

Preliminary Draft – for discussion purposes only

Cover page

- Both IESBA and APESB logos

Title: Technology related considerations for Auditor Independence –Applying the Code’s conceptual framework and Independence standards to scenarios involving technology

2nd page:

Table of Contents

3rd page:

Introduction and purpose of guidance

This publication was developed by the Staff of the Australian Accounting Professional & Ethical Standards Board (APESB) and the International Ethics Standards Board for Accountants (IESBA), with input from the IESBA’s Technology Working Group.

Technology creates many opportunities for professional accountants, but it can also create threats to compliance with the fundamental principles of the *International Code of Ethics for Professional Accountants (Including International Independence Standards)* (the Code), particularly when firms provide non-assurance services to their audit clients. This guide considers how technology intersects with auditor independence and provides professional accountants in public practice with practical examples of how to apply the Code’s conceptual framework in these situations. There are four case studies which highlight technological considerations for auditors.

The scenarios are hypothetical and are solely intended to provide an illustrative aid to those applying the conceptual framework to comply with the Code. The conceptual framework is a specified approach for identifying, evaluating and addressing threats to compliance with the fundamental principles and the Independence Standards.

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 implementation guidance 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.

Professional accountants need to be mindful and 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.

The case studies are based on the *Handbook of the International Code of Ethics for Professional Accountants (including International Independence Standards) 2021 Edition* which includes revisions to the Code for:

- *Revisions to the Non-Assurances Services Provisions of the Code* issued in April 2021 and effective from December 15, 2022; and
- *Revisions to the Code to Promote the Role and Mindset Expected of Professional Accountants* issued in October 2020 and effective from December 31, 2021.

CASE STUDY 1

Provision of Information Technology (IT) Systems Services to an Audit Client

Issues: Auditor Independence; Information Technology Systems Services

Case Outline: At the planning meeting for an audit client, the Finance Manager of the audit client mentions to the audit partner that the company is looking to upgrade its software suite. The audit client's current software suite used for sales and purchases does not automatically integrate with the general ledger. The audit client wants to ensure that both systems integrate to improve the efficiency and accuracy of financial reporting processes and are considering the options they have to either replace the system entirely or customize the existing software systems to interface with each other.

The audit client has one IT employee who is responsible for maintaining the current IT systems and hardware. The IT employee does not have the skill set or the experience to undertake the project to upgrade or replace the company's entire software suite.

The audit partner's firm has a specialist IT services team that can design and implement IT systems including services to aggregate source data, improve internal controls and generate information for accounting records and financial statements. The audit partner is considering whether the Finance Manager should speak with the firm's IT services team for advice on appropriate systems and for assistance with implementation.



Identifying Threats

Self-interest

There is a threat that the audit partner might want to secure the additional revenue stream for the firm from the IT services engagement. The firm might also assume a management responsibility in implementing the IT systems if there is no-one at the client that could take responsibility for key IT decisions (paras R400.13 and R400.14). This threat, and the assumption of a management responsibility, could threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (paras 120.6 A3(a) and 400.13 A2).

Self-review

If the firm's IT services team implements a software system for the company that directly impacts the financial reporting systems, a threat may be created where the audit team will not appropriately evaluate the outputs of the system when forming judgements as part of the audit. The accounting firm might also assume a management responsibility with the design and implementation of IT systems (paras R400.13 and R606.3). This threat, and the assumption of a management responsibility, might impact the audit team's exercise of professional skepticism and threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (paras 120.6 A3(b) and 400.13 A2).



Evaluating Threats

Are Identified Threats at an Acceptable Level?

The audit partner must have an inquiring mind, exercise professional judgement and apply the reasonable and informed third party test when applying the conceptual framework and determining whether the threats are at an acceptable level (para R120.5). Consideration of qualitative and quantitative factors is relevant in the evaluation of threats, as is the combined effect of multiple threats, if applicable (para 120.8 A1).

