



## ISSAI 5300

Starptautiskās Augstāko revīzijas iestāžu organizācijas ISSAI standartus izdevusi Starptautiskā Augstāko revīzijas iestāžu organizācija INTOSAI. Plašākai informācijai apmeklējiet interneta vietni [www.issai.org](http://www.issai.org)

# IT revīzijas veikšanas vadlīnijas

## INTOSAI Profesionālo standartu komiteja

---

PSC-Secretariat

Rigsrevisionen • Store Kongensgade 45 • 1264 Copenhagen K • Denmark  
Tālr.: +45 3392 8400 • Fakss: +45 3311 0415 • E-pasts: info@rigsrevisionen.dk

# INTOSAI



INTOSAI Ģenerālsekretariāts - RECHNUNGSHOF  
(Austrijas Revīzijas palāta)  
DAMPFSCHIFFSTRASSE 2  
A-1033 VĪNE  
AUSTRIJA  
Tālr.: ++43 (1) 711 71 • Fakss: ++43 (1) 718 09 69

[intosai@rechnungshof.gv.at](mailto:intosai@rechnungshof.gv.at)

<http://www.intosai.org>

## Saturs

<b>Priekšvārds.....</b>	<b>4</b>
<b>A. IT revīzijas pamatnostādnes .....</b>	<b>5</b>
1. ISSAI 5300 darbības joma .....	5
2. Ievads IT revīzijās .....	5
3. IT revīzijas definīcija.....	5
4. Pilnvaras IT revīzijas veikšanai.....	6
<b>B. Vispārējās prasības, kas attiecas konkrēti uz IT revīzijām .....</b>	<b>7</b>
5. Uz risku balstīta revīzijas pieeja IT revīzijai .....	7
6. Būtiskums.....	8
7. Dokumentēšana .....	8
8. Spējas .....	10
<b>C. prasības saistībā ar IT revīzijas procesiem .....</b>	<b>10</b>
9. IT revīzijas plānošana.....	10
10. Stratēģiska IT revīzijas plānošana.....	11
11. Ikgadējā IT revīziju plānošana .....	12
12. IT revīzijas plānošana revīzijas grupas līmenī izvēlētajai revīzijai .....	12
13. Atbilstošanas izlases izvēle IT revīzijai .....	13
14. IT revīzijas mērķi .....	14
15. IT revīzijas apjoms .....	16
16. ARI spējas veikt IT revīziju .....	17
17. Resursu piešķiršana .....	17
18. Ārējo resursu piesaiste.....	18
19. Revīzijas uzdevums ar revidējamo vienību.....	18
20. Revīzijas pierādījumi.....	18
21. Revīzijas veikšana – revīzijas pierādījumu iegūšana .....	19
22. Pārraudzība un pārbaude .....	20
23. Krāpšanas, korupcijas un citu pārkāpumu gadījumi.....	20
24. Ierobežojumi.....	21
25. Ieteikumu ieviešanas uzraudzība.....	21
<b>D. IT revīzijas metodes un rīki .....</b>	<b>21</b>
26. IT revīzijai specifisku metožu noskaidrošana .....	21
27. Plānošanas metodes.....	21
28. Revīzijas veikšanas metodes .....	22
29. Atbilstošās sistēmas izvēle informācijas saglabāšanai .....	23
30. IT revīzijas rīki .....	23
<b>E. Ziņošana .....</b>	<b>25</b>
31. Prasības ziņošanai par IT revīziju.....	25
32. IT revīzijas ziņojuma saturs un forma .....	25
<b>A PIELIKUMS – DATU ANALĪZES METODES.....</b>	<b>27</b>

## PRIEKŠVĀRDS

Starptautisko standartu augtākajām revīzijas iestādēm numuri no 5300 līdz 5399 tika piešķirti informācijas tehnoloģiju revīzijas veikšanas vadlīnijām ISSAI pamatnostādņu ietvaros. ISSAI 5300, pirmais ISSAI 5300.sērijā, ir galvenais, vispārējais ISSAI par IT revīzijas veikšanas pamatiem. Tas nosaka vispārējos principus, pieeju un metodoloģiju IT revīzijas veikšanai.

ISSAI 5300 ir arī paredzēts kalpot par ceļvedi augstākajām revīzijas iestādēm IT revīziju veikšanā, IT revīziju apjoma izstrādē un ierobežotu IT revīzijas resursu izmantošanā, lai sniegtu pārlicību revidējamajām vienībām, valdībai un valsts iedzīvotājiem par IT ieviešanas godīgumu, uzticamību un lietderību.

ISSAI 5300 ir izstrādāts starptautisko standartu augtākajām revīzijas iestādēm ietvaros, pārskatot esošos ar IT revīzijām/Informācijas sistēmu revīzijām saistītos standartus, standartus attiecībā uz informācijas sistēmām, valsts un starptautiskos revīzijas standartus, jo īpaši esošos starptautiskos standartus augtākajām revīzijas iestādēm. Vēl viena svarīga ISSAI 5300 iezīme ir tā, ka tas nodrošina, ka IT revīzijām raksturīgas pamatīpašības ir atbilstoši sasaistītas/iestrādātas dažāda veida revīzijās, kuras noteiktas starptautisko standartu augtākajām revīzijas iestādēm 3.līmenī.

Turklāt, esot 4.līmeņa vadlīnijām, šī ISSAI norādes ir sadalītas divās kategorijās: **Prasības** – kuras ir svarīgas, lai veiktu labas kvalitātes IT revīziju; kurām seko **Skaidrojumi** – kuri plašāk skaidro prasības. Tas ir izdarīts, lai nodrošinātu, ka ISSAI saglabā savu pamatfunkciju sniegt vispārējos norādījumus, kā to paredz starptautisko standartu augtākajām revīzijas iestādēm pamatnostādnes.

ISSAI 5300 ir arī ņemti vērā valsts sektora Informācijas sistēmu brieduma līmeņi un dažādās augstākajās revīzijas iestādēs esošie IT revīziju brieduma līmeņi.

ISSAI struktūra ir veidota par šādām galvenajām apakštēmām:

1. IT revīziju pamatnostādnes
2. Vispārējās prasības, kas attiecas konkrēti uz IT revīzijām
3. Īpašas prasības pret IT revīzijas procesiem
4. IT revīzijas metodes un rīki
5. IT revīziju ziņošanas prasības

Atsevišķs Pielikums ir veltīts datu analīzei.

ISSAI liek pamatus turpmākai starptautisko standartu augtākajām revīzijas iestādēm 5300.-5399.sērijā izstrādei un/vai nosaka īpašas vadlīnijas attiecībā uz noteiktām tēmām, kas attiecas uz INTOSAI kopienu IT revīziju jomā.

ISSAI sagatavoja projekta komanda, kas sastāv no Brazīlijas, Indijas (projekta vadītājs), Indonēzijas, Japānas, Polijas un ASV pārstāvjiem.

## **A. IT REVĪZIJAS PAMATNOSTĀDNES**

### **1. ISSAI 5300 darbības joma**

1.1. ISSAI 5300 starptautisko standartu augstākajām revīzijas iestādēm ietvaros sniedz visaptverošas pamatnostādnes IT revīziju veikšanai.

1.2. Šajā ISSAI izklāstītās pamatnostādnes atbilst Publiskā sektora revīziju veikšanas pamatprincipiem (ISSAI 100), Finanšu revīzijas veikšanas pamatprincipiem (ISSAI 200), Lietderības revīzijas veikšanas pamatprincipiem (ISSAI 300) un Atbilstības revīzijas veikšanas pamatprincipiem (ISSAI 400).

1.3. Šīs ISSAI vadlīnijas nosaka profesionālās prakses prasības IT revīzijā, kas papildinātas ar skaidrojumiem, lai padarītu pamatnostādnes skaidrākas un saprotamākas.

1.4. Prasības satur informāciju, kas ir nepieciešama, lai paveiktu augstas kvalitātes IT revīzijas darbu. Tās skaidro revidentiem, kas no viņiem tiek sagaidīts, un ieinteresētajām personām – ko viņas var sagaidīt no ARI veiktās IT revīzijas.

1.5. Skaidrojumi detalizētāk apraksta prasību nozīmi vai uz ko tās attiecas.

1.6. Šo ISSAI sagatavoja projekta komanda, kas sastāv no Japānas, Polijas, Indonēzijas, Indijas, ASV un Brazīlijas pārstāvjiem.

### **2. Ievads IT revīzijās**

2.1. Valsts organizācijas plaši izmanto Informācijas un komunikācijas tehnoloģijas (IKT), lai pildītu savas funkcijas un sniegtu dažādus pakalpojumus. Šādas uz IKT balstītas sistēmas parasti arī sauc par Informācijas sistēmām (IS) vai Informācija tehnoloģiju (IT) sistēmām.

2.2. Augstākajām revīzijas iestādēm (ARI) atbilstoši to revīzijas pilnvarām ir jāveic valdības un tās iestāžu revīzijas<sup>1</sup>.

2.3. Tādejādi ARI veicina valsts pārvaldes produktivitāti, atbildību, efektivitāti un caurskatāmību<sup>2</sup>.

2.4. Nepārtraukta Informācijas un komunikācijas tehnoloģiju attīstība ir padarījusi iespējamu informācijas iegūšanu, uzglabāšanu, apstrādi un piegādi elektroniski. Šī pāreja uz elektronisko apstrādi izraisīja būtiskas izmaiņas vidē, kurā augstākās revīzijas iestādes strādā. Turklāt valsts izdevumi par IT pieaug. Tāpēc ARI ir nepieciešams attīstīt atbilstošas spējas IT revīziju veikšanai.

### **3. IT revīzijas definīcija**

3.1. IT revīzijas ir definētas kā:

„IT sistēmu un ar to saistītu kontroļu apskate un pārbaude, lai iegūtu pārliecību par IT sistēmu un ar to saistītu kontroļu likumību, produktivitāti, ekonomiskumu un efektivitāti vai atklātu šo principu neievērošanu.”

---

<sup>1</sup> ISSAI 1 „Limas deklarācija”.

<sup>2</sup> Apvienoto nāciju organizācijas Ģenerālās asamblejas rezolūcija A/66/209.

3.2. Līdz ar to IT revīzija<sup>3</sup> ir plašs termins, kas ir izplatījies Finanšu revīzijās<sup>4</sup> (novērtēt organizācijas finanšu pārskatu pārējo apgalvojumu pareizību un atbilstību), Atbilstības revīzijās<sup>5</sup> (iekšējās kontroles sistēmas novērtēšana), un Lietderības revīzijās<sup>6</sup> (novērtēt, vai IT sistēmas atbilst lietotāja vajadzībām un nepakļauj organizāciju nevajadzīgam riskam). Tomēr var būt gadījumi, kad dažas revīzijas ir vēltas tikai sistēmas IT sastāvdaļai.

#### **4. Pilnvaras IT revīzijas veikšanai**

4.1. ARI pilnvarām veikt IT revīziju ir jāizriet no vispārējām ARI pilnvarām veikt revīziju<sup>7</sup>. Dažām augstākajām revīzijas iestādēm var būt īpašas pilnvaras veikt IT revīziju vai IT sistēmu revīziju.

4.2. Daudzām augstākajām revīzijas iestādēm pilnvaras veikt finanšu revīzijas, lietderības revīzijas un atbilstības revīzijas ir pietiekamas arī IT revīziju veikšanai. Tas ir tāpēc, ka IT sistēmas atbalsta organizācijas pamatdarbību, kas var ietvert finanšu sistēmas. Līdz ar to IT revīzijām var nebūt vajadzīgas atsevišķas pilnvaras.

4.3. Īpašām pilnvarām, ja tādas ir, būtu jāattiecas uz revīzijas jurisdikciju attiecībā uz tādu IT sistēmu revīzijām, kuras organizācija izmanto, lai izpildītu savus darbības mērķus. Pilnvarās ir jābūt arī noteiktam, ka organizācijai ir jānodrošina savlaicīga, neierobežota, tieša un brīva piekļuve nepieciešamajiem dokumentiem un informācijai<sup>8</sup>, gan fiziski, gan elektroniski, neskatoties uz to, vai funkcijas vai jebkuras to sastāvdaļas pilda organizācija pati, vai to izpildei tiek piesaistīts ārvalsts pakalpojuma sniedzējs.

4.4. ARI pilnvarām IT revīzijas veikšanai ir jāatbilst 1. un 2.līmeņa starptautisko standartu augstākajām revīzijas iestādēm prasībām.

---

<sup>3</sup> IT revīzija tiek arī saukta par IS revīziju, Sistēmu revīziju, Informācijas revīziju, informācijas drošības revīziju, datoru nodrošinājuma pārbaudēm, IT nodrošinājumu utt.

<sup>4</sup> ISSAI 200 „Finanšu revīzijas veikšanas pamatprincipi”.

<sup>5</sup> ISSAI 400 „Atbilstības revīzijas veikšanas pamatprincipi”.

<sup>6</sup> ISSAI 300 „Lietderības revīzijas veikšanas pamatprincipi”.

<sup>7</sup> ISSAI 10 „Mehiko deklarācijas par ARI neatkarību” 3.princips un ISSAI 100 „Publiskā sektora revīziju veikšanas pamatprincipi”.

<sup>8</sup> ISSAI 10 „Mehiko deklarācijas par ARI neatkarību” 4.princips „Neierobežota piekļuve ierakstiem”.



## **B. VISPĀRĒJĀS PRASĪBAS, KAS ATTIECAS KONKRĒTI UZ IT REVĪZIJĀM**

### **5. Uz risku balstīta revīzijas pieeja IT revīzijai**

#### **Prasības:**

**Izmantojot uz risku balstītu revīzijas pieeju, IT revidentiem ir jāņem vērā ar IT revīziju saistītus riskus.**

**IT revīzijām ir jābūt veiktām saskaņā ar uz risku balstītu revīzijas pieeju.**

#### **Skaidrojumi:**

5.1. Uz risku balstīta revīzijas pieeja ietver revidējamās vienības riska elementu<sup>9</sup> noteikšanu, kas tiek vērtēti kopā ar to iespējamo ietekmi, tādējādi nosakot prioritārās revīzijas jomas.

