Safeguards—Issues and Task Force Proposals

How the Project Serves the Public Interest

Varying views exist on what constitutes a safeguard as well as on the effectiveness and appropriateness of safeguards within the Code. This project will address the clarity of the guidance provided on safeguards and examine the robustness of specific safeguards pertaining to non-assurance services (NAS). Through enhanced clarity, the project will promote compliance by professional accountants (PAs) with the fundamental principles. Through enhancing the robustness of safeguards in the Code in addressing threats to compliance with the fundamental principles and threats to independence, the project will serve to support PAs in fulfilling their responsibility to act in the public interest and in supporting audit quality.

Contents

1. This paper sets out the following matters for consideration by IESBA members:

A. Clarifying the Conceptual Framework

2. In considering the reasonable and informed third party concept (see section B), the Task Force also considered the conceptual framework as set out in Section 100 of the Code.[1] It noted that the concept of a reasonable and informed third party is first introduced in the Code in paragraph 100.2(c).

3. The Task Force believes that paragraph 100.2(c) creates ambiguity regarding the objective of the conceptual framework. It noted that paragraph 100.2(c) could be seen to suggest that the objective of the conceptual framework is the application of safeguards rather than the elimination or reduction of threats to the fundamental principles.

4. The Task Force proposes to redraft paragraph 100.2 to:

   - Re-focus the conceptual framework on the elimination or reduction of threats to the fundamental principles; and

[1] Section 100, *Introduction and Fundamental Principles*

- Re-position the discussion on safeguards and the reasonable and informed third party concept later in Section 100.

5. The changes proposed to paragraph 100.2 by the Task Force are shown below:

> This Code contains three parts. Part A establishes the fundamental principles of professional ethics for professional accountants and provides a conceptual framework that professional accountants shall apply to:
>
> (a) Identify threats to compliance with the fundamental principles;
>
> (b) Evaluate the significance of the threats identified; and
>
> (c) ~~Apply safeguards, when necessary, to e~~Eliminate the threats or reduce them to an acceptable level. ~~Safeguards are necessary when the professional accountant determines that the threats are not at a level at which a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances available to the professional accountant at that time, that compliance with the fundamental principles is not compromised.~~
>
> A professional accountant shall use professional judgment in applying this conceptual framework.

6. The Task Force believes that the conceptual framework can be aligned to the approach taken by the International Auditing and Assurance Standards Board's (IAASB's) International Standards on Auditing (ISAs) in relation to performing an audit. The ISA approach requires auditors to:

- Identify and assess risk;[2]
- Design audit response;[3] and
- Evaluate audit response.[4]

7. The Task Force believes the following shows the application of the ISA approach to the conceptual framework.

Identify Threats to Compliance with the Fundamental Principles • Identify threats to compliance with the fundamental principles, through understanding the circumstances or relationships that may compromise compliance with the fundamental principles.
Evaluate the Significance of the Threats Identified • Evaluate the significance of threats to compliance with the fundamental principles, through understanding the circumstances or relationships that may compromise compliance with the fundamental principles. Take into account qualitative as well as quantitative factors.

[2] ISA 315 (Revised), *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment*

[3] ISA 330, *The Auditor's Response to Assessed Risks*

[4] ISA 330

Eliminate Threats to the Fundamental Principles or Reduce Them to an Acceptable Level

Respond to Threats

- Apply safeguards, through designing and implementing appropriate actions or measures in response to those threats.
- In designing and implementing appropriate actions or measures, the professional accountant shall:
  - (a) Consider other circumstances or relationships that the professional accountant knows, or may reasonably be expected to know, also create threats to compliance with the fundamental principles.
  - (b) Determine whether appropriate actions or measures are available and can be applied.
  - (c) Exercise professional judgment and take into account whether a reasonable and informed third party, weighing all the specific facts and circumstances available to the professional accountant at the time, would be likely to conclude that the threats would be eliminated or reduced to an acceptable level by the actions or measures, such that compliance with the fundamental principles is not compromised.
- Decline or discontinue the specific professional activity or service involved or, when necessary resign from the engagement (in the case of a PA in public practice) or employing organization (in the case of a PA in business (PAIB)), if threats are not at an acceptable level.

Evaluate response to threats

- Evaluate/conclude, weighing all the facts and circumstances available at that time, whether the designed actions or measures are effective safeguards before continuing with the professional activity or service involved.
- Re-assess the threat, respond to the threat and evaluate the response[5] whenever new information about a threat or a safeguard arises during an engagement.

8. During its discussions on threats (see section G), the Task Force noted that non-compliance with one fundamental principle could also result in non-compliance with another fundamental principle. For example, non-compliance with the fundamental principle of professional competence and due care could result in non-compliance with the fundamental principle of confidentiality.

9. The Task Force proposes adding guidance to Section 100 to explain that:

   - Non-compliance with one fundamental principle may result in non-compliance with another fundamental principle.
   - Identification of threats supports compliance with the fundamental principles.
   - Other factors may exist which threaten compliance with the fundamental principles.

[5] Section 290, *Independence – Audit and Review Engagements*, paragraph 290.10

10. As a result of the changes proposed to paragraph 100.2(c), the Task Force believes Section 100 would also benefit from adopting the ISA approach and, subject to the work of the Structure of the Code Task Force, being restructured as follows.

