IULIE 2023

APLICAREA CADRULUI CONCEPTUAL CU PRIVIRE LA INDEPENDENȚĂ: ÎNDRUMĂRI PRACTICE PENTRU AUDITORI, CU REFERIRE LA SCENARIILE CARE IMPLICĂ TEHNOLOGIA

IESBA International Ethics Standards Board for Accountants®

APESB Accounting Professional & Ethical Standards Board

CUPRINS

INTRODUCERE

1. Această publicație a fost elaborată de personalul Consiliului pentru Standarde Profesionale de Contabilitate și Etică din Australia (APESB) și al Consiliului pentru Standarde Internaționale de Etică pentru Contabili (IESBA), sub auspiciile fazei 2 a Grupului operativ Tehnologie din cadrul Consiliului pentru Standarde Internaționale de Etică pentru Contabili (IESBA).

2. Tehnologia creează numeroase oportunități pentru profesioniștii contabili, dar folosirea sa poate genera, de asemenea, amenințări la adresa respectării *Codului Etic Internațional pentru Profesioniștii Contabili (inclusiv Standardele Internaționale privind Independența)* (Codul).[1]

3. Această publicație examinează modul în care tehnologia se intersectează cu independența auditorului și le oferă profesioniștilor contabili cu drept de practică trei exemple practice privind aplicarea cerințelor Codului, inclusiv a cadrului conceptual, în astfel de situații. Scenariile sunt ipotetice și au scopul de a ilustra raționamentul exercitat în aplicarea Codului. Analizele din această publicație reflectă faptele și circumstanțele prezentate în scenarii și nu împiedică luarea în considerare a oricăror noi informații sau modificări ale faptelor și circumstanțelor care ar putea afecta evaluarea, de către profesionistul contabil, a concluziilor formulate.

4. Cu scop ilustrativ, scenariile anticipează, de asemenea, următoarele revizuiri, care au fost adoptate și implementate din timp:

   - *Definițiile entității cotate și entității de interes public* (în vigoare pentru auditurile situațiilor financiare emise începând cu 15 decembrie 2024 sau ulterior acestei date),
   - *Revizuiri referitoare la tehnologie* (în vigoare pentru auditurile și revizuirile situațiilor financiare pentru perioadele care încep cu 15 decembrie 2024 sau ulterior acestei date și alte revizuiri ale prevederilor etice ale Codului, în vigoare începând cu 15 decembrie 2024) și
   - *Definiția echipei misiunilor și a auditurilor grupului* (în vigoare pentru auditurile situațiilor financiare și ale situațiilor financiare ale grupului, aferente perioadelor începând cu 15 decembrie 2023 sau ulterior acestei date).

5. Această publicație nu vine în completarea sau nu prevalează asupra Codului, are autoritate doar textul acestuia, de sine stătător. Citirea acestei publicații nu înlocuiește citirea Codului. Îndrumările din această publicație nu își propun să fie exhaustive și trebuie întotdeauna să se facă referire la Codul însuși. Această publicație nu are nicio autoritate și nu reprezintă o reglementare oficială a APESB sau IESBA.

6. Profesioniștii contabili trebuie să ia în considerare faptul că unele jurisdicții pot avea prevederi care diferă de, sau depășesc, prevederile stabilite în Cod. În aceste jurisdicții, contabilii trebuie să fie conștienți de acele diferențe și să se conformeze prevederilor celor mai stricte, cu excepția cazului în care acest lucru este interzis prin lege sau reglementări.

Interzicerea asumării de responsabilități de conducere, inclusiv pentru anumite servicii de sisteme IT

7. O firmă sau o firmă din rețea nu trebuie să își asume o responsabilitate de conducere pentru un client de audit (punctul C400.20). Această interdicție se aplică furnizării de servicii, altele decât cele de asigurare, către toți clienții de audit, fie că sunt entități de interes public (PIE) sau nu (non-PIE).

8. Responsabilitățile de conducere implică controlarea, gestionarea și coordonarea unei entități, inclusiv luarea de decizii cu privire la achiziția, mobilizarea și controlul resurselor umane, financiare, tehnologice, fizice și necorporale (punctul 400.20 A1). Prin urmare, când este efectuată o activitate profesională pentru un client de audit, Codul îi solicită unei firme să se asigure că membrii conducerii clientului exercită toate raționamentele

---

[1] Așa cum prevede Ediția 2022 a Codului, inclusiv revizuirile aprobate cu privire la: *Definițiile entității cotate și entității de interes public*, *Revizuirile referitoare la tehnologie* și *Definiția echipei misiunii și a auditurilor grupului*.

și iau toate deciziile care revin responsabilității de conducere (punctul C400.21).

Servicii de sisteme IT[2]

9. Pentru a nu își asuma o responsabilitate de conducere când furnizează servicii de sisteme IT, firma trebuie să se asigure că (punctul C606.3):

   (a) Clientul de audit își asumă responsabilitatea pentru stabilirea și monitorizarea unui sistem de controale interne,

   (b) Clientul de audit, printr-o persoană (sau persoane) competentă(e), de preferat din cadrul conducerii superioare, ia toate deciziile de conducere care revin responsabilității de conducere cu privire la proiectarea, elaborarea, implementarea, utilizarea, mentenanța, monitorizarea, actualizarea sau dezvoltarea sistemului IT,

   (c) Clientul de audit evaluează gradul de adecvare și rezultatele proiectării, elaborării, implementării, utilizării, mentenanței, monitorizării, actualizării sau dezvoltării sistemului IT și

   (d) Clientul de audit este responsabil pentru funcționarea sistemului IT și pentru datele pe care acesta le generează și le utilizează.

10. De asemenea, Codul stabilește exemple de sisteme IT care implică o asumare de responsabilitate de conducere și ar fi, deci, interzise pentru toți clienții de audit (punctul 606.3 A1). Aceste servicii includ situațiile în care o firmă sau o firmă din rețea:

   - Stochează date sau gestionează (direct sau indirect) găzduirea datelor, în numele clientului de audit și
   - Utilizează, asigură mentenanța sau monitorizează sistemele IT ale clientului de audit, rețeaua sau site-ul acestuia.

11. Totuși, Codul admite că procesele precum colectarea, primirea, transmiterea și păstrarea datelor furnizate de un client de audit pe parcursul unui audit sau pentru a permite furnizarea unui serviciu permis către acel client nu rezultă într-o asumare a unei responsabilități de conducere (punctul 606.3 A2).