5.2. Veicot revidējamās vienības revīziju, riski ietver pastāvošos riskus, kontroles riskus un neatklāšanas riskus. Riska elementi tiek noteikti attiecībā uz visiem trim riskiem. Visi kopā šie trīs riski veido tā saucamo revīzijas risku.

5.3. Pastāvošie riski ir riski, kas ir iestrādāti sistēmā, kas var ietekmēt to funkciju veikšanu, kuras revidējamajai vienībai ir jāveic saskaņā ar pilnvarām. Lietotāju anonimitāte ir pastāvošais risks IT sistēmā, sevišķi tīkla vidē. Organizācijām ir jāievieš kontroles pasākumi pastāvošu risku novēršanai. Dažreiz revidējamā vienība var arī pieņemt esošos riskus, neizstrādājot nekādus pretpasākumus risku novēršanai, ja ir novērtēts, ka to ietekme nav būtiska un līdz ar to tiek ievērots pieņemamais riska līmenis.

5.4. Kontroles riski ir riski, ka kontroles pasākumi, iespējams, var nenotradāt. Šādos gadījumos ir iespējamas būtiskas kļūdas un tām ir jābūt noteiktām nekavējoties. IT sistēmas vienmēr risina šādus gadījumus caur Lietojumprogrammu kontrolēm<sup>10</sup> un Vispārējām kontrolēm<sup>11</sup>. Šo kontroļu stabilitāte nodrošina organizācijas/IT sistēmas veicamo funkciju sniegšanu. Gadījumi, kad šīs kontroles nedarbojas vai tajās ir trūkumi, veido kontroles risku gadījumus.

5.5. Neatklāšanas riski IT revīzijas veikšanā ir riski, ka netiks atklāta IT un saistīto kontroļu neesamība vai trūkumi un ar tiem saistītas nepilnības IT sistēmas darbībā.

5.6. Ir pieejamas daudzas risku novērtēšanas pieejas un metodoloģijas, kuras ARI var izvēlēties. Tās iedalās, sākot no vienkāršas IT sistēmu riska profila klasifikācijas kā augsts, vidējs un zems, pamatojoties uz ARI IT revidenta spriedumu, līdz sarežģītiem zinātniskiem aprēķiniem, kas sniedz IT sistēmu risku skaitlisko novērtējumu<sup>12</sup>.

<sup>9</sup> Riska elementiem ir jābūt saistītiem ar tādām jomām kā IT pārvaldība, sistēmu projektēšana un izstrāde, iekšējie vai ārpalpojumi, darbības, IT drošība, uzraudzība un kontrole.

<sup>10</sup> Lietojumprogrammu kontroles ir kontroles, kuras ir iestrādātas atsevišķās lietojumprogrammās vai saistītu lietojumprogrammu grupā, kas veido IT lietojumprogrammu sistēmu. Tās ir ievades kontroles, apstrādes kontroles, izvades kontroles un galveno datu kontroles, kuras tiek piemērotas IT sistēmas ievades, apstrādes un izvades posmos.

<sup>11</sup> Vispārējās kontroles ir kontroles pār saistītajām sistēmām un procesiem, kas atbalsta IT lietojumprogrammu sistēmu. Tās attiecas uz tādām jomām kā IT sistēmu biznesa lietas, sistēmas projektēšana un izstrāde, iegāde, ārpalpojumi/iekšējie pakalpojumi, darbības (kas nav saistītas ar lietojumprogrammu kontrolēm), cilvēkresursu vadība, IT drošība, uzraudzība u.c. Vispārējās kontroles un lietojumprogrammu kontroles ir savstarpēji saistītas, nodrošinot sekmīgu IT sistēmas ieviešanu. Ja vispārējās kontroles ir vājas, tās ievērojami samazina ticamību tām kontrolēm, kas saistītas ar atsevišķām IT lietojumprogrammām.

<sup>12</sup> WGITA-IDI IT revīziju veikšanas rokasgrāmata Augstākajām revīzijas iestādēm.

## 6. Būtiskums

### Prasība:

**ARI ir jāņem vērā būtiskums visos IT revīzijas veikšanas posmos.**

### Skaidrojumi:

6.1. IT revidentiem ir jāņem vērā būtiskums visā (IT) revīzijas veikšanas gaitā. Apsvērumi saistībā ar būtiskumu ietekmē lēmumus attiecībā uz revīzijas procedūru veidu, laiku un apjomu, kā arī revīzijas rezultātu izvērtēšanu. Apsvērumi var ietvert ieguldītāju intereses, sabiedrības intereses, normatīvo aktu prasības un to ietekmi uz sabiedrību<sup>13</sup>.

6.2. Būtiskums attiecas uz visiem šādu revīziju aspektiem, tādiem kā tēmu izvēli, kritēriju noteikšanu, pierādījumu un dokumentēšanas novērtēšanu, kā arī risku, ka tiks izstrādāti neatbilstoši vai ar zemu ietekmi revīzijas konstatējumi vai ziņojumi, pārvaldīšanu.

6.3. Būtiskumu IT revīzijas jautājumiem jānosaka augstākajā revīzijas iestādes pieņemtās vispārējās būtiskumu noteikšanas sistēmas ietvaros. Būtiskuma aspekti var mainīties atkarībā no IT revīzijas veida. Būtiskums publiskā sektora finanšu, lietderības un atbilstības revīzijās, kuru ietvaros tiek veikta IT revīzija, ir aprakstīts ISSAI 200, 300 un 400<sup>14</sup>.

### 6.4. Būtiskums un Risks

Riska novērtējums, kas tiek izmantots IT revīzijās, ir savstarpēji saistīts ar attiecīgas revīzijas būtiskuma prasībām. Neatbilstības būtiskums ir jānovērtē, pamatojoties uz paredzamo lietotāju spējām ietekmēt pieņemamos lēmumus. Kad pastāvošais risks ir augsts, mazu neatbilstību gadījumi var būt būtiski, jo šādu neatbilstību ietekmei ir iespējams uzkrājošais raksturs. Kad kontroles risks ir augsts (kas nozīmē risku noteikšanai nepieciešamo kontroļu neesamību/trūkumus), arī tad mazas neatbilstības būs būtiskas, ja šādu neatbilstību ietekmei ir iespējams uzkrājošais raksturs.

6.5. IT revidenti ne vienmēr ir spējīgi pārbaudīt visus gadījumus/darījumus/moduļus vai sistēmas, ņemot vērā ierobežotus resursus un revīzijas uzdevuma izmaksu attiecību pret ieguvumiem. Šādos gadījumos IT revidentiem būtu jānosaka būtiskums un jāpielieto revīzijas izlase detalizētām pārbaudēm, lai izdarītu pieņemamus revīzijas secinājumus. Dažāda veida izlases metožu izmantošanai vai lietot IT rīkus. Pastāvošā un kontroles riska līmeņi ietekmē izlases lielumu. Jo augstāks ir pastāvošais risks vai kontroles risks, jo lielākam ir jābūt izlases lielumam.

## 7. Dokumentēšana

### Prasības:

**ARI ir jāveic atbilstoša IT revīzijas procesa un tā rezultātu dokumentēšana, lai nodrošinātu, ka jebkurš pieredzējis IT revidents, kurš nav saistīts ar šo revīziju, varētu to atkārtot.**

**Revidentam ir jā sagatavo pilnīga un detalizēta revīzijas dokumentācija, lai sniegtu vispārēju izpratni par revīziju.**

<sup>13</sup> ISSAI 100 „Publiskā sektora revīziju veikšanas pamatprincipi” 41.punkts.

<sup>14</sup> ISSAI 200 „Finanšu revīzijas veikšanas pamatprincipi”, ISSAI 300 „Lietderības revīzijas veikšanas pamatprincipi” un ISSAI 400 „Atbilstības revīzijas veikšanas pamatprincipi”.



**Dokumentācijas pārskatīšanai ir jāsniedz iespēju jebkuram citam IT revidentam nonākt pie tādiem pašiem revīzijas secinājumiem.**

**Skaidrojumi:**

7.1. Vispārējās dokumentēšanas prasības IT revīzijās galvenokārt izriet no 3.līmeņa starptautiskiem standartiem augstākajām revīzijas iestādēm – ISSAI 100, 200, 300 un 400. Tie attiecas arī uz IT revīzijas veikšanu, Tomēr IT revīzijas raksturs var prasīt īpašas korekcijas dokumentēšanas procesā.

7.2. Dokumentēšanas loma IT revīzijās ir saprast revīzijas plānošanas un veikšanas gaitu, kāds darbs tika veikts, kas pamato revīzijas konstatējumus un secinājumus, un nonākt līdz revīzijas ieteikumiem. Dokumentēšanai ir jābūt pietiekami detalizētai, lai pieredzējis IT revidents, kuram nav iepriekšējo zināšanu par revīziju, saprastu veikto procedūru, kas veiktas saskaņā ar attiecīgo ISSAI, nacionālo standartu un normatīvo aktu prasībām, būtību, laiku, apjomu un rezultātus. Iegūtajiem pierādījumiem, kas pamato revīzijas secinājumus un rekomendācijas, pamatojumiem visiem svarīgiem jautājumiem, kas prasīja profesionāla sprieduma pielietošanu, un saistītiem secinājumiem arī ir jābūt dokumentētiem un viegli saprotamiem jebkuram pieredzējušam IT revidentam. Dokumentācijai ir jābūt ticamai, lai par dokumentācijas saturu nebūtu nesaskaņu ar revidējamo vienību.

7.3. Dokumentēšana IT revīzijās spēlē svarīgu lomu, lai nodrošinātu, ka katrs revīzijas procesa solis un katrs konstatējums ir saistīts ar vai atsaucās uz konkrēta attiecīga normatīvā akta vai standarta ievērošanu vai neievērošanu.

7.4. Kā jebkurā citā revīzijā, ja IT revīzijas gaitā kaut viens konstatējums būtiskajos jautājumos ir pretrunā vispārējiem revīzijas secinājumiem vai pastāv domstarpības ar revidējamo vienību par revīzijas secinājumiem, IT revidentiem ir jādokumentē to, kā viņi ir atrisinājuši šīs pretrunas un/vai domstarpības.

7.5. IT revīzijas dokumentācijas formāts

IT revīzijas dokumenti ietver papīra un elektroniskas veidlapas, lai pierakstītu informāciju par auditētajām IT sistēmām, sapulču ar vadību un revīzijas grupas sapulču protokolus, revīzijas konstatējumus un pierādījumus revīzijas secinājumiem. Starptautiskie standarti augstākajām revīzijas iestādēm nenosaka standarta formātu IT revīzijas dokumentācijai. Turklāt dažādu ARI pielietotie formāti var atšķirties. Katrā ARI var būt noteikts standartizācijas līmenis attiecībā uz kontrolosarakstiem, vēstuļu paraugiem, darba dokumentu kārtošanu u.c.

7.6. IT dokumentācijas saglabāšana

IT revīzijas dokumentācijai ir jābūt saglabātai un aizsargātai no jebkādam izmaiņām un neatļautas dzēšanas. Katra ARI var izstrādāt jaunus standartus IT revīzijas dokumentācijas saglabāšanai vai piemērot esošos standartus, lai ievērotu prasības ar IT revīziju saistītas dokumentācijas saglabāšanai. Šādā veidā noteiktais laika periods dokumentu saglabāšanai ir atkarīgs no katra ARI pilnvarām un statūtiem, kas reglamentē tās darbību.

Īpaša uzmanība ir jāpievērš šo datu formātam, paredzamajam glabāšanas ilgumam, glabāšanas videi un uzglabāšanas prasībām, lai nodrošinātu, ka to pašu var nolasīt laika posmā, kas ir noteikts katras ARI noteiktajā attiecīgo datu saglabāšanas un arhivēšanas politikā. Tāpēc var būt nepieciešams pārveidot datus no viena formāta citā, lai neatpaliktu no tehnoloģiju attīstības vai novecošanās.

## 8. Spējas

### Prasība:

ARI ir jāpārlicinās, ka revīzijas grupa sastāv no locekļiem, kuriem visiem kopā ir atbilstošas spējas IT revīzijas veikšanai atbilstoši standartu prasībām.

### Skaidrojums:

8.1. Nepieciešamas zināšanas, prasmes un spējas ir iespējams iegūt, apvienojot darbinieku apmācības, jaunu darbinieku pieņemšanu vai ārējo resursu piesaistīšanu saskaņā ar ARI stratēģisko plānu.

## C. PRASĪBAS SAISTĪBĀ AR IT REVĪZIJAS PROCESIEM

### 9. IT revīzijas plānošana

#### Prasība:

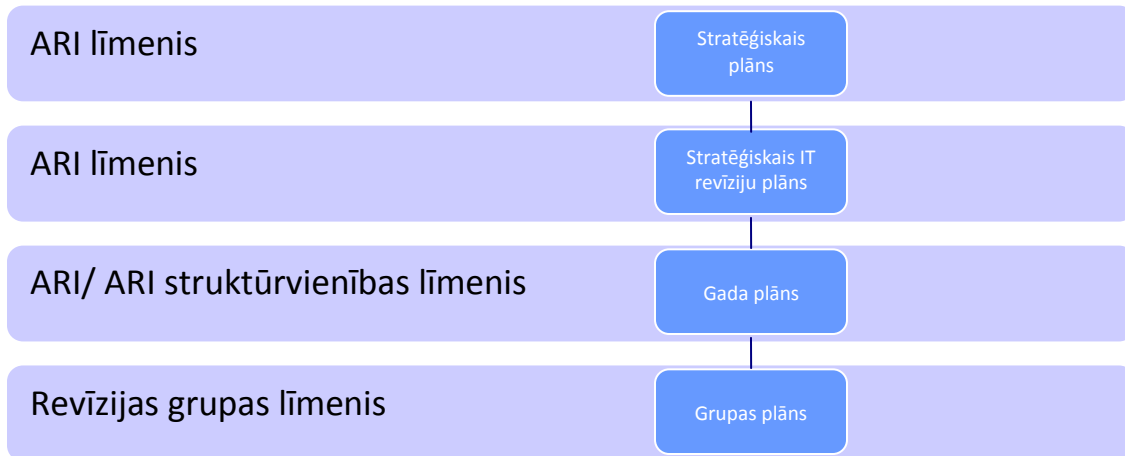
ARI ir jāplāno IT revīzija, pamatojoties uz riska novērtējumu.