Section 100 Extant Code	**Proposed Re-ordering of Section 100**
Introduction • Description of acting in the public interest • Requirement to comply with the Code • Requirement to apply the conceptual framework • Cross reference to other parts of the Code	Introduction • Description of acting in the public interest • Requirement to comply with the Code • **Requirement to comply with the fundamental principles** • Requirement to apply the conceptual framework (paragraph 100.2(c) redrafted)
Fundamental Principles	
Conceptual Framework approach	Conceptual Framework Approach
Threats and Safeguards	*Identify threats to compliance with the fundamental principles* *Evaluate the significance of the threats identified* *Eliminate threats to the fundamental principles or reduce them to an acceptable level* • Acceptable level including reasonable and informed third party • Applying safeguards
Conflicts of Interest *Ethical Conflict Resolution*	Ethical Conflict Resolution
Communicating with TCWG	Communication with TCWG

Stepping Back

11. In its response to the Structure of the Code consultation paper, a regulatory respondent[6] commented as follows:

> In practice, on more than an infrequent basis, auditor oversight and securities regulators have encountered auditors who attempt to justify their actions by indicating compliance with the requirements without stepping back to determine if the facts and circumstances suggest that the fundamental principles may be violated though the requirements were achieved.

[6] International Organization of Securities Commissions

> The fundamental principles are not simply background information but are overarching objectives that auditors must meet whereas the standards-specific requirements capture specific areas identified by the Board to which auditors must comply. We believe greater emphasis should be placed on the need for auditors to step back after complying with the standards-specific requirements to determine if, based on the facts and circumstances, the auditor is independent with respect to the fundamental principles.

12. The Task Force notes that the overarching requirement of the Code is for the professional accountant to comply with the fundamental principles.[7] The Task Force believes the requirement to "step back" is implicit within the conceptual framework. It believes that re-focusing the objective of the conceptual framework on the elimination or reduction of threats to the fundamental principles and the proposals to restructure Section 100 of the Code clarify this requirement further.

13. The Task Force also notes that ISA 220[8] and ISA 300[9] include existing requirements for auditors to assess whether the firm is independent.

Matters for Consideration

1. IESBA members are asked for views on following an ISA-style approach to responding to threats.
2. Do IESBA members agree that re-focusing the conceptual framework on compliance with the fundamental principles and the elimination or reduction of threats clarifies the requirement to "step back?"

B. Reasonable and Informed Third Party

14. The Task Force is of the view that the concept of a reasonable and informed third party is fundamental to assessing whether the safeguards applied are effective in eliminating or reducing the threat to an acceptable level. When applying the conceptual framework, a professional accountant is required to determine whether the safeguards applied are effective at eliminating or reducing threats to an acceptable level. The Code defines an "acceptable level" as:

> A level at which a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances available to the professional accountant at that time, that compliance with the fundamental principles is not compromised.

15. The Task Force notes that the reasonable and informed third party test is also specifically referred to in many places throughout the Code. Through its inclusion within the definition of "Independence in Appearance," the reasonable and informed third party test is also part of the definition of independence.

16. The Task Force believes that the test is intended to be an objective test. It is of the view that the test is important in stepping back to consider whether compliance with the fundamental principles is compromised.

---

7 Paragraph 100.5

8 ISA 220, *Quality Control for an Audit of Financial Statements*, paragraphs 9 – 11

9 ISA 300, *Planning an Audit of Financial Statements*, paragraph 6

17. The Task Force considered whether a reasonable and informed third party should be another professional accountant. It believes that it may be relevant to consider the views or actions of another professional accountant in a similar situation but that this should not be the only consideration.

18. The Task Force is of the view that it is important to clarify that a "reasonable and informed third party" is a conceptual person. It believes that the characteristics of a reasonable and informed third party would rarely be found in one person. Instead, the Task Force believes that the concept is most similar to an arbitrator, i.e., a body that is able to consider all aspects of the facts and circumstances of a situation and the views and positions of multiple parties, such as the professional accountant, client, investors or regulators, who may have an interest in the outcome of a decision. It also believes the test is not intended to represent the views of any one party. However, depending on the specific situation, the views of one or more stakeholders may take priority over the views of other stakeholders.

19. The Task Force recognizes that the public interest, and therefore the view of a reasonable and informed third party, in a specific situation may be different depending on the facts and circumstances and stakeholders concerned.

20. The Task Force is of the view that there may be a lack of understanding of the concept by users of the Code. It believes that clarifying the Code in relation to the reasonable and informed third party test would assist PAs in determining whether the safeguards applied have reduced threats to an acceptable level.

21. Due to the variable nature of a reasonable and informed third party, the Task Force is of the view that it would not be appropriate to define the concept. It believes that the Code could be improved by adding guidance that:

    - Sets out the purpose of the test.
    - Describes the attributes of a reasonable and informed third party, making it clear that it is a conceptual party.
    - Describes the parameters of the facts and circumstances that a reasonable and informed third party is expected to consider, i.e., the information available at the time and knowledge of the Code.

22. The Task Force proposes including the following guidance in the Code:

    (a) A reasonable and informed third party is a conceptual party. Such a party assists the objective thought process of the professional accountant in determining whether compliance with the fundamental principles is compromised or may appear to be compromised.

    (b) A reasonable and informed third party takes advantage of the information including the facts and circumstances that the professional accountant knew, or ought reasonably to have known, at the time. Such facts and circumstances might include:

        - Independence in appearance as perceived by the relevant stakeholders.
        - The intention of the professional accountant.
        - The experiences of the professional accountant.
        - Any relevant empirical evidence available.