Furnizarea de servicii, altele decât cele de asigurare, către un client de audit, inclusiv anumite servicii de sisteme IT

12. Furnizarea de servicii, altele decât cele de asigurare, către clienții de audit ar putea crea amenințări la adresa conformității cu principiile fundamentale și amenințări la adresa independenței. Înainte ca o firmă sau o firmă din rețea să accepte o misiune de a furniza un alt serviciu decât unul de asigurare, care nu este interzis expres prin Cod, unui client de audit, acea firmă trebuie să aplice cadrul conceptual pentru a identifica, evalua și trata orice amenințare la adresa independenței care ar putea fi creată prin furnizarea acelui serviciu (punctul C600.9).

13. Aplicarea cadrului conceptual implică un spirit curios, exercitarea raționamentului profesional și utilizarea testului unei terțe părți rezonabile și informate (punctul C120.5). Dacă o amenințare la adresa principiilor fundamentale și/ sau a independenței nu este la un nivel acceptabil și acea amenințare nu poate fi eliminată sau redusă la un nivel acceptabil prin aplicarea măsurilor de protecție, firma trebuie să refuze sau să înceteze

---

[2] Serviciile de sisteme IT cuprind o gamă largă de servicii, inclusiv (punctul 606.2 A1):

- Proiectarea sau dezvoltarea de sisteme IT de hardware sau software.
- Implementarea de sisteme IT, inclusiv instalarea, configurarea, crearea de interfețe sau personalizarea.
- Utilizarea, mentenanța, monitorizarea, actualizarea sau dezvoltarea sistemelor IT.
- Colectarea sau stocarea de date sau gestionarea (direct sau indirect) a găzduirii datelor.

serviciul (punctul C120.10).[3]

14. Seria de publicații *Explorând Codul IESBA*, în special edițiile 1-5, oferă îndrumări suplimentare, utile în aplicarea cadrului conceptual al Codului, în vederea conformității cu principiile fundamentale și cu cerințele de independență. Amenințările actuale sau percepute la adresa conformității cu principiile fundamentale și de independență pot afecta, de asemenea, exercitarea scepticismului profesional de către echipa de audit (punctele 120.15 A1 și 120.16 A2).

15. Codul cuprinde prevederi specifice care sprijină firmele să identifice, evalueze și trateze amenințările la adresa independenței, create prin furnizarea unui serviciu, altul decât unul de asigurare, unui client de audit (Secțiunea 600). Pragul de semnificație este un factor relevant în evaluarea amenințărilor create prin furnizarea unui serviciu, altul decât unul de asigurare, unui client de audit (punctul 600.11 A1). Totuși, când Codul interzice expres furnizarea unui serviciu, altul decât unul de asigurare, unui client de audit, firmei sau firmei din rețea nu i se permite furnizarea acelui serviciu, indiferent de pragul de semnificație sau de rezultatul acelui serviciu, care nu este unul de asigurare, asupra situațiilor financiare pe marginea cărora firma va exprima o opinie (punctul 600.11 A2).

16. Mai precis, înainte de furnizarea unui serviciu, altul decât unul de asigurare, unui client de audit, o firmă sau o firmă din rețea trebuie să determine dacă furnizarea acelui serviciu ar putea crea o amenințare de autorevizuire[4], evaluând dacă există un risc ca (punctul C600.15):

    (a) Rezultatele acelui serviciu, care nu este unul de asigurare, să facă parte din sau să afecteze înregistrările contabile, controalele interne asupra raportării financiare sau situațiile financiare asupra cărora firma va exprima o opinie și

    (b) Pe parcursul auditului acelor situații financiare asupra cărora firma va exprima o opinie, echipa de audit va evalua sau se va baza pe orice raționamente exercitate sau activități desfășurate de către firmă sau firma din rețea în timp ce aceasta furnizează serviciul, care nu este unul de asigurare.

17. În cazul unui client de audit care este o entitate de interes public (PIE), dacă firma determină că furnizarea unui serviciu, altul decât unul de asigurare, ar putea crea o amenințare de autorevizuire în raport cu auditul situațiilor financiare asupra cărora firma va exprima o opinie, acel serviciu nu trebuie furnizat (punctul C600.17), indiferent de pragul de semnificație. A se consulta, de asemenea, *Întrebări & Răspunsuri ale personalului: Revizuirea Codului cu privire la furnizarea de servicii, altele decât cele de asigurare*.

18. Cerințele și materialele privind aplicarea, relevante pentru firme când analizează furnizarea unui serviciu, altul decât unul de asigurare, către un client de audit, se aplică și când o firmă sau firmă din rețea (punctul 600.6):

    (a) Utilizează tehnologia pentru a furniza un serviciu, altul decât unul de asigurare, unui client de audit, sau

    (b) Furnizează, vinde, revinde sau autorizează tehnologia, având ca rezultat furnizarea unui serviciu, altul decât unul de asigurare, de către firmă sau o firmă din rețea:

        (i) Pentru un client de audit, sau

        (ii) Pentru o entitate care furnizează servicii utilizând acea tehnologie către clienți de audit ai firmei sau ai firmei din rețea.

---

[3] Dacă profesionistul contabil ia cunoștință de noi informații sau modificări ale faptelor și circumstanțelor care pot afecta măsura în care o amenințare a fost eliminată sau redusă la un nivel acceptabil, acesta va evalua din nou și va trata acea amenințare în consecință (punctele C120.9 - 120.9 A2).

[4] O amenințare de autorevizuire este amenințarea prin care o firmă sau o firmă din rețea nu vor evalua corespunzător rezultatele unui raționament anterior exercitat de o persoană din cadrul firmei sau al firmei din rețea, ca parte a unui serviciu, altul decât unul de asigurare, pe care echipa de audit se va baza când își va forma raționamentul ca parte a unui audit (punctul 600.14 A1).

Servicii indirecte

19. Creșterea numărului de servicii de tehnologie înseamnă o posibilitate crescută de apariție a unor servicii indirecte. De exemplu, când o firmă furnizează un software dezvoltat de firmă clienților care nu sunt clienți de audit, acești clienți pot, la rândul lor:

    - Să utilizeze soft-ul intern, fără a-l utiliza pentru a oferi servicii conexe propriilor lor clienți (lipsa serviciilor indirecte).
    - Să utilizeze soft-ul intern și să îl utilizeze pentru a furniza servicii conexe propriilor clienți (servicii indirecte, prevăzute la punctul 600.6(b)(ii)).
    - Să utilizeze soft-ul doar pentru a furniza servicii conexe propriilor clienți, fără a-l utiliza intern (servicii indirecte, prevăzute la punctul 600.6(b)(ii)).

