Comments IIA Nederland on the proposed Global Internal Audit Standards

The Institute of Internal Auditors (IIA) is reviewing and updating all elements of the International Professional Practices Framework (IPPF) including the International Standards for the Professional Practice of Internal Auditing. The proposed new IPPF will include the Global Internal Audit Standards, Topical Requirements, and Professional Guidance.

This document describes the (most important) comments of IIA Nederland on the proposed Standards.

Overall Opinion

To what extent do you agree or disagree with the structure of the proposed Global Internal Audit Standards being organized by Domains, Principles, Standards, and Considerations for Implementation and Considerations for Evidence of Conformance?
- ○ Strongly agree
- ○ Agree
- ○ Neutral (neither agree nor disagree)
- ○ Disagree
- ○ Strongly disagree

General comments

Let us begin with kindly thanking all of those involved in the process of revising the Standards. Their hard and dedicated work is noticeable in the revised Global Internal Audit Standards. We would also like to extend our gratitude for the due process of involving all those interested in replying to this survey. It shows an appreciation for the involvement of relevant stakeholders in the Standard setting process.

We consider the new structure, in which the different components are aligned with each other and the clear distinction of the five domains with underlying principles as positive, solid changes are made to the Standards. It provides more clarity both for internal auditors, but also for those involved with the internal audit function. In that regard, the inclusion of elements into one document, which previously were dispersed over several documents, is something we consider to be an advantage of the proposed Standards as well. We also appreciate the clarity about the distinctions between 'must', 'should' and 'may' as proposed in the Standards.

On a more detailed level, we have provided feedback on several principles and standards in this survey. In addition to these more detailed comments, we would like to highlight a few general considerations that we think are important for having effective Standards.

1. Two tier governance

First of all, the current proposal highlights the responsibilities of the Board, and also details what classifies as the Board. It is suggested that – in the case of a two-tier system – the board should be considered the non-executive board members / the supervisory board.

In the recently revised Corporate Governance Code in The Netherlands, the relationship between the IAF and the Audit Committee is strengthened. Regarding the governance of the internal audit function it states that the executive board is *responsible* for the internal audit function and that the supervisory board *supervises* the internal audit function and has regular contacts with the chief audit executive. In our opinion, the new standards insufficiently take into account the diversity of governance arrangements.

2. Insight as a service

In addition, while over the past years, the IIA emphasised the role of the internal audit function as one of a trusted advisor, which can provide insight, besides assurance and advice, we miss the notion of insight as an internal audit service or product. In our view, the notion of 'insight' as a service or product should be included (again) in the Standards. The binary choice between assurance and advisory services or products is, in our view, too restricted. Insight services do not necessarily have to lead to conclusions, recommendations or action plans, but they are services which can add value to an organisation.

3. Assurance versus advisory services

Next, we observe that the current Standards seems to have removed the difference between assurance and – now – advisory services. While we do agree with a de-emphasis standard-wise, we believe that the removal of these clearly distinctive activities will complicate future implementation of the proposed standards. Especially in domain V, the descriptions do not fit well with the definition of advisory services in the Glossary. For example, the Standards currently indicate that conclusions need to be formulated for *each* engagement, while this may not be applicable for advisory services.

4. Too much rule based conformance

Finally, we would like to highlight a trend we are observing in the proposed Standards which leads us to some critical observations.

First, in general, we see an emphasis on *'conformance' with the Standards*. We would like to highlight that it is not *just* conformance – or evidence thereof – that will lead to an effective internal audit function. In that regard, we would like to propose to change the "evidence of conformance" to "examples of implementation" or "good practices". In our view, such a change would de-emphasise conformance and would emphasise effective implementation. This would also be more in line with the *principle-based axiom*, upon which the Standards are and, in our opinion, should continue to be based.

That brings us to our second question: it seems that the axiom of principle-based Standards is not as clear as it was before. The emphasis on documentation and the level of detail in some Standards give more an impression of rule-based-Standards. We would encourage a re-emphasis on the principle-based nature of these Standards, and consider whether extensive documentation is necessary, in light of the spirit of the principle

Glossary

Glossary
To what extent do you agree or disagree with the proposed content for this element?
- ○ Strongly agree
- ○ Agree
- ○ Neutral (neither agree nor disagree)
- ○ Disagree
- ○ Strongly disagree

Glossary
Additional comments or recommended changes:
- The Definition of 'Board' is not in line with the Dutch Corporate Governance Code, in which the primary responsibility for the IAF lies within the executive board
- The Definition of finding': a finding in itself is neutral – a result form the audit/research; now it's defined as a negative result; this may be confusing for the receivers of audit reports
- There is no definition of internal audit services
- There is no definition of 'conclusion' (as described in Standard 14.5).

