Basis for Conclusions
Prepared by the Staff of the IESBA®
April 2018

International Ethics Standards Board for Accountants®

Revisions Pertaining to Safeguards in the Code

IESBA International Ethics Standards Board for Accountants®

This document was prepared by the Staff of the International Ethics Standards Board for Accountants (IESBA).

The IESBA is a global independent standard-setting board. Its objective is to serve the public interest by setting high-quality ethics standards for professional accountants worldwide and by facilitating the convergence of international and national ethics standards, including auditor independence requirements, through the development of a robust *International Code of Ethics for Professional Accountants™ (including International Independence Standards™)* (the Code).

The structures and processes that support the operations of the IESBA are facilitated by the International Federation of Accountants® (IFAC®).

BASIS FOR CONCLUSIONS:
REVISIONS PERTAINING TO SAFEGUARDS IN THE CODE

CONTENTS

I. Introduction

1. Responsive to concerns raised by stakeholders, in particular by some regulators, in January 2015 the IESBA approved a project with the aim of improving the clarity, appropriateness, and effectiveness of the safeguards in the Code. The IESBA sought to:

   (a) Clarify the safeguards in the extant Code that were perceived as unclear and, where warranted, eliminate those that are inappropriate or ineffective;

   (b) Better correlate each safeguard with the threat it is intended to address; and

   (c) Clarify that not every threat can be addressed by a safeguard.

2. The revised safeguards provisions have been drafted using the new structure and drafting conventions for the Code.[1]

3. This Basis for Conclusions relates to, but does not form part of the *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the restructured Code). The document summarizes the revisions to the safeguards-related provisions in the extant Code and explains how the IESBA has addressed the significant matters raised on exposure. The safeguards-related revisions affect all Parts and Sections of the Code and were approved by the IESBA in December 2017 with the affirmative votes of 16 out of 16 members present.

II. Background

Approach to the Project

4. The Safeguards project was conducted as a two-phased project with two exposure drafts.

Phase 1

5. *Proposed Revisions Pertaining to Safeguards in the Code—Phase 1* (Safeguards ED-1) was released in December 2015 with a comment deadline of March 21, 2016. Safeguards ED-1 proposed an enhanced and more robust conceptual framework (i.e., restructured Section 120),[2] with corresponding changes relating to the application of the conceptual framework to professional accountants in public practice (PAPPs) (restructured Section 300).[3]

6. Fifty three comment letters were received from various respondents, including regulators and audit oversight authorities, national standard setters (NSS), firms, public sector organizations, preparers, IFAC member bodies and other professional organizations. There was general support for the proposals, as well as detailed suggestions for refinements and other comments.

7. The IESBA considered comments on Safeguards ED-1 during its June–December 2016 meetings, taking into account respondents' feedback as well as feedback from its Consultative Advisory Group (CAG), and agreed in principle the text of Phase 1 of the project in December 2016. A staff-prepared document, *Basis for Agreement in Principle for Proposed Revisions Pertaining to Safeguards in the Code—Phase 1* (Safeguards BFAP) was released in January 2017 in conjunction with the agreed-

---

1 The IESBA approved the final structure and drafting conventions for the Code as part of the restructured Code in December 2017 (see Basis for Conclusions for the Structure of the Code project).

2 Part 1 – Complying with the Code, Fundamental Principles and Conceptual Framework, Section 120, *The Conceptual Framework*

3 Part 3 – Professional Accountants in Public Practice, Section 300, *Applying the Conceptual Framework – Professional Accountants in Public Practice*

in-principle text to summarize and explain the rationale for the IESBA's conclusions in Phase 1 of the project.

Phase 2

8. *Proposed Revisions Pertaining to Safeguards in the Code—Phase 2 and Related Conforming Amendments* (Safeguards ED-2) was released in January 2017 with a comment deadline of April 25, 2017. Leveraging the enhancements relating to the conceptual framework in Phase 1 of the project, it proposed revisions to clarify the safeguards in the non-assurance services (NAS) and other sections of the Code.

9. Forty six comment letters were received from various respondents. Respondents from all stakeholder groups, including two Monitoring Group members, generally expressed support for the objective of the project. A substantive number of respondents were of the view that the project enhanced the clarity of provisions relating to safeguards in the Code.

10. The IESBA considered comments on Safeguards ED-2 during its June–December 2017 meetings and approved the safeguards-related revisions as part of the restructured Code in December 2017.