20. Un astfel de software ar putea fi utilizat pentru a ajuta la implementarea și conformitatea cu un nou standard de raportare financiară. În astfel de circumstanțe, orice servicii indirecte ar putea crea o amenințare de autorevizuire, dacă întrunește criteriile prevăzute la punctul C600.15 din Cod și sunt interzise dacă sunt furnizate unui client de audit care este PIE (punctul C600.17). Când circumstanțele ar putea avea drept rezultat servicii indirecte furnizate către un client de audit non-PIE, firma ar trebui să identifice și să evalueze nivelul amenințării de autorevizuire care ar putea fi create și să determine dacă aceasta poate fi redusă la un nivel acceptabil.

21. Poate apărea o relație apropiată de afaceri când o firmă sau o firmă din rețea furnizează, vinde sau autorizează tehnologie către un client. Codul interzice relațiile apropiate de afaceri care sunt semnificative și oferă exemple de astfel de relații, generate în urma unei relații comerciale sau a unui interes financiar comun, la punctele 520.3 A2 și A3. Existența acestor relații de afaceri nu împiedică analiza măsurii în care se aplică cerințele și materialele privind aplicarea din Secțiunea 600, în funcție de fapte și circumstanțe.

Servicii de sisteme IT

22. Codul oferă exemple de factori specifici de luat în considerare în identificarea și evaluarea nivelului amenințărilor de autorevizuire la adresa independenței, create prin furnizarea unui serviciu de sisteme IT. Acești factori includ (punctul 606.4 A2):

    - Natura serviciului.
    - Natura sistemelor IT ale clientului și amploarea cu care serviciul de sisteme IT afectează sau interacționează cu înregistrările contabile ale clientului, cu controalele interne asupra raportării financiare sau cu situațiile financiare ale acestuia.
    - Gradul de credibilitate care va fi acordat acelor sisteme IT specifice, ca parte a auditului.

23. Exemplele de servicii de sisteme IT care crează o amenințare de autorevizuire când fac parte din sau afectează înregistrările contabile ale unui client de audit, sau sistemul intern asupra raportării financiare, includ (punctul 606.4 A3):

    - Proiectarea, elaborarea, implementarea, utilizarea, mentenanța, monitorizarea, actualizarea sau dezvoltarea sistemelor IT, inclusiv cele referitoare la securitatea cibernetică.
    - Sprijinirea sistemelor IT ale unui client de audit, inclusiv aplicațiile legate de rețea și de software.
    - Implementarea unui soft de raportare a informațiilor contabile sau financiare, fie că a fost dezvoltat sau nu de firmă sau de firma din rețea.

24. Pentru clienții de audit care sunt PIE, o firmă sau o firmă din rețea nu trebuie să furnizeze servicii de sisteme IT care ar putea crea o amenințare de autorevizuire (punctul C606.6).

25. Pentru clienții de audit non-PIE, Codul oferă, de asemenea, un exemplu de acțiune care ar putea constitui o

măsură de protecție pentru tratarea unei amenințări de autorevizuire, creată prin furnizarea de servicii de sisteme IT (punctul 606.5 A1).

Tehnologia, frecvența serviciilor și furnizarea de informații

26. Tehnologia poate fi utilizată într-un audit sau în furnizarea de servicii către un client (i) permițând o ofertă mai rapidă și mai frecventă de servicii, datorită automatizării și (ii) oferind informații mai sofisticate (de ex., prin instrumentele de inteligență artificială sau data analytics) în vederea analizării unui volum mare de seturi de date ale clientului.

27. Un factor relevant în identificarea și evaluarea diferitelor amenințări care ar putea fi create prin furnizarea unui serviciu, altul decât unul de asigurare, către un client de audit este dependența clientului de serviciu, inclusiv frecvența cu care va fi furnizat serviciul (punctul 600.10 A2). Dacă aceste servicii sau informații sunt furnizate frecvent de firmă clientului său de audit și sunt utilizate sau luate în considerare de client pentru a-și formula deciziile, sau în desfășurarea controalelor interne, care intră în responsabilitatea directă a conducerii, există un risc ca firma să își asume o responsabilitate de conducere (punctul 400.20 A3) sau să apară o amenințare de autorevizuire.

28. De exemplu, dacă o firmă efectuează evaluări de securitate cibernetică ce implică examinarea cadrului de raportare al clientului sau controalele interne, sau furnizează observații, în mod frecvent, iar aceste evaluări sau observații sunt luate în considerare de către conducerea clientului în monitorizarea controalelor interne sau în trasarea unei direcții strategice, este probabil că firma își asumă o responsabilitate de conducere sau este creată o amenințare de autorevizuire.

Tehnologia și confidențialitatea

29. Utilizarea tehnologiei (de ex., instrumentele de inteligență artificială sau data analytics) pentru a analiza un volum mare de seturi de date ale clientului va face ca firma să dețină datele clientului, dobândite pe parcursul relațiilor sale profesionale și de afaceri. Codul prevede cerințe și materiale privind aplicarea cu privire la responsabilitățile profesionistului contabil:

    - Când acesta dobândește astfel de informații (punctele C114.1 - C114.2)
    - Dacă acesta caută să utilizeze sau să divulge astfel de informații dobândite de la client (punctele C114.3 - 114.3 A3).

    De asemenea, Codul definește în glosar termenul de “informație confidențială”.

30. Când utilizează sau divulgă astfel de informații despre client, ar trebui acordată atenție, printre altele, și dacă sunt identificate conflicte de interese actuale sau posibile (Secțiunea 310).

APLICAREA CODULUI: EXEMPLE PRACTICE

SCENARIUL 1:
Furnizarea de servicii privind sistemele IT către un client de audit

31. În cadrul întâlnirii de planificare a auditului cu un client de audit, directorul financiar îi menționează partenerului de audit cum compania caută să facă un upgrade la suita de software. Directorul financiar explică cum suita de software pe care compania o folosește în prezent pentru vânzări și achiziții nu prevede o integrare automată cu registrul Cartea mare. Compania caută să angajeze un vânzător care să se asigure că ambele sisteme sunt integrate în vederea creșterii eficienței și acurateței proceselor de raportare financiară și ia în considerare

opțiuni de modificare a proceselor curente, fie prin: (i) înlocuirea întregii suite de software, sau (ii) prin personalizarea sistemelor existente, astfel încât acestea să fie integrate pe o interfață comună.

32. Directorul financiar îl informează pe partenerul de audit că există un singur angajat IT în cadrul companiei, responsabil pentru mentenanța sistemului curent de software și hardware. Deși acel angajat IT este un profesionist cu experiență, nu dispune de cunoștințele, aptitudinile sau expertiza necesare pentru a face un upgrade la întreaga suită de software a companiei.