- The actual outcome.

(c) A reasonable and informed third party weighs all the specific facts and circumstances to form a conclusion on whether compliance with the fundamental principles is compromised that is:

- Free from bias.
- Based on an understanding of the issues and decisions the professional accountant has to make, including knowledge of this Code.

(d) A professional accountant might find it useful to consider the views or actions of another professional accountant applying this Code in a similar situation but this should not be the only consideration.

Matters for Consideration

3. Do IESBA members agree with:
   (a) The purpose of the test as set out in part (a) of the proposed guidance?
   (b) The parameters of the facts and circumstances that the reasonable and informed third party is expected to consider as described in part (b) of the proposed guidance?
   (c) The attributes of the conclusion of the reasonable and informed third party described in part (c) of the proposed guidance?

C. Description of a Safeguard

23. The Task Force noted the views expressed by IESBA members at the Board meeting in April 2015. IESBA members expressed two contrasting views:

- Some IESBA members felt that it was important that the PA intends that the actions taken will effectively eliminate or reduce the threat to an acceptable level. They noted that in some situations it could be hard for a PA to be certain that an action would be effective. These IESBA members were of the view that the effectiveness of the actions applied should be reassessed as the circumstances causing the threat change and become clear.
- Other IESBA members held the view that an action should only be described as a safeguard if it is effective at eliminating the threat or reducing it to an acceptable level.

24. In considering how to proceed with improving the description of a safeguard in the Code, the Task Force considered the possible reasons for the difference in views. It also considered the concerns raised by some stakeholders regarding the effectiveness and appropriateness of safeguards in the Code.

25. The Task Force is of the view that the word “safeguards” is used interchangeably throughout the Code in both a broad and narrow sense. It believes that narrowing the definition of a safeguard within the Code may improve the perception of the effectiveness and appropriateness of safeguards in the Code. In addition, it believes that the proposal set out in section A of this paper to re-focus the conceptual framework on eliminating threats or reducing them to an acceptable level would also assist with demonstrating a robust approach to compliance with the fundamental principles.

26. The Task Force notes that the word “safeguards” is a concept that is familiar to PAs and stakeholders and used widely in other ethics regulations.

27. The Task Force believes there may be a "middle way" to convey that the PA intends an action or measure to be credible as an effective safeguard whilst recognizing the difficulties of being certain, i.e., an action is intended to be effective but the proof is only at the end.

28. The Task Force proposes a description of a safeguard such as:

    A safeguard is an action or measure that the professional accountant:

    - *Designs and implements in response to threats to compliance with the fundamental principles; and*
    - *Concludes is effective to eliminate such threats or reduce them to an acceptable level.*

    Depending on the circumstances, safeguards may need to be a combination of actions or measures.

29. The Task Force believes the proposed description demonstrates the need for a clear link between a threat and the response.

30. In parts of the Code where example safeguards are given, the Task Force proposes to introduce the word "possible" to make it clear that the professional accountant would need to apply judgement to determine whether such actions would be effective safeguards in response to the threats identified.

31. The Task Force believes that the PA should be required to re-assess the determination of whether a safeguard is effective whenever new information about a threat or a safeguard arises during an engagement.

Matter for Consideration

4. IESBA members are asked for their views on the suggested description of a safeguard.

D. Types of Safeguard

Background

32. Examples of safeguards are included throughout the extant Code. Safeguards fall into two broad categories:

    - Safeguards created by the profession, legislation or regulation; and
    - Safeguards in the work environment.

Section 100: Safeguards Created by the Profession, Legislation or Regulation

33. Section 100[10] lists safeguards created by the profession, legislation or regulation as follows:

    - Educational, training and experience requirements for entry into the profession.
    - Continuing professional development requirements.
    - Corporate governance regulations.
    - Professional standards.

[10] Paragraph 100.14

- Professional or regulatory monitoring and disciplinary procedures.
- External review by a legally empowered third party of the reports, returns, communications or information produced by a PA.

34. Section 100[11] also includes safeguards created by the profession, legislation, regulation or an employing organization that may increase the likelihood of identifying or deterring unethical behavior.

35. The Task Force believes that safeguards created by the profession, legislation or regulation do not meet the proposed description of a safeguard since they are not designed and implemented by the PA in response to threats to compliance with the fundamental principles. It is of the view that referring to these requirements as safeguards detracts from the intention that safeguards should be responsive to the threat identified. Consequently, the Task Force proposes that these actions and measures should no longer be referred to as safeguards in the Code.

36. The Task Force recognizes the importance of the factors listed in creating an environment conducive to compliance with the fundamental principles. For example, continuing professional development requirements created by the profession directly support compliance with the fundamental principle of professional competence and due care. It believes these factors would exist in a normal environment. While such factors would not reduce a threat to compliance with the fundamental principles, the significance of a threat may increase if such factors are not present. The Task Force is of the view that these factors also support the application of engagement-specific safeguards. Therefore, the Task Force believes that it may be appropriate to include these factors as matters to consider when evaluating the significance of a threat.

37. The Task Force proposes to:

- Move the factors to the part of Section 100 that deals with evaluating threats.
- Introduce the factors as factors to consider when evaluating the significance of a threat.
- Include guidance explaining that the absence of such factors may increase the significance of a threat.

Matter for Consideration

5. Do IESBA members agree that these actions and measures created by the profession, legislation or regulation should not be referred to as safeguards but as factors to consider when evaluating the significance of a threat?