Matters to be Considered as Part of Development of Future IESBA Strategy and Work Plan

11. During the project, the IESBA considered comments from some stakeholders, in particular regulators, who were of the view that the IESBA should address broader concerns about the permissibility of NAS to audit and assurance clients. Specifically, it was suggested that:

- The Code would be improved with more requirements to prohibit the provision of certain NAS.
- The Code should include requirements in relation to fees charged for NAS provided to audit and assurance clients.
- The Code should expand on how materiality applies in the context of the Code. In addition, there were calls for guidance to explain the meaning of "significance" as it relates to identifying, evaluating and addressing threats.
- Additional guidance should be provided in the Code to clarify the IESBA's expectation about how compliance with the enhanced conceptual framework should be documented.
- The independence requirements for other assurance engagements with respect to public interest entities (PIEs) should be the same as for audits of PIEs.

IESBA Decisions

12. The IESBA determined that the above matters were outside of the scope of the project and should be considered as part of the development of its future strategy and work plan (SWP). The IESBA anticipates finalizing its SWP 2019-2023 by the end of 2018.

III. Enhancements to the Conceptual Framework for All Professional Accountants

Enhanced Conceptual Framework and Increased Prominence of Independence Provisions

13. The enhancements made to the conceptual framework include more explicit requirements relating to the threats and safeguards approach, as well as enhanced application material to explain how to

identify, evaluate and address threats to compliance with the fundamental principles and threats to independence.

14. The revisions will require a change in mindset in how PAs and firms apply the conceptual framework. In particular, they will require more careful thinking as to how an identified threat should best be addressed, and in particular whether an action will be effective in addressing the threat and therefore meet the revised description of a safeguard.

Independence

15. As explained in the Safeguards BFAP, and in response to respondents' suggestions, the enhanced conceptual framework now explicitly addresses independence.[4] New application material:

    (a) States that PAPPs are required to be independent when performing audits and other assurance engagements.

    (b) States that independence is linked to the fundamental principles, more specifically the principles of objectivity and integrity as stated in the extant definition of independence.

    (c) States that the conceptual framework set out in Section 120 to identify, evaluate and address threats to compliance with the fundamental principles applies in the same way to compliance with independence requirements.

    (d) Refers to the International Independence Standards (i.e., Part 4A – *Independence for Audits and Review Engagements* and Part 4B – *Independence for Other Assurance Engagements Other than Audit and Review Engagements* of the restructured Code) for requirements and application material regarding the application of the conceptual framework to maintain independence when performing audits and other assurance engagements.

    (e) Explains that the categories of threats to compliance with the fundamental principles (i.e., self-interest, self-review, advocacy, familiarity and intimidation) and the categories of threats to independence are the same.

    Refer also to the discussion in the sections "Overarching Requirements versus Ethical Outcomes" and "Requirement to Apply the Conceptual Framework" in the Basis for Conclusions for the Structure project.

Building Blocks Approach

16. The IESBA has applied a building blocks approach in restructuring the provisions in the extant Code. The enhanced conceptual framework set out in Part 1, Section 120, applies to all PAs and is not repeated in subsequent Parts or sections but is expected to be applied during the course of the engagement.

17. The provisions in Section 120 are not intended to be a "step-by-step checklist." Rather, they specify a logical and systematic approach for PAs to identify, evaluate and address threats irrespective of the facts and circumstances. All the provisions in the subsequent sections of the restructured Code build on the provisions in the conceptual framework, and provide general and context-specific guidance that might be relevant depending on the specific facts and circumstances of a particular

[4] The independence sections in the restructured Code are included in the *International Independence Standards*, which comprise Part 4A – Independence for Audit and Review Engagements (i.e., Sections 400 to 899) and *Part 4B – Independence for* Assurance Engagements Other than Audit and Review Engagements (i.e., Sections 900 to 999).

professional activity or service. Therefore, those subsequent provisions are incremental in nature and generally do not repeat the material in Section 120.

18. As an illustration of the building blocks approach:

    (a) In all situations, paragraphs 120.8 A1 to 120.8 A2 of the conceptual framework identify "factors relevant to evaluating the level of threats."

    (b) Incremental application material for evaluating threats is provided for professional accountants in business (PAIBs) in paragraphs 200.7 A15 to 200.7 A3 and for PAPPs in paragraphs 300.7 A1 to 300.7 A2.

    (c) Incremental context-specific factors are included in each Section and in each Part of the restructured Code to emphasize the factors that are relevant to evaluating the level of the threat created by the specific circumstance.[6] For instance, in relation to threats created by providing NAS to audit clients, paragraphs 600.5 A1 to 600.5 A4 include examples of factors that are relevant to all types of NAS that might be provided. Additionally, within each subsection of Section 600,[7] as appropriate, there are additional examples of factors that also apply based on the specific type of NAS.

