JULY 2023

APPLYING THE CODE'S CONCEPTUAL FRAMEWORK TO INDEPENDENCE:

PRACTICAL GUIDANCE FOR AUDITORS IN TECHNOLOGY-RELATED SCENARIOS

IESBA International Ethics Standards Board for Accountants®

APESB Accounting Professional & Ethical Standards Board

CONTENTS

INTRODUCTION

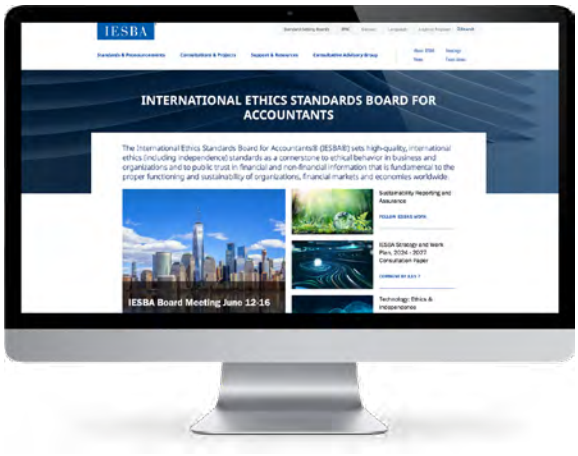
1. This non-authoritative publication was developed jointly by the Staff of the APESB and IESBA under the auspices of the IESBA's Technology Task Force, initiated as part of the IESBA's Phase 2 Technology Working Group activities.

2. Technology creates many opportunities for professional accountants (PAs), but its use can also create threats to compliance with the *International Code of Ethics for Professional Accountants (Including International Independence Standards)* (the Code).[1]

3. This publication considers how technology intersects with auditor independence and provides PAs in public practice with three practical examples of how to apply the Code's requirements, including the conceptual framework, in such scenarios. The scenarios are hypothetical and are intended to provide an aid to illustrate the thought process when applying the Code. The analyses in this publication reflect the facts and circumstances set out in the scenarios and do not preclude the need to consider any new information or changes to the facts and circumstances that might affect a PA's evaluation of the conclusions reached.

4. For illustrative purposes, the scenarios also anticipate that the following revisions to the Code have already been early adopted and implemented:

- *Definitions of Listed Entity and Public Interest Entity* (effective for audits of financial statements for periods beginning on or December 15, 2024);
- *Technology-related Revisions* (effective for audits and reviews of financial statements for periods beginning on or after December 15, 2024, and as of December 15, 2024 for the other revisions to the ethics provisions of the Code); and
- *Definition of Engagement Team and Group Audits* (effective for audits of financial statements and group financial statements for periods beginning on or after December 15, 2023).



5. This publication does not amend or override the Code, the text of which alone is authoritative. Reading this publication is not a substitute for reading the Code. The guidance in this publication is not meant to be exhaustive and reference to the Code itself should always be made. This publication does not constitute an authoritative or official pronouncement of APESB or the IESBA.

6. Professional accountants need to take into consideration that some jurisdictions might have provisions that differ from or go beyond those set out in the Code. In these jurisdictions, accountants need to be aware of those differences and comply with the more stringent provisions unless prohibited by law or regulation.

[1] As set out in the 2022 Edition of the Code, including approved revisions relating to the: *Definitions of Listed Entity and Public Interest Entity*, the *Technology-related Revisions* and *Definition of Engagement Team and Group Audits*

SUMMARY OF KEY RELEVANT TECHNOLOGY-RELATED CODE PROVISIONS

Prohibition on Assuming Management Responsibilities, Including for Certain IT Systems Services

7. A firm or a network firm is prohibited from assuming management responsibility for an audit client (paragraph R400.20). This prohibition applies to the provision of non-assurance services (NAS) to all audit clients, whether they are public interest entities (PIEs) or not public interest entities (non-PIEs).

8. Management responsibilities involve controlling, leading, and directing an entity, including making decisions regarding the acquisition, deployment and control of human, financial, technological, physical and intangible resources (paragraph 400.20 A1). Therefore, when performing a professional activity for an audit client, the Code requires the firm to be satisfied that client management makes all judgments and decisions that are the proper responsibility of management (paragraph R400.21).

IT Systems Services[2]

9. In order not to assume a management responsibility when providing IT system services, the firm must be satisfied that (paragraph R606.3):

(a) The audit client acknowledges its responsibility for establishing and monitoring internal control systems;

(b) The audit client, through a competent individual (or individuals), preferably within senior management, makes all management decisions that are the proper responsibility of management with respect to the design, development, implementation, operation, maintenance, monitoring, updating or upgrading of the IT system;

(c) The audit client evaluates the adequacy and results of the design, development, implementation, operation, maintenance, monitoring, updating or upgrading of the IT system; and

(d) The audit client takes responsibility for operating the IT system and for the data it generates and uses.