#### Skaidrojumi:

9.1. IT revīzijas plānošanu ARI var veikt saskaņā ar likumdošanas pilnvarām, likumdošanas/izpildvaras pieprasījumiem vai pēc savas iniciatīvas.

9.2. Revīzijas plānošana augstākajās revīzijas iestādēs, pamatojoties uz riska novērtējumu

Augstākās revīzijas iestādes var plānot revīzijas, pamatojoties uz riska novērtējumu balstīto izvēli. Šajā procesā ARI nosaka prioritāti un izvēlās revīzijas, kuras tā veiks, pamatojoties uz riska novērtējumu. Uz riska novērtējumu balstīta IT revīzijas plānošana var tikt veikta trīs līmeņos – stratēģiskajā, ikgadējā un grupas līmenī, un tam ir jābūt noteiktam ARI vispārējā stratēģiskajā plānā. Taču ARI var izvēlēties apvienot jebkurus šos līmeņus, pamatojoties uz viņu resursiem un prasībām pret revīziju, kas balstītas uz riska analīzi.



1.attēls. AUGTĀKAJĀM REVĪZIJAS IESTĀDĒM TIPISKA REVĪZIJAS PLĀNOŠANAS HIERARHIJA

## 10. Stratēģiska IT revīzijas plānošana

### Prasības:

**ARI stratēģiskam plānam ir jāietver sadaļa attiecībā uz IT revīzijām un ar tām saistītām vajadzībām.**

**ARI ir jāizstrādā stratēģiskais IT revīziju plāns saskaņā ar vispārējo stratēģisko revīziju plānu.**

### Skaidrojumi:

10.1. Stratēģiskais IT revīziju plāns satur ARI revidējamo valsts organizāciju IT sistēmu revīzijas mērķus un uzdevumus. Plāns parasti tiek noteikts no 3 līdz 5 gadu periodam, atkarībā no tā, kā attīstās IT vide un kā tam pielāgojas valsts organizācijas. Stratēģiskajam plānam IT sistēmu revīzijai ir jābūt saskaņotam ar ARI vispārējo stratēģisko plānu.

10.2. Augtāko revīzijas iestāžu mērķis ir nodrošināt caurskatāmību, atbildību un iesaistīšanos labā pārvaldībā, kas sasaistīta ar to vīziju, misiju un vērtībām. Tādejādi to stratēģiskais plāns vai mērķi var ietvert institucionālo attīstību, organizācijas sistēmas attīstību un profesionālo spēju attīstību, kas ir nepieciešams, lai sasniegtu stratēģiskos mērķus. IT revīzijās augstākās revīzijas iestādes var novērtēt to vidi, veicot aptaujas, sadarbojoties ar revidējamajām vienībām, veicot tehnoloģisko risinājumu vadības un attīstības novērtējumu, novērtējot, kā revidējamās vienības ievieš tehnoloģiskos risinājumus, kā arī izvērtējot jebkuru citu normatīvo aktu vai pilnvaru prasības.

10.3. Šajā posmā būtu jānosaka revīzijas kopums. Augstākās revīzijas iestādes var noteikt savas revīziju prioritātes, pamatojoties uz to vides novērtējumu un revīzijas kopumu, un noteikt savus stratēģiskos mērķus un uzdevumus. Lai sasniegtu viņu vispārējos mērķus ar ierobežotiem līdzekļiem un pieejamiem resursiem, ARI stratēģiskam ieviešanas plānam ir jāiekļauj tādu vajadzību noteikšana, kas saistītas ar institucionālo attīstību, kas ietver pilnvaru piešķiršanu ARI un tiesiskā regulējuma noteikšanu IT revīziju veikšanai, kā arī profesionālo spēju attīstību, lai apgūtu nepieciešamās prasmes un spējas IT revīziju veikšanai.

10.4. Uz risku balstīta revīzijas plānošana

Uz risku balstīta revīzijas plānošana ietver pievēršanos tādiem riska elementiem, kuriem būs ietekme uz revīziju nozīmi un revīzijas rezultātā izdarīto revīzijas secinājumu pareizību. Riska novērtējums stratēģiskās IT revīziju plānošanas līmenī attiecas uz IT revīziju saistību ar augstāko revīzijas iestāžu vispārējiem stratēģiskiem mērķiem, nodrošinot labu pārvaldību, un pārvaldības caurskatāmību un atbildību.

10.5. ARI ir periodiski jāpārskata un jāatjauno stratēģiskais plāns, lai tas atbilstu ARI mērķiem nodrošināt caurskatāmību, atbildību un iesaistīšanos labā pārvaldībā.

10.6. Izskatot jautājumus saistībā ar ARI stratēģisko plānošanu, norādījumus var skatīt starptautiskajos standartos augstākajām revīzijas iestādēm, sevišķi ISSAI 100 „Publiskā sektora revīziju veikšanas pamatprincipi”.

## 11. Ikgadējā IT revīziju plānošana

### Prasības:

IT revīziju gada plānam ir jābūt saskaņā ar stratēģisko IT revīziju plānu.

IT revīziju gada plānam ir jāietver nozīmīgie jautājumi, kas ietverti stratēģiskajā IT revīziju plānā, pamatojoties uz to prioritāti, kas noteikta caur risku novērtējumu.

### Skaidrojumi:

11.1. ARI ir jāizstrādā gada plāns IT revīzijām, kas ir saskaņots ar stratēģisko IT revīziju plānu. Šis plānošanas posms ietver IT sistēmu vai organizāciju izvēli revīzijas veikšanai.

11.2. ARI stratēģiskā IT revīziju plāna ietvaros var tikt izmantota uz risku balstīta pieeja, lai noteiktu prioritātes un izvēlētos piemērotās tēmas. Tas ietver revidējamo organizāciju/IT sistēmu uzskaites izveidošanu un izmantošanu kopā ar galvenajiem kritērijiem riska novērtējuma veikšanai. Šī uzskaitē var būt arī revīzijas kopums, kuru noteica stratēģiskās plānošanas posmā, bet ar detalizētu informāciju par IT sistēmu/organizāciju veidiem un aprakstiem, kas tiks izmantoti, novērtējot riska profilu. Riska novērtējuma sistēma, kuru izstrādāja augstākās revīzijas iestādes, var turpmāk tikt izmantota, lai pabeigtu revīziju izvēli.

11.3. Papildu uz risku balstītai pieejai revīzijas tēmu izvēlē daudzām augstākajām revīzijas iestādēm ir pienākums veikt likumos noteiktās revīzijas, kā arī revīzijas, kuras pieprasa veikt uzraudzības iestādes (kongress, parlaments u.c.) vai izpildvaras iestādes.

## 12. IT revīzijas plānošana revīzijas grupas līmenī izvēlētajai revīzijai

### Prasības:

IT revīziju plānam grupas līmenī ir jābūt saskaņā ar riska novērtējumu IT revīziju gada plānā.

IT revīziju plānam grupas līmenī ir jāaptver jautājumi par nozīmīgām riska jomām, kuras identificētas IT revīziju gada plānā, un jāsaturs detalizēta revīzijas programma.

### Skaidrojumi:

12.1. Šis līmenis ietver detalizētas revīzijas programmas izstrādi, kas sākas ar izvēlētajām IT revīzijas mērķa aprakstu.

12.2. Priekšnosacījums revīzijas programmas izstrādei ir skaidra izpratne par revidējamo vienību, tās informācijas sistēmām un ar IT saistītām darbībām.

12.3. Nepieciešamo zināšanu par revidējamo vienību un tās procesiem daudzumu, kas ir nepieciešams IT revidentam, nosaka revidējamās vienības raksturs un detalizācijas pakāpe, kurā tiks veikts revīzijas darbs. Nepieciešams noteikt IT sistēmas ieviešanas mērķi. Izpratnei par revidējamo vienību ir jāietver biznesa, finanšu un pastāvošos riskus, ar kuriem saskaras revidējamā vienība un tās IT sistēmas. Tai arī jāietver, cik lielā mērā, lai sasniegtu savus mērķus, revidējamā vienība paļaujas uz ārpakalpojumiem, un vai visi biznesa procesi ir iekļauti IT vidē<sup>15</sup>. Revidentiem jāizmanto šī informācija, lai noteiktu iespējamās problēmas, formulētu mērķus un darba apjomu, veiktu darbu un izvērtētu vadības darbības, par kurām IT revidentiem ir jābūt modriem.

<sup>15</sup> Organizācijas, kuras pāriet no manuālas uzskaites uz datorizētu vidi, parasti veic biznesa procesu reorganizācijas (BPR) pasākumus. Var būt gadījumi, kad daži biznesa procesi tiek veikti manuāli, tomēr sadarbībā ar IT sistēmām. Šādiem gadījumiem IT revidentiem ir jāpievērš īpaša uzmanība.

12.4. Uz risku balstītajā revīzijas pieejā kontroles riski ir sasaistīti ar šiem IT vispārējo kontroļu un lietojumprogrammu kontroļu elementiem. Jo augstāks ir kontroles risks, jo vairāk detalizēto pārbaūžu ir jāveic.

12.5. Parasti IT revidenti tiek pieaicināti pārbaudīt ar tehnoloģijām saistītās kontroles, bet citi (ne IT) revidenti pārbauda finanšu, likumības un atbilstības kontroles. Revidenta uzdevums ir izprast potenciālos biznesa un IT riskus, ar kuriem var saskarties revidējamā vienība, un izvērtēt, vai izstrādātās kontroles ir pietiekamas noteiktā mērķa sasniegšanai. Attiecībā uz IT vispārējām kontrolēm revidentam ir svarīgi izprast vispārējo kontroļu plašu sadalījumu un apjomu organizācijas darbībā, novērtēt vadības uzraudzību un darbinieku informētību par šīm kontrolēm un noskaidrot, cik efektīvas ir kontroles, lai nodrošinātu paredzēto funkciju sniegšanu. Pat nelielās organizācijās, kur informācijas sistēmas un biznesa procesi, kas saistīti ar finanšu pārskatiem, nav ļoti sarežģīti, to loma ir nozīmīga<sup>16</sup>. Ja vispārējās kontroles ir vājas, tās ievērojami samazina uzticamību tām kontrolēm, kuras saistītas ar atsevišķām IT lietojumprogrammām<sup>17</sup>. IT revidentam ir svarīgi izprast funkciju, kas iestrādāta lietojumprogrammā ar attiecīgu darba plūsmu. IT revidentam ir jābūt spējīgam noteikt katru ievadi, lietojumprogrammas veiktos procesus un rezultātus, kurus izveido lietojumprogramma. Izpratne par pamatdatiem, kas ietekmē ievadi, apstrādi un iznākumus, kā arī to drošību, palīdzēs IT revidentam izvērtēt, vai IT sistēma atbilst datu pareizības, pilnīguma, godīguma, konfidencialitātes, pieejamības, uzticamības, piemērotības un atbilstības prasībām visos informācijas apstrādes posmos, gan iegūstot datus, gan apstrādājot tos, gan sniedzot informāciju par rezultātiem.

12.6. Pamatojoties uz izveidoto izpratni par informācijas sistēmām un revidējamo vienību, IT revidenti lemj par IT revīzijas pieeju. Galu galā IT revīzija ietvers IT pārvaldību, IT vispārējās kontroles un IT lietojumprogrammu kontroles vai to kombināciju.

### 13. Atbilstošas izlases izvēle IT revīzijai

Revīzijas izlase<sup>18</sup> ir revīzijas procedūru veikšana mazāk nekā 100 procentiem vienību no revīzijai pakļautām darījumu grupām vai populācijām tādā veidā, kā visām izlases vienībām ir vienādas iespējas tikt izvēlētam, tādejādi sniedzot revidentam pietiekamu pamatojumu secinājumu izdarīšanai par visu populāciju. Tas attiecas arī uz izlases vienību izvēli IT revīzijā. Turklāt, veidojot revīzijas izlasi, IT revidentam ir jāņem vērā revīzijas procedūras mērķis, populācijas, no kuras izlase tiks ņemta, īpašības, kā arī metodes un instrumentus, kurus izmanto izlases veidošanā un analizē.

IT revidentam ir jānosaka atbilstošs izlases lielums, lai samazinātu izlases risku līdz pietiekami zēmam līmenim. IT revidentam ir jāizvēlas izlases vienības tādā veidā, lai katrai populācijas vienībai būtu vienlīdzīgas iespējas tikt izvēlētai. Revīzijas veikšana IKT vidē var veicināt populācijas simtprocentīgu analīzi, īpaši sākotnējās novērtēšanas posmā (*skatīt 21.sadaļu zemāk*). Tomēr, lai veiktu detalizētās pārbaudes (*skatīt 21.sadaļu zemāk*) vai detalizētās darījumu pārbaudes, varētu **joprojām** būt nepieciešams veidot izlasi. IT revidenti izlases veidošanai var izmantot ISSAI 1530 sniegtās vadlīnijas vai citus atvasinātus procesus, kurus izmanto viņu ARI<sup>19</sup>.