Domain I. Purpose of Internal Auditing

Domain I. Purpose of Internal Auditing
To what extent do you agree or disagree with the proposed content for this element?
- ❍ Strongly agree
- ❍ Agree
- ❍ Neutral (neither agree nor disagree)
- ❍ **Disagree**
- ❍ Strongly disagree

Domain I. Purpose of Internal Auditing
Additional comments or recommended changes:

The purpose of internal auditing now clearly includes components that used to be dispersed over key documents which is a positive development. However, previously the definition stated which type of *activities* were to be undertaken by internal auditors; and the mission stated the *products* these activities should lead to. In combining the two – one of internal audit's major products – *insight* – is no longer part of the the purpose statement. We consider insight – which is not an audit opinion, conclusion or statement, nor an advice – as an added value for management and the board, and – hence – a clear purpose for internal audit. Therefore, we would propose inclusion of *insight* as a product, along the same lines as *assurance* and *advice*.

Additionally, in the last years the IIA promoted internal auditors as trusted advisors to management and the board. However, we do not see such indication in the purpose statement, nor in other principles or standards. We would expect some consideration of the concept of trusted advisor in the Purpose Statement, since it could help articulate the expected role for internal auditors and the internal audit function as a whole.

Domain II. Ethics and Professionalism

Domain II. Ethics and Professionalism
To what extent do you agree or disagree with the proposed content for this element?
- ❍ Strongly agree
- ❍ Agree
- ❍ Neutral (neither agree nor disagree)
- .x Disagree
- ❍ Strongly disagree

Domain II. Ethics and Professionalism
Additional comments or recommended changes:

Now it states: *Internal auditors" refers to recipients of or candidates for IIA professional certifications and all IIA members, including those who are members of IIA affiliates and chapters. Internal auditors are required to conform with the standards of ethics and professionalism.*
However, if an IAF adopt the IPPF, 'internal auditors' must be defined as <u>all members</u> in the department. The definition of 'Internal Auditor' is chosen too narrow.

_____

Domain II. Ethics and Professionalism
In general   ❍ Agree and   ❍ Neutral
But with some additional comments or recommended changes:

✠ Principle 1 Demonstrate Integrity
There is not a defining of Integrity but only showing elements/characteristics of what behaviour it expected to be is.

✠ Standard 1.2 Organization's Ethical Expectations
It is stated: *Internal auditors must understand and meet the <u>organization's</u> ethical expectations and be able to recognize conduct that is contrary to those expectations*. We suggest to reframe this into 'The organization and public ethical expectation'

It is stated*: referrals are made that the Auditor and the CAE should test and report misconduct or ethical behaviour, not line with the company's standards*.
Also here, the public norm should be added.

✠ Standard 1.3 Legal and Professional Behavior
Many examples are given for discreditable behaviour. However nothing is being said what action should to be taken by the CAE when this is (partly) happening. We suggest to add this.

✠ Standard 2.2 Safeguarding Objectivity
A qualified and competent internal audit must supervise engagements.
We suggest to be more clear that the supervisor can be part of the engagement team, as is often the case in agile working teams .

✠ Standard 4.1 Conformance with Global Internal Audit Standards

The internal audit function's methodologies must be established, documented, and maintained in alignment with the Standards. Internal auditors must follow the Standards and the internal audit function's methodologies when planning and performing internal audit services and when communicating internal audit findings, recommendations, conclusions, and other results.

We suggest to describe in the Considerations (the good practice of) a 'referral matrix' in which the GIAS are linked into the applicable IAF manual in the department. This would make EQAs on completeness way easier but would also for the IAF lead to more transparency.

✠ Standard 4.2 Due Professional Care

Understanding the complexity, materiality, and significance in context is necessary for properly assessing relevant risks and determining which risks should be prioritized for further evaluation.