There is a risk that if IT systems services are provided to the audit company the firm will assume management responsibility, which is prohibited in the Code (para R400.13). Therefore, the firm must be satisfied that:

- a) The audit client acknowledges its responsibility for establishing and monitoring internal control systems;
- b) The audit client assigns the responsibility to make all management decisions regarding the design and implementation of the system to a competent employee, preferably within senior management, such as the Finance Manager;
- c) The audit client makes all management decisions with respect to the design and implementation process;
- d) The audit client evaluates the adequacy and results of the design and implementation of the system; and
- e) The audit client is responsible for operating the system and for the data it uses or generates (para R606.3).

As the IT employee of the audit client does not have the necessary skills to undertake the IT services project themselves, the firm would need to satisfy itself whether the audit client's management can take responsibility for the implementation process.

Even if the firm is satisfied that the audit client can assume management responsibility, the provision of the IT systems service might create a self-review threat if it will affect the financial reports that the firm will be auditing (para 606.4 A1). As the proposed IT systems services will integrate sales and purchases with the company's general ledger (so will impact the accounting records and financial statements) it is likely a self-review threat will be created.

If the audit client is not a Public Interest Entity (PIE), and a self-review threat has been identified, the audit partner should evaluate the threat by considering whether the audit team is likely to place a high degree of reliance on the IT systems (para 606.4 A3).

If the audit client is a PIE, the firm is prohibited from providing the IT systems services if it might create a self-review threat (para R606.6).

Based on an assessment of the factors, a reasonable and informed third party would likely conclude that the threats to one or more of the fundamental principles are not at an acceptable level and the threats would need to be addressed.



Addressing Threats

Eliminate Circumstances

The circumstances could be eliminated if the audit partner does not refer the Finance Manager to the IT services team and if the firm does not provide the IT systems services.

Apply Safeguards and Other Actions

To ensure the firm is not assuming management responsibilities in undertaking the provision of IT System services, the firm should ensure the company assigns responsibility to make all management decisions to a competent senior employee, evaluates the adequacy and results of the IT system and is responsible for operating the system (para R606.3). As the audit client's IT employee has not got the skill set to undertake this project, they may not be able to assume management responsibility for the project. The Finance Manager, or another senior executive at the audit client, may have the capabilities to oversee the project and assess the results of the IT system.

When the audit client is not a PIE audit client, the firm might be able to address the self-review threat by applying a safeguard of using professionals who are not audit team members (including the audit partner) to perform the service (para 606.5 A1). Therefore, the members of the IT services team would need to be separate from the members of the audit engagement team.

Even if the company has an individual who can assume responsibility for the IT systems upgrade project, the level of threats might still not be at an acceptable level, especially as there are multiple threats to the fundamental principles and to the Independence of the auditor in this scenario.

Decline or End Professional Activity

If the audit partner or the firm cannot eliminate the circumstances creating the threats and no safeguards are available or capable of being applied to reduce the threats to an acceptable level, the firm should not provide the IT implementation service or may need to resign from the audit engagement (para R120.10(c)).

CASE STUDY 2

Implementation of IT software to assist with accounting standards application

Issues: Auditor Independence; Information Technology Systems Services

Case Outline: The IT Services division of an accounting firm develops a software program designed to assist clients with the implementation of, and ongoing compliance with, the IFRS 16 *Leases* accounting standard.

The firm makes this software program available to its audit clients and the software generates information that affects the accounting records, financial statements and related disclosures of those clients.

The firm has a broad client base across various industries, including Public Interest Entities (PIEs) and audit clients that are not PIEs.



Identifying Threats

Self-interest

There is a threat that the additional revenue stream for the firm from selling the IFRS 16 *Leases* software to audit clients will inappropriately influence the audit team members' judgment or behavior. This threat could threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (para 120.6 A3(a)).

Self-review

When the leasing software is provided to the firm's audit clients, a self-review threat is created. The outputs of the leasing software directly impact the audit clients' accounting records and financial statements. The firm's audit teams may not appropriately evaluate the outputs generated by the leasing software when forming judgements as part of the audits. This threat might impact the audit teams' exercise of professional skepticism and threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (para 120.6 A3(b)).



Evaluating Threats

Are Identified Threats at an Acceptable Level?