Overarching Requirements

19. To help emphasize the need for a careful thought process when applying the enhanced conceptual framework, the overarching requirements clarify that in all three stages of the conceptual framework, i.e., identifying, evaluating and addressing threats, PAs are required to:

    (a) Exercise professional judgment, based on an understanding of known facts and circumstances;

    (b) Use the reasonable and informed third party test; and

    (c) Remain alert for new information and to changes in facts and circumstances.

Professional Judgment

20. The IESBA concurrently approved new application material relating to professional judgment to clarify the importance of PAs obtaining a sufficient understanding of the facts and circumstances, known to them, when exercising professional judgment in applying the conceptual framework. This new application material was developed as part of the short term project on professional skepticism (see the Basis for Conclusions for Professional Skepticism and Professional Judgment).

Reasonable and Informed Third Party (RITP)

21. Phase 1 of the safeguards project emphasized the existing requirement for PAs to use the RITP test when applying the conceptual framework, clarifying what is meant by the RITP.

22. Respondents were supportive that the description of the RITP test makes it explicit that the RITP does not need to be an accountant. Some respondents, however, queried whether the test should incorporate the views of the public in whose interests the PA has a responsibility to act, for example

---

5 Part 2– Professional Accountants in Business, Section 200, *Applying the Conceptual Framework – Professional Accountants in Business*

6 See relevant sections in Parts 2, 3, and the International Independence Standards (i.e., Parts 4A and 4B).

7 Part 4A, Section 600, *Provision of Non-assurance Services to an Audit Client*

an "investor perception test." In addition, some regulatory respondents expressed concern about use of the word "experience" in the description of RITP.

IESBA Decision

23. It is important that the Code explain the characteristics of the RITP in a manner that is clear. The application material[8] clarifies that the RITP test is:

- Applied from the perspective of a third party who is objective, and one who weighs all the relevant facts and circumstances that the accountant knows, or could reasonably be expected to know, at the time the conclusions are made.
- A consideration by the PA about whether the same conclusions would likely be reached by that third party.

24. The Board reaffirmed its view that:

(a) The RITP does not need to be an accountant but rather applies the lens of an objective third party.

(b) The RITP test should be broad enough to apply to all situations covered by the Code. Accordingly, a focus only on an investor's perspective would be too narrow and might not, for example, address situations in the public and non-profit sectors.

(c) The RITP is not expected to be knowledgeable about all the matters in the Code. However, the RITP cannot be an uninformed member of the public, but rather someone who "would possess the relevant knowledge and experience to understand and evaluate the appropriateness of the accountant's conclusions in an impartial manner."

The Board considered that the meaning of the word "objective" as suggested by a respondent is not substantively different from "impartial" as used in the revised text.

Stages in the Conceptual Framework

25. The IESBA reaffirmed that the three-stage conceptual framework remains appropriate and, as described in the BFAP, refined the proposals in Safeguards ED-1, to clarify the three stages as follows:

(a) Identifying threats;

(b) Evaluating the threats, including a requirement to re-evaluate and address new threats identified as part of the PA's responsibility to properly evaluate threats; and

(c) Addressing the threats, including a new requirement to "step back" to review the overall conclusion about whether the threats have been addressed as part of the PA's responsibility to properly address threats.

Identifying Threats

26. As outlined in the BFAP, the IESBA is of the view that it is an important part of the conceptual framework that PAs be required to identify threats to compliance with the fundamental principles. Accordingly, it has made revisions to:[9]

---

[8] Part 1, Section 120, paragraph 120.5 A4

[9] See Part 1, Section 120, paragraphs R120.6–120.6 A4.

- Explain that understanding the facts and circumstances enables the PA to identify threats. Also, the revisions clarify that "facts and circumstances" include any professional activities, interests and relationships that might compromise compliance with the fundamental principles.
- Indicate that threats to compliance with the fundamental principles might be created by a broad range of facts and circumstances, and that it is not possible to fully describe all of those facts and circumstances in the Code.
- Describe the various categories of threats to compliance with the fundamental principles.
- Explain that the existence of certain conditions, policies and procedures established by the profession, legislation, regulation, the firm or employing organization might assist in identifying threats to compliance with the fundamental principles.

27. The IESBA notes that some respondents are of the view that providing NAS to audit clients always creates some threat(s) to independence. Accordingly, the IESBA has revised the provisions in Section 600 to specify the types of threat(s) that might be created when providing a specific NAS to an audit client.

Evaluating the Level of Threats, Including Re-evaluating and Addressing New threats Identified

28. The enhanced conceptual framework stresses the importance of remaining alert throughout the process of identifying, evaluating and addressing threats. It includes a requirement for PAs to "remain alert for new information and to changes in facts and circumstances" (see paragraph R120.5 (b)). This means that if a 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 accountant is required to re-evaluate and address that threat accordingly. New application material explains that remaining alert throughout the professional activity assists the PA in determining whether new information has emerged or changes in facts and circumstances have occurred (see paragraphs 120.9 A1-120.9 A2).