10. The Code also sets out examples of IT systems services that involve an assumption of management responsibility and would therefore be prohibited for all audit clients (paragraph 606.3 A1). Such services include where a firm or a network firm:

- Stores data or manages (directly or indirectly) the hosting of data on behalf of the audit client; and
- Operates, maintains, or monitors the audit client's IT systems, network or website.

11. However, the Code acknowledges that the collection, receipt, transmission and retention of data provided by an audit client in the course of an audit or to enable the provision of a permissible service to that client does not result in an assumption of management responsibility (paragraph 606.3 A2).

[2] IT systems services comprise a broad range of services including (paragraph 606.2 A1):
- Designing or developing hardware or software IT systems.
- Implementing IT systems, including installation, configuration, interfacing, or customization.
- Operating, maintaining, monitoring, updating or upgrading IT systems.
- Collecting or storing data or managing (directly or indirectly) the hosting of data.

Providing Non-Assurance Services to an Audit Client, Including Certain IT Systems Services

12. Providing NAS to audit clients might create threats to compliance with the fundamental principles and threats to independence. Before a firm or a network firm accepts an engagement to provide a NAS to an audit client that is not expressly prohibited under the Code, that firm is required to apply the conceptual framework to identify, evaluate and address any threat to independence that might be created by providing that service (paragraph R600.9).

13. The application of the conceptual framework involves having an inquiring mind, exercising professional judgment, and using the reasonable and informed third party test (paragraph R120.5). If a threat to the fundamental principles and/or independence is not at an acceptable level, and that threat cannot be eliminated or there are no safeguards to reduce it to an acceptable level, the firm is required to decline or end the service (paragraph R120.10).[3]

14. The *Exploring the IESBA Code* publication series, in particular instalments 1-5, provide additional guidance to assist in applying the Code's conceptual framework to comply with the fundamental principles and independence. Perceived or actual threats to compliance with the fundamental principles and independence might also impact the audit team's exercise of professional skepticism (paragraphs 120.15 A1 and 120.16 A2).

15. The Code contains specific provisions to assist firms when identifying, evaluating, and addressing threats to independence that are created by providing a NAS to an audit client (Section 600). Materiality is a factor that is relevant in evaluating threats created by providing a NAS to an audit client (paragraph 600.11 A1). However, where the Code expressly prohibits the provision of a NAS to an audit client, a firm or a network firm is not permitted to provide that service, regardless of the materiality of the outcome or results of the NAS on the financial statements on which the firm will express an opinion (paragraph 600.11 A2).

16. In particular, before providing a NAS to an audit client, a firm or a network firm is required to determine whether the provision of that NAS might create a self-review threat[4] by evaluating whether there is a risk that (paragraph R600.15):

(a) The results of the NAS will form part of or affect the accounting records, the internal controls over financial reporting, or the financial statements on which the firm will express an opinion; and

(b) In the course of the audit of those financial statements on which the firm will express an opinion, the audit team will evaluate or rely on any judgments made or activities performed by the firm or network firm when providing the NAS.

17. For a PIE audit client, if the firm determines that the provision of the NAS might create a self-review threat in relation to the audit of the financial statements on which the firm will express an opinion, the firm is prohibited from providing the NAS (paragraph R600.17) regardless of materiality. Refer also to the *IESBA Staff Questions & Answers (Q&A): Revised NAS Provisions of the Code*.

18. The requirements and application material relevant to firms when they consider the provision of a NAS to an audit client also apply where a firm or a network firm (paragraph 600.6):

(a) Uses technology to provide a NAS to an audit client; or

(b) Provides, sells, resells or licenses technology resulting in the provision of a NAS by the firm or a network firm:

(i) To an audit client; or

(ii) To an entity that provides services using such technology to audit clients of the firm or network firm.

[3] If the PA becomes aware of new information or changes in facts and circumstances that might impact whether a threat has been eliminated or reduced to an acceptable level, the PA shall re-evaluate and address that threat accordingly (paragraphs R120.9 to 120.9 A2).

