GUID 5100

Smjernice za reviziju informacionih sistema

INTOSAI Smjernice izdaje
Međunarodna organizacija vrhovnih revizorskih institucija, INTOSAI, kao dio INTOSAI okvira profesionalnih izjava.
Za više informacija posjetite
www.issai.org

INTOSAI, 2019.

1) Utvrđen kao ISSAI 5100 - Smjernice za IT reviziju, u 2016. godini.

2) Revidiran i preimenovan u GUID 5100 – Smjernice za reviziju informacionih sistema, u 2019. godini.

SADRŽAJ

1 UVOD

1.1 GUID 5100 pruža sveobuhvatni okvir za provođenje revizije informacionih sistema unutar IFPP-a. GUID je namijenjen da obezbijedi osnovu za razvoj budućih GUID-ova u seriji 5100-5109 u predmetnoj oblasti revizije informacionih sistema, u okviru IFPP-a.

1.2 Okvir postavljen u ovom GUID-u je u skladu sa *Osnovnim principima revizije javnog sektora* (ISSAI 100), *Osnovnim principima finansijske revizije* (ISSAI 200), *Principima revizije učinka* (ISSAI 300) i *Principima revizije usklađenosti* (ISSAI 400).

1.3 Vrhovne revizorske institucije (VRI) imaju mandat da vrše reviziju vlada i njihovih subjekata prema njihovim revizijskim mandatima.[1] Svojim aktivnostima, VRI imaju za cilj da promovišu efikasnost, odgovornost, efektivnost i transparentnost javne uprave.[2]

1.4 Vlade i drugi subjekti javnog sektora kontinuirano usvajaju inovacije informacione tehnologije (IT) u svoje informacione sisteme, kako bi unaprijedili efikasnost i efektivnost u funkcionisanju i pružanju različitih javnih usluga. To je zato što je IT omogućio hvatanje, pohranjivanje, obradu, preuzimanje i isporuku informacija elektronskim putem, što zauzvrat stvara značajan prostor za poboljšanje tačnosti, povjerljivosti i blagovremenosti metrike informacionih sistema. Štaviše, način pružanja javnih usluga brzo prelazi sa fizičkog na elektronski, što rezultira time da vlade moraju funkcionisati kao digitalne platforme koje pružaju usluge, kao i infrastrukturu za druge informacione sisteme vođene IT-om.

1.5 Ovaj prelazak na kompjuterizovane informacione sisteme i elektronsku obradu od strane revidiranih subjekata u javnom sektoru pokrenuo je značajne promjene u okruženju u kojem rade VRI. Rashodi javnog sektora za IT rastu. Također postoji potreba da se osigura da su interne IT kontrole za održavanje povjerljivosti, integriteta i dostupnosti podataka usvojene od strane subjekata javnog sektora. Stoga postaje imperativ za VRI da razviju odgovarajuće kapacitete za sprovođenje temeljnog ispitivanja kontrola u vezi sa informacionim sistemima.

[1] INTOSAI-P 1 Deklaracija iz Lime
[2] Rezolucija Generalne skupštine Ujedinjenih nacija A/66/209

2 CILJ

2.1 ISSAI 100, 200, 300 i 400 postavljaju osnovna pravila revizije u vezi sa finansijskom revizijom, revizijom učinka i revizijom usklađenosti. Ovi ISSAI se odnose na opšta načela, procedure, standarde i očekivanja revizora. One su podjednako primjenjive i na revizije informacionih sistema.

2.2 Cilj ovog GUID-a je pružiti smjernice revizorima o tome kako da sprovode revizije učinka i/ili usklađenosti u vezi sa specifičnim predmetom informacionih sistema ili gdje revizija informacionih sistema može biti dio većeg revizorskog angažmana koji može biti finansijska, revizija usklađenosti ili revizija učinka.

2.3 Revizori mogu primijeniti sadržaj ovog GUID-a na faze planiranja, provođenja, izvještavanja i praćenja[3] procesa revizije.