33. Directorul financiar îl întreabă pe partenerul de audit dacă este disponibilă în cadrul firmei de audit o echipă de consultanță IT, care să sprijine compania cu transformarea acestui sistem. Serviciile ar implica dezvoltarea și implementarea sistemelor IT ale companiei, inclusiv îmbunătățirea controalelor interne IT. Funcționalitățile sistemului IT upgradat ar include vânzări și date sursă de achiziții integrate automat cu registrul Cartea mare, înregistrările contabile și situațiile financiare fiind generate automat de sistemul informatic.

Care sunt câteva considerente-cheie în aplicarea Codului?

Riscul asumării unei responsabilități de conducere

34. Deoarece angajatul IT al companiei nu dispune de aptitudinile, cunoștințele și expertiza necesare, compania nu poate lua deciziile care intră în responsabilitatea conducerii, cu privire la proiectarea, dezvoltarea, implementarea, utilizarea, mentenanța, monitorizarea, actualizarea sau upgradarea sistemului IT (punctul C606.3(b)). Prin urmare, există un risc ca firma să ia decizii cu privire la transformarea sistemului pentru companie, decizii care intră în responsabilitatea conducerii. Totuși, dacă angajatul IT, directorul financiar și alți directori seniori din cadrul companiei au, în moc colectiv, capacitatea de a supraveghea proiectul, de a lua decizii de conducere și de a evalua gradul de adecvare al sistemelor IT curente și propuse, firma poate concluziona că nu își va asuma o responsabilitate de conducere prin furnizarea acelui serviciu propus, altul decât unul de asigurare.

35. Chiar dacă serviciul propus, altul decât unul de asigurare, nu implică asumarea unei responsabilități de conducere pentru companie (punctul C606.3), firmei de audit tot i se solicită să aplice cadrul conceptual pentru a identifica, evalua și trata amenințările la adresa independenței, care pot apărea în urma furnizării de servicii de transformare a sistemelor către companie.

Identificarea și evaluarea amenințărilor

36. Partenerul de audit identifică trei amenințări la adresa independenței care pot apărea dacă firma furnizează serviciul, altul decât unul de asigurare – o amenințare de interes propriu și intimidare și o amenințare de autorevizuire:

- Amenințarea de interes propriu și intimidare – Raționamentul sau comportamentul partenerului de audit ar putea fi influențate necorespunzător dacă procentul onorariilor facturate clientului de audit de echipa de consultanță IT din cadrul firmei este mare în comparație cu onorariile de audit percepute. Aceasta datorită anumitor îngrijorări, de exemplu, în urma presiunilor interne referitoare la posibila pierdere a partenerului de misiune sau a altor servicii (punctul 410.11 A1).

  În acest scenariu, partenerul de audit ar putea determina că deși onorariile facturate clientului de audit pentru serviciile de transformare a sistemelor sunt mari în comparație cu onorariile de audit percepute, nivelul amenințărilor continuă să fie la un nivel acceptabil (punctul 410.11 A2). Aceasta deoarece transformarea sistemelor nu este un serviciu de natură repetitivă și durata în care acest procent mare al onorariilor aferente transformării sistemelor apare ca parte a onorariului de audit este doar de un an, în acest scenariu.

- Amenințarea de autorevizuire – Ar putea fi creată o amenințare de autorevizuire când (a) posibilul serviciu, altul decât unul de asigurare, prin care compania este ajutată să își upgradeze sistemele IT va implica proiectarea și implementarea soft-ului de sistem pentru clientul de audit, care va integra vânzările și achizițiile cu jurnalul Cartea mare al companiei, informațiile rezultate în urma sistemelor IT upgradate

vor face parte din sau vor afecta înregistrările contabile ale clientului, controlul intern asupra raportării financiare și situațiile financiare cu privire la care firma va exprima o opinie (punctul C600.15(a)) și (b) echipa de audit va avea nevoie, ca parte a auditului, să evalueze sau să se bazeze pe raționamentele exercitate sau pe activitățile efectuate de echipa de consultanță IT a firmei, când aceasta a proiectat și elaborat sistemul IT upgradat (punctul C600.15(b)). Aceasta deoarece informațiile rezultate în urma sistemului IT upgradat sunt influențate de activitățile efectuate de echipa de consultanță IT a firmei, când aceasta proiectează sau elaborează sistemul și implică cunoștințe, expertiză și raționamentul echipei de consultanță IT din cadrul firmei (punctul 300.6 A2).

Interzicerea amenințării de autorevizuire pentru clienții de audit PIE

37. Când compania este un client de audit PIE, iar serviciul, altul decât unul de asigurare, ar putea crea o amenințare de autorevizuire, partenerului de audit al firmei i se interzice să furnizeze un astfel de serviciu privind sistemele IT, pentru a veni în sprijinul companiei. Această interdicție s-ar aplica chiar dacă firma (inclusiv partenerul de audit) se asigură că membrii conducerii companiei exercită toate raționamentele și deciziile care intră în responsabilitatea conducerii, în conformitate cu prevederile din Cod (punctul C400.21).

Amenințările identificate sunt la un nivel acceptabil pentru clienții de audit non-PIE?

38. Cum amenințarea de autorevizuire identificată în urma serviciului propus, altul decât unul de asigurare, nu duce la o interdicție absolută pentru clienții de audit non-PIE, partenerul de audit al firmei trebuie să aplice cadrul conceptual pentru a evalua dacă amenințarea de autorevizuire identificată cu privire la conformitatea cu principiile fundamentale, inclusiv cele referitoare la independență, sunt la un nivel acceptabil sau dacă sunt disponibile măsuri de protecție ce ar putea fi aplicate pentru reducerea amenințărilor la un nivel acceptabil.

39. În acest scenariu, pe baza unei evaluări a faptelor și circumstanțelor și luând în considerare că serviciul propus de transformare a sistemului este probabil să aibă un efect semnificativ asupra situațiilor financiare și un impact puternic asupra înregistrărilor contabile ale companiei și controalelor interne asupra raportării financiare (punctele 600.10 A2 și 606.4 A2), partenerul de audit determină că amenințarea de autorevizuire nu este la un nivel acceptabil și trebuie tratată.

