se burimet e teknologjisë së informacionit lejojnë arritjen e qëllimeve të organizatës në mënyrë efikase dhe efektive, dhe se kontrollet e përgjithshme dhe ato të aplikacionit janë efektive në parandalimin, zbulimin dhe korrigjimin e rasteve të tejkalimit, shpërdorimit dhe joefikasitetit në përdorimin dhe menaxhimin e sistemeve të informacion

[4] ***Kontrollet e Përgjithshme*** *janë procedura manuale ose të automatizuara që synojnë të sigurojnë konfidencialitetin, integritetin dhe disponueshmërinë e informacionit në mjedisin fizik brenda të cilit zhvillohen, mirëmbahen dhe operojnë sistemet e informacionit..*

[5] ***Kontrollet e aplikacionit*** *janë procedura manuale ose të automatizuara të varura nga teknologjia e informacionit brenda një sistemi informacioni që ndikon në përpunimin e transaksioneve dhe mund të lidhet me vërtetimin e të dhënave hyrëse, përpunimin e saktë të të dhënave, dërgimin të të dhënave dalëse dhe kontrolleve që lidhen me integritetin e të dhënave kryesore.*

5.3 Bazuar në vlerësimin e riskut, objekti i një auditimi lidhur me sistemet e informacionit mund të nxirret nga ndonjë ose të gjitha fushat e mëposhtme[6] të subjetit që auditohet:

1) Politika organizative lidhur me teknologjinë e informacionit[7]
2) Struktura organizative e qeverisjes lidhur me IT-në
3) Kontrollet e përgjithshme të automatizuara ofruar në fushën e biznesit (organizatës)
4) Menaxhimi i Aseteve
5) Zhvillimi, Përvetësimi dhe Mirëmbajtja e Sistemeve të Informacionit, duke përfshirë hartën e proceseve të biznesit *(organizatës në rastin tonë)* dhe logjikën e programimit përkatës
6) Menaxhimi i Proceseve/veprimeve IT
7) Menaxhimi i mjedisit fizik
8) Menaxhimi i Burimeve Njerëzore
9) Menaxhimi i Komunikimeve
10) Menaxhimi i Sigurisë së Informacionit[8]
11) Menaxhimi i Pëputhshmërisë Statutore
12) Vazhdimësia e biznesit (organizatës) dhe Menaxhimi i Rimëkëmbjes nga Fatkeqësitë
13) Menaxhimi i Kontrolleve të Aplikacionit

5.4. SAI-t mund të zgjedhin periudhën kohore objekt auditimi (p.sh. një vit, tre vjet,etj.) duke përcaktuar drejtimin (fushën) e auditimit të Sistemeve të Informacionit. Mund të zgjidhet një periudhë e përshtatshme kohore, që është e rëndësishme për realizimin e objektivave të auditimit.

5.5. Kur një auditim i Sistemeve të Informacionit është pjesë e një auditimi, SAI mund ta sigurohet që grupi i auditimit punon në mënyrë të integruar për të arritur tërësinë e objektivave të auditimit.

Për të arritur një përfshirje efektive, SAI-et mund të marrin në konsideratë:

1) Dokumentimin e plotë të punës që do të kryhet nga audituesit e sistemeve të informacionit;
2) Krijimi i një protokolli për ndarjen e informacionit mes audituesve të sistemeve të informacionit

dhe audituesve të tjerë;

3) Identifikimi se cilët sisteme informacioni dhe objektiva kontrolli orientojnë fushëveprimin e auditimit;

[6] *Shumica e fushave të përshkruara në renditje janë përshtatur nga* ***ISO/IEC 27001***
[7] *Përfshirë aspektet e menaxhimit strategjik*
[8] *Përfshirë sigurinë kibernetike*

5.6 SAI-t mund të sigurojnë që grupi i auditimit të ketë në përbërje anëtarë që kanë kompetencën e duhur për të kryer auditimet e Sistemeve të Informacionit për të arritur objektivat e synuara të auditimit.

5.7 Njohuritë, aftësitë dhe kompetencat e nevojshme mund të fitohen nëpërmjet kombinimit të trajnimit, rekrutimit dhe angazhimit të burimeve të jashtme, referuar planit strategjik të SAI-t.