[3] ISSAI 100

3 DEFINICIJE

3.1 Informacioni sistemi: Informacioni sistemi se mogu definisati kao kombinacija strateških, upravljačkih i operativnih aktivnosti uključenih u prikupljanje, obradu, skladištenje, distribuciju i korišćenje informacija i povezanih tehnologija. Složenost takvog informacionog sistema može se kretati od jednostavne knjige u kojoj se unosi za prijem i isplatu novca održavaju ručno, do složenijeg IT sistema kao što je sistem za procjenu poreza, u kome su svi procesi – prikupljanje podataka (npr. poreske prijave koje se podnose putem internet portala), skladištenje na serverima, obrada procjene (na osnovu programiranja korišćenjem poreskih pravila) i komunikacija poreskih zahtjeva, povrata i potvrde (u realnom vremenu ili u propisanim intervalima) — automatizovani. Informaciona tehnologija obuhvaća hardver, softver, komunikaciju i druge objekte koji se koriste za unos, skladištenje, obradu, prenos i izlaz podataka u bilo kom obliku.

3.2 Revizija informacionih sistema može se definisati kao ispitivanje kontrola koje se odnose na informacione sisteme vođene IT-om, kako bi se utvrdili slučajevi odstupanja od kriterijuma, koji su zauzvrat identifikovani na osnovu vrste revizorskog angažmana - tj. finansijska revizija, revizija usklađenosti ili revizija učinka.

4 OPSEG

4.1 Revizori mogu koristiti ovaj GUID za obavljanje revizije učinka i/ili usklađenosti u vezi sa specifičnim predmetom informacionih sistema, kao i kada je revizija informacionih sistema dio većeg revizorskog angažmana koji može biti finansijska revizija, revizija usklađenosti i/ili revizija učinka.

4.2 Ova smjernica pruža dalje smjernice o tome kako se bilo koja revizija informacionih sistema može adresirati korištenjem finansijske revizije/revizije učinka/usklađenosti i ne sadrži nikakve dodatne zahtjeve za provođenjem revizije.

5 PLANIRANJE REVIZIJE INFORMACIONOG SISTEMA

5.1 VRI mogu usvojiti planiranje revizije zasnovano na riziku za revizije IS-a, u skladu sa procesom opisanim u ISSAI 100, ISSAI 200 (Finansijska revizija), ISSAI 300 (Revizija učinka) i ISSAI 400 (Revizija usklađenosti), u zavisnosti od ciljeva revizorskog angažmana.

5.2 Rad revizije IS-a će biti određen ciljem i opsegom revizije. Primjeri mogu uključivati:

1) Procijena relevantne opšte kontrole[4] i kontrole primjene[5] koje imaju uticaj na pouzdanost podataka iz informacionih sistema, što zauzvrat ima uticaj na finansijske izvještaje revidiranog tijela.
2) Da se uvjeri u usklađenost procesa informacionih sistema sa zakonima, politikama i standardima koji se primjenjuju na revidirano tijelo.
3) Da se osigura da IT resursi omogućavaju da se ciljevi organizacije postignu efikasno i efektivno, i da su relevantne opšte kontrole i kontrole primjene efikasne u prevenciji, otkrivanju i ispravljanju slučajeva suvišnosti, ekstravagancije i neefikasnosti u korišćenju i upravljanju informacionim sistemima.

5.3 Na osnovu procjene rizika, opseg revizije IS-a može se izvući iz bilo kojeg ili svih sljedećih domena[6] revidiranog tijela:

1) Organizaciona politika o informacionim tehnologijama[7]
2) Organizaciona upravljačka struktura na temu IT-a
3) Opšte kontrole koje se pružaju u poslovnoj oblasti koja se automatizuje
4) Upravljanje imovinom
5) Razvoj, nabavka i održavanje informacionih sistema, uključujući mapiranje poslovnih procesa i pripadajuću programsku logiku
6) Upravljanje IT operacijama
7) Upravljanje fizičkim okruženjem
8) Upravljanje ljudskim resursima