The firm must have an inquiring mind, exercise professional judgement and apply the reasonable and informed third party test when applying the conceptual framework and determining whether the threats are at an acceptable level (para R120.5). Consideration of qualitative and quantitative factors is relevant in the evaluation of threats, as is the combined effect of multiple threats, if applicable (para 120.8 A1).

There is a risk that if IT systems services are provided to the firm's audit clients, the firm will assume management responsibility, which is prohibited in the Code (para R400.13). Therefore, the firm must be satisfied that:

Preliminary Draft – for discussion purposes only

- a) The audit client acknowledges its responsibility for establishing and monitoring internal control systems;
- b) The audit client assigns the responsibility to make all management decisions regarding the design and implementation of the system to a competent employee, preferably within senior management;
- c) The audit client makes all management decisions with respect to the design and implementation process;
- d) The audit client evaluates the adequacy and results of the design and implementation of the system; and
- e) The audit client is responsible for operating the system and for the data it uses or generates (para R606.3).

The provision of the leasing software might create a self-review threat if the software, and its outputs, form part of the internal control over financial reporting or generate information for the client's accounting records or financial statements (para 606.6 A1) and will affect the financial reports that the firm will be auditing (para 606.4 A1). As the leasing software assists the clients with the implementation and ongoing compliance with the standard and affects the client's accounting records, financial statements and related disclosures, it is likely a self-review threat will be created.

If the firm's audit client is a PIE, the firm is prohibited from providing IT System Services, such as the leasing software, that might create a self-review threat (para R606.6).

If the firm's audit client is not a PIE, and a self-review threat has been identified, the audit partner should evaluate the threat by considering whether the audit team is likely to place a high degree of reliance on the IT systems (para 606.4 A3).

The firm should also consider whether bias could affect the exercise of professional judgement when evaluating the level of this self-review threat (paras 120.12 A1 and A2). Automation bias, being the tendency to favour the outputs from automated systems, could unduly impact the firm's judgment of the accuracy of the outputs produced by the software and its impact on self-review threats.

As the leasing software generates information that forms part of the accounting records or financial statements, a reasonable and informed third party would likely conclude the threats to independence are not at an acceptable level and the threats would need to be addressed.

Addressing Threats



Eliminate Circumstances

The firm could eliminate the circumstances that are creating the threats by not providing or selling the leasing software to its audit clients.

Apply Safeguards and Other Actions

To ensure the firm is not assuming management responsibilities in providing the leasing software to their audit clients, the firm should ensure the company assigns responsibility to make all management decisions to a competent senior employee, evaluates the adequacy and results of the IT system and is responsible for operating the system (para R606.3). However, as the leasing software was designed by the firm's IT Services division, it is unlikely that the audit clients could assign the responsibility to make all management decisions with respect to the design of the software to a competent employee, preferably within senior management (para R606.3(b)).

Preliminary Draft – for discussion purposes only

As the leasing software generates information that forms part of the accounting records and the financial statements, and the audit team is likely to rely on this information, it is unlikely that the firm would be able to apply safeguards to reduce the threats to an acceptable level. Therefore, the firm should not provide or sell the leasing software to its audit clients.

Decline or End Professional Activity

As the audit partner or the firm cannot eliminate the circumstances creating the threats and no safeguards are available or capable of being applied to reduce the threats to an acceptable level, the firm should decline to provide or sell the leasing software to its audit clients (para 120.10(c)).

DRAFT

CASE STUDY 3

Automated processes and routine or mechanical

Issues: Auditor Independence; Accounting and Bookkeeping Services

Case Outline: The Managing Director of a company has engaged an accounting firm to prepare the company's year-end financial statements. The company's Finance Manager resigned in the lead up to the year-end, and 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.

The firm's practice software 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 journals and then populate a proforma set of financial statements. The firm's staff review the computer-generated financial statements and any adjusting journal entries generated through this process. The financial statements are then presented to the Managing Director and other management of the company for review and approval.

The Managing Director is impressed with how efficiently and quickly the firm was able to prepare the financial statements, and have enquired as to whether the firm would also be able to undertake the engagement for the external audit. The audit partner is considering this request and whether the preparation of the financial statements would be considered as routine or mechanical accounting or bookkeeping services.