29. From a practical perspective, it is expected that PAs would apply the provisions for evaluating threats by considering the factors that are relevant to evaluating threats provided in Section 120 as well as those included in subsequent sections of the restructured Code. The factors that are relevant to evaluating threats would likely be considered:

    (a) When a threat is identified to determine whether it is at an acceptable level. No further action need be taken for threats that are at an acceptable level; and

    (b) To determine whether an action taken by the PA is effective in reducing the threat to an acceptable level, and therefore qualifies as a safeguard.

30. Some regulators, including a Monitoring Group member, suggested that the re-evaluation of threats should not be restricted to when there is new information but "rather as a constant state of awareness" and that PAs should engage in periodic re-evaluation of threats on a timely basis to evaluate new information or potential changes in facts and circumstances.

IESBA Decision

31. The application material clarifies that if new information results in the identification of a new threat, the PA is required to evaluate and, as appropriate, address the threat. With respect to the suggestion to set a specific timeframe for re-evaluating threats in the Code, the IESBA determined that a

principles-based approach based on the re-evaluation being triggered by the PA's knowledge of new information or changes in facts and circumstances, coupled with the requirement to remain alert throughout the professional activity to such changes, would be more robust.

Addressing Threats, Including "Step Back" Provisions

32. Phase 1 of the project established a new requirement to assist PAs in addressing threats, requiring an overall assessment which involves:

    (a) Forming an overall conclusion about whether the actions that they have taken, or intend to take, to address the threats will eliminate those threats or reduce them to an acceptable level; and

    (b) Reviewing any significant judgments made or conclusions reached, and using the reasonable and informed third party test.

33. Some respondents sought further guidance as to how PAs should determine the appropriateness of actions taken to reduce threats to an acceptable level. A regulator, who was also a Monitoring Group member raised a concern about a perceived lack of clarity regarding the timing of the overall assessment.

IESBA Decision

34. The IESBA considers that the proper application of the enhanced conceptual framework is critical to ensure that threats to compliance with the fundamental principles that are not at an acceptable level are appropriately addressed.

35. The enhanced conceptual framework makes it explicit that applying safeguards is only one of three ways to address threats. Specifically, threats can be addressed by:

    (a) Eliminating the circumstances, including interests or relationships, that are creating the threat;

    (b) Applying safeguards, when available and capable of being applied; or

    (c) Declining or ending the specific professional activity.

36. The enhanced conceptual framework requires PAs to think about the specific facts and circumstances, including the nature of the professional activity, interests and relationships, creating the threats to determine whether an "action(s) taken to address them are, individually or in combination, effective in reducing such threats to an acceptable level."

37. The PA's understanding of the facts and circumstances and the PA's exercise of professional judgment are both critical to determining the appropriateness and effectiveness of safeguards.

38. The IESBA determined that the enhanced conceptual framework, properly applied, will guide PAs and firms to determine the appropriateness and effectiveness of a safeguard.

39. In response to the regulatory concern regarding the timing of the overall assessment, the IESBA has positioned the requirement for an overall assessment under a revised sub-heading titled "Consideration of Significant Judgments Made and Overall Conclusions Reached" within the "Addressing Threats" subsection to make it clear that the overall assessment forms part of the "Addressing Threats" stage of the conceptual framework.

Determining when a Threat is Reduced to an Acceptable Level

Conditions, Policies and Procedures

40. In finalizing Phase 1 of the project, the IESBA determined that conditions, policies and procedures, are no longer categorized as safeguards. Once a threat is identified, the PA is required to evaluate whether the threat is, or is not at an acceptable level. The IESBA determined that conditions, policies and procedures are the factors that are to be considered when evaluating whether a threat is at an acceptable level. If a threat is not at an acceptable level, the PA is required to address the threat either by:

    (a) Eliminating the circumstances, including interests or relationships, that are creating the threats;

    (b) Applying safeguards, where available and capable of being applied, to reduce the threats to an acceptable level; or

    (c) Declining or ending the specific professional activity.

41. Feedback received from respondents to Safeguards ED-2 indicated that there was some confusion between "factors relevant to evaluating threats" and "safeguards." Also, some respondents, particularly from the small and medium practices (SMPs) community, expressed concern about the reduction in the number of safeguards being available to firms when applying the revised conceptual framework.