<sup>16</sup> ISSAI 1315 „Būtisku neatbilstību risku identificēšana un izvērtēšana, gūstot izpratni par uzņēmumu un tā vidi”.

<sup>17</sup> WGITA-IDI IT revīziju veikšanas rokasgrāmata Augstākajām revīzijas iestādēm.

<sup>18</sup> ISSAI 1530 “Izlases metode revīzijā”.

<sup>19</sup> ISSAI 1530 „Izlases metode revīzijā” 15.lpp.

## 14. IT revīzijas mērķi

### Prasība:

IT revīzijas mērķiem ir jāatbilst revīzijas grupas līmenī IT revīzijas plānošanas laikā identificētām riska jomām, ņemot vērā iecerēto revīzijas pieeju – finanšu, atbilstības vai lietderības revīziju.

### Skaidrojumi:

14.1. IT revīzijas mērķiem ir jābūt pārbaudīt, vai IT procesi un IT resursi ir apvienoti kopā, lai izpildītu paredzētos organizācijas mērķus, lai nodrošinātu organizācijas darbības efektivitāti, produktivitāti un ekonomiskumu, ievērojot pastāvošos noteikumus un līdzsvarojot riskus.

14.2. Tādejādi IT revīzijas var būt revīzijas par visaptverošu IT sistēmu vai konkrētām sfērām, tādām kā IS drošība, biznesa risinājumu iegūšana, IT vispārējās kontroles, lietojumprogrammu kontroles, sistēmas izstrāde un darbības nepārtrauktība, vai arī citas jomas, kā tas ir noteikts WGITA IDI rokasgrāmatā.

14.3. IT revīzijas ir savstarpēji saistītas ar finanšu revīzijas, atbilstības revīzijas vai lietderības revīzijas sfērām. IT revīzijas var atbalstīt visu trīs veidu revīzijas, vai arī var tikt veiktas kādas no šīm revīzijām ietvaros vai šo revīziju apvienojuma ietvaros, t.i. finanšu revīzijās, atbilstības revīzijās vai lietderības revīzijās<sup>20</sup>.

#### 14.4. Mērķi attiecībā uz finanšu revīzijām

Finanšu revīzijas definīcija<sup>21</sup> izceļ jautājumus par pārliecību, finanšu pārskatu sagatavošanu atbilstoši finanšu pārskatu sagatavošanas pamatnostādņēm un finanšu pārskatu noformēšanu atbilstoši būtiskuma prasībām. Tas ietver plašus uzdevumus pārliecības gūšanai, ka finanšu sistēma atbilst ziņošanas pamatnostādņēm attiecībā uz finanšu pārskatu sagatavošanu un finanšu rezultātu uzrādīšanu bez būtiskām kļūdām. IT sistēmai ir jāaptver visas prasības attiecībā uz finanšu pārskatu sagatavošanu, t.i. finanšu informācijas iegūšanu, pamatnostādņu prasību pielietošanu, informācijas apstrādi un uzrādīšanu nepieciešamajā formātā. Kopumā, šie ir jautājumi saistībā ar lietojumprogrammu ievades, apstrādes un izvades kontrolēm, izņemot galvenos datus un lietojumprogrammu drošību. Tomēr lietojumprogrammu kontroles ir atkarīgas no atbilstoša IT vispārējo kontroļu un IT pārvaldības atbalsta. Līdz ar to finanšu revidentiem pirms viņu revīzijas veikšanas ir jāgūst pārliecība par IT sistēmas un ar to saistīto kontroļu atbilstību. Pārliecība par IT sistēmu ir jāgūst no IT revīzijas par šo sistēmu, pievēršot uzmanību visiem IT pārvaldības, IT vispārējo kontroļu un IT lietojumprogrammu kontroļu jautājumiem.

Ja pilnvērtīgas IT revīzijas rezultātā ir iegūta pārliecība par IT sistēmu, nav nepieciešams veikt IT revīziju katrā finanšu revīzijā par vienu un to pašu sistēmu, ja droši var apgalvot, ka laika periodā kopš pēdējās IT revīzijas nav notikušas nekādas izmaiņas vai atkāpes no šīs sistēmas.

#### 14.5. Mērķi attiecībā uz atbilstības revīzijām

Atbilstības revīziju veikšana ir neatkarīgs novērtējums par to, vai apskatāmais jautājums atbilst attiecīgām prasībām, kas identificētas kā kritēriji. Atbilstības revīzijas tiek veiktas, izvērtējot, vai darbības, finanšu darījumi un informācija visos būtiskajos aspektos atbilst prasībām, kas regulē revidējamās vienības darbību.

<sup>20</sup> ISSAI 100: „Augstākās revīzijas iestādes var veikt apvienotās revīzijas, kuras ietver finanšu, lietderības un/vai atbilstības aspektus”.

<sup>21</sup> ISSAI 200 „Finanšu revīzijas veikšanas pamatprincipi”.



Publiskā sektora atbilstības revīziju veikšanas mērķis ir ļaut iespēju ARI novērtēt, vai publiskā sektora organizāciju veiktās darbības atbilst prasībām, kas regulē šo iestāžu darbību. Tas ietver ziņošanu par to, cik lielā mērā revidējamā vienība atbilst noteiktajiem kritērijiem. IT revīzija ļauj veikt šo noteikšanu automatizētajām sistēmām. Atbilstības revīzijas var būt saistītas ar likumību (atbilstību ārējiem kritērijiem, tādiem kā atbilstošo likumu, noteikumu vai vienošanos prasībām) vai pareizību (vispārējo principu, kas nosaka labu finanšu pārvaldību un valsts amatpersonu rīcību, ievērošanu). Kaut arī atbilstības revīzijās galvenā uzmanība ir likumībai, tomēr pareizība arī var būt piemērojama, ņemot vērā publiskā sektora apstākļus, kur pastāv noteiktas cerības attiecībā uz finanšu pārvaldību un publiskā sektora organizāciju un amatpersonu uzvedību. Atkarībā no ARI pilnvarām, revīzijas apjomā līdz ar to var tikt iekļauti arī pareizības jautājumi<sup>22</sup>.

Atbilstības revīziju mērķi un raksturojumi norāda uz nepieciešamību ievērot attiecīgos procesus, likumību un pareizību. Publiskā sektora IT sistēmām arī ir nepieciešams atbilst attiecīgo normatīvo aktu prasībām, kā arī organizācijas pieņemtajiem standartiem un vadlīnijām. IT revidentiem ir jānovērtē IT sistēmas atbilstību šādu normatīvo aktu prasībām, kā arī standartiem, vadlīnijām un dažādiem organizācijas darbības parametriem, lai izstrādātu revīzijas secinājumus. Šādai novērtēšanai ir jābūt veiktai, salīdzinot ar noteiktajiem kritērijiem, kas iegūti no normatīvo aktu prasībām, standartiem, darbības kritērijiem vai pat pareizības prasībām. Atbilstības novērtējums attiecībā uz IT pārvaldību iekļauj pārlicības gūšanu par mehānismiem, lai nodrošinātu, ka pārvaldības funkcijas ir veiktas un periodiski uzraudzītas, ka iekšējās kontroles sistēma darbojas efektīvi un ka visas IS prasības ir īstenotas atbilstoši plānotajam. Atbilstības novērtējums attiecībā uz IT vispārējām kontrolēm iekļauj novērtējumu, vai organizācijā pastāv kontroles ar atbilstošu uzraudzības un risku mazināšanas mehānismiem un tiek ievēroti organizācijas noteiktie standarti un darbību izpildes parametri. IT lietojumprogrammu novērtējums iekļauj izvērtēšanu, vai biznesa procesi un noteikumi ir iestrādāti IT sistēmā un ievades, apstrādes un izvades kontrolēs, kas saistītas ar datu apstiprināšanu, pilnīgumu, pareizību un procesu ticamību.

IT sistēmas atbilstības revīzija var vienmēr prasīt datorizēto revīzijas metožu (Computer Assisted Audit Techniques - CAATs) izmantošanu, lai veiktu informācijas analīzi un noteiktu izņēmumus.

#### **14.6. Mērķi attiecībā uz lietderības revīzijām**

Lietderības revīziju veikšana ir neatkarīga, objektīva un ticama pārbaude par to, vai valsts uzņēmumi, sistēmas, operācijas, programmas, aktivitātes vai organizācijas darbojas saskaņā ar ekonomiskuma, produktivitātes un efektivitātes principiem un vai ir iespējami uzlabojumi.

IT revidentiem ir jāpārbauda ieviestās IT sistēmas attiecībā uz ekonomiskuma, produktivitātes un efektivitātes kritērijiem, kā arī, vai tās sniedz labumu sabiedrībai.

IT sistēmu ieviešanas ekonomiskuma pārbaude varētu galvenokārt ietvert resursu izmaksu samazināšanu visā IT sistēmu dzīves ciklā, t.i. sākot ar sistēmas iegādi līdz ieviešanai un pastāvīgai darbībai. Gadījumā, ja jebkuras funkcijas īstenošanai tiek izmantots ārpakalpojums, šāda ārpakalpojuma izmaksām ir jābūt pēc iespējas mazākām. Viens no labākajiem veidiem šādu izmaksu samazināšanai ir tirgus izpēte. Tomēr neproduktīva lietotāju prasību noteikšana organizācijas nepietiekamu zināšanu par šādām prasībām dēļ var traucēt šādai pieejai un novest pie augstākām izmaksām. Iespējas izvērtēšana, vai IT pakalpojumi, kuriem izmantots ārpakalpojums, varētu tikt sniegti, izmantojot pieejamos resursus, var norādīt uz neekonomisku resursu izmantošanu. Tādejādi lietderības revīzijas par IT iegādi laikā IT revidenti varētu norādīt uz to, ka varētu pastāvēt organizācijas vai iegādes procesa ierobežojumi.

IT sistēmu ieviešanas produktivitātes pārbaude ietvert resursu maksimālu izmantošanu vai līdz ar to neproduktīvas resursu izmantošanas samazināšanu, saglabājot gala rezultātu apjomu

<sup>22</sup> ISSAI 400 „Atbilstības revīzijas veikšanas pamatprincipi”.

(pilnīgumu), kvalitāti (pareizību un ticamību) un savlaicīgumu (pieejamību). IT revidenti var norādīt uz neproduktivitāti, ja pastāv jebkādu procesu dublēšanas, nepamatota jebkuru procesu dīkstāve, sistēmā iestrādātas nevajadzīgas pārbaudes utt.

IT sistēmu ieviešanas efektivitātes pārbaude ietver noteikšanu, vai tika sasniegti IT sistēmas ieviešanas mērķi, kas savukārt atbilst organizācijas vispārējiem mērķiem un izdevumiem. Organizācijas mērķu nesasniegšana, izmantojot IT sistēmas, varētu norādīt uz neefektīvu IT resursu izmantošanu.

Lietderības revīziju veikšana veicina arī atbildību un caurskatāmību. Lietderības revīzijas koncentrējas uz jomām, kurās tās var sniegt pievienoto vērtību iedzīvotājiem un kurās ir vislielākās iespējas uzlabošanai. Tās sniedz konstruktīvu motivāciju atbildīgajām personām veikt atbilstošus pasākumus. Vairākās valstīs un valsts organizācijās IT ieviešana visbiežāk ir jauna iniciatīva. Tādejādi lietderības revīziju pieejai IT revīzijās, lai konstruktīvi veicinātu valdību izmantot IT sistēmas, ir jābūt kā vienam no stūrakmeņiem IT revidentu pieejā. Atklātajām neatbilstībām ir jābūt norādītām tādā veidā, kas noved pie sistēmas uzlabojumiem, nevis nogalina iniciatīvu.

14.7. IT revidenti var tikt pieaicināti palīdzēt revīzijās CAAT izmantošanā. Šādā gadījumā būtu jāizlemj un revīzijas uzdevuma nosacījumos jāatrunā, vai revīzijas uzdevums veidos daļu no IT revīzijas. CAAT izmantošana tikai datu analīzes veikšanai nav uzskatāma par IT revīziju, ja netiek veikta IT sistēmu novērtēšana.

## 15. IT revīzijas apjoms

### Prasība:

**IT revidentiem plānošanas posma laikā ir jānosaka revīzijas apjoms, lai nodrošinātu revīzijas mērķa sasniegšanu.**

### Skaidrojumi:

15.1. Nosakot IT revīzijas mērķus, IT revidentiem ir arī jānosaka revīzijas apjoms. Šīs divas darbības parasti tiek veiktas vienlaicīgi. IT revīzijas apjoma noteikšana ietver lēmuma pieņemšanu par revīzijas pārbaudes apjomu attiecībā uz to, kādas IT sistēmas un to funkcionalitāte tiks pārbaudīta, kādi IT procesi tiks pārbaudīti, IT sistēmu atrašanās vietas, kas jāiekļauj revīzijā, apskatāmais laika periods un papildus arī revīzijas veids (finanšu/ atbilstības/ lietderības revīzija). Galvenokārt tā ir revīzijas robežu noteikšana.

15.2. IT sistēmas atbalsta organizācijas darbības funkcijas un parasti ietver konkrētus IT procesus, tādus kā datu ievadi sistēmā, informācijas pieprasīšanu, un atskaišu veidošanu. Lielākā daļa IT sistēmu atrodas speciālā vietā kopā ar saistīto tīkla aprīkojumu. Fiziskās atrašanās vietas un tajā esoša aprīkojuma drošības pārbaude var tikt ietverta IT revīzijā.

15.3. Revidentam ir jāizvēlas laika posms, par kuru tiks veikta revīzijas analīze (t.i. apskatīt viena gada informāciju, 3 gadu vai vairāku gadu utt.), lai dotu iespēju IT revidentiem izstrādāt piemērotus secinājumus par veikto revīziju. Veicot revīziju par IT sistēmām, parasti laika posmu, par kuru tiks veiktas pārbaudes, nosaka, pamatojoties uz konkrētas revīzijas prasībām.