Identifying Threats



Self-interest

There is a threat that the audit partner might want to secure the additional revenue stream for the audit engagement. The accounting firm might also assume a management responsibility in the preparation of the financial statements when establishing the system to automate the process (para R400.13). This threat, and the assumption of a management responsibility, could threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (paras 120.6 A3(a) and 400.13 A2).

Self-review

There is a threat that the financial statements and notes will not be appropriately evaluated when forming judgements as part of the audit given that they were prepared by the firm. This self-review threat could threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (para 120.6 A3(b)).



Evaluating Threats

Are Identified Threats at an Acceptable Level?

The audit partner must have an inquiring mind, exercise professional judgement and apply the reasonable and informed third party test when applying the conceptual framework and determining whether the threats are at an acceptable level (para R120.5). Consideration of qualitative and quantitative factors is relevant in the evaluation of threats, as is the combined effect of multiple threats, if applicable (para 120.8 A1).

If the company is a PIE, the firm is prohibited from providing accounting and bookkeeping services, including preparing the financial statements and notes, and also auditing those financial statements (para R601.6).

If the company is not a PIE, the firm is prohibited from providing accounting and bookkeeping services, including preparing the financial statements and notes, that the firm will be auditing unless the services are of a routine or mechanical nature and the auditor addresses any threats to independence that are not at an acceptable level (para R601.5).

Accounting and bookkeeping services that are routine or mechanical involve information, data or material in relation to which the client has made any necessary judgements or decisions and require little or no professional judgement (para 601.5 A1). An example of such a service is “preparing financial statements based on information in the client-approved trial balance and preparing related notes based on client-approved records” (para 601.5 A2). Such services may be provided to non-PIE audit clients provided the firm does not assume a management responsibility in connection with the service and the firm addresses any threats that are not at an acceptable level (paras R400.14, R601.5(b) and 601.5 A2).

In this scenario, the firm has established computer assisted processes that allows the firm’s software programs to ‘automatically’ prepare the financial statements. While it might appear that the computer program is making those judgments or decisions, in establishing the processes, the firm would have made decisions and used professional judgement to establish how general ledger accounts are captured within the financial statements, which is a management responsibility. Therefore, the system generated preparation of financial statements would not be routine or mechanical accounting or bookkeeping services as the client did not make the necessary judgments or decisions and professional judgement was required by the firm (paras R601.5 and 601.5 A1). The audit partner is likely to conclude that the firm, in making the decisions and assumptions in establishing the computer processes, have assumed a management responsibility (paras R400.13 to R400.14).

Based on an assessment of the factors, a reasonable and informed third party would likely conclude that the threats to one or more of the fundamental principles are not at an acceptable level and the threats would need to be addressed.



Addressing Threats

Eliminate Circumstances

The audit partner might not be able to eliminate the circumstances creating the threat to independence, as the firm has already prepared the financial statements.

Preliminary Draft – for discussion purposes only

Apply Safeguards and Other Actions

To ensure the firm is not assuming management responsibilities in relation to the financial statements, the firm should ensure that the management of the company take responsibility for the advice and recommendations received (para R400.14) and make any judgments or decisions that might be necessary (para 601.5 A1). A suitably qualified and knowledgeable individual at the company would need to be responsible for the recommendations, understand the service that is provided, be able to evaluate the adequacy of the results and accepts responsibility for the actions to be undertaken as a result of this service. Based on the fact that the company did not have an employee who had the skills to prepare the financial statements, it is unlikely that the company would be able to take responsibility for the preparation of the financial statements.

Decline or End Professional Activity

As the firm cannot eliminate the circumstances creating the threats and no safeguards are available or capable of being applied to reduce the threats to an acceptable level, the audit partner or the firm should not accept the external audit engagement for the company (para R120.10(c)).

DRAFT

CASE STUDY 4

Business insights and Auditor Independence

Issues: Auditor Independence; Advice and Recommendation Services; Confidentiality

Case Outline: An accounting firm is undertaking the external audit for a client that operates in an industry where there are only a few competitors (e.g., oligopoly). The accounting firm undertakes the external audit function for the majority of the companies within this industry.