5.8. SAI-t mund të sigurohen që grupet e auditimit të Sistemeve të Informacionit të kenë kapacitetin për të:

1) Kuptuar elementet teknike të një sistemi informacioni të drejtuar nga IT-ja, duke përfshirë të gjitha instancat relevante të aplikacionit në përdorim, në mënyrë që të jeni në gjendje të aksesoni dhe të përdorni infrastrukturën e IT-së për procesin e auditimit

2) Kuptuar rregullat ekzistuese, rregulloret dhe mjedisin në të cilin operojnë sistemet e informacionit drejtuar nga IT-ja e subjektit të audituar

3) Të kuptuar hartëzimin e proceseve të biznesit (të organizatës) në logjikën e programimit për sistemin informacionit të subjektit të audituar

4) Zbatuar të dyja si njohuritë e biznesit(organizatës) dhe të IT-së për të vlerësuar riskun e devijimit manual të një programi ose konfigurimit të sistemit që do të lejonte përpunimin e transaksioneve në mënyrë të jashtëzakonshme.

5) Vlerësuar grafikën dhe testuar efektivitetin e funksionimit të kontrolleve të aplikacionit në sistemet përkatëse të informacionit

6) Kuptuar metodologjinë e auditimit, duke përfshirë standardet dhe udhëzimet përkatëse të auditimit të zbatueshme për SAI-n

7) Kuptuar kriteret e performancës/përputhshmërisë së IT me të cilat do të krahasohen gjetjet e auditimit, duke përfshirë kornizat për menaxhimin e Sistemeve të Informacionit , si COBIT, ITIL, TOGAF

8) Kuptuar teknikat e Sistemeve të Informacionit për të mbledhur evidencën e auditimit nga sistemet e automatizuara

9) Kuptuar mjetet e auditimit të Sistemeve të Informacionit për të mbledhur, analizuar dhe riprodhuar rezultatet e një analize të tillë ose për të ri-kryer funksionet e audituara

10) Qasja dhe përdorimi i Infrastrukturës të Sistemeve të Informacionit për të kapur dhe mbajtur evidencën e auditimit

11) Qasja dhe përdorimi i Mjeteve të Auditimit të Sistemve të Informacionit për të analizuar evidencën e mbledhur

5.9. SAI-et mund të marrin në konsideratë opsione të ndryshme për të shpërndarë burimet njerëzore sipas angazhimit që kërkon auditimi i Sistemeve të Informacionit. Kjo mund të realizohet nga krijimi i një grupi të përqëndruar me specialistë të IT-së që ndihmojnë grupet e tjera të auditimit brenda SAI-it për të kryer këto auditime ose duke rritur dhe zhvilluar specialistët e IT-së sipas kërkesave të fushës. Ndërsa numri i auditimeve të Sistemit të Informacionit rritet, SAI-t mund të konsiderojnë krijimin e një grupi ose funksioni dedikuar auditimit të Sistemeve të Informacionit. Këtij grupi mund t'i besohet përgjegjësia e kryerjes së të gjitha auditimeve të Sistemeve të Informacionit për SAI-n dhe ndërveprimi me ekipe të tjera brenda SAI-it që kanë njohuri të trashëguara për subjektin e audituar, në mënyrë që të kuptojnë shpejt funksionet e njësisë ekonomike dhe proceset e lidhura të biznesit (organizatës). Ndërsa teknologjia bëhet më e atashuar në sistemet e informacionit, SAI-t mund të sigurojnë që të gjithë audituesit të fitojnë aftësitë e duhura të auditimit të Sistemeve të Informacionit.