Section 200: Safeguards in the Work Environment

38. For PAs in public practice, safeguards in the work environment can be further sub-divided into:

- Firm-wide safeguards; and
- Engagement-specific safeguards.

[11] Paragraph 100.16

39. Section 200 currently lists examples of firm-wide[12] and engagement-specific safeguards.[13] It also includes safeguards that the client has implemented.[14]

Firm-Wide Safeguards and International Standard on Quality Control (ISQC) 1[15]

40. The Task Force is aware of some criticism that the firm-wide safeguards listed in Section 200 of the Code are not safeguards specific to threats but are pre-requisites for good practice. For example, it has been noted that applying the requirements of a standard such as ISQC 1 should not be considered a safeguard.

41. The Task Force believes that firm-wide safeguards have an important role in ensuring that engagement-specific safeguards can be effective in eliminating or reducing threats to an acceptable level. Firm-wide safeguards may include written policies which, although not safeguards, may increase the robustness of the response to threats. The Task Force is of the view that the current "laundry-list" of examples diminishes the importance of the firm-wide safeguards.

42. The Task Force notes that ISQC 1 requires firms to :

- Establish policies and procedures designed to provide the firm with reasonable assurance that the firm and its personnel comply with relevant ethical requirements.[16]
- Document their policies and procedures and communicate them to their personnel.[17]

ISQC 1 also includes specific requirements relating to the policies and procedures that a firm is required to implement regarding the maintenance of independence where required by relevant ethical requirements.[18]

43. The Task Force is of the view that many of the firm-wide safeguards listed in Section 200 also appear in ISQC 1. The Task Force therefore considered including a reference to the requirements of ISQC 1 in the Code. However, the Task Force notes that ISQC 1 applies only to firms of professional accountants that perform audits and reviews of financial statements, and other assurance and related services engagements, i.e., the requirements of ISQC 1 do not apply to PAs in public practice who do not provide these types of engagements. It also notes that ISQC 1 may not be adopted by firms who do not comply with IAASB pronouncements for some or all of their engagements. The Task Force believes it is appropriate to include in the Code key principles and guidelines equivalent to those found in ISQC 1 for the benefit of all PAs in public practice.

44. The Task Force believes that the firm-wide safeguards included in Section 200 create an effective ethical framework for engagement-specific safeguards to be effective for all PAs in public practice.

---

[12] Paragraph 200.12

[13] Paragraph 200.13

[14] Paragraph 200.14

[15] ISQC 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*

[16] ISQC 1 paragraph 20

[17] ISQC 1 paragraph 17

[18] ISQC 1 paragraphs 21 – 25; ISQC 1 defines "relevant ethical requirements" to mean: "Ethical requirements to which the engagement team and engagement quality control reviewer are subject, which ordinarily comprise Parts A and B of the International Ethics Standards Board for Accountants' *Code of Ethics for Professional Accountants* (IESBA Code) together with national requirements that are more restrictive."

As a consequence, it proposes to increase the prominence of the firm-wide safeguards in Section 200 by including a clear introduction explaining the importance of having such policies and procedures in place.

45. The Task Force proposes to retain the examples of firm-wide safeguards included in the extant Code under the following headings, which are derived from ISQC 1:

- Leadership responsibilities for ethical environment
- Relevant ethical requirements
- Acceptance and continuance of client relationships and specific engagements
- Human resources
- Engagement performance
- Monitoring

Matter for Consideration

6. Do IESBA members agree that firm-wide safeguards are important in creating an effective ethical framework in which to apply engagement-specific safeguards?

Engagement-specific Safeguards

46. Examples of engagement-specific safeguards that might be applied to eliminate threats or reduce them to an acceptable level appear throughout Part B of the Code but are summarized in Section 200.[19]

47. The Task Force is of the view that the current listing of the safeguards does not add anything to the Code. It believes that adding a discussion of how a PA may be able to eliminate threats or reduce them to an acceptable level would improve the clarity and effectiveness of the engagement-specific safeguards noted in Section 200.

48. The Task Force notes that the engagement-specific safeguards listed in Section 200 are currently provided in isolation without any reference to threats. It believes that presenting the safeguards in the context of threats would demonstrate the expected correlation between threats and safeguards required to eliminate threats or reduce them to an acceptable level.

49. The Task Force proposes to reduce the number of examples given for each category of threat and replace them with more focused examples. This would include the fundamental principle in respect of which compliance is threatened and the safeguards that might be available to eliminate the threat or reduce it to an acceptable level.

Matter for Consideration

7. Do IESBA members agree with the proposals to present examples of threats, the relevant fundamental principles and possible safeguards together in Section 200?

[19] Paragraph 200.13

Safeguards Implemented by the Client

50. The Code[20] notes that a PA in public practice may be able to rely, although not entirely, on safeguards that the client has implemented. It includes examples of such safeguards as follows:

    - The client requires persons other than management to ratify or approve the appointment of a firm to perform an engagement.
    - The client has competent employees with experience and seniority to make managerial decisions.
    - The client has implemented internal procedures that ensure objective choices in commissioning non-assurance engagements.
    - The client has a corporate governance structure that provides appropriate oversight and communications regarding the firm's services.

51. The Task Force is of the view that these are not safeguards that eliminate a threat or reduce it to an acceptable level but may be factors to consider when evaluating the significance of the threat.

