Non-assurance Services
Issues and Task Force Proposals*

Richard Fleck, Task Force Chair

IESBA Meeting
New York
December 3-5, 2018

* The Task Force Chair will use an abbreviated version of this slide deck to present to IESBA meeting participants.

Agenda

• Introduction
  – Current landscape
  – Project objective and scope
  – Guiding principles

• Timeline | Task Force’s Approach

• Issues and Task Force Proposals
  – Analysis of current provisions, including types of NAS
  – Proposed decision trees for PIEs and non-PIEs
  – Other matters | Matters for future consideration

• Appendices 1 and 2
  – Effect of proposals on existing NAS provisions
Introduction

Current Landscape

- NAS provisions already in effect since 2016
  - Removal of “emergency situations” bookkeeping and taxation services
  - Clarifications about management responsibility and the concept of “routine or mechanical” services
- More revisions to come into effect in June 2019
  - Prohibitions more prominently identified
  - Conceptual framework has been enhanced and is more robust
  - Clearer safeguards that are more closely aligned to threats
  - Emphasis that if threats cannot be addressed, firm must decline or end the NAS or audit engagement
More Work Needed on NAS Provisions

- Financial reporting landscape; legal and regulatory environments and public expectations about auditor independence have changed
  - Public perception about “acceptable level” of threats to independence is different
  - More focus on independence in appearance
  - Less tolerance from stakeholders for self-review threats in context of NAS
  - Revision of internal firm policies and procedures with respect to providing NAS to audit clients
- Now is the time for a full review of NAS, especially permissibility issues

Summary of NAS Project Scope

Project Objective: To ensure that NAS provisions are **robust and of high quality** for global application, thereby increasing confidence in the independence of audit firms

**Matters to Consider**
- Self-review threat
- Materiality
- PIE vs. non-PIE
- New and emerging services
- Communication with TCWG
- NAS disclosure by firms
- Consideration of breaches
- Period for which independence is required (“Cleansing”)

**Matters not to be Pursued**
- “Blacklist” in the Code
- NAS disclosure by audited entities
- NAS fee cap
- Audit quality issues arising from the scale of multi-disciplinary consulting and advisory services provided by major audit firms
Guiding Principles

1. Be responsive to changes and public interest expectations about auditor independence when audit firms provide NAS to their audit clients
2. Develop a principles-based approach that is globally operable with a view to harmonization and simplification of NAS regimes
3. Cater for advancing technologies as well as new and emerging NAS
4. Ensure proposals are compatible with rest of Code (e.g., changes to approach to dealing with SR threats)
5. Apply the restructured Code drafting conventions

Feedback from Forum of Firms and SMPC

- Views sought about NAS project scope, issues and timing in Oct 2018
- Complimented the information gathering phase of project, in particular roundtables
- General support for direction of travel
  - No push back on suggestion to prohibit NAS that create self-review threats for PIEs
  - No support for equivalent treatment of non-PIEs
  - Request to revisit appropriateness of provisions relating to breaches in NAS context
### Proposed Timeline (up to ED Exposure)

- **December 2018**
  - Issues and Task Force and Preliminary Proposals
- **March 2019 (CAG and Board)**
  - Issues and Task Force Proposals | First read of proposed text
- **June 2019**
  - Remaining Issues and Task Force Proposals | Second read of proposed text
- **September 2019 (CAG and Board)**
  - Consider and finalize proposed text | Approve ED for exposure

**Questions?**
Task Force’s Approach

Step 1 – Prioritized Issues

• First, the Task Force developed preliminary proposals in relation to
  – Description of NAS
  – Self-review threats
  – Materiality
  – PIE vs. non-PIE
  – Communication with TCWG

• Next, the Task Force exchanged views about
  – New and emerging services
  – NAS disclosure by firms
  – Consideration of breaches
  – Period for which independence is required (“Cleansing”)
Step 2 – Reviewed and Assessed Current Code

- Reviewed existing NAS provisions and approach in the Code
  - Considered the different types of threat and the potential effectiveness of safeguards
  - Reviewed and assessed the categories of threats and likelihood of threats that are created by each individual NAS

- Deliberated about how each type of NAS should be dealt with in the Code, including whether:
  - The NAS was to be provided to a PIE or non-PIE;
  - To retain a "materiality qualifier"
  - To retain an exemption