Tratarea amenințărilor pentru clienții de audit non-PIE

40. Amenințările care nu sunt la un nivel acceptabil sunt tratate fie prin: (i) eliminarea circumstanțelor care au creat amenințarea la adresa independenței, (ii) aplicarea de măsuri de protecție, când acestea sunt disponibile și pot fi aplicate, sau (iii) refuzul sau încetarea respectivei activități profesionale. Utilizarea testului unei terțe părți rezonabile și informate este relevant pentru concluzia generală a firmei când evaluează dacă acțiunile pe care intenționează să le întreprindă pentru a trata amenințările la adresa independenței vor fi adecvate pentru a le elimina sau reduce la un nivel acceptabil (punctul C120.11). De exemplu:

    (i) Poate firma să ajusteze domeniul de aplicare al serviciului propus, astfel încât să fie eliminate circumstanțele specifice care crează amenințarea? De exemplu, s-ar putea ca domeniul de aplicare al asistenței pe care o furnizează firma să fie restricționat, astfel încât să evite aspectele ce țin de dezvoltarea sau implementarea sistemului IT, aspecte care:

    - Fac parte din controlul intern al companiei asupra raportării financiare.
    - Implică generarea de informații pentru înregistrările contabile ale clientului sau situațiile financiare ale companiei.

    În acest scenariu, date fiind nevoile companiei și domeniul de aplicare al serviciului de transformare a sistemului IT pe care compania l-a solicitat din partea firmei, probabil această abordare nu va fi una practică.

    (ii) Poate firma să aplice o măsură de protecție care ar reduce la un nivel acceptabil amenințarea de autorevizuire? De exemplu, firma poate lua măsuri pentru a se asigura că membrii echipei care vor

furniza serviciul de transformare a sistemului nu vor face parte din echipa de audit (punctul 606.5 A1).

În acest scenariu, este probabil că o parte rezonabilă și informată va concluziona că nivelul amenințării de autorevizuire nu este unul acceptabil, chiar în urma aplicării unei măsuri de protecție, deoarece serviciul de transformare a sistemului are un efect semnificativ asupra situațiilor financiare și un impact puternic asupra înregistrărilor contabile ale companiei și a controalelor interne asupra raportării financiare (punctele 600.10 A2, 600.11 A1 și 606.4 A2).

(iii) Pentru motivele previzate la punctele (i) și (ii) de mai sus, este probabil că firma va decide să nu furnizeze serviciul, care nu este unul de asigurare, către companie, prin urmare compania va trebui să găsească un alt furnizor. Aceasta nu îl va împiedica pe partenerul de audit să poarte cu compania o discuție tehnică, ca parte a auditului, cu privire la gradul de adecvare a controlului financiar și contabil și al metodelor utilizate în determinarea sumelor precizate în situațiile financiare și în prezentările de informații conexe.

Concret, s-ar ajunge la aceeași concluzie dacă serviciul este considerat un serviciu de contabilitate și expertiză contabilă (Secțiunea 601) și nu un serviciu IT (Secțiunea 606), deoarece serviciul propus nu ar îndeplini criteriile de a reprezenta un serviciu de contabilitate și expertiză contabilă “de rutină sau de natură repetitivă„. Aceasta deoarece serviciul de transformare a sistemelor ar implica dezvoltarea și implementarea unor funcționalități IT upgradate care includ integrarea automată a datelor-sursă de vânzări și achiziții cu registrul Cartea mare și generarea de înregistrări contabile și situații financiare generate de sistem – care nu ar trece testul ce implică *“raționament profesional limitat sau lipsă.”* A se vedea punctele 62 și 63 de mai jos.

SCENARIUL 2:
Acordarea de licențe pentru programe IT ca sprijin în aplicarea standardelor contabile

41. Departamentul de servicii IT al unei firme a dezvoltat un program de software menit să asiste clienții în implementarea și conformitatea permanentă cu standardul contabil IFRS 17 *Contracte de asigurare*. Soft-ul poate fi personalizat individual, ca răspuns la nevoile clienților și generează informații în raport cu IFRS 17, care afectează înregistrările contabile, situațiile financiare și prezentările aferente. Departamentul de servicii IT al firmei acordă licența de utilizare a acestui program software, personalizat conform nevoilor specifice ale unei companii, clienților săi care nu sunt clienți de audit, pentru a-i sprijini în adoptarea pentru prima dată a IFRS 17.

42. Directorul financiar al clientului de audit al firmei este la curent cu existența acestui program și îl întreabă pe partenerul de audit despre posibilitatea primirii licenței pentru acest software. Partenerul de audit analizează dacă departementul de servicii IT al firmei ar putea să acorde licența utilizării acestui program software clientului său de audit și dacă ar putea furniza servicii de asistență permanentă, la nevoie sau pachete de actualizări aferente soft-ului.

Care sunt câteva considerente-cheie în aplicarea Codului?

Riscul asumării unei responsabilități de conducere

43. Pentru a preveni ca firma să își asume o responsabilitate de conducere când acordă licența de utilizare a soft-ului clientului său de audit, aceasta ar trebui să se asigure că acel client de audit a efectuat aranjamentele necesare ca responsabilitatea pentru deciziile și raționamentele de conducere să fie alocate unui angajat(unor angajați) cu competența corespunzătoare, care să evalueze caracterul adecvat al rezultatelor în urma folosirii soft-ului, să răspundă de funcționarea sistemului și să stabilească și mențină un sistem de controale interne (punctul C606.3). Disponibilitatea angajaților competenți ar putea diferi la clienții de audit PIE, față de clienții de audit non-PIE.

44. Această evaluare a caracterului adecvat al rezultatelor soft-ului ar putea include testarea a posteriori sau rularea în paralel a soft-ului de către clientul de audit și comparația cu metodologiile anterioare, astfel încât clientul de audit să poată evalua gradul de adecvare al soft-ului și să valideze rezultatele generate.

45. Firma nu își asumă nicio responsabilitate de conducere când persoana(persoanele) cu competența adecvată din cadrul clientului de audit exercită o supraveghere a procesului de personalizare a soft-ului și au capacitatea de a revizui și de evalua acuratețea rezultatelor generate de soft. Acest soft ar putea, de asemenea, fi sub forma unor fișiere Excel avansate. Pe de altă parte, dacă soft-ul este conceput ”ca o cutie neagră„ (black box) (adică este neclar cum sunt derivate rezultatele generate de soft) și clientul nu a fost implicat în raționamentul ce a stat la baza dezvoltării, este puțin probabil ca acesta să poată aloca responsabilitatea de luare a deciziilor și exercitare a raționamentelor de conducere cu privire la implementarea și conformitatea permanentă cu IFRS 17 unui (unor) anume angajat (angajați). Mai mult, dacă soft-ul ia o decizie (ce ține de expertiza sau raționamentul firmei) în generarea rezultatelor, sunt puține șanse ca conducerea să fie percepută drept cea care a luat toate deciziile ce intră în responsabilitatea sa, cu privire la implementarea și conformitatea cu IFRS 17.