15.4. Revīzijas apjoms iekļauj arī uzmanības pievēršanu konkrētajām IT sistēmu sfērām, kuras attiecas uz IT revīzijas mērķi. Tipiskākās IT sfēras ir IT pārvaldība, izstrāde un iegūšana, IT darbības, ārpakalpojumi, IT drošība, darbības nepārtrauktības plāns un katastrofu novēršanas plāns, kā arī lietojumprogrammu kontroles<sup>23</sup>. Šādas sfēras parasti ietver jebkura IT sistēma.

<sup>23</sup> WGITA-IDI IT revīziju veikšanas rokasgrāmata Augstākajām revīzijas iestādēm.

Tomēr, tā kā IT joma pastāvīgi mainās, IT revidenti nevar izslēgt iespēju, ka var būt arī jaunas jomas, kuras nepieciešamības gadījumā būtu jāiekļauj revīzijas apjomā<sup>24</sup>. Visaptverošai IT revīzijai būtu jāiekļauj visu IT sfēru pārbaudi.

15.5. Revīzijas apjoms ir atkarīgs no revidējamo IT sistēmu riska profila, kā arī pieejamiem resursiem. Ja risks ir augstāks, apjoms varētu būt šaurāks, bet plaši aptverts IT revīzijas ietvaros.

## **16. ARI spējas veikt IT revīziju**

### **Prasības:**

**ARI ir jābūt atbilstošām spējām, lai veiktu IT revīziju.**

**ARI ir jāattīsta atbilstošas spējas, ja tādas nav pieejamas, pirms uzsākt IT revīziju.**

### **Skaidrojums:**

16.1. Augstāko revīzijas iestāžu galvenā funkcija ir veikt revīzijas, un tām jau ir jābūt spējām revīzijas veikšanai. Tomēr IT revīzijas prasa īpašas spējas. Dažas spējas, kurām ir jābūt IT revīzijas grupā kopā, ietver:

- i. IT jomā kvalificēts un zinošs personāls
- ii. Izpratne par pastāvošajiem likumiem un noteikumiem vai vidi, kurā IT sistēma darbojas
- iii. Izpratne par IT revīzijas standartiem/vadlīnijām, kuras jāievēro ARI
- iv. Izpratne par IT metodēm revīzijas pierādījumu savākšanai no automatizētām sistēmām.
- v. Izpratne par atbilstošajiem IT revīzijas rīkiem, lai ievāktu, analizētu, atkārtotu šādas analīzes rezultātus vai atkārtoti veiktu revīzijas funkcijas
- vi. Atbilstoša IT infrastruktūra, lai iegūtu un saglabātu revīzijas pierādījumus
- vii. Atbilstošu IT revīzijas rīku pieejamība, lai analizētu savāktos pierādījumus

## **17. Resursu piešķiršana**

### **Prasība:**

**ARI ir jānosaka un jāpiešķir atbilstoši un kompetenti resursi IT revīzijas veikšanai.**

### **Skaidrojumi:**

17.1. Augstākajām revīzijas iestādēm ir dažādas iespējas, lai piešķirtu resursus IT revīzijai.

17.2. Visizplatītākā pieeja ir, ka tiek izveidota centrālā grupa ar IT speciālistiem vai ekspertiem, kuri palīdz pārējiem darbiniekiem veikt IT revīzijas. Uzsākot IT revīziju veikšanu, ARI sākotnēji var piesaistīt tikai dažus speciālistus ar nepieciešamajām zināšanām IT revīzijās.

17.3. Cita iespēja ir noalgot IT speciālistus katrai ARI revīzijas grupai. Tomēr, ja katra grupa veic tikai dažas IT revīzijas, tā varētu būt neproduktīva IT speciālistu izmantošana. Pieaugot IT revīziju skaitam, augstākās revīzijas iestādes mēdz izveidot atsevišķu IT revīzijas grupu vai funkciju. Šādā gadījumā šī grupa ir atbildīga par visām IT revīzijām, kuras ARI veic.

17.4. Lai veicinātu IT revīzijas veikšanu, IT revīziju grupa var sadarboties ar citām ARI revīziju grupām, kurām ir uzkrātas zināšanas par revidējamo vienību, tas ļauj IT revīzijas grupai

---

<sup>24</sup> WGITA-IDI IT revīziju veikšanas rokasgrāmatas Augstākajām revīzijas iestādēm 9.nodaļa „Papildu interesējošas tēmas”.

ātri iegūt izpratni par revidējamās vienības misiju un sasaistīt revidējamās vienības biznesa procesus ar attiecīgām IT sistēmām.

## **18. Ārējo resursu piesaiste**

### **Prasība:**

**ARI var piesaistīt ārējos resursus IT revīziju veikšanai, ja nepieciešamie resursi nav pieejami ARI ietvaros.**

### **Skaidrojumi:**

18.1. ARI var izlemt izmantot ārējos resursus, vai noligt ārpakalpojumu IT revīzijas veikšanai, ja tai nav nepieciešamo resursu. Šādi resursi pārsvarā ir ārējie konsultanti vai darbuzņēmēji, kuriem ir nepieciešamās zināšanas par IT revīzijas metodēm un līdzekļiem, ieskaitot datubāzes, programmēšanu un citas jomas, kas attiecas uz IT revīziju. Resursi iekļauj arī jebkādu IT infrastruktūru, kas nepieciešama ARI, lai veiktu revīziju. Tas parasti ir tāpat kā veikt jebkuru citu revīziju, tomēr IT revīzijā var būt nepieciešama īpaša analīze, kā arī datu pārveidošanas un uzglabāšanas līdzekļi.

18.2. Ja ARI piesaista ārpakalpojumu, ārējo resursu veiktajam darbam ir jābūt atbilstoši uzraudzītam, izmantojot rakstisko līgumu vai pakalpojuma līmeņa vienošanos ar ARI. Veiktajam darbam un gala rezultātam, ko iesniedz augstākajai revīzijas iestādei, ir jāatbilst ARI noteiktajiem procesiem un standartiem. Tas nozīmē, ka ARI joprojām ir nepieciešami kvalificēti un zinoši darbinieki, lai uzraudzītu darbu pat tad, kad ARI nolemj izmantot ārējos resursus.

## **19. Revīzijas uzdevums ar revidējamo vienību**

### **Prasība:**

**ARI ir jānoslēdz revīzijas uzdevums ar revidējamo vienību pirms revīzijas uzsākšanas.**

### **Skaidrojumi:**

19.1. Kā jebkurā citā revīzijā, revidējamā vienība ir jāiepazīstina ar revīzijas apjomu un mērķiem, un, ja nepieciešams, ir jāizrunā revīzijas novērtēšanas kritēriji. Ja nepieciešams ARI var uzrakstīt revīzijas uzdevuma vēstuli revidējamajai vienībai, kurā var norādīt arī šīs revīzijas noteikumus.

19.2. Attiecībā tieši uz IT revīzijām, ARI ir jāpārliecinās, ka no revidējamās vienības tiek pieprasīta atbilstoša sadarbība un palīdzība revīzijas pabeigšanai, ieskaitot pieeju ierakstiem un informācijai, un ir nodrošināts, ka jebkura elektroniska informācija tiks saņemta nepieciešamajā formātā, lai varētu veikt tās analīzi.

## **20. Revīzijas pierādījumi**

### **Prasības:**

**ARI jāpārliecinās, ka revīzijas pierādījumi ir pietiekami, ticami un precīzi, lai pamatotu revīzijas novērojumus.**

**Revīzijas pierādījumiem ir jābūt pieejamiem, lai varētu atkārtoti veikt un pārskatīt revīzijas procesu pēc revīzijas slēgšanas.**

### **Skaidrojumi:**

20.1. Revīzijas pierādījumi ir IT revidentu iegūto datu, ierakstu, dokumentu un informācijas savākšana, lai pietiekami, ticami un precīzi pamatotu IT revidentu novērojumus attiecīgai (-ām) ieinteresētai (-ām) personai (-ām) attiecīgajā laika posmā (revīzijas laikā vai pēc tās slēgšanas).

20.2. Tādejādi pierādījumiem ir jābūt pietiekamiem, ticamiem un pareiziem/precīziem saskaņā ar ARI iekšējiem kvalitātes nodrošināšanas standartiem.

20.3. IT revīzijās pierādījumiem ir jābūt atbilstoši iegūtiem un saglabātiem tādā veidā, lai tie būtu pieejami arī nākotnē bez izmaiņām datos. IT revidentiem jānodrošina, ka pierādījumiem ir nepieciešamie laika zīmogi<sup>25</sup> izmaiņām, ja pastāv risks, ka pierādījumi varētu tikt izmainīti.

20.4. IT revīzijām ir savādāks un īpašs veids pierādījumu noteikšanai, savākšanai, uzglabāšanai un saglabāšanai. Pierādījumi var būt savākti no īpašajām pārbaudēm, kas veiktas revīzijas izlasei. IT revidenti var veikt pārbaudes atbilstoši nepieciešamībai, vai nu par visiem darījumiem, vai arī tikai par izlasi, bet elektroniskie dati vienmēr var tikt pārbaudīti uz atbilstību kritērijiem visi kopā. Tomēr izņēmumu apstiprināšana var tikt veikta izlases veidā, ja izņēmumu skaits ir ļoti liels. Revīzijas izlasi var izvēlēties nejauši vai sistemātiski. IT revidenti var izvēlēties izmantot monetārās vienības izlasi vai izvēlēties izlasi, pamatojoties uz saviem spriedumiem.

20.5. Specifiskas metodes un rīki revīzijas pierādīju savākšanai IT revīzijās ir turpmāk aprakstīti D sadaļā.

## **21. Revīzijas veikšana – revīzijas pierādījumu iegūšana**

### **Prasība:**

**IT revidentam ir jāiegūst atbilstoši un pietiekami revīzijas pierādījumi un jāveic to analīze, lai nodrošinātu, ka revīzijas mērķiem ir pievērsta pienācīga uzmanība.**

### **Skaidrojumi:**

#### 21.1. Sākotnējā IT kontroļu novērtēšana

IT revidentiem jāveic revidējamās sistēmas sākotnējā IT kontroļu novērtēšana, lai iegūtu izpratni, vai pastāvošās IT kontroles (vispārējās IT kontroles un lietojumprogrammu IT kontroles) ir ticamas un darbojas saskaņā ar atbilstošām IT pārvaldes pamatnostādņēm. Kontroļu novērtēšana šajā līmenī iekļauj:

- a) Novērtēšanu, ka attiecīgais IT pārvaldes mehānisms pastāv un darbojas.
- b) Novērtēšanu, ka IT mērķi atbilst darbības mērķiem.
- c) Novērtēšanu, ka pastāv atbilstošs mehānisms, lai nodrošinātu:
  - i. Efektīvu IT projektu vadību.
  - ii. IT risinājumi iegādi un izstrādi (ieskaitot IT lietojumprogrammas, datortehniku, programmatūru, darbaspēku, tīklu, pakalpojumu risinājumus utt.).
  - iii. IT sistēmu darbību.
  - iv. Informācijas drošību.
  - v. Darbības nepārtrauktību un katastrofu novēršanu.
  - vi. Pienācīgu izmaiņu vadību.
  - vii. Pakalpojumu sniegšanu un atgriezenisko saikni.
  - viii. Atbilstību noteiktām prasībām, noteikumiem un procedūrām, veicot uzraudzību un kontroli.

---

<sup>25</sup> Laika zīmogs ir dati, kas pievienoti informācijai (elektroniski, papīra, video utt.), lai atzīmētu laiku, kad informācija tika izveidota, savākta vai mainīta. Laika zīmogi var būt tik detalizēti, cik tas informācijai ir nepieciešams (diena, datums, stundas, minūtes, sekundes, milisekundes utt.)

Iepriekšminētais, izņemot (vii) punktā noteikto, veido vispārējās IT kontroles, kuras nav raksturīgas kādai konkrētai darījumu plūsmai vai lietojumprogrammai, bet attiecas uz vispārējo IT infrastruktūru organizācijā, ieskaitot ar IT saistītas politikas, procedūras un darba praksi, kā arī kontrolēm par datu centra darbībām (IT politikām un standartiem), sistēmas programmatūras iegādi un uzturēšanu, pieejas (fiziskās un loģiskās) drošību, pienākumu sadali, darbības nepārtrauktības un katastrofu novēršanas kontrolēm, kā arī lietojumprogrammu sistēmas attīstību un uzturēšanu.

Papildus IT vispārējo kontroļu novērtēšanai būtu jāiegūst izpratne par biznesa procesiem, biznesa procesu sasaistīšanu ar IT sistēmām un saistītajām IT lietojumprogrammu kontrolēm.

Sākotnējās novērtēšanas laikā konstatētie izņēmumi norāda uz nepieciešamību veikt IT sistēmas un tās kontroļu detalizētās pārbaudes.

#### 21.2. Detalizētās pārbaudes

Detalizētās pārbaudes ietver IT kontroļu detalizētu pārbaudi, kas saskaņā ar sākotnējo novērtējumu ietver dažādas metodes un rīkus informācijas pieprasīšanai, iegūšanai un analīzei. Detalizētās pārbaudes ir izstrādātas, lai pamatotu apgalvojumu atbilstību revīzijas mērķiem. Pārbaudes ir jāizveido, izmantojot vienu vai vairākas metodes<sup>26</sup>, kas noteiktas D sadaļā.