Step 3 – Developed Preliminary Proposals

Against the background of Task Force’s analysis of the current NAS provisions:

- Key policy issues were identified
- Possible revisions and recommendations were developed to address those issues
  - Task Force is seeking to clarify the types of NAS that are prohibited, as well as those that are permissible
The Task Force’s proposals and recommendations include proposed decision trees that summarize the proposed NAS approach:

(i) PIEs
(ii) non-PIEs

Step 5 – Determined Practical Implications

• Applied proposed decision trees to each type of NAS that is specifically dealt with in the subsections of Section 600
  – Assess the implications of potential proposals and recommendations
  – Develop preliminary views about areas in the Code that should be revised
• A summary of the Task Force’s assessments are set out in
  – Appendix A for PIEs
  – Appendix B for non-PIEs
Steps 1, 2 and 3 -
Consideration of Prioritized Issues
Review and Assessment of Current NAS Provisions
Development of Preliminary Proposals and Recommendations
Types of Non-assurance and Terminology

- Although NAS may vary by type, in general they can be categorized as
  - Services required by legislation or contract to be undertaken by the auditors of the business
  - Services that auditors are best positioned to provide because of their existing knowledge of the business, or because the information required is a by-product of the audit process (e.g., tax preparation services)
  - Services that could be provided by other firms that do not do the audit (e.g., tax advice, recruiting and management or corporate finance consulting services)

- When different terms are used to describe similar topics across jurisdictions, questions are raised about
  - Whether the Code is clear and can be consistently applied across jurisdictions

Non-assurance versus Non-audit Services

Task Force Views

- Non-assurances services used in Code when referring to engagements that do not meet the definition of an assurance engagement
  - Code includes descriptions of assurance engagements (Glossary); and other assurance engagements (Part 4B, 900.7 to 900.11)

- **Questions about whether “assurance engagements” includes “audits”**
  - In some jurisdictions (e.g., UK, US), NAS = “non-audit” services
  - Non-audit services = “non-assurance services” + “assurance services other than audit”

- Task Force notes calls for Code to clarify what is meant by NAS
  - Is a definition of “non-assurance services” needed?
1. Do IESBA members believe that the Code should include a description for the term “non-assurance services”?

Existing NAS Provisions (2018)

Addressing Threats Created by Providing NAS

- Prohibitions for certain types of NAS in certain circumstances
  - Stricter prohibitions for audit clients that are PIEs
  - Many prohibitions are triggered by a materiality qualifier
  - Exceptions provided to prohibitions in specific circumstances

- Applying the conceptual framework for NAS
  - Identify category of threat (e.g., whether self-review)
  - Evaluate whether identified threat is at an acceptable level
  - Address threat by either: eliminating it; applying safeguards; or declining the NAS or audit engagement
  - Key terms clarified | Closer link b/w safeguards and specific threat
Categories of NAS Safeguards in the Current Code

- Segregation of responsibilities
  - Using professionals who are not audit team members to perform the service
- Review of audit work or NAS work
  - Having an appropriate reviewer who was not involved in providing the service review the audit work or service performed
  - Having a professional review audit work or result of NAS
  - Having a professional who was not involved in providing NAS review the accounting treatment or presentation in financial statements
- Confirm outcome of NAS
  - Obtaining pre-clearance from the tax authorities

Determining Whether an Action is a Safeguard

- Safeguards are actions, individually or in combination, that PA takes to effectively reduce threats to compliance with FPs to an acceptable level
  - By definition, an action is only a safeguard when it is effective
  - Safeguards vary depending on facts and circumstances
  - Effectiveness of safeguards requires exercise of PJ and use of RITP
- Acceptable level is the level at which a PA using the RITP test would likely conclude that PA complies with FPs
  - Simply put, the RITP test takes into account the public’s perspectives
  - Public perceptions about the importance of auditor independence differ for PIEs and non-PIEs. Therefore, conclusions about “acceptable level” is expected to differ depending on the type of entity
Two topics already identified as requiring clarification/revision are:
- Assuming management responsibility
- Administrative services

Based on its review of NAS provisions in the Code, the Task Force believes that in drafting its proposals, it will be critical to extensively review the descriptions for each individual NAS topic, taking into account:
- Current practice/changing business models
- New services
- New techniques
- Technology

The Code prohibits firms from assuming a management responsibility when providing any type of NAS to an audit client. It is unclear from the Code whether assuming management responsibility itself is a type of NAS that is generally prohibited; or whether it is an unacceptable threat arising from the nature of the engagement and/or the capability of management.