5.10. SAI-et mund të angazhohen në burime të jashtme si konsulentë IT-je, kontraktorë, specialistë dhe ekspertë për të kryer auditimin e Sistemeve të Informacionit, në rastet kur burimet janë të kufizuara. SAI-t mund të sigurojnë që burimet e jashtme të trajnohen dhe të ndërgjegjësohen ndaj udhëzimeve për sjelljen profesionale, proceduarat dhe materialet e Auditimit të Sistemeve të Informacionit të zbatueshme për SAI-et, në mënyrë që puna e tyre të monitorohet në mënyrë të përshtatshme përmes një kontrate të dokumentuar ose një marrëveshjeje të përshtatshme në nivel shërbimi, gjithashtu përfshirja e stafit të SAI-t në fazat e planifikimit, kryerjes, raportimit dhe zbatimit të rekomandimeve. SAI-et mund të kenë nevojë për anëtarë të ekipit të aftë dhe që zotërojnë njohuritë e duhura për të monitoruar punën e ***burimeve të jashtme*** dhe për të zbatuar respektimin e udhëzimeve dhe marrëveshjeve në nivel shërbimi.

5.11. Për kryerjen e vlerësimit të riskut për auditimin e Sistemeve të Informacionit, parimet e përcaktuara në ISSAI 100, 200, 300 dhe 400 mund të përdoren nga audituesit, përveç atyre të përdorura në kryerjen e një çështjeje specifike të auditimit të Sistemeve të Informacionit, siç përshkruhet më poshtë:

1) Risku i brendshëm lidhet me probabilitetin që disa veçori të sistemeve të informacionit të drejtuara nga IT-ja brenda njësisë ekonomike të audituar, nga vetë natyra e tyre, mund të rezultojnë të kenë impaktin e kundërt(ndikim negativ) në realizimin e funksionit të përcaktuar për t'u kryer nga subjekti i audituar. Për shembull, një sistem informacioni i një subjekti të audituar, i cili kërkohet të vërë informacionin në dispozicion për të gjithë anëtarët e publikut, mbart riskun e brendshëm të performancës që përtej një kufiri maksimal të parashikuar të përdoruesit, sistemi i informacionit mund të dështojë duke mos u përgjigjur dhe informacioni nuk do të jetë i disponueshëm për çdo përdorues.

Ndërkohë subjekti i audituar mund të realizojë kontrolle për të zbutur risqet e qenësishme(e brendshme), në shumë raste, ku mund t'i duhet thjesht të tolerojë ekzistencën e këtyrerisqeve, brenda një niveli të pranueshëm risku. Rreziku i brendshëm mund të vlerësohet përpara se ndikimi i riskut të kontrollit ose zbulimit të merret *parasysh nga audituesit.*

2) Risku i kontrollit për një Sistem Informacioni lidhet me probabilitetin që kontrollet e IT-së që janë miratuar nga subjekti i audituar mund të dështojnë në zbutjen e ndikimit negativ ndaj të cilit janë projektuar për tu përgjigjur (reaguar). Për shembull, një sistem informacioni i një subjekti të audituar, i cili kërkohet të sigurojë që qasja në të dhënat konfidenciale është e kufizuar për personelin e autorizuar, mund të nxis aprovimin e kontrollit për të kërkuar paraqitjen e një emri përdoruesi dhe fjalëkalimi nga personeli që përpiqet të fitojë akses. Risku i kontrollit në këtë situatë është se emri i përdoruesit dhe fjalëkalimi nuk janë mjaftueshëm të sigurta dhe mund të hamendësohen nga personeli i paautorizuar nëpërmjet përpjekjeve të përsëritura, duke rezultuar në humbjen e konfidencialitetit dhe ndikimin e mundshëm negativ mbi subjektin. Një subjekt që insiston në përdorimin e fjalëkalimeve të sigurta, jo të parëndësishme, të cilat kanë një kombinim të alfabeteve, numrave dhe simboleve të veçanta, dhe siguron që sistemi i informacionit të parandalojë aksesin në emrin e përdoruesit përtej një numri të caktuar përpjekjesh të dështuara për të fituar akses, do të kishte një risk kontrolli më të ulët se një sistem që nuk i ka këto veçori.

3) Risku i zbulimit konsiston në probabilitetin që mungesa, dështimi ose pamjaftueshmëria e kontrolleve IT të miratuara nga subjekti, që mund të kenë një ndikim potencialisht negativ tek ky i fundit, të mos zbulohen nga audituesit.