IESBA Decisions

42. The IESBA reaffirmed its Phase 1 decision that conditions, policies and procedures are no longer safeguards under the revised description of a safeguard because they are not specific actions that the PA, firm or network firm takes to reduce threats to an acceptable level. However, a practical consideration that will factor into a PA's evaluation of the level of a specific threat is the PA's judgment about whether those conditions, policies and procedures contribute in reducing the threat to an acceptable level.

43. In response to feedback received from respondents, the IESBA has made a refinement to refer to those conditions, policies and procedures as "factors that are relevant in evaluating the level of threats…" (refer to paragraph 120.8 A2). This change is intended to clarify the role of conditions, policies and procedures in applying the conceptual framework. The refinement also improves the connectivity between Phases 1 and 2 of the project because it introduces the phrase "…factors that are relevant in evaluating the level of threats…" (which is used throughout the Code) into the conceptual framework set out in Section 120.

44. The IESBA acknowledges that some firms, particularly those in the SMP community, might continue to face practical challenges in applying appropriate safeguards given resource constraints.

Description of Safeguards

45. The revised description of a "safeguard"[10] clarifies that safeguards are actions, individually or in combination, that the PA takes that effectively reduces threats to compliance with the fundamental principles to an acceptable level. The revisions to the description of safeguards in the agreed-in-principle text emphasized that safeguards are applied when available, and capable of being applied to reduce threats to an acceptable level (see paragraph R120.10(b)).

46. Respondents to Safeguards ED-2 requested further guidance to help PAs and firms determine whether an action is effective and appropriate in reducing a threat to an acceptable level, and therefore qualifies as a safeguard. A more detailed discussion of the IESBA's response to

[10] Part 1, Section 120, paragraph 120.10 A2

respondents' comments about the appropriateness of NAS safeguards and what is involved in a review that meets the description of a safeguard is included below under the subheading titled "Examples of Actions that Might be Safeguards."

IESBA Decision

47. In response to the feedback from respondents, the IESBA determined to make the following enhancements:

- Amending the description of a safeguard to emphasize that safeguards are applied to *reduce* threats to an acceptable level. The idea that a safeguard reduces threats implies that safeguards are addressing specific threats.
- Repositioning examples of actions that might eliminate threats before examples of actions that might be safeguards.
- Clarifying that safeguards cannot eliminate threats. Accordingly, revised application material under a sub-heading "Actions to Eliminate Threats" explains that there are some situations in which threats can only be addressed by declining or ending the specific professional activity.[11]

48. A more consistent approach is used across the various sections in the Code to achieve the objective of increasing the connectivity of the examples of actions that might be safeguards to specific types of threats. This includes having:

(a) An introductory paragraph that emphasizes the specific type or category of threats that might be created by a particular circumstance (unless it is determined that all threats are likely to be created);

(b) Tailored application material to assist in evaluating and addressing specific threats that might be created. This application material provides:

(i) Examples of factors that might be relevant in evaluating threats;

(ii) Examples of actions that might eliminate threats; and

(iii) Examples of actions that might be safeguards to address the specific type or category of threat(s).

49. Regarding the examples of actions that might be safeguards in the restructured Code, in most situations where the facts and circumstances are similar to those described in the Code, the IESBA expects that such actions would be effective in reducing threats to an acceptable level and would therefore be safeguards. However, the list of examples in the Code is not intended to be all-inclusive, and the examples of actions included therein are not guaranteed to be safeguards in all situations.

Description of Acceptable Level

50. The description of the term "acceptable level" was revised to be expressed in an affirmative manner in the agreed-in-principle text, to state that "An acceptable level is the level at which a professional accountant using the reasonable and informed third party test would likely conclude that the accountant complies with the fundamental principles."[12]

---

[11] Part 1, Section 120, paragraph 120.10 A1

[12] Part 1, Section 120, paragraph 120.7 A1

51. A few respondents expressed concern that the term “acceptable level” sets too low a bar and that the words “would likely” may not convey certainty.

IESBA Decision

52. The IESBA reaffirmed that the new description of the term “acceptable level” in paragraph 120.7 A1 is appropriate. The IESBA did not take on the suggestion to replace the word “likely” with “probably”, because the IESBA determined that these two words mean essentially the same thing. The IESBA, however, agreed to give the concept of “acceptable level” greater prominence in the restructured Code by positioning it under its own subheading titled “Acceptable Level”.

IV. Revisions to PAIB Provisions

53. Incremental application material that builds on the enhanced conceptual framework for evaluating threats has been added for PAIBs (refer paragraphs 200.7 A1 - A3). Some respondents questioned whether certain provisions in Safeguards ED-2 were consistent with the safeguards-related agreed-in-principle text.