52. The Task Force believes the first two examples are addressed by the recently approved revisions to the provisions in the Code addressing management responsibility.

53. The Task Force proposes to remove the examples listed as safeguards implemented by the client. It also proposes to refer to considering the client's systems and procedures in relation to evaluating the significance of a threat.

Matter for Consideration

8. Do IESBA members agree with the proposals to remove the examples of safeguards implemented by the client from the Code?

Overview of Section 200

54. As a result of the proposals suggested in this section, the Task Force has considered the purpose of Section 200.

55. The Task Force believes the objective of Section 200 is to demonstrate to PAs in public practice how to apply the conceptual framework, particularly where a situation not specifically addressed in the Code occurs. It also believes the proposals made earlier in the paper—related to: re-positioning firm-wide safeguards and following an ISQC 1 approach; linking examples of engagement-specific safeguards to threats and fundamental principles; and removing the examples of safeguards implemented by the client—would result in Section 200 becoming a robust overview of how the conceptual framework described in Part A of the Code can be applied by PAs in public practice.

56. The Task Force is of the view that the examples of threats given in Section 200 could be improved by identifying the fundamental principle that is threatened by the situation.

57. The Task Force proposes that Section 200 should have the following:

    - Introduction

[20] Paragraphs 200.14 & 200.15

- Categories of threat
- Threats and eliminating them or reducing them to an acceptable level
    - The importance of applying professional judgement when identifying and evaluating threats and eliminating them or reducing them to an acceptable level.
    - Discussion on firm-wide safeguards, potentially renamed.
    - Considering the client's systems and procedures when evaluating the significance of the threat.
    - For each of the five categories of threat, include two to three examples of situations that could cause the threat, including the fundamental principle in respect of which compliance is threatened, and the safeguards that may be available to eliminate the threat or reduce it to an acceptable level.
    - Discussion that a situation may give rise to more than one threat and may therefore require different safeguards for each category of threat created.
    - Explanation that there may be some situations where safeguards are not available to eliminate the threat or reduce it to an acceptable level (and therefore the professional activity or service is prohibited), including examples.

Matter for Consideration

9. Do IESBA members agree with the proposals to redraft Section 200 of the Code as an overview of how the conceptual framework can be applied by a PA in public practice?

E. Those Charged with Governance as a Safeguard

Background

58. In 2013, the Board undertook a survey of a number of jurisdictions to gather input into its NAS project. Respondents were asked whether their national ethical requirements addressed the involvement of TCWG (for example, pre-approval of NAS) with respect to the provision of NAS by a firm to an audit client. The survey findings indicated that rules addressing the involvement of TCWG with respect to the provision of NAS varied among jurisdictions. However, there were some jurisdictions that do require specific communications with TCWG regarding the provision of NAS.

59. The Task Force notes that the extant Code encourages regular communication between the firm and TCWG regarding relationships and other matters that might reasonably bear on independence.[21]

60. The Task Force notes that the extant Code requires auditors to communicate with TCWG in the following circumstances:

    - When an entity becomes a related entity of an audit client as a result of a merger or acquisition, and interests or relationships that would not be permitted under the Code cannot reasonably be terminated by the date of the merger or acquisition.[22]

[21] Section 290, *Independence – Audit and Review* Engagements, paragraph 28

[22] Paragraphs 290.34 - 36

- When a breach of a provision in Section 290 or 291 occurs.[23]
- When an audit client is a public interest entity (PIE) and for two consecutive years the total fees from the client and its related entities represent more than 15% of the total fees of the audit firm.[24]
- When an entity becomes an assurance client during or after the period covered by the subject matter information and the firm provided NAS that would not be permitted during the period of the engagement.[25]

61. In other circumstances, the Code encourages regular communication between the firm and TCWG of the audit client.[26]

62. The Task Force is of the view that communication with TCWG is not a safeguard, but the involvement of TCWG could further assist with the evaluation of the significance of threats or the effectiveness of safeguards applied.

63. The Task Force believes that communication with TCWG increases transparency around the identification and evaluation of threats to compliance with the fundamental principles, and the actions or measures taken to eliminate or reduce those threats to an acceptable level. Importantly, it believes that the views of TCWG may be one, but not the only, indicator of the conclusion that a reasonable and informed third party might reach when determining whether safeguards have eliminated a threat or reduced it to an acceptable level.

64. The Task Force believes that strengthening the requirements in the Code to communicate with TCWG would promote stakeholder confidence in the profession. Doing so would also clarify that auditor independence is a joint responsibility. The Task Force also believes that such strengthening of requirements would respond to regulators who have expressed views that a party other than the auditor itself should consider the auditor's independence.

65. The Task Force believes that when there is a discussion between the auditor and TCWG regarding the provision of a NAS that bears upon independence, the following matters should be addressed:

- A description of the NAS provided during the period covered by the financial statements for audit and non-audit services provided by the firm and network firms to the entity and components controlled by the entity.
- The nature and amount of the fees for the above NAS.
- The steps taken by management to avoid the risk of the firm assuming a management responsibility.
- The safeguards put in place to eliminate the threat or reduce it to an acceptable level.
- If necessary, any consultation with other individuals within the firm or network or with a professional body.
- The details of any breaches of independence, if any.

---

[23] Paragraphs 290.45 – 48, and Section 291, *Independence – Other Assurance Engagements*, paragraphs 35 – 36

[24] Paragraph 290.219

[25] Paragraph 291.32

[26] Paragraph 290.28

- A conclusion that the auditor is independent.