46. Chiar dacă serviciul propus, care nu este unul de asigurare, nu implică asumarea unei responsabilități de conducere de către companie (punctul C606.3), firma de audit tot trebuie să aplice cadrul conceptual pentru a identifica, evalua și trata amenințările la adresa independenței ce pot apărea în urma acordării unei licențe aferente programului software (punctul 600.6(b)).

Identificarea și evaluarea amenințărilor

47. Firma identifică următoarele amenințări la adresa independenței care ar putea apărea în urma acordării unei licențe de către firmă unui client de audit, pentru utilizarea unui software – o amenințare de interes propriu și intimidare și o amenințare de autorevizuire:

- Amenințarea de interes propriu și intimidare – Raționamentul sau comportamentul partenerului de audit ar putea fi influențate în mod necorespunzător dacă procentul de onorarii aferente acordării licenței, perceput de departamentul de servicii IT al firmei clientului de audit este mare în comparație cu onorariile de audit facturate. Cauza ar putea fi îngrijorările rezultate, de exemplu, în urma presiunilor interne cu privire la posibila pierdere a misiunii de audit sau a altor servicii (punctul 410.11 A1).

  În acest scenariu, partenerul de audit ar putea determina că posibilele amenințări identificate cu privire la furnizarea serviciului sunt la un nivel acceptabil, deoarece procentul onorariilor aferente acordării licenței, care ar putea fi percepute de la clientul de audit, nu sunt mari în comparație cu onorariile de audit facturate.

- Amenințarea de autorevizuire – Ar putea fi creată o amenințare de autorevizuire deoarece (a) soft-ul îl sprijină pe client în implementarea și conformitatea permanentă cu IFRS 17, rezultatele generate de soft făcând parte din, sau afectând, înregistrările contabile și situațiile financiare ale clientului de audit, inclusiv prezentările de informații aferente și controlul intern asupra raportării financiare (punctul C600.15(a)) și (b) echipa de audit va trebui, ca parte a auditului, să evalueze sau să se bazeze pe raționamentele exercitate sau pe activitățile desfășurate de firmă când aceasta a proiectat sau a dezvoltat soft-ul (punctul C600.15(b)). Aceasta deoarece rezultatul generat de software (de ex., calculul și raportarea contractelor de asigurare ale companiei, în conformitate cu IFRS 17) este influențat de modul în care un astfel de soft a fost proiectat și dezvoltat, ceea ce implică cunoștințe, expertiză și raționament din partea departamentului de servicii IT al firmei (punctul 300.6 A2).

  În mod similar, din moment ce serviciul aflat în discuție generează o amenințare de autorevizuire, serviciul de asistență permanentă ar însemna că amenințarea de autorevizuire va continua să existe (punctul 606.4 A3) deoarece (a) rezultatele generate de soft vor face parte din, sau vor afecta, înregistrările contabile și situațiile financiare ale clientului de audit, inclusiv prezentările de informații aferente și controlul intern asupra raportării financiare (punctul C600.15(a)) și (b) echipa de audit va

trebui, ca parte a auditului, să evalueze sau să se bazeze pe raționamentele exercitate sau pe activitățile desfășurate de către firmă când abordează aspectele care apar sau actualizările necesare ale soft-ului (punctul C600.15(b)).

Interdicția amenințării de autorevizuire pentru clienții de audit PIE

48. Dacă clientul de audit este o entitate de interes public (PIE), dat fiind că serviciul, altul decât unul de asigurare, ar putea crea o amenințare de autorevizuire, partenerului de audit al firmei i se interzice să acorde licența unui program software care să sprijine compania. Această interdicție s-ar aplica și când firma (inclusiv partenerul de audit) s-a asigurat că toate raționamentele și deciziile care intră în responsabilitatea conducerii sunt luate de către conducerea companiei, în conformitate cu prevederile Codului (punctul C400.21).

Amenințările identificate sunt la un nivel acceptabil pentru clienții de audit non-PIE?

49. Cum amenințarea de autorevizuire identificată în urma serviciului propus, altul decât unul de asigurare, nu generează o interdicție absolută pentru clienții de audit non-PIE, partenerul de audit al firmei trebuie să aplice cadrul conceptual pentru a evalua dacă amenințarea de autorevizuire identificată privind conformitatea cu principiile fundamentale, inclusiv cu principiile de independență, este la un nivel acceptabil sau dacă sunt disponibile măsuri de protecție ce ar putea fi aplicate în vederea reducerii sale la un nivel acceptabil.

50. În cazul în care contractele de asigurare calculate și raportate de soft sunt nesemnificative pentru situațiile financiare ale companiei, amenințarea de autorevizuire ar putea fi la un nivel acceptabil, deoarece impactul sau interacțiunea soft-ului și a rezultatelor generate de acesta asupra înregistrărilor contabile ale clientului, controalelor interne asupra raportării financiare sau situațiilor financiare, sau gradul de încredere acordat soft-ului ca parte a auditului, ar fi nesemnificative. Totuși, în cazul în care contractele de asigurare calculate și raportate de soft sunt semnificative pentru situațiile financiae, atunci este puțin probabil ca nivelul amenințării de autorevizuire să fie la un nivel acceptabil (punctele 600.10 A2, 600.11 A1 și 606.4 A2).

Abordarea amenințărilor pentru clienții de audit non-PIE

51. Amenințările care nu sunt la un nivel acceptabil sunt tratate fie prin: (i) eliminarea circumstanțelor care generează amenințarea la adresa independenței, (ii) aplicarea de măsuri de protecție, dacă sunt disponibile și pot fi aplicate, sau (iii) refuzarea și încetarea respectivei activități profesionale. Utilizarea testului unei terțe părți rezonabile și informate este relevantă pentru concluzia general exprimată de firmă în evaluarea măsurii în care acțiunile pe care intenționează să le întreprindă pentru a trata amenințările la adresa independenței vor fi adecvate pentru a le elimina sau reduce la un nivel acceptabil (punctul C120.11). De exemplu:

    (i) Firma are capacitatea de a ajusta domeniul de aplicare al serviciului propus, astfel încât circumstanțele specifice care generează amenințarea să fie eliminate? De exemplu, cum soft-ul este personalizabil, domeniul de aplicare al soft-ului pentru care firma acordă licența clientului său de audit ar putea fi restricționat, astfel încât soft-ul și rezultatele pe care le generează să nu:

    - Facă parte din controlul intern asupra raportării financiare a companiei.
    - Implice generarea de informații cu privire la înregistrările contabile ale clientului sau situațiile financiare ale companiei.

    În acest scenariu, având în vedere nevoile companiei și domeniul de aplicare al implementării IFRS 17 și al serviciului de conformitate pe care compania l-a propus firmei, este puțin probabil ca aceasta să fie o abordare practică.