## 22. Pārraudzība un pārbaude

### Prasība:

**ARI ir jānodrošina, ka IT revidenti tiek uzraudzīti un periodiski pārbaudīti.**

### Skaidrojums:

22.1. Revīzijas personāla darbam revīzijas laikā ir jābūt pienācīgi uzraudzītam un revīzijas grupas vadītājam jāpārbauda IT revīzijas grupas dokumenti (ISSAI 40 5.elements “Revīzijas un citu darbu izpilde”). Revīzijas personāla vecākajiem locekļiem ir jābūt nepieciešamajām zināšanām, lai sniegtu norādījumus, atbalstu un konsultācijas revīzijas veikšanas laikā.

## 23. Krāpšanas, korupcijas un citu pārkāpumu gadījumi

### Prasības:

**ARI un IT revidentiem ir jānosaka un jānovērtē ar IT revīziju mērķiem saistītie riski un krāpšanās.**

**ARI ir jāveic atbilstošie pasākumi, kā to nosaka attiecīgo likumu prasības, lai risinātu krāpšanās, korupcijas un citu pārkāpumu gadījumus.**

### Skaidrojumi:

23.1. IT revidenti, veicot revīzijas, var sastapties ar krāpšanās, korupcijas un ar to saistīto pārkāpumu gadījumiem. Prasības ziņot par krāpšanos var būt noteiktas revīzijas pilnvaru īpašajos noteikumos vai saistītajos likumos vai noteikumos, un revidentam var būt pienākums ziņot par šādiem jautājumiem personām ārpus revidējamās vienības, tādām kā likumdošanas un tiesībsardzības iestādēm. Šādos gadījumos ARI ir jāveic nepieciešamie atbilstošie pasākumi, kā to nosaka viņu pilnvaras vai attiecīgie likumi.

23.2. Veicot revīziju, IT revidentiem ir jāaglabā profesionālā skepse un ir jābūt modriem attiecībā uz krāpšanas iespējamību visā revīzijas procesa laikā.

---

<sup>26</sup> Metodes var tikt izmantotas gan atbilstības, gan detalizētajās pārbaudēs. IT revidenti var izmantot jebkuru metodi vai vairākas metodes, veicot jebkuru no diviem izvērtējumiem.



## **24. Ierobežojumi**

### **Prasība:**

**ARI atbilstošajos līmeņos ir jānosaka, jānorāda un jāinformē par ierobežojumiem katrā revīzijas posmā.**

### **Skaidrojumi:**

24.1. IT revīzijas ierobežojumiem ir jābūt norādītiem katrā IT revīzijas posmā atbilstošajos līmeņos, izmantojot atbilstošu dokumentētu komunikāciju.

24.2. IT revīzijas ierobežojumiem ir jābūt norādītiem ziņojumā.

24.3. Tipiskākie ierobežojumi varētu būt neatbilstoša pieeja datiem un informācijai, datorizācijas procesa nepienācīga dokumentēšana, kā rezultātā IT revidentiem ir jāizdomā savas izmeklēšanas metodes un analīzes, lai izstrādātu secinājumus. Jebkuri citi ierobežojumi, ar kuriem saskaras IT revidenti, ir pienācīgi jānorāda ziņojumā.

## **25. Ieteikumu ieviešanas uzraudzība**

### **Prasība:**

**ARI ir jāveic ieteikumu ieviešanas uzraudzībā par ziņojumā iekļautajiem jautājumiem, kuri IT revīzijas ziņojumā tika norādīti kā būtiski.**

### **Skaidrojums:**

25.1. Augstākajām revīzijas iestādēm ir jāseko uzraudzības pasākumiem, kurus veic atbildīgās personas attiecībā uz revīzijas ziņojumā norādītajiem jautājumiem. Sekošanai jāpievērš uzmanība tam, vai revidējamā vienība pienācīgi risina attiecīgos jautājumus, ieskaitot jebkuru plašāku ietekmi, piemēram, ja viena un tā pati IT sistēma tiek izmantota vairākās valsts organizācijās, revidējamās vienības nepietiekama vai neapmierinoša darbība var radīt nepieciešamību ARI sniegt papildu ziņojumu.

## **D. IT REVĪZIJAS METODES UN RĪKI**

### **Prasība:**

**ARI ir jāizmanto atbilstošas IT revīzijas metodes saskaņā ar revīzijas uzdevuma raksturu un revīzijas mērķu prasībām.**

### **Skaidrojumi:**

## **26. IT revīzijai specifisku metožu noskaidrošana**

26.1. IT revīzijas metodes ir saistītas ar metožu un procedūru izmantošanu, ar kuru palīdzību var veikt IT sistēmu izpēti, savākt revīzijas pierādījumus un veikt analīzi, lai pārliecinātos, ka kontroles ir atbilstošas.

## **27. Plānošanas metodes**

27.1. Plānojot IT sistēmas revīziju, revidentam sākumā ir jāsaprot, kā konkrēta lietojumprogramma atbalsta biznesa procesus revidējamajā vienībā. Šim nolūkam ir jāiegūst pamatinformācija par to, kā biznesa funkcionalitāte plūst cauri sistēmai. Tradicionālās revīzijas metodes tādas kā dokumentu izpēte, intervijas ar vadošo personālu – gan biznesa procesu īpašniekiem, gan IT organizēšanā iesaistītiem darbiniekiem, kā arī procedūru novērošana ir noderīga, lai iegūtu izpratni par to, kā sistēma atbalsta organizācijas biznesus. Iepazīšanās ar IT

politikām un procedūrām, ar lietojumprogrammām saistītām rokasgrāmatām, dokumentiem par IT ārpakalpojumu līgumiem, funkcionālās projektēšanas dokumentiem, pārdevēja piegādātajām tehniskās informācijas rokasgrāmatām un atskaišu (standarta un pielāgoto) saraksts palīdz izprast vidi, kurā sistēma darbojas un identificēt biznesa riskus, kurus izraisa kontroles kļūdas.

27.2. IT revīziju ikgadējās un revīzijas grupas līmenī plānošanas posmos, riska novērtēšana tiek veikta par IT sistēmām, kuras ir izstrādātas vai tiek izmantotas dažādās revidējamajās vienībās. To objektīvi var izdarīt, izmantojot metodes, kas ir aprakstītas šī dokumenta plānošanas sadaļā.

## 28. Revīzijas veikšanas metodes

28.1. Metožu izvēle ir kritiska, veicot atbilstības un detalizētās pārbaudes. Detalizētās pārbaudes ir izstrādātas, lai pamatotu apgalvojumu atbilstību revīzijas mērķiem. Šīm pārbaudēm ir jābūt speciāli izstrādātām, izmantojot vienu vai vairākas metodes<sup>27</sup>, tādās kā intervija, aptauja, novērošana, caurskatpārbaude, blokslēmas, datu iegūšana un analīze, apstiprināšana, pārreķināšana, atkārtota apstrāde, apstiprinājuma no trešajām pusēm iegūšana utt.

28.2. Lai veiktu vispārējo datoru kontroli (ieskaitot IT pārvaldības sfēras, sistēmu izstrādi un iegādi, IT operācijas, informācijas drošību un darbības nepārtrauktības plānošanu) pareizības novērtēšanu, pielietotās metodes ir līdzīgas tām, kuras izmanto citos revīziju veidos.

28.3. IT revīzijai raksturīgas revīzijas metodes galvenokārt ir paredzētas IT lietojumprogrammu kontroli novērtēšanai. Pārbaudot lietojumprogrammu kontroles revidentam ir nepieciešams:

- I. Noteikt būtiskās lietojumprogrammas sastāvdaļas un informācijas plūsmu cauri sistēmai, un iegūt detalizētu izpratni par lietojumprogrammu, pārskatot pieejamos dokumentus un intervējot atbilstošos darbiniekus.
- II. Izprast lietojumprogrammu kontroli riskus un to ietekmi, pārskatot to biznesa procesu svarīgumu, kurus ietekmē lietojumprogrammas sastāvdaļa.
- III. Izstrādāt pārbaudes stratēģiju, lai noteiktu kontroles stiprās un vājās puses un novērtētu turpmāko ietekmi.

28.4. Labākai izpratnei par revidējamo sistēmu, ieskaitot tās galvenos kontroles punktus, un izstrādājot pārbaudes stratēģiju, kas tiks pielietota, vienmēr ir lietderīgi apskatīt saistītos dokumentus, tādus kā funkcionālas projektēšanas specifikācijas, pārmaiņu vadības dokumentāciju kopš ieviešanas sākuma vai pēdējās revīzijas, lietotāju rokasgrāmatas, pārdevēja piegādātajām tehniskās informācijas rokasgrāmatas utt.

28.5. Pārbaudes stratēģija būs arī atkarīga no tādiem faktoriem kā riska aktīvi, lietojumprogrammas pastāvēšanas laiks uzņēmējdarbības, darījumu jutīgums, nozīmīgas izmaiņas biznesa procesos, kas izraisa izmaiņas lietojumprogrammā, un iepriekšējo revīziju rezultāti, ja tādi ir bijuši.

28.6. Pienākumu sadales un ievades atļauju novērtēšanai ir svarīgi pārskatīt darba aprakstus, salīdzināt tos ar sistēmā piešķirtajām tiesībām, pārskatīt atļauju piešķiršanas procedūras un apstiprināt darbības reģistru eksistenci to lietotāju kontos, kuriem ir administratora tiesības. Izmaiņu darbības pārskats ir jāpārbauda, lai iegūtu pierādījumus par vadības pārbaudēm.

28.7. Revidējamajām vienībām katrai ir sava datortehnikas, operētājsistēmu, datubāzu vadības sistēmu, lietojumprogrammu programmatūras, tīklu programmatūras utt. kombinācija. IT

---

<sup>27</sup> Šīs metodes var tikt izmantotas gan sākotnējās, gan detalizētās pārbaudēs. Daudzu metožu izmantošana ir aprakstīta WGITA-IDI IT revīziju veikšanas rokasgrāmata Augstākajām revīzijas iestādēm.

revidentiem ir jābūt spējīgiem iegūt no šiem resursiem informāciju, lai varētu veikt nepieciešamo IT lietojumprogrammu analīzi. Svarīgs solis datu ieguvei ir izpratne par organizācijas IT sistēmu un datubāzēm, tādām kā iesaistītiem biznesa procesiem, to nozīmi organizācijai, iesaistītiem protokoliem utt. Detalizētās pārbaudes par lietojumprogrammu kontroļu atbilstību iekļauj:

- a. Attiecīgo organizācijas biznesa datu ieguvei
- b. Datu pārveidi un ielasīšanu rīkā
- c. Datu analīzes veikšanu
- d. Pārbaudes rezultātu apstiprināšanu
- e. Revīzijas secinājumu veidošanu

Šīs procedūras IT revidenti var veikt, izmantojot A pielikumā aprakstītas metodes.

## **29. Atbilstošās sistēmas izvēle informācijas saglabāšanai**

29.1. IT revidentiem ir jānodrošina revīzijas rezultātu un revīzijas pierādījumu saglabāšana, lai viņi varētu izpildīt ticamības, pilnīguma, atbilstības un pareizības prasības. Tāpat IT revidentiem ir svarīgi nodrošināt, ka arī revīzijas process ir saglabāts, lai nodrošinātu revīzijas analīzes procedūru turpmāko apstiprināšanu. Tas ietver atbilstošas metodes dokumentēšanai, kas pēc tam tiek veikta.

29.2. Izmantojot datu izrakstus, ciktāl tas ir iespējams, var lietot pāradresācijas vēstuli. Ja tas nav iespējams, ir jāizveido iekšējie dokumenti, pierakstot svarīgu informāciju, tādu kā datums, kurā dati tika nodoti, no kāda faila datu izraksts<sup>28</sup> tika izveidots un vai dati bija no ražošanas vides vai no kādas citas utt. Elektroniskiem pierādījumiem, kas tika izveidoti un izmantoti revīzijas ziņojuma sagatavošanā, ir jābūt saistītiem ar šādiem dokumentiem.

29.3. IT revidentiem ir jāizvērtē vienas vai vairāku iepriekš minēto metožu izmantošanas atbilstība un jāpārlicinās par šīs metodes integritāti un lietderību. Jebkuras no iepriekšminētām metodēm izmantošanai nevajadzētu ietekmēt revidējamās vienības lietojumprogrammas sistēmas un to datu integritāti.

## **30. IT revīzijas rīki**

### **Prasība:**

**ARI ir jāizmanto IT revīzijas rīki, kas ir atbilstoši revīzijas uzdevuma riska novērtējumam un ARI ietvaros pieejamajiem resursiem un spējām.**

### **Skaidrojumi:**

30.1. IT revīzijas veikšana prasa labas zināšanas par procesiem un metodēm, kā arī spējas pielietot IT revīzijas rīkus, tā kā šīs revīzijas pēc savas būtības attiecas uz informāciju, kura tiek glabāta un apstrādāta elektroniskā veidā un revīzijas veikšanas gaita ārēji nav redzama.

30.2. Datorizētās revīzijas metodes (Computer Assisted Audit Techniques - CAATs) ir IT rīki, kuri palīdz revidentam veikt dažādas automatizētās pārbaudes, lai novērtētu IT sistēmu vai datus, un ir ļoti noderīgi, ja nozīmīgs revidējamās vienības datu apjoms ir pieejams elektroniskā veidā. CAATs ir noderīgas kontroļu pārbaūžu un detalizēto pārbaūžu veikšanai finanšu revīzijā, atbilstības revīzijā un lietderības revīzijā. CAATs izmantošana un izmantošanas apjoms tiek noteikts, pamatojoties uz dažādiem faktoriem, revīzijas plānošanas un revīzijas veikšanas posmā.

30.3. CAATs izmantošanas lietderība:

---

<sup>28</sup> Datu izraksts (data dump) ir liels datu apjoms, kas ir pārņemts no vienas sistēmas vai atrašanās vietas uz citu.