Task Force believes that the Code should clarify whether assuming management responsibility:
- Is a type of service
- Is a risk that can arise in relation any type of NAS from nature of engagement and/or capability of management
- Gives rise to multiple threats that cannot be eliminated or addressed with safeguards.
In the context of today’s environment, the Task Force questions whether Section 600 should continue to have a stand-alone subsection titled “Administrative Services.”

Based on the review of the description and examples in subsection 602, the Task Force also questions whether:

- Firms are providing the services described
- A new or revised definition might better describe the nature of services currently being provided
- The types of activities that are covered under “administrative services” in the Code may be repositioned to another subsection in Section 600

Task Force welcomes the Board’s input about whether the Code should continue to include a stand-alone “Administrative Services” subsection.
Self-review Threat

- Self-review (SR) threat – threat that a [firm] will not appropriately evaluate the results of previous judgment made, or an activity performed (either by a PA or another individual within the PA’s firm), on which PA will rely when forming a judgment as part of performing a current activity
  - SR threat description in the Code is general, but some national Codes (e.g., UK) provide more context in relation to NAS
  - Code provides examples of safeguards that might address SR threats, but examples
    - Generally involve a review by others within the firm
    - Are focused on threats at the individual level/ EP level and not the firm itself

Task Force Views about Self-review Threats

**BUT**

- An increasing number of stakeholders view self-review threats as being incompatible with the concept of an independent audit
  
- Some stakeholders do not consider that a “review by others in the firm” adequately addresses SR threats for a firm

In these circumstances, the Task Force believes that there is a need to reconsider how the Code deals with self-review threats that are created by providing NAS to an audit client
Task Force Proposal re Self-review Threats (1)

Task Force believes that different approaches for PIEs and non-PIEs remain appropriate

- **In the case of PIEs:**
  - There are changes in public perceptions about self-review and independence in appearance
  - There is a prevailing view that self-review threats created by providing NAS to audit clients cannot be eliminated, or reduced to an acceptable level by applying safeguards

- **In the case of non-PIEs:**
  - NAS provisions should remain proportionate to SMEs circumstances (e.g., to recognize resource constraints and the challenges involved in keeping up with changes in regulation)
  - This is important to ensure a vibrant SME sector and is in the public interest given the importance of the SME to most countries GDP

Task Force Proposal re Self-review Threats (2)

Based on its analysis, the Task Force proposes

- To prohibit, without qualification or exemption, the provision of NAS to **PIEs** where a potential self-review threat is identified
- To clarify circumstances in which the provision of NAS to **non-PIEs** would be prohibited – by refining/better explaining any “materiality” qualifier
  - Non-PIEs would not be subject to the unqualified self-review prohibition that would apply to PIEs
**Self-interest Threats**

- Self-interest (SI) threat – threat that a financial or other interest will inappropriately influence a [firm’s or] PA’s judgment or behavior
  - It is not viable or appropriate to prohibit NAS involving SI threats
    - Personal SI threats can be addressed by eliminating the circumstances creating the threat
    - Residual SI interest always exist because firms are paid by their audit clients
  - Questions remain about how to deal with SI threats created by advancing technologies
    - Blurred lines between clients’ services and business relationships

---

**Advocacy Threats**

- Advocacy threat – the threat that a [firm] will promote a client’s position to the point that the firm’s objectivity is compromised
  - Advocacy threat is relevant to NAS only when it impacts the independence of the firm in the context of performing the audit engagement
  - Task Force believes that there is a need to revisit
    - The use of words “…to the point that…” in the description
    - The likelihood that advocacy threats are created
    - The appropriateness of the examples of safeguards in the Code
Familiarity Threats

- Familiarity threat – the threat that due to a long or close relationship with a client or employing organization, [a firm or] PA will be too sympathetic to their interests or too accepting of their work
  - NAS familiarity threats arise in relation to recruiting activities and involve personal relationships which impact individuals and their mindset or behavior
  - Code prohibits certain recruiting activities that impact certain financial reporting roles i.e., directors and senior management
  - Firms are permitted to provide recruiting services that don’t impact key financial reporting roles