5.12. Për kryerjen e vlerësimeve të sistemeve të bazuara në risk dhe drejtuar nga IT-ja, SAI-et mund të zgjedhin një metodologji që është e përshtatshme për qëllimin e tyre. Metodologji të tilla mund të variojnë nga klasifikime të thjeshta të profilit të riskut lidhur me mjedisin e IT-së së subjektit të audituar, klasifikuar ky si : i lartë, i mesëm dhe i ulët bazuar në të kuptuarit e SAI-it për subjektin në auditim dhe gjykimin profesional të grupit të auditimit të Sistemeve të Informacionit të një SAI, në llogaritje komplekse dhe numerike të cilat përcaktojnë **masën e vlerësimit** të riskut bazuar në të dhënat objektive të mbledhura nga subjekti i audituar.[9]

5.13. Materialiteti i çështjeve të auditimit të Sistemeve të Informacionit mund të vendoset sipas kuadrit të përgjithshëm për vendosjen e materialitetit në një SAI. Perspektiva e materialitetit mund të ndryshojë në varësi të natyrës së auditimit të Sistemeve të Informacionit. Materialiteti në sektorin publik për auditimet financiare, të performancës dhe të përputhshmërisë, mbi të cilat do të duhet të ndërtohet dhe auditimi i Sistemeve të Informacionit , përshkruhet në ISSAI 100, 200, 300 dhe 400.[10]

[9] *Manuali ËGITA IDI mbi Auditimet e TI-së për Institucionet Supreme të Auditimit*

[10] *Parimet e auditimit financiar ISSAI 200, Parimet e auditimit të performancës ISSAI 300, Parimet e auditimit të përputhshmërisë ISSAI 400*

6 Drejtimi i Auditimit të Sistemeve të Informacionit

6.1 SAI-t mund të kryejnë auditime të Sistemeve të Informacionit në përputhje me procedurat e përshkruara sipas parimeve të Auditimit Financiar (ISSAI 200), Auditimit të Performancës (ISSAI 300) dhe Auditimit të Përputhshmërisë (ISSAI 400), sipas rastit, bazuar në natyrën e auditimit.

6.2 Konkretisht për një auditim të Sistemeve të Informacionit, audituesit mund të kërkojnë bashkëpunimin dhe mbështetjen e duhur të subjektit të audituar në përfundim të auditimit, duke përfshirë aksesin tek të dhënat dhe informacioni. Audituesit mund të identifikojnë mënyrën e aksesit në të dhënat elektronike, formatin e nevojshëm për të lejuar analizën, në konsultim me subjektin e audituar. Mënyra e aksesit tek të dhënat do të duhet të ishte specifike për SAI-in.

6.3 Përpara vlerësimit të kontrolleve në një sistem informacioni, audituesit mund të fokusohen tek zhvillimi i të kuptuarit të arkitekturës së sistemit, dhe fokusi tek të dhënat dhe burimet e tyre për të identifikuar mjetet dhe teknikat e kërkuara të auditimit.

6.4 Në rast të marrjes së bazës të të dhënave[11] nga subjekti i audituar, audituesit mund të sigurojnë që çdo bazë të dhënash të shoqërohet me një letër nga subjekti i audituar. Një letër e tillë përcjellëse mund të specifikojë

1) Burimin (përmes referencës në vulën kohore të gjenerimit të gjenerimit të të dhënave/përcaktoj numrin për bazën e të dhënave) e të dhënave për qëllim të sigurimit të vërtetësisë të të dhënave, identifikimit [12] dhe mosrefuzimit[13].

2) Parametrat e përdoruar për të nxjerrë dhe krijuar bazën e të dhënave, d.m.th., pyetjet e përdorura/raportet e realizuara.

3) Nëse një letër e tillë përcjellëse nga subjekti i audituar nuk është marrë, dokumentet e brendshme mund të gjenerohen nga audituesit duke vënë në dukje informacione të rëndësishme si data në të cilën janë dorëzuar të dhënat, nga cili skedar është krijuar baza e të dhënave dhe nëse të dhënat janë nga mjedisi që i gjeneron apo nga ndonjë mjedis tjetër, etj.