CAATs ir ļoti noderīgi, lai veiktu tādas IT revīzijas darbības kā lietotāju ierakstu analīzi, pārskatu sagatavošanu par atkāpēm, apkopošanu, failu salīdzināšanu, datu sadalīšanu kategorijās, izlases veidošanu, divreiz ievadītās informācijas pārbaudi, atšķirību noteikšanu, sadalīšanu pēc vecuma, virtuālo lauku aprēķinus utt. (tas ir detalizēti izklāstīts sadaļā par IT revīzijas metodēm). CAATs izmantošana sniedz vairākas priekšrocības, salīdzinot ar manuālo pārbaudi. Dažas no priekšrocībām ir šādas:

- a) Liela apjoma datu detalizētās pārbaudes un analīze var tikt paveikta īsā laika periodā un ar mazāku piepūli
- b) Pārbaudes var tikt viegli atkārtotas dažādiem failiem/datiem
- c) Elastīgas un sarežģītas pārbaudes var veikt, izmainot parametrus
- d) Automatizēta revīzijas pārbaude un rezultātu dokumentēšana
- e) Produktīvāka revīzijas resursu izmantošana

30.4. CAATs izvēle, veicot IT revīziju: CAATs izmantošana ir saistīta ar izmaksām par licenzētu programmatūru, saderīgu datortehniku un kvalificēta revīzijas personāla algošanu. Līdz ar to, daži svarīgi faktori, kas ir jāizvērtē, lemjot par CAATs izmantošanu IT revīzijā ir šādi:

- a) Vai CAATs izmantošana sniedz revīzijai pievienoto vērtību?
- b) Vai pārbaudes tiks atkārtotas citās/turpmākajās revīzijās šajā revidējamajā vienībā vai citās revidējamās vienībās ar līdzīgu uzņēmējdarbības veidu un darbībām?
- c) Vai darījumi tiek veikti tiešsaistē un/vai reālajā laikā?
- d) Vai citu revīzijas metožu izmantošana radīs augstākas izmaksas un papildu laiku?

30.5. Daži uzskatāmi CAATs piemēri ir šādi:

- Vispārēja mērķa revīzijas programmatūra ir izstrādāta, lai apmierinātu īpašas revidentu prasības, un satur pārbaudes, kuras revidenti parasti veic IT revīzijās, un tās ietver vienkāršas funkcijas, tādas kā datu iegūšanu, summēšanu, sadalīšanu pēc vecuma, datu sadalīšanu kategorijās, divreiz ievadītās informācijas pārbaudi utt.
- Strukturētā vaicājumu valoda (Structured Query Language – SQL) ir valoda, kas nav orientēta uz procedūrām un ir noderīga, lai noteiktu un ietekmētu datus radniecīgo datubāzu vadības sistēmās (Relational Database Management Systems – RDBMS).
- Elektroniskās tabulas arī ir noderīgas CAATs un var tikt izmantotas, lai izpildītu vienkāršus vaicājumus, tādus kā datu iegūšanu, kas atbilst iepriekšnoteiktajiem kritērijiem, šķirošanu, apkopošanu utt.
- Datu ieguves rīki palīdz atklāt paraugus lielās datu kopās, izvilkt informāciju no šādām datu bāzēm un pārveidot to saprotamā struktūrā turpmākai izmantošanai caur datu vizualizāciju.
- Nozarēm raksturīga revīzijas programmatūra ir izstrādāta ar nolūku nodrošināt funkcionalitāti, kas apmierinātu parastās revīzijas funkcijas, kas saistītas ar konkrētu nozari, piemēram, tās attēlo nozarei specifisku loģiku, lai izveidotu revīzijas vaicājumus utt. Tās ir atrodamas nozarēs ar labi dokumentētiem un izstrādātiem biznesa procesiem, tādās kā banku, ražošanas, naftas un gāzes, kravu pārvadāšanas nozarē u.tml.
- Utilitātprogrammatūra veic funkcijas, kas ir izstrādātas, lai palīdzētu analizēt, konfigurēt, optimizēt vai uzturēt IKT infrastruktūru. Galvenie ar IT revīzijām saistīto utilitātprogrammatūru piemēri ir pārskatīšanas kontroles pakalpojumi, atklūdotāji, diska

vietas analizētājs, failu pārvaldītājs, tīkla pakalpojumi un sistēmas profilu programmas (*system profilers*).

- Labi izstrādātas sistēmas ietver iestrādātus revīzijas moduļus (specializētu revīzijas programmatūru), kas veido standarta un pielāgotas atskaites. Tie uzreiz tiek iestrādāti Organizācijas resursu plānošanas (Enterprise Resource Planning - ERP) lietojumprogrammās. Papildus ir arī lasīšanas programmatūra, kas IT revidentiem sniedz tikai lasīšanas pieeju ERP datiem, izmantojot uz interfeisu balstītas lietojumprogrammas.

30.6. Lai izmantotu CAATs kādas konkrētas jomas revīzijā, revidentam ir jāveic detalizēta plānošana. Pirms CAATs izmantošanas revīziju veikšanā ir svarīgi izprast un iegūt informāciju par to, kā tabulas/faili ir savstarpēji saistīti, informāciju par datubāžu vārdnīcām/trigeriem, ierakstu izkārtojumu, kontroles kopsummām, datu lielumu/formātu un sistēmas dokumentāciju.

## E. ZIŅOŠANA

### Prasības:

**IT revīzijas ziņojumam ir jāatspoguļo IT revīzijas procesā iegūtie konstatējumi atkarībā no šo konstatējumu būtiskuma attiecībā uz revīzijas mērķiem.**

**IT revīzijas ziņojumam ir jābūt visaptverošam, līdzsvarotam, pārlicinošam, savlaicīgam un viegli lasāmam.**

### Skaidrojumi:

#### 31. Prasības ziņošanai par IT revīziju

31.1. Tā kā IT revīzija pēc būtības var tikt veikta finanšu revīzijas, lietderības revīzijas, atbilstības revīzijas vai šo revīziju kombinācijas ietvaros, ziņošanas prasības IT revīzijai izriet no ISSAI 100-400, un atkarībā no revīzijas rakstura no ISSAI 1700, 1705 un 1706 finanšu revīzijas gadījumā un attiecīgajiem 4.līmeņa ISSAI atbilstības un lietderības revīzijas gadījumā.

31.2. Daži apsvērumi, kas IT revidentiem būtu jāņem vērā sagatavojot ziņojumu ir nepieciešamība ierobežot tehniskā žargona lietošanu un apzināties tādas uzrādāmās informācijas konfidencialitāti, kā piemēram, paroles, lietotāju vārdi, ID un personīgā informācija.

#### 32. IT revīzijas ziņojuma saturs un forma

32.1. IT revīzijas ziņojuma vispārējais izkārtojums iekļauj šādas sadaļas:

- a. Revīzijas mērķi
- b. Revīzijas apjoms
- c. Par kuru laika periodu revīzija tiek veikta
- d. Revīzijas kritēriji
- e. Revīzijas metodoloģija
- f. Kopsavilkums
- g. Revīzijas konstatējumi
- h. Revīzijas secinājumi
- i. Revīzijas ieteikumi
- j. Jebkuri saistīti cēloņi un riski, ierobežojumi, atrunas vai bažas, kuras revidents uzskata par saistītām ar veikto revīziju

32.2. Neskatoties uz IT revīzijas tehnisko raksturu, IT revidentiem ir jāpārliecinās, ka revīzijas ziņojums ir pilnīgi saprotams augstākajai vadībai, revidējamajai vienībai, ieinteresētām personām un sabiedrībai.

32.3. IT revidenti var pārrunāt revīzijas ziņojuma melnrakstu ar IT sistēmu vadību pirms ziņojuma pabeigšanas un publicēšanas, un ja nepieciešams iekļaut galīgajā ziņojuma versijā vadības atbildes uz konstatējumiem, secinājumiem un ieteikumiem.

32.4. Revidējamā vienība var izlemt pieņemt risku un neveikt izmaiņas tajos apstākļos, kas iekļauti ziņojumā, ņemot vērā labojumu izmaksas, sarežģītību vai citus apsvērumus. IT revidentu ziņojumā ir jāsniedz informācija atbildīgajām amatpersonām par šādiem gadījumiem saskaņā ar viņu iekšēji izstrādātām pamatnostādņēm.

32.5. Gadījumā ja IT revidenti un revidējamā vienība nevar vienoties par kādu konkrētu ieteikumu vai revīzijas piebildi, revīzijas ziņojuma pielikumā var norādīt abus viedokļus un domstarpību iemeslus. Revidējamās vienības viedoklis var tikt atklāts arī revīzijas ziņojumā vai pavadvēstulē.

32.6. IT revidentiem ir jāizvērtē iespējamās negatīvas sekas, kuras radīs revīzijas ziņojums, tiklīdz augstākās revīzijas iestādes revīzijas ziņojums tiks publicēts. Piemēram, ja IT revidenti ir atklājuši kādas drošības problēmas IT sistēmā un ir ziņojuši par to pirms IT sistēmā ir veiktas izmaiņas, IT sistēmas ievainojamība kļūst zināma sabiedrībai pirms nepilnības ir novērstas. Šādos gadījumos ARI var izvērtēt iespēju ziņot par konstatētām nepilnībām pēc tam, kad IT sistēmās kļūdas ir izlabotas vai arī neziņot detalizēti par IT sistēmu ievainojamību, lai izvairītos no ziņojuma negatīvas ietekmes.

32.7. Jebkuras revīzijas ieteikumu ieviešanas uzraudzība ir visa IT revīzijas procesa noslēguma posms. Tā tiek veikta, lai pārliecinātos, ka ir veiktas atbilstošas darbības attiecībā uz visām nepilnībām, kas tika atklātas IT revīzijas veikšanas gaitā. Parasti tas ir ARI veiktā nepārtraukta riska novērtējuma rezultāts. IT revīzijas, par kuru tika sagatavots revīzijas ziņojums, ieteikumu ieviešanas uzraudzības procesa ietvaros IT revidents atkārtoti apmeklē revidējamo vienību pēc saprātīga laika intervāla, lai pārliecinātos, ka visi ieteikumi ir ieviesti.



## A pielikums – Datu analīzes metodes

### 1. Atbilstošo organizācijas biznesa datu iegūšana:

Izprot datu struktūru, iegūstot no revidējamās vienības un iepazīstoties ar dokumentiem, kuros dati ir definēti. Ja revidējamā vienība ir piešķirusi lasīšanas tiesības sistēmām, tad tabulās saglabātos datus, kas attiecas uz revīzijas uzdevumu, var iegūt, izveidojot pieprasījumu datubāzei, ja prasmju kopums eksistē. Pretējā gadījumā, revidējamai vienībai var pieprasīt sniegt kopiju no attiecīgiem izejas datiem. Datus var saņemt datubāzes izraksta veidā, kas satur ierakstus par tabulas struktūru un/vai datus no datubāzes, un parasti ir SQL paziņojumu saraksta formā. IT revidentiem var būt nepieciešams izveidot līdzīgu vidi (savienojamu versiju vienkāršām datubāžu lietojumprogrammām, operētājsistēmu, datortehniku utt.) tai, kāda pastāv revidējamajā vienībā, lai importētu/analizētu datus no iegūta datu izraksta kopijas. Daudzos gadījumos tas attēlo lietojumprogrammu kontroļu pārbaudes vissvarīgākos aspektus, tā kā precīza datu iegūšana palīdz veiksmīgi īstenot turpmākos procesus. IT revidentiem var būt nepieciešams arī pārveidot datus no vienas formas citā, lai veicinātu labāku informācijas lasīšanu un analīzi.

### 2. Datu pārveide un ielāde:

Izmanto revīzijas programmatūru/ Iegūšanas, pārveidošanas un ielādes (Extract, Transform and Load - ETL) rīkus, lai importētu datus no dažādām datubāzes platformām. Visbiežāk izmantoti datu analīzes rīki (skaidroti sadaļā par rīkiem) atļauj datu importēšanu no vairākām datubāzēm rīku ierastajā izklājlapu formātā. Šie rīki parasti izmanto importēšanas vedni, lai palīdzētu importēt (interpretēt, konvertēt, formatēt) datus turpmākajai analīzei. Revidentam ir nepieciešams veikt dažas iepriekšējās formatēšanas darbības izejas datiem, lai atvieglotu analīzes izmantošanu. Vispārējā revīzijas programmatūra vai konkrēta utilitātprogrammatūra var arī tikt izmantota, lai novērtētu dažādu IT sistēmas pakalpojumu funkcionalitāti. Jebkura no šiem pakalpojumiem vai to kombinācijas izmantošana ir atkarīga no revīzijas mērķa un apjoma, kas ir jāaptver, veicot IT revīziju.

### 3. Datu analīzes veikšana:

Galvenie soļi, kas ir iesaistīti revidējamās vienības biznesa datu analīzē, lai sniegtu pārlicību par lietojumprogrammu kontroļu kvalitāti, ir kopīgi visa veida datu analīzei. Galvenie apsvērumi datu analīzē ir:

- Noskaidrot analīzes vai projekta mērķi;
- Saprast pētamo(-os) paraugu(-us);
- Saprast, kādi instrumenti tika lietoti, lai savāktu datus;
- Būt informētiem par datu izkārtojumu un formātu<sup>29</sup>; un
- Izveidot unikālu identifikatoru, ja saskanības noteikšana vai apvienošana ir nepieciešama.
- IT revidentiem ir jāplāno:
  - Paziņojums par izpētes jautājumiem/ mērķiem
  - Izmantotās metodes, lai atbildētu uz izpētes jautājumiem
    - Novērtēšanas kritēriji
    - Pierādījumi
    - Analīze
    - Secinājumi

<sup>29</sup> Šie ir vissvarīgākie soļi pirms datu analīzes veikšanas. Izkārtojums nozīmē izpratni par dažādām datubāzēm, tajās iekļautajām tabulām, izmantotiem kodēšanas modeļiem un saistību starp tabulu un datubāzi. Šajā sakarā būtu noderīga arī izpratne par dažādiem datubāžu modeļiem.