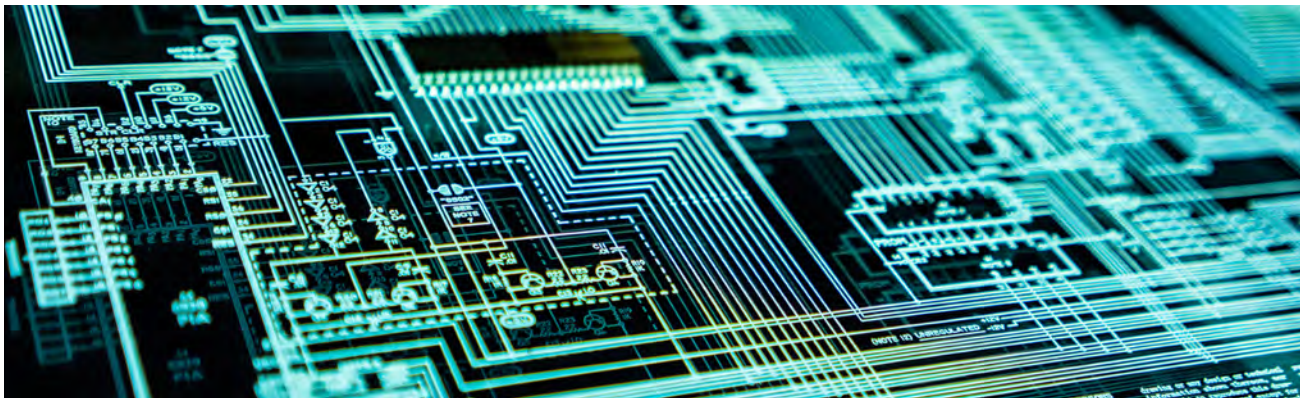
[4] A self-review threat is the threat that a firm or a network firm will not appropriately evaluate the results of a previous judgment made or an activity performed by an individual within the firm or network firm as part of a NAS on which the audit team will rely when forming a judgment as part of an audit (paragraph 600.14 A1).

Indirect Services

19. The increase in technology-related services means that there is an increased possibility that indirect services may occur. For example, where a firm provides a firm-developed software to customers that are non-audit clients, such customers may:

- Only use the software internally, without using it to provide related services to their own customers (no indirect services).
- Use the software internally and also to provide related services to their own customers (indirect services captured under paragraph 600.6(b)(ii)).
- Only use the software to provide related services to their own customers, without using the software internally (indirect services captured under paragraph 600.6(b)(ii)).

20. Such software might, for example, be used to assist in the implementation of, and compliance with, a new financial reporting standard. In such circumstances, any indirect service might create a self-review threat if the criteria set out in paragraph R600.15 of the Code are met, and would therefore be prohibited if the audit client is a PIE (paragraph R600.17). Where circumstances might result in indirect services to a non-PIE audit client, the firm should identify and evaluate the level of self-review threat that might be created and determine whether such threat can be reduced to an acceptable level.



21. A close business relationship might arise where a firm or a network firm provides, sells, or licenses technology to a client. The Code prohibits close business relationships that are material and significant. It also sets out examples of close business relationships arising from a commercial relationship or common financial interest in paragraphs 520.3 A2 and A3. The existence of such business relationships does not preclude the consideration of whether the requirements and application material in Section 600 apply, taking into account the facts and circumstances.

IT Systems Services

22. The Code provides examples of specific factors to consider in identifying and evaluating the level of self-review threat to independence created by providing an IT systems service. Such factors include (paragraph 606.4 A2):

- The nature of the service.
- The nature of the client's IT systems and the extent to which the IT systems service impacts or interacts with the client's accounting records, internal controls over financial reporting or financial statements.
- The degree of reliance that will be placed on the particular IT systems as part of the audit.

23. Examples of IT systems services that create a self-review threat when they form part of or affect an audit client's accounting records or internal controls over financial reporting include (paragraph 606.4 A3):

- Designing, developing, implementing, operating, maintaining, monitoring, updating or upgrading IT systems, including those related to cybersecurity.
- Supporting an audit client's IT systems, including network and software applications.
- Implementing accounting or financial reporting software, whether or not it was developed by the firm or a network firm.

24. For PIE audit clients, a firm or a network firm is prohibited from providing IT systems services that might create a self-review threat (paragraph R606.6).

25. For non-PIE audit clients, the Code also provides an example of an action that might be a safeguard to address a self-review threat created by the provision of an IT systems service (paragraph 606.5 A1).

Technology, Frequency of Services and Provision of Insights

26. Technology may be used in an audit or the provision of services to a client by (i) enabling a quicker or more frequent delivery of services through automation, and (ii) providing more sophisticated insights (e.g., using AI or data analytics tools) to analyze large datasets of the client.

27. A factor relevant in identifying and evaluating the different threats that might be created by a NAS to an audit client is the client's dependency on the service, including the frequency with which the service will be provided (paragraph 600.10 A2). If such services or insights are provided by the firm to its audit client frequently and are used or relied upon by the client to form the basis of decisions, or in the execution of internal controls, that are the proper responsibility of management, there is a risk of the firm assuming management responsibility (paragraph 400.20 A3) or creating a self-review threat.

28. For example, if a firm performs cybersecurity assessments that involve consideration of the client's reporting framework or internal controls, or provides observations, on a frequent basis where such assessments or observations are being relied upon by client management in monitoring internal controls or setting strategic direction, the firm is likely to assume management responsibility or create a self-review threat.