[4] Opšte kontrole su ručne ili automatizirane procedure koje imaju za cilj da obezbjede poverljivost, integritet i dostupnost informacija u fizičkom okruženju u okviru kojeg se informacioni sistemi razvijaju, održavaju i rade.
[5] Kontrole primjene su ručne ili automatizirane procedure koje zavise od IT-a, unutar informacionog sistema, koje utiču na obradu transakcija, a mogu se odnositi na validaciju ulaznih podataka, tačnu obradu podataka, isporuku izlaznih podataka i kontrole u vezi sa integritetom matičnih podataka.
[6] Većina gore opisanih domena su usvojene iz ISO/IEC 27001
[7] Uključuje aspekte strateškog menadžmenta

9) Upravljanje komunikacijama
10) Upravljanje sigurnošću informacija[8]
11) Upravljanje zakonskom usklađenošću
12) Upravljanje kontinuitetom poslovanja i oporavkom od katastrofe
13) Upravljanje kontrolama aplikacija

5.4 VRI mogu odabrati vremenski period za analizu revizije (npr. godinu dana, tri godine itd.) u definisanju obima angažmana revizije IS-a. Može se odabrati odgovarajući vremenski period, koji je relevantan za ciljeve definisane za revizorski angažman.

5.5 Kada je revizija IS-a dio revizorskog angažmana, VRI može osigurati da revizorski tim kao cjelina radi na integrisan način kako bi se postigao opći cilj revizije. Da bi se postigla efikasna integracija, VRI mogu razmotriti:

1) Sveobuhvatno dokumentovanje posla koji treba da obave revizori IS-a;

2) Formulisanje protokola za razmjenu informacija između revizora IS-a i drugih revizora;

3) Utvrđivanje informacionih sistema i kontrolnih ciljeva koji su u okviru revizije;

5.6 VRI mogu osigurati da je tim za reviziju sastavljen od članova koji zajedno posjeduju kompetentnost za obavljanje angažmana revizije IS-a, radi postizanja planiranih ciljeva revizije.

5.7 Neophodna znanja, vještine i kompetencije mogu se steći kombinacijom obuke, upošljavanja i angažovanja vanjskih resursa, prema strateškom planu VRI-ja.

5.8 VRI mogu osigurati da timovi za reviziju IS-a zajedno imaju kapacitet da:

1) Razumiju tehničke elemente informacionog sistema vođenog IT-om, uključujući sve relevantne primjere aplikacije u upotrebi, kako bi mogli pristupiti i koristiti IT infrastrukturu za proces revizije

2) Razumjeti postojeća pravila, propise i okruženje u kojem djeluju informacioni sistemi revidiranog tijela vođeni IT-om

3) Razumjeti mapiranje poslovnih procesa u programsku logiku za informacioni sistem revidiranog tijela

[8] Uključuje cyber sigurnost

4) Primijeniti i poslovno i informatičko znanje za procjenu rizika od ručnog zaobilaženja sistemskog programa ili konfiguracije koja bi omogućila iznimnu obradu transakcija

5) Procijeniti dizajn i testirati operativnu efikasnost kontrole aplikacija u relevantnim informacionim sistemima

6) Razumjeti metodologiju revizije, uključujući relevantne revizorske standarde i smjernice primjenjive na VRI

7) Razumjeti IT performanse/kriterij usklađenosti u odnosu na koje treba uporediti revizorske nalaze, uključujući okvire za upravljanje IS-om, kao što su COBIT, ITIL, TOGAF

8) Razumjeti tehnike IS-a za prikupljanje revizorskih dokaza iz automatiziranih sistema

9) Razumjeti alate revizije IS-a za prikupljanje, analizu i reprodukciju rezultata takve analize ili ponovno izvođenje revidiranih funkcija

10) Pristup i korištenje IS infrastrukture za prikupljanje i zadržavanje revizijskih dokaza

11) Pristup i korištenje IS revizorskih alata za analizu prikupljenih dokaza

5.9 VRI može razmotriti različite opcije za alokaciju ljudskih resursa za angažmane revizije IS-a. To bi moglo biti uspostavljanje centralne grupe sa IT stručnjacima koji pomažu drugim revizorskim timovima u VRI-ju da izvrše revizije, ili raspoređivanje IT stručnjaka prema zahtjevima. Kako se broj poduzetih angažmana revizije IS-a povećava, VRI mogu razmotriti uspostavljanje posebne grupe ili funkcije za reviziju IS-a. Ovoj grupi se može povjeriti odgovornost za obavljanje svih angažmana revizije IS-a za VRI, te interakciju s drugim timovima u VRI-ju koji imaju naslijeđeno znanje o revidiranom tijelu, kako bi brzo stekli razumijevanje o funkcijama tijela i povezanim poslovnim procesima. Kako tehnologija postaje sve više ugrađena u informacione sisteme, VRI mogu osigurati da svi revizori steknu odgovarajuće vještine revizije IS-a.