---

[11] Baza e të dhënave definohet si një sasi e madhe të dhënash të transferuara nga një sistem ose vend në tjetrin

[12] Identifikimi përkufizohet si akti i verifikimit të identitetit të një përdoruesi - Fjalorth i Termave ISACA

[13] Mos-refuzimi përkufizohet si siguria se një palë nuk mund të mohojë më vonë të dhënat e origjinës; sigurimi i provës së integritetit dhe origjinës së të dhënave dhe mund të verifikohet nga një palë e tretë – Fjalorth i Termave ISACA

6.5 Audituesit mund të kryejnë një vlerësim të kontrolleve të IT-së (kontrollet e përgjithshme dhe ato të aplikacioneve) të miratuara nga subjekti i audituar, me qëllim që të ekzaminohet besueshmëria dhe mjaftueshmëria e tyre. Vlerësimi mund të kryhet duke përdorur një kombinim të përshtatshëm të teknikave të mëposhtme: Intervista, Pyetësor, Vëzhgime, Teknika e depërtimit, Grafikë , Kapja dhe Analiza e të Dhënave, Verifikimi, Rillogaritja, Ripërpunimi dhe Konfirmimi i palëve të treta. Fusha e vlerësimit të kontrolleve të IT-së mund të përfshijë ekzaminimin që:

1) Politika e Sistemeve të Informacionit është përcaktuar, miratuar dhe komunikuar
2) Struktura e qeverisjes së Sistemeve të Informacionit është e vendosur dhe është funksionale
3) Inventari i aseteve të Sistemeve të Informacionit është kryer periodikisht dhe janë identifikuar kërkesat për shtesë, zëvendësim dhe heqje
4) Proceset për ndarjen e infrastrukturës dhe shërbimeve të përbashkëta për sistemet e informacionit me entet e tjera publike janë të vendosura dhe funksionale.
5) Proceset për zhvillimin, blerjen dhe mirëmbajtjen e Sistemeve të Informacionit janë përcaktuar, miratuar dhe komunikuar (përfshirë atë të menaxhimit të ndryshimeve)
6) Janë përcaktuar, miratuar dhe komunikuar proceset lidhur me operacionet IT (në-burim, jashtë-burimit, marrëveshje shërbimi)
7) Janë marrë masa për të garantuar sigurinë fizike dhe kushtet e synuara fizike të punës.
8) Janë miratuar masa për trajnimin dhe sensibilizimin e burimeve njerëzore për të siguruar konfidencialitetin, integritetin dhe disponueshmërinë e informacionit, si dhe përputhshmërinë me kërkesat e strukturës politikë-bërëse të Sistemeve të Informacionit.
9) Janë miratuar masa për të siguruar konfidencialitetin, integritetin dhe disponueshmërinë e mënyrave dhe kanaleve të ndryshme të komunikimit
10) Janë miratuar masa për menaxhimin e sigurisë së informacionit
11) Janë miratuar masat për Menaxhimin e Përputhshmërisë Statutore
12) Janë miratuar masa për vazhdimësinë e biznesit (organizatës) dhe menaxhimin e rimëkëmbjes nga fatkeqësitë
13) Kontrollet e aplikacionit të miratuara brenda çdo sistemi informacioni janë të përshtatshme dhe të besueshme. Një vlerësim i tillë mund të përfshijë identifikimin e komponentëve të rëndësishëm të aplikacionit, identifikimin e kritikës ndaj aplikacionit për subjektin, rishikimin e dokumentacionit në dispozicion, intervistën e personelit, kuptimin e riskut të kontrollit lidhur me aplikacionin dhe ndikimin e tyre brenda njësinë ekonomike, si dhe zhvillimin e testeve për të ekzaminuar përshtatshmërinë dhe besueshmërinë e kontrolleve të aplikacionit.

6.6 Vlerësimi i kontrolleve të përgjithshme dhe të zbatimit mund të mbulojë, politikat, proceset, individët dhe sistemet e subjektit të audituar, në përputhje me objektivat e auditimit të Sistemeve të Informacionit.