- Failu pārstrukturēšanas procedūras (sintakses izveide, jaunu mainīgo pievienošana pēc nepieciešamības)
- Datu tīrīšanas procedūras (piemēram, izlecošo vērtību izņemšana)

Lielāka daļa analīžu var tikt veikta tieši no darba datu faila. Dažas analīzes var prasīt izejas datu, apakškopu vai konkrētu ievades datu pārveidi, lai atbilstu statistikas programmatūrai vai rīkiem, kurus revidents var izmantot.

#### 4. Izpratne par datu tiem un attēliem

Datu analīze parasti tiek veikta, izmantojot no revidējamās vienības saņemto datu kopiju, lai saglabātu oriģinālus vēlākai apstiprināšanai un pārskatīšanai, ja būs nepieciešams.

Vispārējā mērķa revīzijas programmatūra vai specializētā revīzijas programmatūra var tikt izmantota, lai veiktu informācijas analīzi. Šie rīki sniedz iespējas importēt, kā arī analizēt datus. Datu analīzei var izmantot arī strukturētu vaicājumu valodu. Sarežģītajās sistēmās, tādās kā ERP sistēmās, informācija ir pieejama, izmantojot detalizētus pārskatus. IT revidentiem ir jāgūst izpratne par šādiem pārskatiem un jāiegūst atbilstošie pārskati, lai veiktu atbilstošu analīzi. IT revidentiem ir jābūt uzmanīgiem, nodrošinot, ka iegūtie dati ir ticami, atbilstoši, pieņemami un pietiekami. Cik vien tas ir iespējams, tiem ir jābūt ar laika zīmogu un pienācīgi pārbaudītiem no revidējamās vienības puses.

It īpaši mainīgie dažādos datu laukos var prasīt speciālu kodēšanu dažādi datu attēlošanai

- Skaitlisku
- Rindas
- Datuma un laika
- Naudas vienībās

Datu analīzes individuālās metodes lietojumprogrammas integritātes pārbaudei arī ir atkarīgas no revīzijas mērķiem. Šīs metodes ir šādas:

**1. Testdatu izmantošana:** Testdatu analīze tiek veikta gadījumos, kad ir paredzēts pārbaudīt programmas kvalitāti. Tiek pieņemts, ka, ja atsevišķu īpašu pārbaudu rezultāti ir ticami, tad šos rezultātus ir iespējams vispārināt arī uz kopēju programmas uzticamību. Testdatu izmantošana ietver testdatu izstrādi un izveidi pirms programmas palaišanas ar testdatiem. Bieži vien šo metodi pielieto pats izstrādātājs lietojumprogrammas testēšanas posmā, pirms lietojumprogramma vai izmaiņas tajā tiek pārnestas uz ražošanu (t.i., reālu darbību veikšanu). Revidējot nesen izveidotu IT sistēmu vai izmaiņu vadības procesus, revidenti var pārskatīt testēšanas posmā veiktās procedūras.

**2. Kodu salīdzināšana:** Izstrādātāji izmanto kodu salīdzināšanas metodi, kas ietver programmas vai tās izmaiņu izejas koda salīdzināšanu ar standarta izstrādāto metodoloģiju konkrētai programmēšanas valodai ar mērķi noteikt kļūdas, drošības pārkāpumus vai programmēšanas nosacījumu pārkāpumus. Šī pārsvarā ir izstrādātāju izmantotā metode un IT revidenti to reti izmanto. Revidentu loma šajā pārbaudē būtu noteikt, vai kodu izlasei, kuru izvēlējas neatkarīga drošības pārbaudes komanda, tika pārbaudīta kodu drošība un vai rezultāti tika dokumentēti un iekļauti ziņojumā, kā arī, vai atklātie pārkāpumi un apdraudējumi tika atbilstoši novērsti. Tomēr revidenti ar atbilstošām zināšanām var pielietot kodu salīdzināšanu attiecībā uz izmaiņu vadību vai lietojumprogrammas nodošanu ekspluatācijā, ja revīzijas apjoms to paredz.

**3. Datu integritātes pārbaude:** datu integritātes pārbaude ir detalizēto pārbaudu kopums, kas pārbauda sistēmā pieejamo datu pareizību, pilnīgumu, konsekvenci un autorizāciju. Šīs pārbaudes nosaka ievades un apstrādes kontroļu trūkumus. Datu integritātes pārbaudes palīdz

noteikt relāciju integritātes noturību, pārbaudot apstiprināšanas kārtību, kas tika iestrādāta lietojumprogrammā, izstrādājot ievades nosacījumu ierobežojumus un datu īpašības tabulu noteikšanas posmā datubāzes izstrādes ietvaros.

Šīs pārbaudes ietver noteiktas datu analīzes metodes, kuras IT revidenti var pielietot, izmantojot vienkāršus analīzes rīkus vai vispārējo revīzijas programmatūru.

**1. Izlase:** Izlases metode ir noderīga, lai izdarītu atbilstošus secinājumus, pamatojoties uz statistiski pietiekamām pārbaudēm, kas veiktas par ierobežotu datu apjomu. Pastāv divas galvenās metodes, kuras izmanto IT revidenti. Tās ir atsevišķo vienību izlase un mainīgo izlase. Atsevišķo vienību izlasi parasti izmanto, veicot atbilstības pārbaudes, tā attiecas uz kvalitatīvo pazīmju esamību vai neesamību un sniedz secinājumus, kas ir izteikti kā iestāšanās gadījumu biežums. Mainīgo izlase parasti tiek piemērota detalizētajās pārbaudēs, tā attiecas uz darījumu grupas mainīgajām īpašībām, un sniedz secinājumus, kas saistīti ar novirzēm no normas.

Veicot pārbaudi par apstiprināšanu un citām ievades kontrolēm sistēmā, kura darbojas ar lielu datu kopumu, revidents var uzskatīt par noderīgu izmantot sistēmas datubāzē saglabāto darījumu ierakstu nejaušo izlasi.

Lielākā daļa no datu analīzes lietojumprogrammām, ieskaitot izklājlapas lietojumprogrammu un vispārēja mērķa revīzijas programmatūru, nodrošina vienkāršas funkcijas, lai izvēlēties konkrētu datu elementu (lauks/kolonna/vektors) un saistītas datu šūnas, un veido nejaušas apakškopas no izvēlētas datu kopas, izmantojot algoritmus, kas balstās uz nejaušām skaitliskām vērtībām, vai vienkāršas formulas.

**2. Apkopošana un sadalīšana kategorijās:** Šīs divas metodes palīdz profilēt datus pirms jebkādu kontroļu testu veikšanas. Datu apkopošana palīdz noteikt darījumu kopsummas atbilstoši noteiktām pazīmēm, kas palīdz revidentam iegūt vispārējo izpratni par darījumiem. Piemēram, debitoru parādu konta kopsummu noteikšana pēc pircēju veidiem sniedz noderīgu ieskatu par augstas vērtības maksājumu nemaksātājiem. Ļoti noderīga funkcija, kas ir pieejama izklājlapās un vispārēja mērķa revīzijas rīkos, ir rakurstabula. Tā palīdz ļoti īsā laikā izveidot kopsavilkuma informāciju no lielas datubāzes.

Datu sadalīšana kategorijās sagatavo datu biežuma sadalījumu pēc apgabaliem vai intervāliem. Tā var sniegt revidentam nozīmīgu informāciju par datu veidu un var arī palīdzēt mums noteikt jomas, kurās būtu jāveic detalizētās pārbaudes.

**3. Nosacījuma vaicājumi:** Datu izvilšanas metode, kas balstās uz nosacījumu vaicājumiem, ir noderīga, lai veiktu vairākas pārbaudes par lietojumprogrammu kontroļu kvalitāti, kas ietver sevī pilnīguma, integritātes un pareizas biznesa nosacījumu atspoguļošanas pārbaudi.

**a. Ievades kontroļu pārbaude:** Piemēram, IT sistēmā, kas atbalsta konkrētu valdības finansētu izglītības/labklājības programmu, ir svarīgi datubāzē izveidot pastāvīgus ierakstus par labuma guvējiem pamatdatu tabulas formā. Ievades kontroles pārbaude šādā gadījumā ir izvilkta izlasi no pamatierakstiem, kas glabājas pamattabulā, un pārbaudīt, vai atlasītie dati satur tukšas vietas, neatbilstošas vērtības, divkāršus ierakstus utt. attiecībā uz saistītām raksturīpašībām (unikāli ID, vārdi, adreses, atrašanās vietas ID). Pierādījumi par jebkuru no šīm kļūdām norādīs uz trūkumiem datu aprakstos tabulu izstrādes laikā.

**b. Apstrādes kontroļu pārbaude:** Apstrādes kontroļu pārbaudei īpaša detalizētā pārbaude var būt noskaidrošana, vai konkrēti biznesa noteikumi ir atbilstoši atspoguļoti IT sistēmā, kas tiek izmantota, lai veiktu darījumu apstrādi. Piemēram, sistēmā, kuru izmanto nodokļu departaments, pārbaude var būt gūt pārliecību, ka nosacījumi nodokļu atlaides piešķiršanai ir

atspoguļoti sistēmā. Šādā gadījumā, izvilkumu no ierakstiem var veikt no parauga nodokļu datu kopas ar nosacījumu, kas imitē biznesa nosacījumu. Jebkuri šī izvilkuma pārbaudes rezultāti, kas neatbilst biznesa nosacījumiem, var norādīt uz neatbilstošu apstrādes kontroli vai biznesa nosacījumu neatspoguļošanu. Šāda neatspoguļošana var novest pie atkārtotām kļūdām, kas var radīt būtisku ietekmi uz uzņēmuma finansēm.

IT revidentiem ir nepieciešamas detalizētas zināšanas par organizācijas biznesa noteikumiem, lai izstrādātu atbilstošus nosacījuma vaicājumus, lai pārbaudītu, vai biznesa noteikumi ir atbilstoši atspoguļoti lietojumprogrammā.

**1. Divkāršu ierakstu identificēšana:** Izplatīta pārbaude datubāzes attiecīgo datu integritātei ir pārbaudīt, vai pastāv divkārši ieraksti gadījumos, kad tādiem pēc loģikas nebūtu jābūt, attiecībā uz organizācijas noteikto biznesa noteikumu nosacījumiem. Piemēram, nodokļu vai sociālas drošības datubāzē attiecīgajam identifikatoram saskaņā ar likumu ir jābūt unikālam. Pierādījumi par dubultiem ierakstiem šajā datu laukā norāda uz nepareizu pastāvīgo datu ievades apstiprināšanu, kas izraisa operacionālo vai finanšu risku revidējamajai vienībai. Analīzes rīki sniedz vienkāršas funkcijas, lai noteiktu divkāršos ierakstus. Tos var atrast pat darījumu tabulās, kas var palielināt dubulto maksājumu risku.

IT revidentiem ir jānovērtē šādu pārbaudu nepieciešamība, atkarībā no lietojumprogrammu kontrolēm, kas tika testētas procesa ietvaros. Piemēram, ja revidents pārskata finanšu kontroles kreditoru parādu apstrādes lietojumprogrammā, iespēja, ka sistēma radīs divus vienādus pasūtījuma numurus, ir maz ticama. Tomēr, ja revidentam ir jāpārbauda kontroles par divkāršu piegādātāja rēķina iesniegšanu (ārējā ievade), kas nav sistēmas izveidota ievade, šādu pārbaudi var veikt.

**2. Atšķirību analīze:** Šīs metodes izmantošanas mērķis ir pārliecināties par pilnīgumu un pārbaudīt atšķirības skaitliskajā datu laikā, kurā ir jābūt secīgai numerācijai. MS Excel to var izdarīt sērijveidā šķirojot vērtības pārbaudāmajā datu laukā, pieskaitot aprēķināto lauku, pamatojoties uz secīgu loģiku, un tad filtrējot rindas, kurās parādās izņēmumi. Vispārējā revīzijas programmatūra izmanto vienkāršu pārrāvumu noteikšanas funkciju, kur jānosaka pārbaudāmais lauks atšķirību noteikšanai. Lai izmantotu divkāršo ierakstu vai atšķirību noteikšanas funkcijas, revidentam nav nepieciešama liela vaicājumu veidošanas pieredze.

**3. Strādāšana ar vairākiem failiem:** Avota datubāze bieži vien satur lielu darījumu un pamattabulu daudzumu, lai izpildītu datu normalizācijas vajadzības. Strādājot ar importētām datu kopām, bieži vien ir noderīgi apvienot konkrētus laukus vienā datu tabulā, izmantojot savienošanas atslēgu (lauku). GAS ļauj veikt šādu vairāku failu apvienošanu ar „apvienošanas” funkcijas palīdzību. Apvienošanas funkciju vai apvienoto tabulu nosacījuma vaicājumu izmantošana palīdz revidentam novērtēt datu pilnīgumu datu tabulās vai pat atsevišķās saistītajās biznesa lietojumprogrammās, kuras izmanto organizācija.

Piemēram, ja organizācija reģistrē potenciālos piegādātājus interneta portālā un izmanto atsevišķu iepirkumu lietojumprogrammu, lai veidotu pirkumu pasūtījumus, biznesa nosacījumiem būtu jānosaka, ka piegādātāju datubāzei ir jābūt savienotai ar iepirkumu datubāzi. Apvienotas tabulas no šīm divām atsevišķām datubāzēm, izmantojot atbilstošus pārdevēju vārdus vai pārdevēju ID, palīdzēs noteikt saskarnes atbilstību starp divām saistītām biznesa lietojumprogrammām.

IT revidentiem ir jāpiemēro šo metožu kombināciju, lai iegūtu pārlicību par lietojumprogrammas kontrolēm.