5.10 U slučajevima ograničenja resursa, VRI mogu angažovati eksterne resurse kao što su IT konsultanti, izvođači radova, stručnjaci i eksperti za obavljanje revizije IS-a. VRI mogu osigurati da takvi vanjski resursi budu adekvatno obučeni i senzibilizirani za smjernice profesionalnog ponašanja, i za procese i proizvode revizije IS koji se primjenjuju na VRI, te da se njihov rad adekvatno prati kroz

dokumentovani ugovor ili ugovor o nivou usluge i odgovarajuće uključivanje osoblja DRI u faze planiranja, provođenja, izvještavanja i praćenja revizije. VRI će stoga možda trebati kvalifikovane i obrazovane članove tima, kako bi nadgledali rad eksternih resursa i sprovodili poštovanje smjernica i sporazuma o nivou usluga.

5.11 Za provođenje procjene rizika za angažmane IS revizije, revizori mogu koristiti principe postavljene u ISSAI 100, 200, 300 i 400, pored onih koji se koriste u obavljanju specifičnih predmeta revizije IS, kako je navedeno u nastavku:

1) Inherentni rizik bi se sastojao od vjerovatnoće da određene karakteristike informacionih sistema vođenih IT-om revidiranog tijela, po svojoj prirodi, mogu dovesti do štetnog uticaja na isporuku funkcije koju revidirano tijelo mora obavljati. Na primjer, informacioni sistem revidiranog tijela od kojeg se traži da učini dostupnim informacije za sve članove javnosti nosi inherentni rizik učinka da preko predviđene najviše granice korisnika, informacioni sistem možda neće odgovoriti i informacije neće biti dostupne bilo kom korisniku. Iako revidirano tijelo može usvojiti kontrole za ublažavanje inherentnih rizika, u mnogim slučajevima, tijelo će možda morati jednostavno tolerisati postojanje takvih rizika, u okviru prihvatljivog nivoa rizika. Inherentni rizik se može procijeniti prije nego što revizori razmotre uticaj rizika kontrole ili otkrivanja.

2) Kontrolni rizik za IS sastojao bi se od vjerovatnoće da IT kontrole koje je usvojilo revidirano tijelo možda neće uspjeti umanjiti negativan uticaj na koji su osmišljene kao odgovor. Na primjer, informacioni sistem revidiranog tijela koji je obavezan da osigura da je pristup povjerljivim podacima ograničen na ovlašteno osoblje, može usvojiti kontrolu zahtijevanja predstavljanja korisničkog imena i lozinke od strane osoblja koje pokušava da dobije pristup. Rizik kontrole u ovoj situaciji je da korisničko ime i lozinka nisu na odgovarajući način sigurni i da ih neovlašteno osoblje može pogoditi kroz ponovljene pokušaje, što rezultira gubitkom povjerljivosti i potencijalnim negativnim uticajem na tijelo. Tijelo koje insistira na korištenju sigurnih, netrivijalnih lozinki koje imaju kombinaciju abecede, brojeva i posebnih simbola, te osigurava da informacioni sistem onemogućava pristup korisničkom imenu nakon određenog broja neuspjelih pokušaja pristupa, imao bi manji kontrolni rizik od onog koji nema ove karakteristike.

3) Rizik otkrivanja bi se sastojao od vjerovatnoće da revizor ne otkrije odsustvo, neuspjeh ili neadekvatnost IT kontrola koje je usvojilo tijelo, a koje mogu imati potencijalno negativan uticaj na tijelo.