The audit manager on this engagement is, for the first time, using a data analytics program developed by the accounting firm. The program can identify exceptions in data and identify a proposed sample for detailed audit testing. It is also able to analyze the audit client's data using various data sets, including an industry data set which the accounting firm has compiled from its industry knowledge.

When reviewing the results from the data analytics program for the sales figures, the audit manager noticed a particular pattern in the sales for the audit client's three key customers where low sales to these customers contrast to high sales peaks by others within the industry. The frequency of this pattern occurring is increasing. The analysis indicates these customers are likely being successfully targeted by the audit client's competitors.

The audit manager is impressed with the analysis provided by the data analysis tool and is considering how to present this information to the audit client including whether the audit manager can recommend potential sales strategies for those key clients



Identifying Threats

Self-interest

There is a threat that the audit manager will want to provide the additional insights to the audit client to either secure an additional revenue stream for advice and recommendation services or to promote the accounting firm. The accounting firm might also assume a management responsibility when providing the insights and identifying potential sales strategies (para R400.13), which could threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (paras 120.6 A3(a) and 400.13 A2).

Self-review

There is a threat that any sales strategy adopted by the audit client in response to the insight provided by the firm may not be appropriately evaluated when forming judgements as part of the audit. The advice and recommendations provided by the firm might create a self-review threat (para 600.11 A1). If the firm assumes a management responsibility when providing the insights and identifying potential sales strategies it will create a self-review threat (paras R400.13 and 400.13 A2). This self-review threat could threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (para 120.6 A3(b) and 400.13 A2).

Advocacy

There is a threat that the audit manager will promote the benefits of the data analysis tool to the audit client to a point where objectivity is compromised. This could threaten the fundamental principles of objectivity, professional competence and due care, and professional behavior (para 120.6 A3(c)).



Evaluating Threats

Are Identified Threats at an Acceptable Level?

The audit manager must have an enquiring mind, exercise professional judgement and apply the reasonable and informed third party test when applying the conceptual framework and determining whether the threats are at an acceptable level (para R120.5). Consideration of qualitative and quantitative factors is relevant in the evaluation of threats, as is the combined effect of multiple threats, if applicable (para 120.8 A1).

In evaluating whether providing advice and recommendations creates a self-review threat, the firm must determine whether there is a risk that the results of the service will form part of the accounting records, internal controls over financial reporting, or the financial statements being audited, and that the audit team will evaluate or rely on the judgments made or activities performed in the other service during the audit (paras 600.11 A1 and R600.14).

If the audit client is a PIE, the firm is prohibited from providing a service if it might create a self-review threat (para R600.16). There is an exception to this prohibition where the firm provides advice and recommendations to the PIE audit client that relates to information or matters arising in the course of the audit, provided the firm does not assume management responsibility and the conceptual framework is applied to any threats to independence, other than self-review threats (para R600.17).

If the audit client is not a PIE, and as a self-review threat has been identified, then the audit manager is required to apply the conceptual framework to address the threat (para 600.11 A1). The audit manager should consider whether bias could affect their exercise of professional judgement when evaluating the threats (paras 120.12 A1 and A2). Automation bias, being the tendency to favour the outputs from automated systems, could impair the audit manager's judgment of the accuracy of the data analysis tool's outputs and evaluation of threats. The audit manager could mitigate the effect of this bias by consulting with others, such as the engagement partner, to ensure there is appropriate challenge as part of the evaluation process (para 120.12 A3).

The audit manager should consider whether the provision of the advice and recommendations, insights and potential sales strategy would be providing services that arise in the course of an audit (para 600.17 A1) and if the audit client is responsible for making decisions. While dialogue between a firm and the management of the audit client does occur, it would normally happen in the course of an audit when:

- Advising on accounting and financial reporting standards and policies, financial statement disclosures, the appropriateness of financial and accounting controls, the methods used to determine the stated amounts in the financial statements and related disclosures and compliance with group accounting policies.
- Proposing adjusting journal entries from audit findings.
- Discussing findings on internal controls over financial reporting and processes and recommending improvements or resolving account reconciliation problems.