Technology and Confidentiality

29. The use of technology (e.g., AI or data analytics tools) to analyze large client datasets will result in the firm holding client data acquired in the course of its professional and business relationships. The Code sets out requirements and application material regarding PAs' responsibilities:

- When they acquire such information (paragraphs R114.1 to R114.2).
- If they seek to use or disclose such client information (paragraphs R114.3 to 114.3 A3).

The Code also defines what is "confidential information" in the glossary.

30. When using or disclosing such client information, among other matters, consideration should also be given to whether there is any actual or perceived conflicts of interest (Section 310).

APPLYING THE CODE: PRACTICAL EXAMPLES

SCENARIO 1:

Provision of IT Systems Services to an Audit Client

31 At the audit planning meeting with an audit client, the finance manager mentions to the audit partner that her company is looking to upgrade its software suite. The finance manager explains that the software suite that the company currently uses for sales and purchases does not automatically integrate with the general ledger. The company is looking to hire a vendor to help ensure that both systems are integrated to improve the efficiency and accuracy of the financial reporting processes. The company is considering options to change its current process by either replacing the entire software suite or customizing the existing software systems so that they can better interface with each other.

32 The finance manager informs the audit partner that the company has only one IT employee responsible for maintaining the company's current IT system software and its hardware. Although that IT employee is an experienced professional, they do not have the relevant expertise, skills or experience needed to upgrade the company's entire software suite.

33 The finance manager asks the audit partner whether an IT consulting team is available at the audit firm to assist the company with such system transformation. The service would involve designing and implementing the company's IT systems, including improving IT-related internal controls. The upgraded IT system's functionalities would include automatically integrating sales and purchases source data with the general ledger and producing system-generated accounting records and financial statements.

What Are Some Key Considerations When Applying the Code?

Risk of Assuming a Management Responsibility

34. As the company's IT employee does not possess suitable skills, knowledge and experience, the company cannot make the decisions that are the proper responsibility of management with respect to the design, development, implementation, operation, maintenance, monitoring, updating or upgrading of the IT system (paragraph R606.3(b)). Therefore, there is a risk that the firm might make the decisions over the system transformation being performed for the company that are the proper responsibility of management. However, if the IT employee, finance manager, and other senior executives at the company, collectively have the capabilities to oversee the project, make management decisions, and assess and evaluate the adequacy of the current and proposed IT systems, the firm might conclude that it would not assume a management responsibility by providing the proposed NAS.

35. Even if the proposed NAS does not involve assuming a management responsibility for the company (paragraph R606.3), the audit firm is still required to apply the conceptual framework to identify, evaluate and address threats to independence that might arise from providing the company with a systems transformation service.

Identifying and Evaluating Threats

36. The audit partner identifies three threats to independence that might arise if the firm provides the NAS – a self-interest, intimidation and a self-review threat:

- Self-interest and Intimidation – The audit partner's judgment or behavior might be inappropriately influenced if the proportion of the fees charged by the firm's IT consulting team to the audit client is large in comparison to the audit fees charged. This could be due to concerns, for example resulting from internal pressures, about the potential loss of either the audit engagement or other services provided to the audit client (paragraph 410.11 A1).

  In this scenario, the audit partner might determine that although the fees charged to the audit client for the systems transformation service are large in comparison to the audit fees, the level of threats is still at an acceptable level (paragraph 410.11 A2) because the systems transformation is not a recurring service, and the relatively short time during which this large proportion of fees for the systems transformation to the audit fee exists, which is one year in this scenario.

- Self-review – A self-review threat is created as (a) the potential NAS to assist the company with upgrading its IT systems will involve designing and implementing a software system for the audit client that will integrate sales and purchases with the company's general ledger, and the output of the upgraded IT systems will form part of or affect the audit client's accounting records, the internal control over financial reporting and the financial statements on which the firm will express an opinion (paragraph R600.15(a)); and (b) the audit team will need, as part of the audit, to evaluate or rely on the judgments made or activities performed by the firm's IT consulting team when they designed and developed the upgraded IT system (paragraph R600.15(b)). This is because the output of the upgraded IT system is influenced by the activities performed by the firm's IT consulting team when they designed and developed the system. These activities will involve the knowledge, expertise or judgment of the firm's IT consulting team (paragraph 300.6 A2).

Self-review Threat Prohibition for PIE Audit Clients

37. If the company is a PIE audit client, and as the NAS will create a self-review threat, the audit firm is prohibited from providing the IT systems service. That prohibition would apply even if the firm (including the audit partner) is satisfied that the company's management makes all judgments and decisions that are the proper responsibility of management in accordance with the provisions in the Code (paragraph R400.21).

Are Identified Threats at an Acceptable Level for Non-PIE Audit Clients?

38. As the self-review threat created from providing the proposed NAS does not give rise to a prohibition for non-PIE audit clients, the audit firm is required to apply the conceptual framework to evaluate whether the identified self-review threat to compliance with the fundamental principles, including independence, is at an acceptable level.