Intimidation Threats

- Intimidation threat – the threat that a [firm] will be deterred from acting objectively because of actual or perceived pressures, including attempts to exercise undue influence over the [firm]
  - NAS intimidation threats arise in relation to recruiting activities that impact financial reporting – directors and senior management roles – which are prohibited
  - Important to consider likelihood of intimidation threats that might arise from providing new and emerging services (e.g., pressure from overwork and compressed deadlines)
Likelihood of Threats Created by NAS

• Existing NAS provisions include statements about the likelihood of threats created by each type of NAS

• Statements vary in term of the level of precision
  – …creates threats…
  – …might create threats…
  – …do not usually create threats…

• Proposed way forward involves a re-assessment of both the:
  – Category of threat that is created (e.g., whether it is a SR threat); and
  – Likelihood of the threat being created by the specific type of NAS

The Distinction Between PIE and non-PIEs

• Task Force deliberated extensively about whether to retain the current PIE/non-PIE demarcation in the Code

• The Code (R400.8) already encourages firms to determine whether additional entities should be treated as PIEs based on specific factors (e.g., nature of business, state owned entities, not-for-profits etc.)

• Task Force believes that for now IESBA should
  – Retain different approaches for PIEs and non-PIEs in the NAS of the Code
  – Avoid revising the definition of PIE as part of NAS project
  – Include in the NAS explanatory memo (EM) an explanation of the perceived concerns about PIE description, describe options proposed and a specific question to solicit public input
Issues relating to Materiality

- Materiality is not used in a consistent manner in Section 600
  - The concept of materiality is a factor for evaluating threats (600.5 A1)
  - The word “material” or “significant” is a threshold to assess permissibility of a NAS
  - The concept of materiality is used as a qualifier to trigger certain NAS prohibitions
- Also, there are concerns that terms such as “materiality” and “significant” are inappropriate because they
  - Are unclear in the context of making conclusions about ethics and independence
  - Involve subjective judgment and allow auditors too much flexibility
  - Are susceptible to “abuse” by some auditors

Task Force Views about Materiality

For PIEs
- Materiality as a qualifier to trigger prohibition is of no continuing relevance if firms are prohibited from providing NAS that create self-review threats
- Materiality to be retained as a factor for evaluating threats, but the justification for this will be reviewed further

For Non-PIEs
- Review references to materiality and determine how it is used (e.g., whether in f/s context)
  - Retain the concept of materiality as a qualifier, but consider replacing the words “material” and “significant” with a word that more clearly articulates the appropriate threshold
  - Consider the need for new application material to explain the revised approach
Issues and Proposal re Pre-approval by TCWG

- Communication with TCWG provisions in R300.9, R300.10 & 400.40
  - IAASB’s ISA 260 (Revised) also include communication req’ts about auditor independence
- Some jurisdictions require TCWG discussions about/ pre-approval of NAS
- Task Force believes that the Code should reinforce provisions relating to pre-approval of NAS by TCWG
  - Require for PIEs, encourage for non-PIEs
  - Firms to obtain pre-approval by TCWG for NAS engagements by either pre-determined criteria or specific approval
  - Provide guidance about timing and format of communication (i.e., should be in writing)
  - Leverage material in ISA 260 (Revised)

Overview of Task Force’s Analysis

- For each type of NAS in S600, Task Force:
  - Reviewed the description/ definition of each NAS
  - Determined which category of threat(s) is created
  - Formed a view about the likelihood of such threat(s)
  - Determined whether the NAS should be prohibited in the Code, and whether the prohibition should:
    - Apply to PIEs or non-PIEs
    - Be triggered by a “materiality qualifier”
    - Be exempt in certain circumstances
- Appendices 1 and 2 summarize the Task Force’s conclusions
Steps 4 and 5
Development of Proposed Decisions Trees for Determination of Practical Implications

Proposed Decision Tree for PIEs

Step 1
Is NAS expressly prohibited in the Code?
- Yes = Prohibited
- No = Proceed to 2

Step 2
Does NAS involve assuming a management responsibility?
- Yes = Prohibited
- No = Proceed to 3

Step 3
Does NAS create self-review threats?
- Yes = Prohibited
- No = Proceed to 4