    (ii) Firma are capacitatea de a aplica o măsură de protecție care ar reduce la un nivel acceptabil amenințarea de autorevizuire? De exemplu, firma ar putea întreprinde măsuri pentru a se asigura că membrii echipei implicați în dezvoltarea programului software și care ar furniza acordarea licenței și serviciile de asistență permanentă nu ar fi membri ai echipei de audit (punctul 606.5 A1).

    În acest scenariu, o parte terţă rezonabilă şi informată ar concluziona că amenințarea de autorevizuire

nu este la un nivel acceptabil, chiar dacă este aplicată o măsură de protecție, deoarece contractele de asigurare calculate și raportate de software sunt semnificative pentru situațiile financiare ale companiei (punctele 600.10 A2, 600.11 A1 și 606.4 A2).

(iii) Din motivele prevăzute la punctele (i) și (ii) de mai sus, probabil că firma ar decide să nu furnizeze sau să vândă sau să acorde licența software clientului său de audit.

Concret, s-ar ajunge la aceeași concluzie dacă serviciul este considerat un serviciu de contabilitate și evidență contabilă (Secțiunea 601) și nu un serviciu de sisteme IT (Secțiunea 606), deoarece serviciul propus nu ar îndeplini criteriul de a reprezenta un serviciu de contabilitate și evidență contabilă "de rutină sau de natură repetitivă". Aceasta deoarece clientul nu a fost implicat în exercitarea raționamentelor necesare sau a deciziilor cu privire de dezvoltarea programului de software IFRS 17 preexistent pentru clienții săi, în general, și este puțin probabil ca adoptarea pentru prima dată a IFRS 17 să treacă testul ce implică *"raționament profesional limitat sau lipsă.„* A se vedea punctele 62 și 63 de mai jos.

SCENARIUL 3:

Procese automatizate și procese "de rutină sau de natură repetitivă„

52. Directorul general al unei companii a rugat firma de audit să întocmească situațiile financiare ale companiei de la sfârșitul exercițiului. Directorul financiar al companiei și-a dat demisia spre sfârșitul exercițiului financiar. Deși personalul financiar rămas poate asigura intrarea datelor în sistemele contabile ale companiei, acesta nu deține experiența sau cunoștințele de a compila situațiile financiare de la sfârșitul exercițiului.

53. Firma dispune de un software care are capacitatea de a interoga înregistrările și sistemele contabile ale companiei, de a extrage și recoda registrul în sistemul firmei, de a face ajustări ale intrărilor în registru și apoi de a popula un set proforma de situații financiare. Directorul general sugerează ca personalul firmei să revizuiască situațiile financiare generate de computer și orice intrări în registru generate pe parcursul acestui proces. Situațiile financiare pot fi apoi prezentate directorului general și altor membri ai conducerii companiei, pentru aprobare.

54. Firma de audit analizează dacă să furnizeze acest serviciu de contabilitate și evidență contabilă[5] clientului său de audit.

Care sunt câteva considerente-cheie în aplicarea Codului?

Riscul asumării unei responsabilități de conducere

55. În acest scenariu, deși ar putea părea că soft-ul întocmește "automat„ situațiile financiare și generează ajustări ale intrărilor în registru, firma ar trebui să fi luat decizii de programare referitoare la dezvoltarea sistemului software, inclusiv cu privire la modul în care situațiile din registrul Cartea mare sunt preluate în situațiile financiare.

56. Mai mult, compania nu are un angajat care să dispună de aptitudinile, cunoștințele și experiența de a supraveghea și evalua gradul de adecvare al situațiilor financiare și firma ar raporta direct către persoanele responsabile cu guvernanța (de. ex., directorul general al companiei) în numele conducerii.

57. În consecință, probabil că firma ar prelua responsabilitatea de luare a deciziilor și ipotezelor atunci când

[5] Serviciile de contabilitate și evidență contabilă cuprind o gamă largă de servicii, inclusiv (punctul 601.3 A1):
- Întocmirea registrelor contabile și a situațiilor financiare.
- Înregistrarea tranzacțiilor.
- Furnizarea de servicii de salarizare.
- Soluționarea problemelor privind reconcilierea registrelor.
- Convertirea situațiilor financiare existente de la un cadru de raportare financiară la altul.

programează soft-ul și raportează către persoanele responsabile cu guvernanța companiei (punctul 400.20 A3). Prin urmare, ar fi interzisă furnizarea acestui serviciu propus de contabilitate și evidență contabilă.

58. Pentru a preveni ca firma să își asume responsabilități de conducere în relație cu situațiile financiare, aceasta se poate asigura că membrii conducerii companiei exercită toate raționamentele și iau toate deciziile care intră în responsabilitatea directă a conducerii. Aceasta include asigurarea ca membrii conducerii clientului (punctul C400.21):

- Să desemneze o persoană(persoane) cu aptitudinile, cunoștințele și experiența corespunzătoare pentru a răspunde la orice moment de deciziile clientului și pentru a supraveghea activitățile.
- Să exercite supravegherea activităților și să evalueze gradul de adecvare al rezultatelor activităților desfășurate în scopul clientului.
- Să își asume responsabilitatea pentru acțiunile, dacă există, ce ar fi luate în urma rezultatelor activităților.

De exemplu, aceasta ar putea însemna ca membrii conducerii clientului să îi furnizeze firmei manuale și proceduri ce prezintă principiile – cheie care ar sta la baza sistemului contabil al clientului când firma programează soft-ul, sau ca directorul general al companiei sau alte persoane din conducere sau o combinație a acestora să dispună de aptitudinile, cunoștințele și experiența corespunzătoare pentru a supraveghea activitățile (de .ex., prin revizuirea modului de identificare a conturilor în capturile situațiilor financiare, înainte ca firma să configureze soft-ul), sau ca membrii conducerii clientului să revizuiască și să aprobe situațiile financiare și rezultatele generate de soft cu privire la intrările ajustate în registru, înainte de a fi raportate către directorul general, etc.

59. Chiar dacă acest serviciu de contabilitate și evidență contabilă nu implică asumarea unei responsabilități de conducere de către companie (punctele 601.2 A1 și C400.21), firma de audit tot trebuie să aplice cadrul conceptual pentru a identifica, evalua și trata amenințările la adresa independenței care ar putea apărea în urma furnizării serviciului de contabilitate și evidență contabilă către companie.