39. In this scenario, based on an assessment of the facts and circumstances and taking into consideration that the proposed system transformation service is likely to have a material effect on the financial statements and an extensive impact on the company's accounting records and internal controls over financial reporting (paragraphs 600.10 A2 and 606.4 A2), the audit partner determines that the self-review threat is not at an acceptable level and needs to be addressed.

Addressing Threats for Non-PIE Audit Clients

40. Threats that are not at an acceptable level are addressed either by: (i) eliminating the circumstances creating the threats to independence; (ii) applying safeguards, where available and capable of being applied; or (iii) declining or ending the specific professional activity. The use of the reasonable and informed third party test is relevant to the firm's overall conclusion in assessing whether the actions it intends to take to address the threats to independence will be appropriate to eliminate or reduce the threats to an acceptable level (paragraph R120.11). For example:

(i) Is the firm able to adjust the scope of the proposed service such that the specific circumstances creating the threat are eliminated? For instance, could the scope of the assistance the firm provides be restricted so that it avoids designing or implementing aspects of the IT system that:

- Form part of the internal control over financial reporting for the company.
- Involve generating information for the client's accounting records or financial statements for the company.

In this scenario, given the needs of the company and the scope of the system transformation service that the company has asked the firm to undertake, this is unlikely to be a practical approach.

(ii) Is the firm able to apply a safeguard that would reduce the self-review threat to an acceptable level? For example, the firm might take steps to ensure that the team members who would provide the system transformation service would not be audit team members (paragraph 606.5 A1).

In this scenario, a reasonable and informed third party will likely conclude that the self-review threat is not at an acceptable level even after a safeguard is applied, since the systems transformation service has a material effect on the financial statements and an extensive impact on the company's accounting records and internal controls over financial reporting (paragraphs 600.10 A2, 600.11 A1 and 606.4 A2).

(iii) For the reasons set out in (i) and (ii) above, it is likely that the firm would decide not to provide the NAS to the company with the consequence that the company must find another provider. This would not preclude the audit partner from having a technical discussion with the company as part of the audit in relation to the appropriateness of financial and accounting control and the methods used in determining the stated amounts in the financial statements and related disclosures.

Effectively, the same conclusion will be reached if the service is considered an accounting and bookkeeping service (Section 601) instead of an IT systems service (Section 606) because the proposed service would not meet the criteria to be a "routine or mechanical" accounting and bookkeeping service. That is because the systems transformation service would involve designing and implementing upgraded IT systems functionalities that include automatically integrating sales and purchases source data with the general ledger and producing system-generated accounting records and financial statements – which would not meet the test of involving "little or no professional judgment." See paragraphs 62 and 63 below.

SCENARIO 2:

Licensing of IT Software to Assist with the Application of Accounting Standards

41 The IT services division of a firm develops a software program designed to assist clients with implementing and maintaining ongoing compliance with the IFRS 17 Insurance Contracts accounting standard. The software is capable of being individually customized for the specific client needs and generates information in relation to IFRS 17 that affects the accounting records, financial statements and related disclosures. The firm's IT services division licenses such a software program to its clients that are not audit clients, customized to their specific needs, to help in their first-time adoption of IFRS 17.

42 The finance manager of the firm's audit client is aware of such a software program and asks the audit partner about the possibility of licensing the software program. The audit partner is considering whether the firm's IT services division would be able to license the software program to its audit client, and to provide ongoing support service should there be any issues or update patches needed with the software program.

What Are Some Key Considerations When Applying the Code?

Risk of Assuming a Management Responsibility

43. To prevent the firm from assuming management responsibility when licensing the software to its audit client, the firm should satisfy itself that the audit client has arranged for responsibility for management decisions and judgments to be allocated to a competent employee(s). That competent employee(s) evaluates the adequacy of the results of the software and is responsible for operating the system as well as establishing and monitoring a system of internal controls (paragraph R606.3). The availability of competent employees might differ in PIE versus non-PIE audit clients.

44. Such evaluation of the adequacy of the output of the software might include backtesting or parallel running of the software by the audit client and comparison with former methodologies, so that the audit client is able to assess the adequacy of the software and validate its output.

45. No management responsibility is assumed by the firm if the audit client's competent employee(s) provides oversight over the customization of the software and is able to review and evaluate the accuracy of the outputs of the software. Such software might, for example, be in the form of sophisticated Excel worksheets. On the other hand, if the software is a "black box" (i.e., it is unclear how the output of the software is derived) and the audit client was not involved in the development of the underlying logic, then it is unlikely that it could assign the responsibility for making management decisions and judgments concerning the implementation of, and ongoing compliance with, IFRS 17 to a competent employee. Furthermore, if the software makes a decision (representing the firm's expertise or judgment) when generating the output, it is unlikely that management can be regarded as having made all the decisions that are the proper responsibility of management with regard to the implementation of, and compliance with, IFRS 17.