6.7 Në varësi të objektit të auditimit, audituesit mund të merren me hartimin, zbatimin dhe efektivitetin e funksionimit të kontrolleve. Kur Audituesi ka të bëjë me hartimin e kontrollit, një intervistë ose shqyrtim i rregullave të dokumentuara të biznesit (organizatës) mund të jetë i mjaftueshëm. Aty ku Audituesi ka të bëjë me zbatimin e kontrolleve, inspektimi mund të mos jetë i mjaftueshëm dhe mund të jetë e nevojshme të kryhet një analizë e të dhënave ose të kryhet analiza e të dhënave për të vërtetuar se kontrolli siç është projektuar është zbatuar. Së fundi, nëse Audituesi ka të bëjë me efektivitetin operativ të kontrollit, atij mund t'i kërkohet të testojë një kampion transaksionesh për të demonstruar se kontrolli ka funksionuar në mënyrë efektive gjatë gjithë periudhës përkatëse.

6.8 Audituesit gjithashtu mund të marrin në konsideratë se si evidenca në lidhje me kontrollet e përgjithshme ndikon në natyrën, kohën dhe tërësinë e provave të nevojshme për të marrë siguri në lidhje me funksionimin e kontrolleve të aplikacionit. Nëse Audituesi ka marrë evidencë të mjaftueshme dhe të përshtatshme në lidhje me efektivitetin e kontrolleve të përgjithshme që mbështesin aksesin logjik të personelit në sistemet e IT-së dhe menaxhimin e ndryshimit brenda mjedisit të prodhimit, ai mund të jetë në gjendje të konkludojë mbi efektivitetin operativ të procedurave të kontrollit për apliakcionin e automatizuar. Kjo mund të bëhet duke testuar një kampion më të vogël transaksionesh, sepse efektiviteti i mjedisit të përgjithshëm të IT-së i ofron audituesit evidencë mbi efektivitetin e kontrollit të aplikacionit në periudhën përkatëse. Në rast të procedurave manuale të kontrollit të aplikacionit, Audituesve mund t'u duhet të testojnë një numër më të madh kampionësh të përshtatshëm për të arritur nivelin e duhur të kredibilitetit.

6.9 Bazuar në vlerësimin e kontrolleve të IT-së, audituesit mund të identifikojnë fushat prioritare për realizimin e Testimit themelor (mbi bazat), i cili përfshin testimin e detajuar të kontrolleve të IT-së duke përdorur teknika të ndryshme të auditimit me ndihmën e kompjuterit (CAAT) për kërkimin, nxjerrjen dhe analizën e të dhënave. Audituesit mund të hartojnë dhe të realizojnë një Testim themelor (mbi bazat) në mënyrë që të provojnë objektivat e auditimit. Audituesit mund të zgjedhin teknikat CAAT më të përshtatshme, bazuar kjo dhe në kërkesat e tyre.

6.10 Audituesit mund të përdorin teknikat CAAT për të realizuar auditimet e IT-së, të tilla si analiza e regjistrit të përdoruesit, raportimi i përjashtimeve, totali gjetjeve në terren, krahasimi i skedarëve, shtresimi, kampionimi, kontrollet e dyfishta, zbulimi i boshllëqeve, vjetërsia, llogaritjet e fushës virtuale etj. Përparësitë e përdorimit të teknikave CAAT-ve përfshijnë vëllime të mëdha të të dhënave, teste të përsëritura në grupe të ndryshme të dhënash dhe me kritere të ndryshme dhe dokumentacion i automatizuar i testeve dhe rezultateve të auditimit me stampime kohore.