Based on the facts in this scenario, the insights discovered by the audit manager would be outside the normal course of an audit, especially due to the specialized industry knowledge in the industry data set. As such, the exception to the self-review threat prohibition for PIE audit clients would not be available (paras R600.16 and R600.17).

Preliminary Draft – for discussion purposes only

Additionally, setting the strategic direction for the business is a management responsibility (para 400.13 A3). This raises a concern that the Firm might be assuming a management responsibility (paras R400.13 to 400.13A4) by developing a potential sales strategy for the audit client's key customers.

Based on an assessment of the factors, a reasonable and informed third party would likely conclude that the threats to one or more of the fundamental principles are not at an acceptable level and the threats would need to be addressed.



Addressing Threats

Eliminate Circumstances

The audit manager should consider whether it is appropriate for the data analytics tool to provide the additional sales analysis, especially in light of the specific industry data set they have developed from their other audit clients in the same industry. The audit manager could discuss this matter with the engagement partner and suggest the additional insights are not provided to the audit client.

Apply Safeguards and Other Actions

To ensure the firm is not assuming management responsibilities in making these recommendations, the firm should ensure that the management of the audit client take responsibility for the advice and recommendations received (paragraph R400.14). A suitably qualified and knowledgeable individual at the audit client would need to be responsible for the recommendations, understand the service that is provided, be able to evaluate the adequacy of the results and accept responsibility for the actions to be undertaken as a result of this service. As the recommendations are provided through the data analytics tool, the individual at the audit client would have to have strong technological skills to be able to assess the results of the service.

Even if the audit client has an individual who can assume responsibility for the insights and the proposed sales strategy, the level of the threats might still not be at an acceptable level, especially as there are multiple threats to the fundamental principles and to the Independence of the auditor in this scenario.

Decline or End Professional Activity

If the audit manager or the firm cannot eliminate the circumstances creating the threats and no safeguards are available or capable of being applied to reduce the threats to an acceptable level, the audit manager should not disclose the business insights to the audit client (para R120.10(c)).

Preliminary Draft – for discussion purposes only

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 auditor independence requirements, which seek to raise the bar for ethical conduct and practice for all professional accountants through a robust, globally operable *International Code of Ethics for Professional Accountants (including International Independence Standards) (the Code)*.

Key Contacts

- Channa Wijesinghe, Chief Executive Officer, APESB channa.wijesinghe@apesb.org.au
- Ken Siong, Senior Technical Director, IESBA kensiong@ethicsboard.org
- Diane Jules, Deputy Director, IESBA dianejules@ethicsboard.org

The International Code of Ethics for Professional Accountants™ (including International Independence Standards™) is published by, and copyright of, IFAC. APESB, IESBA and IFAC do not accept responsibility for loss caused to any person who acts or refrains from acting in reliance on the material in this publication, whether such loss is caused by negligence or otherwise.

The 'Accounting Professional & Ethical Standards Board', 'APESB' and the APESB logo are registered trademarks of APESB in Australia and New Zealand. The 'International Ethics Standards Board for Accountants', 'International Code of Ethics for Professional Accountants (including International Independence Standards)', 'International Federation of Accountants', 'IESBA', 'IFAC', the IESBA logo, and IFAC logo are trademarks of IFAC, or registered trademarks and service marks of IFAC in the US and other countries.

DISCLAIMER: This paper is a non-authoritative publication. The Australian Accounting Professional & Ethical Standards Board (APESB), the International Federation of Accountants (IFAC), and the International Ethics Standards Board for Accountants (IESBA) do not accept responsibility for loss caused to any person who acts or refrains from acting in reliance on the material in this publication, whether such loss is caused by negligence or otherwise.

While this paper has been developed with contributions from the IESBA's Technology Working Group, it has not been discussed or approved by the IESBA. The views expressed in the paper are those of the authors and contributors and do not necessarily reflect the IESBA's views.

Copyright © [November 2021] APESB and IFAC. All rights reserved. Written permission from APESB or IFAC is required to reproduce, store or transmit, or to make other similar uses of, this document, save for where the document is being used for individual, non-commercial use only. Contact: <<xxx.yyy>>.

For translation requests, please consult IFAC's translation policy statement, and submit your request(s): Permission Request or Inquiry (log in required).