Step 4
Apply CF to identify, evaluate & address threats
- NAS is prohibited if threats cannot be eliminated/reduced to acceptable level
- Threats at acceptable level/eliminated
  - = Proceed to 5

Step 5
Obtain a pre-approval of NAS from TCWG
- Not Approved
  - = Prohibited
- Approved
  - = Provide NAS
Proposed Decision Tree for non-PIEs

Step 1
Is the type of NAS expressly prohibited in the Code?
- Yes = Prohibited
- Not prohibited/not addressed in = Proceed to 2

Step 2
Does NAS involve assuming a management responsibility?
- Yes = Prohibited
- No = Proceed to 3

Step 3
Apply CF to identify, evaluate & address threats
- NAS is prohibited if threats cannot be eliminated/reduced to acceptable level
- Threats at acceptable level/eliminated = Provide NAS

Pre-approval of NAS from TCWG encouraged

Matters for IESBA Consideration

2. Do IESBA members support the Task Force’s assessments and conclusions set out in Appendices 1 and 2?

3. Do IESBA members agree with the Task Force’s views and proposals, in particular those relating to:
   - Self-review threats?
   - Materiality?
   - PIE and non-PIEs?
   - Preapproval of NAS by TCWG?
Other Matters

Breaches

- Absolute prohibitions will increase focus on how breaches are addressed in the Code
- Competing public interest issues may arise – e.g. tension arising if breach is identified as financial statements are being finalized
- Is there a need for a more structured, independent process?
  - Should two independent assessments of breaches (firm and entity) be required?
  - Is more specificity in Code provisions required to meet public perceptions in today’s environment?
  - Need to expand on objectivity?
  - Will IAASB’s proposed revised QC standards help?
- Concept of “significant” is prominently featured in breaches section
  - Impact of consequential amendments arising from NAS changes to be made
Questions about Periods Requiring Independence

- Code requires firms to maintain independence during both:
  - Audit engagement period
  - Period covered by the financial statements
- Implications of undertaking NAS which have an ongoing relevance to the f/s (e.g. IT systems) in the context auditor independence
  - Should the Code specify a period that must elapse before provider of certain types of NAS can take on the audit (“cooling in” period)?
- Consider how others (e.g., EU and SEC) deal with the issue

Questions about NAS in a Group Audit Context

- Definition of audit client determines treatment of related entities, including subsidiaries
- Code addresses position of parent entities and its other immediate subsidiaries (R600.10 permits NAS not subject to audit) – but different approaches exist
  - EU prohibits those services to parents
  - SEC allows in certain circumstances
- Is there a need to reconsider how the Code deals with situation?
Potential Conforming Amendments

- In addition to S950, amendments to S523 and S525 of the Code may be needed
  - The Task Force questions whether serving as a company secretary and temporary personnel assignments are essentially types of NAS that might be better dealt with in S600
- In S523, serving as Director or Officer is prohibited, but taking position as Company Secretary is not
- In S525, in relation to temporary personnel assignments, the Task Force is concerned about
  - Period of time
  - Appropriateness for PIEs
  - Inability to effectively oversee/supervise

Matters for IESBA Consideration

4. IESBA members are asked for views on the approach to be taken to the following matters:
   a) Breaches
   b) The need for a “cooling in” period
   c) Consideration of NAS in group audit context
   d) Company secretary/ Temporary personnel assignments
Matters for Future Consideration

Transparency, Ratio of NAS fees, New and Emerging Services

Coordination with Fees Task Force

Matters identified in June 2018 Fees Final Report

- Having regard for the merits of transparency, consider how best to enhance disclosures about NAS fees
- Consider req'ts for firms to re-evaluate threats to independence when the ratio of NAS fees to audit fees reach a particular threshold

Suggestions for enhanced communication with TCWG and pre-approval by TCWG are already being considered by the Task Force
Challenges with Achieving Transparency

- Establish NAS disclosure req’ts at global level
- What to disclose? NAS fees?
- Confidentiality?
- Where to disclose it?
- Jurisdictions to determine how best to respond to transparency issues

Ratio of NAS fees to Audit Fees

- No support at roundtables to specify maximum ratio for NAS fees to audit fees
  
  _But,_

- Clarification is needed as to how firms should address self-interest threats created by fees from NAS
  - Add cross-reference to existing fee-dependency provisions in Section 410?
  - Require firms to re-evaluate threats to independence when ratio of NAS to audit fees reach a specific threshold?
  - Prohibit the provisions of certain types of NAS?
New and Emerging Services