6.11 Audituesit mund të mos jenë gjithmonë në gjendje të shqyrtojnë të gjitha rastet, transaksionet, modulet ose sistemet e IT-së, duke pasur parasysh burimet e kufizuara dhe llogarinë kosto-përfitim gjatë ushtrimit të auditimit. Në një situatë të tillë, SAI-et, bazuar në konsideratat e materialitetit, mund të miratojnë kampionet e auditimit për ekzaminim të detajuar në mënyrë që të nxjerrin konkluzione të arsyeshme auditimi. SAI-t mund të përdorin teknikat CAAT të përshtatshme për kryerjen e llojeve të ndryshme të kampionimit dhe të përcaktojnë një madhësi të përshtatshme kampioni, në varësi të risqve të brendshme dhe të kontrollit. Kampionët e auditimit[14] janë nxjerrë në mënyrë që t'i ofrohet audituesit një bazë e arsyeshme mbi të cilën mund të nxjerrë përfundie për të gjithë popullatën e të dhënave, bazuar mbi konkluzionet e nxjerra nga aplikimi i procedurave të auditimit dhe analiza e kampionit të auditimit. Audituesit mund të marrin në konsideratë qëllimin e procedurës së auditimit dhe karakteristikat e popullatës nga e cila do të merret kampioni dhe të përcaktojnë një madhësi të mjaftueshme të kampionit për të reduktuar riskun e kampionimit brenda një niveli të pranueshëm. Auditimi në një mjedis IT mund të lehtësojë analizën në masën 100 % të një popullsie, veçanërisht në fazën e vlerësimit paraprak. Megjithatë, për kryerjen e Testimit themelor (mbi bazat), kampionët mund të jenë të nevojshëm. Kur realizohet një kampionim brenda fushës së auditimit financiar, audituesit e Sistemeve të Informacionit mund të aplikojnë rregullat që parashikon ISSAI 2530 për përzgjedhjen e kampionit.[15]

6.12 Audituesit mund të sigurojnë që evidenca elektronike e mbledhur dhe e dokumentuar është e mjaftueshme, e besueshme dhe e saktë për të mbështetur vëzhgimet e auditimit. Një dëshmi e tillë elektronike mund të përbëhet nga skedarë të dhënash, regjistra të përdoruesve, modele analitike, raporte të menaxhimit të sistemeve të informacionit, etj. që mund të mblidhen dhe ruhen në mënyrë të përshtatshme në një mënyrë të tillë që ato të jenë të disponueshme për të dhënë siguri mbi saktësinë dhe vlefshmërinë e procesit të

[14] *ISSAI 2530, Auditimi Financiar, Kampioni i Auditimit, Seksionet 6 deri 9.*
[15] *ISSAI 2530, Auditimi Financiar, Kampioni i Auditimit, Seksionet 6 deri 9.*

auditimit. Provat e mbledhura gjatë një auditimi të sistemeve të informacionit mund të kenë vulat kohore dhe detajet e nevojshme që përmbajnë hapat e analizës së të dhënave të kryera, në mënyrë që të ketë qartësi se kur u krijua, u ruajt dhe kur u modifikua së fundmi evidenca, për të zbutur riskun e ndryshimeve të mëvonshme.

6.13 Dokumentacioni i auditimit të sistemeve të informacionit mund të ruhet dhe mbrohet nga çdo modifikim dhe fshirje e paautorizuar. SAI-t mund të zhvillojnë standarde të reja për ruajtjen e dokumentacionit të auditimit të Sistemeve të informacionit ose të përshtatin standardet ekzistuese për të përmbushur kërkesat e ruajtjes së dokumentacionit të lidhur me auditimin e Sistemeve te Informacionit. Periudha e ruajtjes së dokumentacionit arritur në këtë mënyrë do të ishte një funksion i mandatit të SAI-t individual dhe statutit(eve) që rregullon aktivitetet e tij. Vëmendje e veçantë mund t'i kushtohet medias, formatit, jetëgjatësisë dhe kërkesave të ruajtjes për këto të dhëna, për të siguruar që të dhënat të jenë të lexueshme brenda kornizës kohore të përcaktuar në politikën e ruajtjes dhe arkivimit të të dhënave të çdo SAI. Kjo mund të kërkojë konvertimin e të dhënave nga një format në tjetrin për të vijuar me përparimet teknologjike dhe amortizimin.

6.14 Në rast të ekzaminimit të raporteve teknike të përgatitura nga audituesit e palëve të treta për çështje specifike të teknologjisë, audituesit mund të përshtasin procedurat e duhura për të dhënë siguri lidhur me aspektet e përputhshmërisë, financiare ose të performancës të këtyre raporteve.[16] Nëse, si rezultat i këtyre procedurave, **siguria** mbështetet në përmbajtjen e këtyre raporteve, fakti i kësaj të fundit mund të shpaloset në mënyrë të përshtatshme.