46. Even if the proposed NAS does not involve assuming a management responsibility for the company (paragraph R606.3), the audit firm is still required to apply the conceptual framework to identify, evaluate and address threats to independence that might arise from licensing the software program (paragraph 600.6(b)).

Identifying and Evaluating Threats

47. The firm identifies three threats to independence that might arise with the firm's licensing of software to an audit client – a self-interest, intimidation and a self-review threat:

- Self-interest and Intimidation – The audit partner's judgment or behavior might be inappropriately influenced if the proportion of the licensing fees charged by the firm's IT services division to the audit client is large in comparison to the audit fees. This could be due to concerns, for example resulting from internal pressures, about the potential loss of either the audit engagement or other services provided to the audit client (paragraph 410.11 A1).

  In this scenario, the audit partner might determine that the potential threats identified in providing the service are at an acceptable level because the proportion of licensing fees that might be charged to the audit client is not large in comparison to the audit fees charged.

- Self-review – A self-review threat is created as (a) the software assists the client with the implementation of, and ongoing compliance with, IFRS 17, and the software's outputs will form part of or affect the audit client's accounting records and financial statements and internal control over financial reporting (paragraph R600.15(a)); and (b) the audit team will need, as part of the audit, to evaluate or rely on the judgments made or activities performed by the firm when it designed and developed the software (paragraph R600.15(b)). This is because the

output of the software (i.e., the calculation and reporting of the company's insurance contracts in accordance with IFRS 17) is influenced by how such software was designed and developed, which involves the knowledge, expertise or judgment of the firm's IT services division (paragraph 300.6 A2).

Similarly, since the underlying service creates a self-review threat, the on-going support service would mean that the self-review threat continues to exist (paragraph 606.4 A3) because (a) the software's outputs will form part of or affect the audit client's accounting records and financial statements and internal control over financial reporting (paragraph R600.15(a)); and (b) the audit team will need, as part of the audit, to evaluate or rely on the judgments made or activities performed by the firm when it is addressing issues relating to the software or updating patches needed for it (paragraph R600.15(b)).

Self-review Threat Prohibition for PIE Audit Clients

48. If the company is a PIE audit client, and as the NAS creates a self-review threat, the audit partner's firm is prohibited from licensing the software program to assist the company. That prohibition would apply even if the firm (including the audit partner) is satisfied that the company's management makes all judgments and decisions that are the proper responsibility of management in accordance with the provisions in the Code (paragraph R400.21).

Are Identified Threats at an Acceptable Level for Non-PIE Audit Clients?

49. As the self-review threat created by the proposed NAS does not give rise to a prohibition for non-PIE audit clients, the audit firm is required to apply the conceptual framework to evaluate whether the identified self-review threat to compliance with the fundamental principles, including independence, is at an acceptable level.

50. If the insurance contracts calculated and reported by the software are immaterial to the company's financial statements, the self-review threat might be at an acceptable level as the impact or interaction of the software and its output on the client's accounting records, internal controls over financial reporting or financial statements, or the degree of reliance placed on the software as part of the audit, would be immaterial. However, if the insurance contracts calculated and reported by the software are material to the financial statements, then the level of self-review threat is likely not to be at an acceptable level (paragraphs 600.10 A2, 600.11 A1 and 606.4 A2).

Addressing Threats for Non-PIE Audit Clients

51. Threats that are not at an acceptable level are addressed either by: (i) eliminating the circumstances creating the threat to independence; (ii) applying safeguards, where available and capable of being applied; or (iii) declining or ending the specific professional activity. The use of the reasonable and informed third party test is relevant to the firm's overall conclusion in assessing whether the actions it intends to take to address the threats to independence will be appropriate to eliminate or reduce the threats to an acceptable level (paragraph R120.11). For example:

(i) Is the firm able to adjust the scope of the proposed service such that the specific circumstances creating the threat are eliminated? For instance, as the software is customizable, the scope of the software licensed by the firm to its audit client could be restricted, such that the software and its outputs do not:

- Form part of the internal control over financial reporting for the company.
- Involve generating information for the client's accounting records or financial statements for the company.

In this scenario, given the needs of the company and the scope of the IFRS 17 implementation and compliance service that the company has proposed for the firm to undertake, this is unlikely to be a practical approach.

(ii) Is the firm able to apply a safeguard that would reduce the self-review threat to an acceptable level? For instance, the firm might take steps to ensure that the team members involved in the development of the software program and who would provide the licensing and ongoing support services would not be audit team members (paragraph 606.5 A1).

In this scenario, a reasonable and informed third party will likely conclude that the self-review threat is not at an acceptable level even after a safeguard is applied, since the insurance contracts calculated and reported by the software are material to the company's financial statements (paragraphs 600.10 A2, 600.11 A1 and 606.4 A2).