Servicii de contabilitate și evidență contabilă

60. Firma de audit identifică trei amenințări la adresa independenței care ar putea apărea dacă firma furnizează serviciul – o amenințare de interes propriu și intimidare și o amenințare de autorevizuire:

- Amenințarea de interes propriu și intimidare – Raționamentul sau comportamentul partenerului de audit ar putea fi influențate necorespunzător dacă procentul de onorarii percepute de la clientul de audit pentru serviciul de contabilitate și evidență contabilă este mare în comparație cu onorariile de audit facturate. Aceasta s-ar putea datora unor îngrijorări, de exemplu rezultate în urma presiunilor interne cu privire la posibila pierdere fie a misiunii de audit, fie a altor servicii (punctul 410.11 A1).

  În acest scenariu, partenerul de audit determină că amenințările posibile identificate cu privire la furnizarea serviciului sunt la un nivel acceptabil, deoarece procentul onorariilor pentru serviciul de contabilitate și evidență contabilă care ar putea fi perceput de la clientul de audit nu este mare în comparație cu onorariile de audit facturate.

- Amenințarea de autorevizuire – O amenințare de autorevizuire ar putea fi creată dacă (a) rezultatele generate de soft vor face parte sau vor afecta înregistrările contabile și situațiile financiare ale clientului de audit, inclusiv prezentările de informații aferente și controlul intern asupra raportării financiare (punctul C600.15(a)) și (b) echipa de audit va trebui, ca parte a auditului, să evalueze sau să se bazeze pe raționamentele exercitate sau pe activitățile desfășurate de firmă când a proiectat sau dezvoltat soft-ul (punctul C600.15(b)). Aceasta deoarece rezultatul serviciului de contabilitate și evidență contabilă este influențat de modul în care aceste procese asistate de computer sunt proiectate și dezvoltate, ceea ce implică cunoștințe, expertiză și raționament din partea departamentului de servicii IT al firmei (punctul 300.6 A2).

Interdicția serviciilor de contabilitate și evidență contabilă pentru clienții de audit PIE

61. Când compania este o entitate de interes public (PIE), firmei i se interzice să furnizeze astfel de servicii de contabilitate și evidență contabilă unui client de audit PIE (punctul C601.6).

Servicii de rutină sau de natură repetitivă pentru clienții de audit non-PIE

62. Când compania nu este o entitate de interes public (PIE), firmei tot i se interzice să furnizeze astfel de servicii de contabilitate și evidență contabilă unui client de audit non-PIE, cu excepția cazului în care aceste servicii sunt de rutină sau de natură repetitivă. Dacă serviciile sunt de rutină sau de natură repetitivă, auditorul tratează orice amenințări la adresa independenței care nu sunt la un nivel acceptabil și se asigură că firma nu își asumă o responsabilitate de conducere cu privire la serviciu (punctele C601.5 și 601.5 A3).

63. Serviciile de contabilitate și evidență contabilă care sunt de rutină sau de natură repetitivă implică informații, date sau materiale cu privire la care clientul și-a exercitat orice raționamente și a luat orice decizii necesare și care presupun un raționament profesional limitat sau lipsă. Pentru a determina dacă un serviciu automatizat de contabilitate și evidență contabilă este de rutină sau de natură repetitivă, factorii de luat în considerare includ activitățile și rezultatele acestora efectuate prin intermediul tehnologiei și dacă tehnologia furnizează un serviciu automatizat care are la bază sau necesită expertiza sau raționamentul firmei sau al firmei din rețea (punctele 601.5 A1 și A2).

64. În acest scenariu, firma a stabilit procese asistate de computer care le permit programelor de soft ale firmei să întocmească ”automat„ situațiile financiare, inclusiv intrările necesare de ajustare în registru. Probabil că firma a luat decizii cu privire la programare, legate de dezvoltarea întregului sistem software, stabilind inclusiv modul în care conturile generale din registru sunt preluate în situațiile financiare, precum și în revizuirea de către firmă a intrărilor în registru, cu scop de ajustare.

65. În consecință, probabil că partenerul de audit va concluziona că serviciul propus de contabilitate și evidență nu a îndeplinit criteriul de a fi “de rutină sau de natură repetitivă„ și, prin urmare, este interzisă furnizarea serviciului către un client de audit non-PIE.

Despre APESB

Consiliul pentru Standarde Profesionale de Contabilitate și Etică (APESB) a fost înființat în 2006 ca organism național independent de elaborare de standarde în Australia, având ca obiectiv principal elaborarea de standarde profesionale de contabilitate și etică în interes public pentru membrii celor trei organisme profesionale contabile din Australia și anume Contabili Autorizați Australia și Noua Zeelandă, CPA Australia și Institutul Contabililor Publici. Cele trei organisme profesionale contabile sunt membre ale APESB.

Despre IESBA

Consiliul pentru Standarde Internaționale de Etică pentru Contabili (IESBA) este un organism global independent de elaborare de standarde. Misiunea IESBA este de a servi interesul public prin instituirea de standarde de etică, inclusiv cerințe privind independența, ca piatră de temelie a comportamentului etic în mediul de afaceri și în cadrul companiilor, și a încrederii publice în informațiile financiare și non-financiare care sunt fundamentale pentru funcționarea adecvată și sustenabilitatea organizațiilor, piețelor financiare și economiilor din întreaga lume.

Alături de Consiliul pentru Standarde Internaționale de Audit și Asigurare (IAASB), IESBA este parte a Fundației Internaționale pentru Etică și Audit (IFEA).

PERSOANE DE CONTACT

Channa Wijesinghe, Director executiv APESB channa.wijesinghe@apesb.org.au

Jacinta Hanrahan, Director APESB jacinta.hanrahan@apesb.org.au

Ken Siong, Director de program și director tehnic senior IESBA kensiong@ethicsboard.org

Kam Leung, Director IESBA kamleung@ethicsboard.org

MULȚUMIRI

Echipa este recunoscătoare pentru îndrumările importante și feed-back-ul primit de la evaluatorii independenți pe parcursul elaborării acestei publicații cu rol orientativ: Jacinta Hanrahan și Channa Wijesinghe din partea APESB; David Clark, Brian Friedrich, Diane Jules, Kam Leung și Ken Siong din partea Grupului de lucru Tehnologie Faza 2 al IESBA; James Barbour, Greg Driscoll, Richard Fleck, Hironori Fukukawa, Rich Huesken și Luigi Nisoli ca membri ai Grupului Operativ Tehnologie al IESBA; Saadiya Adam, Mark Babington, Keith Billing, Marta Kramerius și Andrew Pinkney ca membri sau consilieri tehnici IESBA; Caroline Lee ca fost vice-președinte IESBA și Jason Bradley, Director Tehnologia Asigurării în cadrul Consiliului de Raportare Financiară din Marea Britanie și membru al grupului de experți în tehnologie al IESBA.