66. The Task Force has considered a number of options for IESBA members to consider when and how to involve TCWG in relation to the provision of NAS. The options are broadly set out in order of increasing impact on PAs and the level of involvement of TCWG.

Option One: Informing TCWG of the NAS Provided to the Client

67. The Task Force notes that ISA 260,[27] deals with the auditor's responsibility to communicate with TCWG in an audit of financial statements. ISA 260 applies irrespective of the size of an entity. However, its requirements recognize the differences between entities where all of TCWG are involved in their day to day management and those where TCWG may be distant from these activities. In relation to auditor independence, the requirements of ISA 260 relate only to listed entities. However, the application material notes that the requirement may be relevant in the case of some other entities that have a wide range of stakeholders. Relevant extracts of ISA 260 are included in the appendix.

68. In the same way as placing requirements on TCWG is not within the remit of Code, except perhaps to the extent that the members of TCWG may be PAIBs, the Task Force notes that this is also not within the remit of ISA 260, which applies only to audits of financial statements. It also notes that ISA 260 recognizes the importance of effective two-way communication with TCWG and provides a framework for such communication, including specific matters to be communicated with them.

69. The Task Force notes that ISA 260 includes a requirement for auditors of listed entities to communicate the following matters in writing with TCWG:[28]

    - All relationships and other matters between the firm, network firms, and the entity that may reasonably be thought to bear on independence.
    - Total fees charged during the period covered by the financial statements for audit and non-audit services provided by the firm and network firms to the entity and components controlled by the entity.
    - Safeguards that have been applied to eliminate identified threats to independence or reduce them to an acceptable level.

70. The Task Force is of the view that since this requirement already exists within ISA 260 for listed entities, a cross reference to ISA 260 could be added to the Code without extending the responsibilities of auditors of listed entities.

71. For all audited entities, the Task Force notes that ISA 260 requires communication with TCWG on a timely basis.[29] Application material in the ISA recognizes that "a timely basis" may vary with the circumstances of the engagement and the matters to be communicated. In the application material,[30] ISA 260 notes the following:

    - Communications regarding planning matters may often be made early in the engagement.

---

27 ISA 260, *Communication with Those Charged with Governance*

28 ISA 260, Paragraph 17

29 ISA 260, Paragraph 21

30 ISA 260, Paragraph A40

- Communications regarding independence may be appropriate whenever significant judgements are made about threats and related safeguards, for example, when accepting an engagement to provide NAS, and at a concluding discussion.

Option Two: Obtaining the Concurrence of TCWG for the Provision of NAS by the Auditor

72. The Task Force notes that in the case of a breach of the independence provisions in the Code, where the firm believes action can be taken to satisfactorily address the breach, the firm is required to discuss the breach with TCWG as soon as possible, unless alternative timing for reporting breaches has been specified by TCWG.[31] The Code also requires that any matters discussed with TCWG regarding the breach be followed by communication of such discussion in writing.[32]

73. The Task Force notes that in the light of input received from a 2012 survey of audit committee chairs and directors, and to recognize the element of dialogue that was envisaged in relation to breaches, the IESBA included a requirement for the firm to obtain the concurrence of TCWG that such action can be, or has been, taken to satisfactorily address the consequences of the breach. The auditor is required to take steps to terminate the engagement, where permitted by law or regulation, if TCWG do not concur with the auditor's conclusion that the actions satisfactorily address the consequences of the breach.[33]

74. The Task Force notes that it may be appropriate for the auditor and TCWG to agree in advance the parameters for matters that require early concurrence.

Option Three: Pre-approval by TCWG for the Provision of NAS by the Auditor

75. In the 2013 survey, a few jurisdictions indicated that some form of pre-approval from TCWG was required with respect to the provision of NAS by a firm to an audit client. The Task Force notes that the new EU audit legislation requires that for PIEs,[34] the provision of any permitted NAS to the audited PIE will be subject to audit committee approval and application of general principles of independence.

Option Four: A Combination of Options One, Two and Three Determined by Professional Judgment

76. The Task Force recognizes the potential challenges of obtaining concurrence or pre-approval of the provision of NAS to audit clients. It believes such challenges might include:

    - Infrequent meetings of TCWG;
    - Determining the types of matters that require concurrence or pre-approval;
    - The challenges if concurrence is not received after the NAS has been provided; and
    - Variations in the quality of TCWG in different jurisdictions.

77. The Task Force notes that an auditor could apply professional judgement to determine which of the options: one; two; three; or four, set out above, is most appropriate depending on the significance of

---

31 Paragraph 290.46

32 Paragraph 290.47

33 Paragraph 290.47

34 In the EU, PIEs are defined as entities with transferable securities on an EU regulated market, credit institutions, insurance undertakings, and other entities designated PIE by EU Member State

the potential threats to independence. It believes the choice of option could depend on factors such as:

- The size or nature of the NAS.
- The expected duration of the NAS.
- The size or nature of the NAS fee.

Matters for Consideration

10. IESBA members are asked for their views on:

    (a) The matters to be presented to TCWG when discussing the provision of a NAS that bears upon independence; and

    (b) The options for communication with TCWG.