(iii) For the reasons set out in (i) and (ii) above, it is likely that the firm would decide not to provide or sell or license the software to its audit client.

Effectively, the same conclusion will be reached if the service is considered an accounting and bookkeeping service (Section 601) instead of an IT systems service (Section 606), because the proposed service would not meet the criteria of being a "routine or mechanical" accounting and bookkeeping service. That is because the client was not involved in making the necessary judgments or decisions connected with the design of the firm's pre-existing IFRS 17 software program for its clients in general, and the first-time adoption of IFRS 17 is unlikely to meet the test of involving "little or no professional judgment." See paragraphs 62 and 63 below.

SCENARIO 3:

Automated Processes and "Routine or Mechanical"

52 The managing director of a company has asked the audit firm to prepare the company's year-end financial statements. The company's finance manager resigned in the lead up to the year-end. While the remaining finance staff can maintain the input of data into the company's accounting systems, they do not have the experience or knowledge to compile the year-end financial statements.

53 The firm has software that has the capability to interact with the company's accounting systems and records, extract and recode the ledger into the firm's system, make adjusting journal entries and then populate a proforma set of financial statements. The managing director suggests that the firm's staff review the computer-generated financial statements and any adjusting journal entries generated through this process. The financial statements can then be presented to the managing director and other management of the company for approval.

54 The audit firm is considering whether to provide this accounting and bookkeeping service[5] to its audit client.

[5] Accounting and bookkeeping services comprise a broad range of services including (paragraph 601.3 A1):
- Preparing accounting records or financial statements.
- Recording transactions.
- Providing payroll services.
- Resolving account reconciliation problems.
- Converting existing financial statements from one financial reporting framework to another.

What Are Some Key Considerations When Applying the Code?

Risk of Assuming a Management Responsibility

55. In this scenario, while it might appear that the software is 'automatically' preparing financial statements and generating adjusting journal entries, the firm would have made programming decisions connected with the design of the software system, including establishing how general ledger accounts are captured within the financial statements.

56. Additionally, the company does not have an employee who has the skills, knowledge and experience to oversee and evaluate the adequacy of the financial statements, and the firm would directly report to those charged with governance (i.e., the managing director of the company) on behalf of the management.

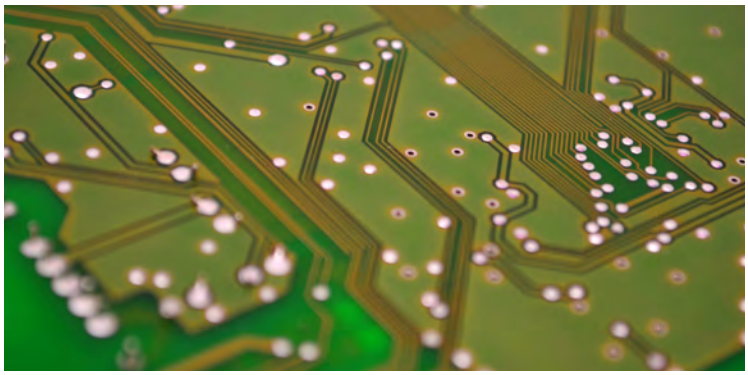
57. Accordingly, the firm would likely take responsibility for making the decisions and assumptions when programming the software and reporting to those charged with governance of the company (paragraph 400.20 A3). Therefore, the provision of this proposed accounting and bookkeeping service would be prohibited.

58. To prevent the firm from assuming management responsibilities in relation to the financial statements, the firm can ensure that the company's management makes all judgments and decisions that are the proper responsibility of management. This includes ensuring that the client's management (paragraph R400.21):

- Designates an individual who possesses suitable skill, knowledge and experience to be responsible at all times for the client's decisions and to oversee the activities.
- Provides oversight of the activities and evaluates the adequacy of the results of the activities performed for the client's purpose.
- Accepts responsibility for the actions, if any, to be taken arising from the results of the activities.

For example, this might mean that client management provided the firm with detailed manuals and procedures outlining the key principles that should underlie the client's accounting system when the firm programs the software, or that the managing director of the company or other management had suitable skill, knowledge and experience to oversee the activities (i.e., by reviewing the mapping of the accounts into the financial statement captions prior to the firm configuring the software), or that client management reviews and approves the financial statements and adjusted journal entries outputs of the software before reporting to the managing director.

59. Even if this accounting and bookkeeping service does not involve assuming a management responsibility for the company (paragraphs 601.2 A1 and R400.21), the audit firm is still required to apply the conceptual framework to identify, evaluate and address threats to independence that might arise from providing the company with this accounting and bookkeeping service.



Accounting and Bookkeeping Services

60. The audit firm identifies three threats to independence that might arise if the firm provides this service – a self-interest, intimidation and a self-review threat:

- Self-interest and Intimidation – The audit partner's judgment or behavior might be inappropriately influenced if the proportion of the fees to the audit client for the accounting and bookkeeping service is large in comparison to the audit fees charged. This could be due to concerns, for example resulting from internal pressures, about the potential loss of either the audit engagement or other services provided to the audit client (paragraph 410.11 A1).