IESBA Decision

54. In response to requests from some respondents on Safeguards ED-2, the IESBA has included safeguards-related consistency revisions in Section 200. Those revisions relate to:

- How the term “facts and circumstances” is used.
- The introductory paragraphs in each section of the Code.
- How threats are described in the Code.
- The examples of factors relevant to evaluating threats.
- The examples of actions to address threats.

V. Revisions to PAPP Provisions

55. As explained in the BFAP, respondents to Safeguards ED-1 were generally supportive of proposals in Section 300 to enhance the application of the conceptual framework by PAPPs. However, some respondents, sought clarification on the linkage between the conceptual framework set out in Section 120 and the provisions relating to PAPPs applying the conceptual framework in Section 300.

56. Some respondents sought clarification as to what is involved in a review that meets the description of a safeguard and whether or not the professional doing the review should be independent.

57. Some regulators queried the appropriateness of “using professionals who are not members of the firm’s audit team to provide the NAS or, if the work is done by a member of the audit team, having another professional outside the audit team review the work” as a safeguard.

IESBA Decision

58. In order to clarify the linkage between Sections 120 and 300, the IESBA made several refinements to Section 300, which include removing the following as examples of safeguards in Section 300:

- “…consulting or seeking approval from those charged with governance or an independent third party…”; and
- “… providing advice…”

59. In response to questions about characteristics and attributes of the "professional" doing a "review" that meets the description of a safeguard, the following clarifications were made in paragraphs 300.8 A1 to 300.8 A4):

- The term "appropriate professional" has been changed to "appropriate reviewer";
- An "appropriate reviewer" is a professional, who in many instances may be a PA; and
- An "appropriate reviewer" would have the necessary knowledge, skills, experience and authority to review, in an objective manner, the relevant work performed or service provided.

60. Also, within Section 300, the IESBA made refinements to the examples of factors and actions that might be safeguards so that they address the specific category of threat and the situation described. For example:

- Self-interest threats created from contingency fees (see paragraphs 330.4 A2 to 330.4 A3; 410.12 A2 to 410.12 A3; and 905.9 A3).[13]
- Self-interest threats created when a PA pays or receives a referral fee or receives a commission in relation to a client (see paragraph 330.5 A2).
- Familiarity or self-interest threats created by long association with a client (see paragraphs 540.3 A6 and 940.3 A6).[14]
- Self-review threats created by providing tax calculations (see paragraphs 604.5 A1 to 604.6 A1).

61. A more detailed discussion of the IESBA's response to respondents' comments about the appropriateness of NAS safeguards and what is involved in a review that meets the description of a safeguard is included below under the subheading titled "Examples of Actions that Might be Safeguards."

VI. NAS Provisions for Audits

Overview of Key Provisions Relating to NAS

62. The changes made to the NAS sections of the Code are to explain how firms and network firms should apply the enhanced conceptual framework to identify, evaluate and address threats to independence created by providing NAS to audit or assurance clients. The changes also clarify the examples of actions that might be safeguards to address threats created by providing a NAS to an audit client by, ensuring that they:

(a) Meet the enhanced description of safeguards; and

(b) Are linked to, and address specific threats.

63. With the exception of recruiting services which is discussed under the heading titled "Prohibition of Certain Recruiting Services," the IESBA did not propose changes to the specific types of NAS addressed in the Code, or the provisions relating to the permissibility of NAS (see section titled

---

[13] Part 3, Section 330, *Fees and Other Types of Remuneration*

Part 4A, Section 410, *Fees*

Part 4B, Section 905, *Fees*

[14] Part 4A, Section 540, *Long Association of Personnel (Including Partner Rotation) with an Audit Client*

Part 4B, Section 940, *Long Association of Personnel with an Assurance Client*

"Matters to be Considered as Part of the Development of Future IESBA Strategy and Work Plan" above).

64. In finalizing Safeguards ED-2, the IESBA reassessed and retained most of the examples of safeguards relating to NAS. However, the IESBA determined to make a number of refinements to:

    (a) Explain that the examples are "actions that might be safeguards" to address the threat created by providing the specific type of NAS. This change is intended to prompt firms and network firms to be mindful of other actions that might be more appropriate to address specific threats, depending on the facts and circumstances of each specific engagement and NAS;

    (b) Clarify that seeking advice from another party no longer meets the revised description of a safeguard;[15]

    (c) Increase the prominence of the requirement that prohibits firms from assuming a management responsibility when providing a NAS to an audit client;

    (d) Add new application material for evaluating and addressing threats in relation to NAS, specifically new application material with respect to materiality in relation to an audit client's financial statements;

    (e) Include clear, explicit and prominent statements that in certain situations, the Code prohibits firms and network firms from providing certain NAS to an audit client because there can be no safeguards to address the threats to independence. These highlight that safeguards may not in all cases be sufficient to address an independence threat; and

    (f) Clarify that the threats created from providing multiple NAS to an audit client are to be identified, evaluated in aggregate and addressed.