Technology is blurring lines between professional services and business relationships
- Clarity needed about how Code should apply to new and emerging services
- Ability to respond quickly (Staff Publication?)
- Coordination with Technology WG anticipated
Appendices 1 and 2
Effect of Task Force’s Proposals for PIEs and non-PIEs

The material in the following appendices summarize the Task Force’s current thinking and its assessments of the practical implications of the proposals being explored. Appendix 1 includes the summary for PIEs and Appendix 2 includes the summary for non-PIEs.

### Effect of Proposed Approach – For PIEs (1)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting and booking</td>
<td>Might create</td>
<td>SR</td>
<td>Yes</td>
<td>No</td>
<td>Yes No</td>
</tr>
<tr>
<td></td>
<td>Creates</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative services^</td>
<td>Does not usually</td>
<td>All threats</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>create</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valuation</td>
<td>Might create</td>
<td>SR/ Ad</td>
<td>Yes</td>
<td>Yes No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Creates</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

^ Task Force questions whether firms currently provide administrative services and whether there is a need to modernize examples
### Effect of Proposed Approach – for PIEs (2)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Tax Services</td>
<td>Might create*</td>
<td>SR, Ad</td>
<td>No, Yes, if there is a SR threat</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4(a). Tax preparation</td>
<td>Does not usually create</td>
<td>All threats</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4(b). Tax calculation</td>
<td>Might create</td>
<td>SR</td>
<td>Yes</td>
<td>Yes-No</td>
<td>No</td>
</tr>
<tr>
<td>4(c). Tax planning and tax advisory (general)</td>
<td>Might create*</td>
<td>SR, Ad</td>
<td>Yes, if there is a SR threat</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>4(d). Tax planning when effectiveness of advice is dependent on accounting treatment/presentation</td>
<td>Might create Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes-No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Effect of Proposed Approach – For PIEs (3)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4(e). Tax valuation w/ direct effect on f/s</td>
<td>Might create Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes-No</td>
<td>No</td>
</tr>
<tr>
<td>4(f). Assistance in resolution of tax disputes (general)</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No, Yes, if there is a SR threat</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4(g). Assistance in resolution of tax disputes as an advocate</td>
<td>Might create Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes-No</td>
<td>Yes-No</td>
</tr>
</tbody>
</table>
### Appendix 1 – Summary of Task Force’s Current Thinking

#### Effect of Proposed Approach – For PIEs (4)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Internal audit (general)</td>
<td>Might create</td>
<td>SR</td>
<td>No, <em>Yes, if there is a SR threat</em></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5(a). Internal audit (ICFR)</td>
<td>Creates</td>
<td>SR</td>
<td>Yes</td>
<td><em>Yes No</em></td>
<td>No</td>
</tr>
<tr>
<td>6. IT systems services (general)</td>
<td>Might create</td>
<td>SR</td>
<td>No, <em>Yes, if there is a SR threat</em></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6(a). IT systems services (ICFR)</td>
<td>Creates</td>
<td>SR</td>
<td>Yes</td>
<td><em>Yes No</em></td>
<td>No</td>
</tr>
</tbody>
</table>