5.12 Za provođenje procjena zasnovanih na riziku sistema vođenih IT-om, VRI mogu odabrati metodologiju koja je prikladna za njihovu svrhu. Takve metodologije mogu se kretati od jednostavnih klasifikacija profila rizika IT okruženja revidiranog tijela kao Visokog, Srednjeg i Niskog, na osnovu VRI-jevog razumijevanja tijela, njegovog okruženja i profesionalnog prosuđivanja tima za reviziju IS-a jedne VRI, do više složene i numeričke kalkulacije koje kvantificiraju ocjenu rizika na osnovu objektivnih podataka prikupljenih od revidiranog tijela.[9]

5.13 Značajnost pitanja revizije IS-a može se odlučiti u okviru opšteg okvira za odlučivanje o materijalnosti u VRI-ju. Perspektiva materijalnosti može varirati u zavisnosti od prirode angažmana revizije IS-a. Materijalnost za finansijske revizije, reviziju učinka i usaglašenost javnog sektora, iz kojih bi se izvukao angažman revizije IS-a, opisana je u ISSAI 100, 200, 300 i 400.[10]

[9] WGITA IDI Priručnik za IT reviziju za Vrhovne revizorske institucije

[10] ISSAI 200 Principi finansijske revizije, ISSAI 300 Principi revizije učinka, ISSAI 400 Principi revizije usklađenosti

6 SPROVOĐENJE REVIZIJE INFORMACIONOG SISTEMA

6.1 VRI mogu provoditi revizije IS-a u skladu s procesom opisanim za Finansijsku reviziju (ISSAI 200), Reviziju učinka (ISSAI 300) i Reviziju usklađenosti (ISSAI 400), u skladu sa prirodom angažmana.

6.2 Konkretno za reviziju IS-a, Revizori mogu tražiti odgovarajuću saradnju i podršku revidiranog tijela u završetku revizije, uključujući pristup evidenciji i informacijama. Revizori mogu identifikovati način pristupa elektronskim podacima u formatu neophodnom za analizu, u konsultaciji sa revidiranim tijelom. Način pristupa podacima bio bi specifičan za VRI.

6.3 Prije pokretanja procjene kontrola u informacionom sistemu, revizori mogu razviti razumijevanje arhitekture sistema, te temeljnih podataka i njihovih izvora, kako bi identificirali potrebne alate i tehnike revizije.

6.4. U slučaju prijema *dump* podataka[11] od revidiranog tijela, revizori mogu osigurati da svaki *dump* podataka bude popraćen pismom revidiranog tijela. Takvo pismo za proslјeđivanje može navesti:

1) Izvor (putem upućivanja na vremensku oznaku generiranja *dump* podataka/*hash* broja za *dump* podataka) podataka u svrhu osiguranja integriteta podataka, autentikacije[12] i neporicanja[13]

2) Parametri ekstrakcije koji se koriste za kreiranje *dump* podataka, tj. korišteni upiti/izvještaji.

3) Ako takvo proslijeđeno pismo od revidiranog tijela nije primljeno, interne dokumente mogu generirati revizori koji primjećuju važne informacije kao što su kao datum kada su podaci predati, iz koje datoteke je napravljen *dump* podataka i da li su podaci iz proizvodnog okruženja ili iz nekog drugog okruženja, itd.

6.5 Kako bi se ispitala njihova pouzdanost i dovoljnost, revizori mogu izvršiti procjenu IT kontrola (opće i aplikativne kontrole) koje je usvojilo revidirano tijelo. Procjena se može izvršiti korištenjem odgovarajuće kombinacije sljedećih tehnika: Intervju, Upitnik, Posmatranje, Prolaz kroz podatke, Dijagrami toka, Prikupljanje i

[11] *Dump* podataka se definiše kao velika količina podataka prenesenih sa jednog sistema ili lokacije na drugu.