General Provisions

65. The IESBA is of the view that, as a result of new business practices, the evolution of financial markets and changes in information technology amongst other developments that it is impossible for the Code to include an all-inclusive list of NAS that might be provided to an audit client. Accordingly, the IESBA's proposals in Safeguards ED-2 states this, and built on the provisions in the enhanced conceptual framework to emphasize the general provisions that are always applicable, irrespective of the type of NAS being provided. Also, increased prominence was given to the extant provisions related to the prohibition to assume a management responsibility when providing a NAS to an audit client, and the following new application material added to:

    - Remind firms of the responsibility to evaluate the level of any threats created by providing a NAS to an audit client, including a list of factors to consider to assist PAs in making that evaluation.
    - Explain materiality in context of a financial statement audit.
    - Clarify the provision relating to circumstances in which a firm provides multiple NAS to the same audit client.

66. Respondents to Safeguards ED-2 were generally supportive of the enhanced general NAS provisions in the Code, but some, including two Monitoring Group members, suggested refinements and

[15] The extant include "providing advice" as an example of a safeguard (see extant Part B – *Professional Accountants in Public Practice*, Section 290, *Independence – Audit and Review Engagements*, paragraphs, 290.180, 290.186, 290.187, 290.205, 290.207, 290.211 and 290.212).

clarifications. The Monitoring Group members questioned whether sufficient guidance had been provided in the Code in relation to addressing threats, in particular when applying a safeguard.

IESBA Decision

67. The IESBA determined to revise and refine paragraphs R600.4 to R600.10 to incorporate the several suggestions from respondents to Safeguards ED-2 in relation to the general provisions that firms are expected to apply in all circumstances when providing a NAS to an audit client. Significant revisions made to the proposals in Safeguards ED-2 include:

- New application material to better link the provisions in Section 600 to (a) the overarching requirements to address threats in the conceptual framework set out in Section 120; and (b) the examples of actions, including safeguards, that might address threats to independence (see paragraphs 600.6 A1 to 600.6 A2).
- Refinements to the examples of factors for evaluating the level of any threats created by providing a NAS to an audit client (see paragraph 600.5 A1).
- Improvements to the structure of the general provisions, including changes to the placement of the material and to the subheadings.

Prohibition of Certain Recruiting Services

68. Respondents' views were mixed about the proposal to expand the prohibition on auditors providing certain recruiting services to all audit clients. The prohibition in the extant Code is for audits of PIEs only.

69. While many regulators and NSS supported the proposal, there were strong concerns from SMPs on the grounds that:

- Audit clients that are not PIEs look to the expertise of their auditor to assist them in finding strong, qualified candidates for finance and accounting positions within their organization. In their view, the proposal would create significant challenges for SMPs who lack the resources to recruit competent directors or senior management.
- The existence of any self-interest or familiarity threats that may be created by performing these recruiting services could be reduced to an acceptable level with the application of safeguards. Therefore, there was a view that the proposal went beyond the scope of the project.

IESBA Decision

70. One objective of the project was to eliminate safeguards that are inappropriate or ineffective. The IESBA considered examples of safeguards that respondents believed might address threats created by providing specific types of recruiting service to entities that are not PIEs.

71. After further careful deliberation, the IESBA reaffirmed its decision to extend the prohibition as proposed. The IESBA remains of the view that there are no safeguards that will be effective in reducing actual or perceived self-interest and familiarity threats created by searching for or seeking candidates and undertaking reference checks for directors, officers or a member of senior management in a position to exert significant influence over the preparation of the client's accounting records or financial statements for audit clients. As a result, consistent with the objective of eliminating safeguards that are inappropriate or ineffective, the IESBA reaffirmed that this amendment was within the scope of the project.

72. In recognition of the concerns raised by SMPs, however, the IESBA agreed to:

    (a) Include new guidance to describe recruiting services more broadly to emphasize the wide range of services that might be provided (see paragraph 609.3 A1);

    (b) Establish a new requirement to establish the prerequisite client responsibilities for when a firm or network firm provides recruiting services to an audit client in order for the firm or network firm to avoid assuming management responsibility (see paragraph R609.4). This requirement is consistent with existing requirements relating to providing IT and internal audit services to audit clients.

    (c) Clarify the types of recruiting services that do not usually create threats and indicate those might involve assuming management responsibilities (see paragraph 609.3 A2). In this regard, the IESBA has added subheadings to emphasize the types of recruiting services that are prohibited (see the subheading titled "Recruiting Services that are Prohibited" above paragraphs R609.6 to R609.7).