#### Effect of Proposed Approach – For PIEs (5)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Legal services</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7(a). Acting in an advisory role</td>
<td><em>Might create</em></td>
<td>SR, Ad</td>
<td><em>Yes if there is a SR threat</em></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7(b). Acting as general counsel</td>
<td>Creates</td>
<td>n/a</td>
<td>Yes, acting as mgt</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7(c). Acting in advocacy role</td>
<td><em>Might create</em></td>
<td>SR, Ad</td>
<td>Yes</td>
<td><em>Yes No</em></td>
<td>No</td>
</tr>
<tr>
<td>8. Litigation support (general)</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No, <em>Yes, if there is a SR threat</em></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>8(a). Litigation – estimating damages or other amounts</td>
<td>Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td><em>Yes No</em></td>
<td>No</td>
</tr>
</tbody>
</table>
### Effect of Proposed Approach – For PIEs (6)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Recruiting (general)</td>
<td>Might create SI, familiarity, intimidation</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>9(a). Acting as a negotiator</td>
<td>Creates SI, familiarity, intimidation</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>9(b). Searching for/ seeking out candidates for officers and senior mgt in f/r role</td>
<td>Creates SI, familiarity, intimidation</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>9(c). Undertaking reference checks for officers and senior mgt in f/r role</td>
<td>Creates SI, familiarity, intimidation</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Effect of Proposed Approach – For PIEs (7)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Corporate finance services (general)</td>
<td>Might create SR, Ad</td>
<td>No Yes, if there is a SR threat</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>10(a). Promoting/ dealing in/ underwriting shares</td>
<td>Creates SR, Ad</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>10(a). Corp fin when effectiveness of advice is dependent on accounting treatment/ presentation</td>
<td>Creates SR, Ad</td>
<td>Yes</td>
<td>Yes No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
## Effect of Proposed Approach – For non-PIEs (1)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Accounting and bookkeeping (general)</td>
<td>Might create Creates</td>
<td>SR</td>
<td>Yes</td>
<td>No</td>
<td>Yes (for routine or mechanical)</td>
</tr>
<tr>
<td>2. Administrative services*</td>
<td>Does not usually create</td>
<td>All threats</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3. Valuation</td>
<td>Might Creates</td>
<td>SR/ Ad</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (materiality + subjectivity)</td>
</tr>
</tbody>
</table>

* Task Force questions whether firms currently provide administrative services and whether there is a need to modernize examples.
### Effect of Proposed Approach – For non-PIEs (2)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Tax Services (604)</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4(a). Tax return preparation</td>
<td>Does not usually create</td>
<td>All threats</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4(b). Tax calculation</td>
<td>Might create</td>
<td>SR</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4(c). Tax planning and tax advisory (general)</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No Yes</td>
<td>No Yes</td>
<td>No</td>
</tr>
<tr>
<td>4(d). Tax planning when effectiveness of advice is dependent on accounting treatment/presentation</td>
<td>Might create Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Effect of Proposed Approach – For non-PIEs (3)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4(e). Tax valuation w/ direct effect on f/s</td>
<td>Might create Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (materiality + subjectivity)</td>
</tr>
<tr>
<td>4(f). Assistance in resolution of tax disputes (general)</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4(g). Assistance in resolution of tax disputes as an advocate</td>
<td>Might create Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Effect of Proposed Approach – For non-PIEs (4)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Internal audit (general)</td>
<td>Might create</td>
<td>SR</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5(a) Internal audit (ICFR)</td>
<td>Might create</td>
<td>SR</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6. IT systems services (general)</td>
<td>Might create</td>
<td>SR</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

## Effect of Proposed Approach – For non-PIEs (5)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Legal services</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>7(a). Acting in an advisory role</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7(b). Acting as general counsel</td>
<td>Creates</td>
<td>n/a</td>
<td>Yes, acting as</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7(c). Acting in advocacy role</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>8. Litigation support (general)</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>8(a). Estimating damages/ other amounts</td>
<td>Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (materiality + subjectivity)</td>
</tr>
</tbody>
</table>
### Effect of Proposed Approach – For non-PIEs (6)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition?</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Recruiting (general)</td>
<td>Might create</td>
<td>SI, familiarity, intimidation</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9(a). Acting as a negotiator</td>
<td>Creates</td>
<td>SI, familiarity, intimidation</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9(b). Searching for/ seeking out candidates for officers and senior mgt in f/r role</td>
<td>Creates</td>
<td>SI, familiarity, intimidation</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9(c). Undertaking reference checks for officers and senior mgt in f/r role</td>
<td>Creates</td>
<td>SI, familiarity, intimidation</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Effect of Proposed Approach – For non-PIEs (7)

<table>
<thead>
<tr>
<th>Type of Service</th>
<th>Likelihood of threat?</th>
<th>Type of Threat</th>
<th>Explicit Prohibition in S600/ Proposed Position</th>
<th>Materiality Qualifier?</th>
<th>Exemption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Corporate finance services (general)</td>
<td>Might create</td>
<td>SR, Ad</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>10(a). Promoting/ dealing in/ underwriting shares</td>
<td>Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>10(b). Corp fin when effectiveness of advice is dependent on accounting treatment/ presentation</td>
<td>Creates</td>
<td>SR, Ad</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>