[12] Autentikacija se definiše kao čin provjere identiteta korisnika – Rječnik pojmova ISACA

[13] Neporicanje se definiše kao garancija da strana ne može kasnije da porekne izvorne podatke; pružanje dokaza o integritetu i porijeklu podataka koje može provjeriti treća strana – Rječnik pojmova ISACA

analiza podataka, Provjera, Ponovno izračunavanje, Ponovna obrada i Potvrda treće strane. Opseg procjene IT kontrola može uključivati ispitivanje da je:

1) IS politika definisana, usvojena i saopštena

2) Struktura upravljanja IS-om uspostavljena i funkcionalna

3) Da je periodično vršen popis imovine IS-a i da su utvrđeni zahtjevi za povećanje, zamjenu i uklanjanje

4) Da su procesi za dijeljenje infrastrukture i zajedničkih usluga za informacione sisteme sa drugim javnim subjektima uspostavljeni i funkcionalni

5) Da su procesi za razvoj, nabavku i održavanje informacionih sistema definisani, usvojeni i saopšteni (uključujući upravljanje promjenama)

6) Da su procesi za IT operacije (*in-sourcing, outsourcing*, ugovori o uslugama) definisani, usvojeni i saopšteni

7) Da su usvojene mjere za osiguranje fizičke sigurnosti i predviđenih fizičkih uslova rada

8) Da su usvojene mjere za obuku i senzibilizaciju ljudskih resursa kako bi se osigurala povjerljivost, integritet i dostupnost informacija, kao i usklađenost sa zahtjevima IS Politike i strukture upravljanja.

9) Da su usvojene mjere za osiguranje povjerljivosti, integriteta i dostupnosti različitih načina komunikacije i da su kanali usvojeni

10) Da su usvojene mjere za upravljanje sigurnošću informacija

11) Da su usvojene mjere za upravljanje usklađenošću sa zakonskim propisima

12) Da su usvojene mjere za kontinuitet poslovanja i upravljanje oporavkom od katastrofe

13) Da su kontrole usvojene u okviru svakog informacionog sistema adekvatne i pouzdane. Takva procjena može uključivati identifikaciju značajnih komponenti aplikacije, identifikaciju kritičnosti aplikacije za tijelo, pregled dostupne dokumentacije, intervju s osobljem, razumijevanje rizika kontrole aplikacije i njihovog uticaja na tijelo, te razvoj testova za ispitivanje adekvatnosti i pouzdanosti takvih kontrola aplikacija.

6.6. Procjena opštih kontrola i kontrola primjene stoga može obuhvatiti politike, procese, ljude i sisteme revidiranog tijela, u skladu sa ciljevima revizije IS-a.

6.7 U zavisnosti od cilja revizije, Revizori se mogu baviti dizajnom, implementacijom i operativnom efektivnošću kontrola. Kada se Revizor bavi dizajnom kontrole, intervju ili inspekcija dokumentiranih poslovnih pravila može biti dovoljna. Kada je Revizor zabrinut za implementaciju kontrola, upit možda neće biti dovoljan i može biti potrebno provesti pregled ili izvršiti analizu podataka, kako bi se potvrdilo da je kontrola sprovedena onako kako je dizajnirana. Konačno, ako je revizor zabrinut za operativnu efektivnost kontrole, od njega se može zahtijevati da testira uzorak transakcija, kako bi pokazao da je kontrola djelovala efikasno tokom relevantnog perioda.

6.8 Revizori također mogu razmotriti kako dokazi o opštim kontrolama utiču na prirodu, vrijeme i obim dokaza potrebnih za dobijanje uvjerenja o funkcionisanju kontrola primjene. Ako je Revizor pribavio dovoljne i odgovarajuće revizijske dokaze u vezi s djelotvornošću općih kontrola koje podržavaju logičan pristup osoblja IT sistemima i upravljanje promjenama unutar proizvodnog okruženja, možda će moći zaključiti o operativnoj efikasnosti automatiziranih procedura kontrole aplikacija. To se može uraditi testiranjem manjeg uzorka transakcija, jer efektivnost opšteg IT okruženja pruža revizoru dokaz o efektivnosti kontrole aplikacije u relevantnom periodu. U slučaju ručnih procedura kontrole aplikacija, revizori će možda morati testirati veličinu uzorka koja odgovara odabranom nivou pouzdanosti.

6.9 Na osnovu procjene IT kontrola, revizori mogu utvrditi prioritetna područja za preuzimanje Supstantivnog testiranja, koje uključuje detaljno testiranje IT kontrola primjenom različitih Kompjuterski potpomognutih revizorskih tehnika (CAAT) za izdvajanje i analizu podataka. Revizori mogu osmisliti i izvršiti Substantivno testiranje, kako bi potkrijepili ciljeve revizije. Revizori mogu odabrati odgovarajuće Kompjuterski potpomognute revizorske tehnike (CAAT), na osnovu svojih zahtjeva.