F. Documentation Requirements in the Code

78. The Task Force notes that the extant Code includes documentation requirements in relation to independence as follows:[35]

> Documentation provides evidence of the professional accountant's judgments in forming conclusions regarding compliance with independence requirements. The absence of documentation is not a determinant of whether a firm considered a particular matter nor whether it is independent.
>
> The professional accountant shall document conclusions regarding compliance with independence requirements, and the substance of any relevant discussions that support those conclusions. Accordingly:
>
> (a) When safeguards are required to reduce a threat to an acceptable level, the professional accountant shall document the nature of the threat and the safeguards in place or applied that reduce the threat to an acceptable level; and
>
> (b) When a threat required significant analysis to determine whether safeguards were necessary and the professional accountant concluded that they were not because the threat was already at an acceptable level, the professional accountant shall document the nature of the threat and the rationale for the conclusion.

79. The Task Force notes that ISA 220[36] expands on the general documentation requirements of ISA 230[37] and requires the auditor to document:

    (a) Issues identified with respect to compliance with relevant ethical requirements and how they were resolved.

    (b) Conclusions on compliance with independence requirements that apply to the audit engagement, and any relevant discussions with the firm that support these conclusions.

---

35 Paragraph 290.29

36 ISA 220, *Quality Control for an Audit of Financial Statements*, paragraph 24

37 ISA 230, *Audit Documentation*

(c) Conclusions reached regarding the acceptance and continuance of client relationships and audit engagements.

(d) The nature and scope of, and conclusions resulting from, consultations undertaken during the course of the audit engagement.

80. The Task Force believes that the documentation requirements in the extant Code[38] are sufficient but may benefit from alignment with the requirements and guidance included in ISA 220.

Matters for Consideration

11. Do IESBA members agree that the documentation requirements in the extant Code are sufficient and adequate?

12. Do IESBA members agree with the proposal to align the documentation requirements and guidance in the Code with those included in ISA 220?

G. Other Matters

Threats

81. To inform its work on safeguards, the Task Force reviewed the threats appearing in other ethics codes and regulations in the G20 and other major financial centers. As a result, it noted the following possible categories of threats:

- Management threat – The Task Force believes the revisions to the NAS provisions, approved by the Board in January 2015 and effective from April 2016, form a robust approach to dealing with management participation and therefore a management threat should not be included in the Code
- Undue influence threat – The Task Force believes the undue influence threat is aligned to the intimidation threat in the Code and therefore should not be included in the Code
- Adverse interest threat – The Task Force believes the adverse influence threat is adequately addressed through specific examples in the Code.

82. The Task Force believes that the categories of threats identified are captured in the existing categories of threats in the Code and remain appropriate.

83. The Task Force was asked to consider how the threats and safeguards relate to the public interest and the fundamental principles. It notes that the Code states that in acting in the public interest a PA shall observe and comply with the Code,[39] i.e. shall comply with the fundamental principles and apply the conceptual framework.

84. The Task Force has mapped all threats and safeguards as stated in the Code to the fundamental principles. The mapping shows that at least one of the five threats in the Code is relevant to each fundamental principle.

85. The summary of the detailed mapping included below shows where the Code includes specific examples for each threat to the fundamental principles. The Task Force notes that paragraph

[38] Paragraph 290.29

[39] Paragraph 100.1

290.6(a) states that "Independence of mind" allows an individual to act with integrity and exercise objectivity. Therefore it believes that, although not specifically stated in the Code, the specific examples of threats to independence also apply to integrity and objectivity. The Task Force wishes to bring the gaps in the examples, as specifically stated in the Code, to the attention of IESBA members.

	Self-interest	Self-review	Advocacy	Familiarity	Intimidation
Integrity	✓				✓
Objectivity	✓	✓		✓	✓
– Independence	✓	✓	✓	✓	✓
Professional competence and due care	✓				
Confidentiality	✓				✓
Professional behavior	✓				✓

86. In relation to NAS, the Task Force believes the examples of threats noted in the Code adequately address the threats to compliance with the fundamental principles. However, it believes that further consideration may be necessary in relation to other situations which may threaten compliance with the fundamental principles.

Clarifying the Application of the Conceptual Framework to PIEs

87. The Task Force notes that the Code requires PAs to comply with five fundamental principles through the application of the conceptual framework.

88. The Code recognizes that PIEs attract greater public interest given their large number and wide range of stakeholders, and factors such as their size and nature of business.

89. The Task Force believes that due to the characteristics of a PIE, the:

- Perceived significance of a threat is likely to be higher; and
- Perceived "acceptable level" is likely to be lower.

90. As a result, the Task Force notes that, for certain situations, the safeguards available may not be effective for PIEs. Therefore, for some NAS, the application of the conceptual framework results in more stringent requirements or additional prohibitions regarding the provision of NAS to PIEs.

91. The Task Force believes that it would be appropriate to add guidance to the Code explaining the differences between the evaluation of the significance of the threat and the acceptable level for a PIE and a non-PIE.

Matter for Consideration

13. Do IESBA members agree that it would be appropriate to add guidance to the Code in relation to the application of the conceptual framework to PIEs?

Material and Significant

92. The Task Force notes that "material" and "significant" are terms used throughout the Code as a method of evaluating the threats identified.

93. The Task Force believes that the use of "material" within the NAS provisions, where it is used in the same context as the ISAs, is appropriate. It is of the view that the use of material within the NAS provisions forms a link to the self-review threat since, if a NAS has a material effect on the financial statements, it will be subject to review by the auditor.