  In this scenario, the audit partner determines that the potential threats identified in providing the service are at an acceptable level, because the proportion of fees for the accounting and bookkeeping service that might be charged to the audit client is not large in comparison to the audit fees charged.

- Self-review – A self-review threat is created as (a) the outputs of the computer program will form part of or affect the audit client's accounting records and financial statements and internal control over financial reporting (paragraph R600.15(a)); and (b) the audit team will need, as part of the audit, to evaluate or rely on the judgments made or activities performed by the firm when it designed and developed the software (paragraph R600.15(b)). This is because the output of the accounting and bookkeeping service is influenced by how such computer-assisted processes are designed and developed, which involves the knowledge, expertise or judgment of the firm's IT services division (paragraph 300.6 A2).

Prohibition on Accounting and Bookkeeping Services for PIE Audit Clients

61. If the company is a PIE, the firm is prohibited from providing such an accounting and bookkeeping service to the PIE audit client (paragraph R601.6).

Routine or Mechanical Accounting and Bookkeeping Services for non-PIE Audit Clients

62. If the company is not a PIE, the firm is also prohibited from providing such an accounting and bookkeeping service to the non-PIE audit client unless (i) the services is of a routine or mechanical nature, (ii) the audit firm addresses any threats to independence that are not at an acceptable level, and (iii) the firm does not assume a management responsibility in connection with the service (paragraphs R601.5 and 601.5 A3).

63. Accounting and bookkeeping services that are routine or mechanical involve information, data or material in relation to which the client has made any necessary judgments or decisions and require little or no professional judgment. In determining whether an automated accounting and bookkeeping service is routine or mechanical, factors to be considered include the activities performed by, and the output of, the technology, and whether the technology provides an automated service that is based on or requires the expertise or judgment of the firm or network firm (paragraphs 601.5 A1 and A2).

64. In this scenario, the firm has established computer-assisted processes that allow the firm's software programs to 'automatically' prepare the financial statements, including the necessary adjusting journal entries. The firm would likely have made programming decisions connected with the design of the entire software system, including establishing how general ledger accounts are captured within the financial statements, as well as in the firm staff's review of the adjusting journal entries.

65. Accordingly, the audit partner is likely to conclude that the proposed accounting and bookkeeping service has not met the criteria of "routine or mechanical" and therefore the provision of the service to a non-PIE client is prohibited.

About APESB

Accounting Professional & Ethical Standards Board (APESB) was formed in 2006 as an independent national standards setter in Australia with the primary objective of developing professional and ethical standards in the public interest for the members of the three Australian Professional Accounting Bodies, namely Chartered Accountants Australia and New Zealand, CPA Australia and the Institute of Public Accountants. The three Professional Accounting Bodies are the members of APESB.

About IESBA

The International Ethics Standards Board for Accountants (IESBA) is an independent global standard-setting board. The IESBA's mission is to serve the public interest by setting ethics standards, including independence requirements, as a cornerstone to ethical behavior in business and organizations, and to public trust in financial and non-financial information that is fundamental to the proper functioning and sustainability of organizations, financial markets and economies worldwide.

Along with the International Auditing and Assurance Standards Board (IAASB), the IESBA is part of the International Foundation for Ethics and Audit (IFEA).

KEY CONTACTS

Channa Wijesinghe, Chief Executive Officer, APESB channa.wijesinghe@apesb.org.au

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

Ken Siong, Program and Senior Director, IESBA kensiong@ethicsboard.org

Kam Leung, Principal, IESBA kamleung@ethicsboard.org

ACKNOWLEDGMENTS

The drafting team for this publication is grateful for the important guidance and feedback provided by peer reviewers during the development of this non-authoritative publication: Jacinta Hanrahan and Channa Wijesinghe on behalf of the APESB; David Clark, Brian Friedrich, Kam Leung, Diane Jules, and Ken Siong on behalf of the IESBA's Phase 2 Technology Working Group; James Barbour, Greg Driscoll, Richard Fleck, Hironori Fukukawa, Rich Huesken, and Luigi Nisoli as members of IESBA's Technology Task Force; Saadiya Adam, Mark Babington, Keith Billing, Marta Kramerius, and Andrew Pinkney as members or technical advisors of the IESBA; Caroline Lee as former vice chair of the IESBA; and Jason Bradley, Head of Assurance Technology at the UK Financial Reporting Council and member of the IESBA's Technology Experts Group.

IESBA International Ethics Standards Board for Accountants®

www.iethicsboard.org | @ethics_board | company/iesba

APESB Accounting Professional & Ethical Standards Board

www.apesb.org | company/accounting-professional-&-ethical-standards-board/