6.10 Revizori mogu koristiti CAAT-ove za izvršavanje tehnika revizije IS-a kao što su analiza korisničkog dnevnika, izvještavanje o izuzecima, zbrajanje na terenu, poređenje datoteka, stratifikacija, uzorkovanje, provjere duplikata, otkrivanje praznina, starenje, kalkulacije virtualnog polja itd. Prednosti upotrebe analize CAAT-a uključuju velike količine podataka, ponovljivost testova na različitim skupovima podataka i sa različitim kriterijumima, i automatizovano dokumentovanje revizorskih testova i rezultata sa vremenskim oznakama.

6.11 Sobzirom na ograničenja resursa i kompromise između troškova i koristi revizije, revizori možda nisu uvijek u poziciji da ispitaju sve instance, transakcije ili module ili IT sisteme. U takvoj situaciji, VRI mogu, na osnovu razmatranja

materijalnosti, usvojiti revizijski uzorak za detaljno ispitivanje, kako bi izvukle razumne revizorske zaključke. VRI mogu koristiti odgovarajuće CAAT-ove za provođenje različitih tipova uzorkovanja i odrediti odgovarajuću veličinu uzorka, ovisno o osnovnim inherentnim i kontrolnim rizicima. Revizijski uzorci[14]1 se izrađuju kako bi se revizoru pružila razumna osnova za izvođenje zaključaka o cjelokupnoj populaciji podataka, a na osnovu zaključaka izvedenih primjenom revizijskih procedura i analiza na revizijski uzorak. Revizori mogu razmotriti svrhu postupka revizije i karakteristike populacije iz koje će biti uzet uzorak, te odrediti veličinu uzorka dovoljnu da smanji rizik uzorkovanja u okviru prihvatljivog nivoa. Revizija u IT okruženju može olakšati analizu 100 posto populacije, posebno u fazi preliminarne procjene. Međutim, za provođenje substancialnog ispitivanja, uzorci mogu biti potrebni. Kada vrše uzorkovanje u okviru finansijske revizije, revizori IS-a mogu primijeniti ISSAI 2530 za odabir uzorka.[15]

6.12 Revizori mogu osigurati da su prikupljeni i dokumentovani elektronski dokazi dovoljni, pouzdani i tačni da podrže zapažanja revizije. Takvi elektronski dokazi mogu se sastojati od datoteka sa podacima, korisničkih dnevnika, analitičkih modela, upravljanja izvještajima informacionih sistema itd. i mogu biti na odgovarajući način prikupljeni i pohranjeni na način da budu dostupni za dobijanje uvjerenja o tačnosti i valjanosti procesa revizije. Dokazi prikupljeni tokom revizije IS-a mogu imati potrebne vremenske oznake i detalje koji sadrže korake izvršene analize podataka, tako da postoji jasnoća o tome kada je dokaz kreiran, pohranjen i posljednji put modificiran, kako bi se umanjio rizik od naknadnih promjena.

6.13 Dokumentacija revizije IS-a može se zadržati i zaštititi od bilo kakve izmjene i neovlaštenog brisanja. VRI mogu razviti nove standarde za čuvanje dokumentacije revizije IS-a ili prilagoditi postojeće standarde kako bi ispunili zahtjeve zadržavanja dokumentacije vezane za IS reviziju. Tako postignuti period zadržavanja bio bi u funkciji mandata pojedinačne VRI i statuta koji reguliše(u) njene aktivnosti. Posebna pažnja se može posvetiti medijima, formatu, očekivanom vijeku trajanja i zahtjevima za skladištenje ovih podataka, kako bi se osiguralo da su podaci čitljivi u vremenskom okviru definisanom u politici čuvanja i arhiviranja podataka svake VRI. Kako bi se pratio tehnološki napredak i zastarjelost, to može zahtijevati konverziju podataka iz jednog formata u drugi.