Examples of Actions that Might be Safeguards

73. The examples of actions in Section 600 that might be safeguards to address specific threats created by providing NAS to audit clients may be categorized as follows:

    (a) Using professionals who are not audit team members to perform the NAS.

    (b) If the NAS is performed by an audit team member, using professionals who are not audit team members, with appropriate expertise to review the NAS.

    (c) Having a professional review the audit work or result of the NAS.

    (d) In some cases, having a professional who was not involved in providing the NAS review the accounting treatment or presentation in the financial statements.

74. One key objective of the project was to align the examples of actions that might be safeguards in the Code to the specific types of threats that they are intended to mitigate.

75. Some respondents to Safeguards ED-2 expressed concerns:

    - That examples of safeguards should be tailored so that they are appropriate to address specific threats.
    - About the withdrawal of certain safeguards, for example, the removal of "obtaining advice from a third party" in certain circumstances.
    - That the example of an individual PA within a firm doing a review may not be an appropriate safeguard because that individual may be inclined to make judgments that protect the economic and other interests of the firm rather than the public interest.
    - That the Code does not explicitly address "use of independent external consultants."

IESBA Decision

76. The IESBA carefully reviewed the appropriateness of the examples of actions that might be safeguards, depending on the specific facts and circumstances. As a result, the IESBA made a number of refinements to ensure that there is an explicit linkage between the examples of actions and the specific threats in subsections 601 to 610.

77. The IESBA considered whether safeguards involving the use of another professional to review the audit or NAS work should be limited to a professional external to the firm, but agreed that the Code should remain principles-based. The IESBA determined that the examples of safeguards in the Code should be neutral and should not distinguish between actions that might be performed by professionals who are employed by the firm versus those who are external to the firm, provided that those professionals are not involved in the audit. The exercise of professional judgment is needed to help firms and network firms make that determination. For example, for SMPs, it might be appropriate for the professionals used for reviewing the NAS or the audit work to be individuals external to the firm or network firm.

Advocacy Threats

78. Some respondents to Safeguards ED-2 requested further guidance for identifying, evaluating and addressing advocacy threats, in particular in relation to NAS provisions.

79. Concern was expressed by some that anytime an auditor promotes or advocates on behalf of the client, the auditor's objectivity is compromised and the auditor will be biased in advancing the client's interests (i.e., the existence of an advocacy threat would exist irrespective of whether the amounts involved are immaterial).

IESBA Decision

80. The restructured Code indicates that assuming a management responsibility creates a familiarity threat and might create an advocacy threats because the firm or network firm becomes too closely aligned with the views and interests of management.

81. The IESBA has added a number of more specific references to "advocacy threats" created by providing a specific type of NAS to subsections relating to valuation services, tax services, litigation support, legal services and corporate finance services. The additional material includes examples of factors to evaluate such advocacy threats and examples of actions that might address such threats.

82. The IESBA revisited the list of factors in evaluating and addressing the level of advocacy threats throughout the Code to determine their appropriateness in light of the specific facts and circumstances described.

83. The IESBA reaffirmed its view about the appropriateness of the examples of factors that are relevant in evaluating the level of threats and examples of actions that might: (i) eliminate a threat, or (ii) be a safeguard to address each specific threat.

VII. NAS Provisions for Other Assurance Engagements

84. The IESBA agreed that the revisions made in finalizing Section 600 in Part 4A for audit engagements should form the basis for revising the NAS section of the Code relating to other assurance engagements in Part 4B, Section 950.[16] Therefore, while they are adapted as necessary, the provisions in Section 950 are closely aligned to those in Section 600.

85. A substantive number of respondents expressed support for the approach taken to develop Section 950. However, some respondents, in particular regulators, questioned whether the independence provisions relating to other assurance engagements in Part 4B should be the same as those for audits

[16] Part 4B, Section 950, *Provision of Non-assurance Services to Assurance Clients Other than Audit and Review Engagement Clients*

and review engagements, in particular for PIEs in Part 4A.

IESBA Decision

86. The IESBA determined that a consideration of extending the independence provisions in the Code that apply to assurance engagements other than audits as suggested by some of the respondents would go beyond the scope of the project.

VIII. Effective Date

87. The effective date for the restructured Code, to which the safeguards-related provisions are a part of, is discussed in the Basis for Conclusions for the Structure project.

Published by: IFAC International Federation of Accountants®

IESBA
International
Ethics Standards
Board for Accountants®

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 **F** +1 (212) 286-9570
www.ethicsboard.org