94. The Task Force notes that for the provision of NAS, "significant" is used in relation to the provision of valuation services, [40] internal audit services[41] and IT systems services.[42]

95. The Task Force proposes that the use of "significant" in relation to the provision of NAS should be in context and should be accompanied by a description of the factors that would increase the level of significance.

Matters for Consideration

14. Do IESBA members agree with continuing to use "material," where it is used in the same context as the ISAs, in relation to the provision of NAS?

15. Do IESBA members agree with the proposals to use "significant" in relation to the provision of NAS in context and alongside a description of the factors that would increase the level of significance?

H. SMP Considerations

96. In commenting on the April 2015 IESBA agenda material for this project, the IFAC SMP Committee noted that what constitutes a PIE varies considerably around the world in terms of the size of entity, and thus the degree of sophistication/level of resources of their respective finance function. SMPs noted the importance of the Task Force considering the wide variety of PIEs and the dependence of the Code's extant definition of PIE on local legislation.

97. The Task Force understands the challenges caused by the variations in the entities that are considered PIEs around the world. It intends to add guidance to the Code explaining the reasons for the different treatment of PIEs and other entities. The Task Force believes this may assist PAs in understanding the more stringent requirements for PIEs. The Task Force believes such guidance may also assist jurisdictions in setting their own definition of PIE. In relation to communication with TCWG, the Task Force recognizes the differences for entities where all of TCWG are involved in the

[40] Paragraphs 290.174 and 290.176

[41] Paragraphs 290.193, 290.195, 290.197

[42] Paragraphs 290.199, 290.201 and 290.203

day to day management of an entity and those, particularly PIEs, where TCWG may be distant from these activities.

98. The Task Force continues to consider the challenges faced by the SMP sector in employing safeguards involving the segregation of duties.

I. Next Steps

Safeguards Specific to NAS

99. At its meeting in May 2015, the Task Force began its review of the specific safeguards that pertain to NAS. During its work, the following themes were identified:

Theme	**Potential Next Steps**	**Example**
Circumstances causing multiple threats but example safeguards included in the Code are not clearly linked to threats.	Clarify the threats that example safeguards relate to.	Acting in an advocacy role in resolving a dispute or litigation when amounts involved are not material to the financial statements (para. 290.209)
Circumstances where no safeguards are identified in the Code but no prohibition currently exists.	Consider any safeguards that might be effective. If none, introduce prohibition.	Resourcing activities for non-PIEs (para. 290.211)
Circumstances where the safeguard is unclear.	Clarify the safeguard.	If such services are performed by a member of the audit team, using a partner or senior staff member with appropriate expertise who is not a member of the audit team to review the work performed. (para. 290.168)

100. The Task Force will continue to review safeguards as they pertain to NAS. It believes that this review might result in proposals that could significantly change the substance of the Code as it pertains to NAS. The Task Force believes this may have an impact on the timing of the project.

Appendix

Extracts of ISA 260 Related to Independence

ISA 260, *Communication with Those Charged With Governance*

17. In the case of listed entities, the auditor shall communicate with those charged with governance:

    (a) A statement that the engagement team and others in the firm as appropriate, the firm and, when applicable, network firms have complied with relevant ethical requirements regarding independence; and

        (i) All relationships and other matters between the firm, network firms, and the entity that, in the auditor's professional judgment, may reasonably be thought to bear on independence. This shall include total fees charged during the period covered by the financial statements for audit and non-audit services provided by the firm and network firms to the entity and components controlled by the entity. These fees shall be allocated to categories that are appropriate to assist those charged with governance in assessing the effect of services on the independence of the auditor; and

        (ii) The related safeguards that have been applied to eliminate identified threats to independence or reduce them to an acceptable level. (Ref: Para. A21–A23)

20. The auditor shall communicate in writing with those charged with governance regarding auditor independence when required by paragraph 17.

21. The auditor shall communicate with those charged with governance on a timely basis. (Ref: Para. A40–A41)

A22. The relationships and other matters, and safeguards to be communicated, vary with the circumstances of the engagement, but generally address:

    (a) Threats to independence, which may be categorized as: self-interest threats, self-review threats, advocacy threats, familiarity threats, and intimidation threats; and

    (b) Safeguards created by the profession, legislation or regulation, safeguards within the entity, and safeguards within the firm's own systems and procedures.

    The communication required by paragraph 17(a) may include an inadvertent violation of relevant ethical requirements as they relate to auditor independence, and any remedial action taken or proposed.

A23. The communication requirements relating to auditor independence that apply in the case of listed entities may also be relevant in the case of some other entities, particularly those that may be of significant public interest because, as a result of their business, their size or their corporate status, they have a wide range of stakeholders. Examples of entities that are not listed entities, but where communication of auditor independence may be appropriate, include public sector entities, credit institutions, insurance companies, and retirement benefit funds. On the other hand, there may be situations where communications regarding independence may not be relevant, for example, where all of those charged with governance have been informed of relevant facts through their management activities. This is particularly likely where the entity is owner-managed, and the auditor's firm and network firms have little involvement with the entity beyond a financial statement audit.

A40. The appropriate timing for communications will vary with the circumstances of the engagement. Relevant circumstances include the significance and nature of the matter, and the action expected to be taken by those charged with governance. For example:

- Communications regarding planning matters may often be made early in the audit engagement and, for an initial engagement, may be made as part of agreeing the terms of the engagement.
- Communications regarding independence may be appropriate whenever significant judgments are made about threats to independence and related safeguards, for example, when accepting an engagement to provide non-audit services, and at a concluding discussion.