6.14 U slučaju ispitivanja tehničkih izvještaja koje su pripremili revizori trećih strana o temama specifičnim za tehnologiju, revizori mogu usvojiti odgovarajuće

[14] ISSAI 2530, *Finansijska revizija, Uzorkovanje revizije, odjeljci 6 do 9*
[15] ISSAI 2530, *Finansijska revizija, Uzorak revizije, Odjeljci 6 do 9*

procedure kako bi se uvjerili u usklađenost, finansijske aspekte ili aspekte učinka takvih izvještaja.[16] Ako je, kao rezultat takvih procedura, oslonac postavljen na sadržaj takvih Izvještaja, činjenica oslanjanja može biti otkrivena na odgovarajući način.

6.15 ISSAI predviđaju da revizori treba da uspostave efikasnu komunikaciju tokom cijelog procesa revizije i obavještavaju revidirano tijelo o svim pitanjima koja se odnose na reviziju (vidi ISSAI 100 stav 43). U revizijama koje uključuju rad IS revizije, rezultat revizije IS-a može u nekim slučajevima biti saopšten revidiranom tijelu putem posebnog pisma. U tim slučajevima, može biti važno objasniti kako se rezultat revizijskog rada odnosi na druge komunikacije koje su dio iste finansijske revizije, revizije performanse ili revizije usklađenosti, i to kako rezultati rada revizije IS-a mogu biti relevantni za rezultirajući revizijski izvještaj VRI-ja.

[16] Kada je djelokrug unutar finansijske revizije, revizori mogu koristiti ISSAI 2402. *Revizijska razmatranja koja se odnose na tijelo koji koristi uslužnu organizaciju*

7 IZVJEŠTAVANJE O REVIZIJI INFORMACIONOG SISTEMA

7.1 Budući da bi angažman revizije informacijskog sistema bio ili Finansijska revizija (ISSAI 200), Revizija učinka (ISSAI 300) ili Revizija usklađenosti (ISSAI 400), u skladu sa tim Revizori mogu uzeti u obzir zahtjeve izveštavanja. To bi bilo specifično za VRI. Slično tome, svaka VRI može imati svoje vlastite pragove izvještavanja na osnovu materijalnosti nalaza revizije. Isto tako, Revizor, prilikom izvještavanja o angažmanu revizije IS-a, može uzeti u obzir zakonska i interna ograničenja u objelodanjivanju finansijskih i tehničkih informacija.

7.2 Revizori mogu biti svjesni potrebe da ograniče upotrebu tehničkog žargona i osjetljivosti informacija koje su predstavljene u izvještaju (npr. lozinke, korisnička imena, ID i lični podaci). Uprkos tehničkoj prirodi revizije IS-a, revizori mogu osigurati da izvještaj bude u potpunosti razumljiv višem rukovodstvu revidiranog tijela, zainteresovanim stranama i široj javnosti. Revizori mogu uključiti odgovarajući detaljni glosar pojmova u izvještaje, koji upućuju na definiciju akronima ili termina, sa objašnjenjem zasnovanim na scenariju o tome kako to funkcionira u kontroliranom okruženju.

7.3 Revizori mogu razmotriti potencijalni negativan utjecaj izvještaja nakon objavljivanja izvještaja revizije IS-a. Na primjer, ako izvještaj revizije IS otkrije neke sigurnosne rizike u informacionom sistemu revidiranog tijela i isti se prijave prije nego što su usvojene neophodne kontrole za ublažavanje rizika, ranjivost informacionog sistema može biti izložena javnosti. U takvom scenariju, revizori mogu razmotriti opcije kao što je izvještavanje tek nakon što su potrebne kontrole usvojene, ili neizvještavanje o tačnom sigurnosnom riziku u potpunosti, kako bi se izbjegao potencijalni negativan uticaj na revidirano tijelo.

8 PRAĆENJE

8.1 Pošto se revizijski angažman o Informacionim sistemima izvodi iz jedne ili više glavnih vrsta revizije, revizori mogu smatrati da su naknadni zahtjevi za takve revizijske angažmane jednaki onima za Finansijsku reviziju (ISSAI 200), Reviziju učinka (ISSAI 300) i Reviziju usklađenosti (ISSAI 400).