6.15 ISSAI-t parashikojnë që audituesit duhet të krijojnë komunikim efektiv gjatë gjithë procesit të auditimit dhe të mbajnë të informuar subjektin e audituar për të gjitha çështjet që lidhen me auditimin (shih ISSAI 100 paragrafi 43). Në auditimet që përfshijnë punën e auditimit të sistemeve të Informacionit, rezultati i auditimit të Sistemeve te Informacionit në disa raste mund t'i komunikohet subjektit nëpërmjet një letre të veçantë. Në këto raste, mund të jetë e rëndësishme të shpjegohet se si rezultati i punës së auditimit lidhet me komunikime të tjera që janë pjesë e të njëjtit auditim financiar, performancë ose përputhshmërie dhe se si rezultatet e punës së auditimit të Sistemeve të Informacionit mund të jenë të rëndësishme për rezultatet e raportit të auditimit të SAI-it.

[16] *Kur qëllimi është brenda auditimit financiar, audituesit mund të përdorin ISSAI 2402 Konsideratat e Auditimit në lidhje me një subject që përdor një shërbim*

7 Raportimi i Auditmit të Sistemeve të Informacionit

7.1 Meqenëse një auditim i sistemeve të informacionit do të ishte një Auditim Financiar (ISSAI 200), Auditim i Performancës (ISSAI 300) ose Auditim i Përputhshmërisë (ISSAI 400), audituesit mund të marrin në konsideratë kërkesat e raportimit në përputhje me rrethanat. Kjo do të ishte specifike për SAI-et. Në mënyrë të ngjashme, çdo SAI mund të ketë pragjet e veta të raportimit bazuar në materialitetin e gjetjeve të auditimit. Po kështu, një auditues, gjatë raportimit të auditimit të sistemeve të informacionit, mund të marrë parasysh kufizimet statutore dhe të brendshme për zbulimin e informacionit financiar dhe teknik.

7.2 Audituesit mund të jenë të vetëdijshëm lidhur me nevojën për të kufizuar përdorimin e zhargonit teknik dhe për ndjeshmërinë e informacionit të paraqitur (p.sh. fjalëkalimet, emrat e përdoruesve, ID-në dhe informacionin personal) në raportet e auditimit. Pavarësisht natyrës teknike të një auditimi të Sistemeve të Informacionit, audituesit mund të sigurojnë që raporti të jetë plotësisht i kuptueshëm nga stafi drejtues i subjektit të audituar, palët e interesuara dhe publiku i gjerë. Audituesit mund të përfshijnë një fjalor të detajuar të termave në raporte auditimi, i cili referon përkufizimin e një shkurtimi ose një termi me një shpjegim të bazuar në skenarin se si funksionon kjo në një mjedis të kontrolluar.

7.3 Audituesit mund të marrin në konsideratë ndikimin e mundshëm negativ të raportit pasi të publikohet raporti i auditimit të sitemeve të informacionit. Për shembull, nëse raporti i auditimit të sistemeve të informacionit zbulon disa risqe sigurie në sistemin e informacionit të një subjekti të audituar dhe të njëjtat raportohen përpara se të miratohen kontrollet e nevojshme për të zbutur risqet, cenueshmëria e sistemit të informacionit mund të ekspozohet ndaj publikut. Në një skenar të tillë, audituesit mund të marrin në konsideratë opsione të tilla si raportimi vetëm pasi të jenë aprovuar kontrollet e nevojshme, ose mos raportimi i plotë dhe i saktë i riskut të sigurisë, në mënyrë që të shmanget ndikimi i mundshëm negativ në subjektin e audituar.

8 Zbatimi i Rekomandimeve

8.1 Meqenëse auditimi në Sistemet e Informacionit është nxjerrë nga një ose më shumë nga llojet kryesore të auditimit, audituesit mund t'i konsiderojnë kërkesat për zbatimin e rekomandimeve edhe për angazhime auditimi në një nivel me Auditimin Financiar (ISSAI 200), Auditimin e Performancës (ISSAI 300).) dhe Auditimin e Përputhshmërisë (ISSAI 400).