With this text, generic topics as complexity and materiality and significance are mentioned. However only significance is defined in the Glossary. It might add value to define all three topics (what is it, how to measure it and conclude upon)

Domain III. Governing the Internal Audit Function

Domain III. Governing the Internal Audit Function
To what extent do you agree or disagree with the proposed content for this element.
◯ Strongly agree
◯ Agree
◯ Neutral (neither agree nor disagree)
◯ Disagree
◯ Strongly disagree

Domain III. Governing the Internal Audit Function
See our previous general comment on definition of the board: It is suggested that – in the case of a two-tier system – the board should be considered the nonexecutive or the supervisory board. In that regard, we underscore that the relationship between the board and the internal audit function is governed differently in the Netherlands.

Regarding the Standards:
In general   ◯ Agree and   ◯ Neutral
But with some additional comments or recommended changes:

❏ Standard 6.1 Internal Audit Mandate
On (Page 29) it is stated: **Joint Responsibilities:** *The board and the chief audit executive must discuss and agree upon the internal audit function's mandate. The chief audit executive must document the agreed-upon internal audit mandate in an internal audit charter, which is approved by the board.*
We have 2 questions regarding this:
•   With approving of the mandate by the Board, the joint agreement is signed. The oversight responsibility and role is stated for the Supervisory Board member. With this, he/she gets operational responsibility for oversight and partly also on audit capacity, quality and functioning. We would like you to consider to mention that this should also be stated in the job-profile as most Supervisory Board members do not have operational responsibility.
•   We would like you to consider to describe if and how the Mandate should be published (to demonstrate and communicate)?

❏ Standard 7.1 Organizational Independence
On (Page 33) it is stated: *The board is responsible for ensuring the independence of the internal audit function.* As the CAE and the IAF are on the payroll of the organization, they will never be 100% independent.. It might be good to define this as 'independent in the company to the extent possible'. This shows the boundaries on independency.

❏ Standard 7.3 Safeguarding Independence
On (Page 38) it is stated: *When the chief audit executive has ongoing nonaudit responsibilities, the responsibilities, the nature of work, and established safeguards must be documented in the internal audit charter. ….* We suggest to add that this is also the case if one of his/her staff is having such a role/responsibility.

❑ Standard 8.4 External Quality Assessment
○ Disagree

The SAIV: there seems to be an inconsistency between p45 (where it says the EQA can be performed by …. or a SAIV') and p46 where it says that the SAIV does not fully replace the requirement to conduct EQA (and may be done only once every 10 years).

We strongly advocate seeing the SAIV as a full-fledged EQA or assessment of conformity with the standards, as is also the case now. This also enhances the possibility to have an EQA performed every 5 years for smaller IAFs (of which there are many). Removing this possibility may lead to budget problems for them.

The difference between the 'normal' EQA and the SAIV is at the moment mainly the discussion of best practices and benchmarking with others; a (small) IAF can also design this discussion in a different way. The essence of the EQA is establishing the conformance.

Note: the definition of the SAIV used to be more clear; the 3rd bullet o p46 might lead to confusion: "*benchmarking, leading practices was not in the SAIV and is about the scope*; the interviews mentioned are indeed also in the SAIV important, but are about the way of conducting the SAIV. So we propose, to make this distinction and to delete the first part of this sentence.

Domain IV. Managing the Internal Audit Function

Domain IV. Managing the Internal Audit Function
To what extent do you agree or disagree with the proposed content for this element?
- ❍ Strongly agree
- ❍ Agree
- ❍ Neutral (neither agree nor disagree)
- ❍ Disagree
- ❍ Strongly disagree

Domain IV. Managing the Internal Audit Function
Regarding the specific Standards:

✠ Standard 9.3 Internal Audit Charter
❍ Agree

The consideration for implementation mentions signatures as typical part of the audit charter. We believe agreement can also be shown on another way, f.e. by a report or minutes showing that all stakeholders have agreed to the audit charter?

✠ Standard 9.5 Internal Audit Plan
❍ Disagree

Both on page 58 and 59 it says: *to develop the internal audit plan, the chief audit executive considers the results of the levels of **residual** risk.* This is not correct: here it should be the inherent risk (the risk without the mitigating impact of internal controls, as Internal Audit is auditing whether these internal controls are adequate)

Domain V. Performing Internal Audit Services

Domain V. Performing Internal Audit Services
To what extent do you agree or disagree with the proposed content for this element?
- ○ Strongly agree
- ○ Agree
- ○ Neutral (neither agree nor disagree)
- ○ Disagree
- ○ Strongly disagree

Domain V. Performing Internal Audit Services
See our previous general comment: we observe that the current Standards seems to have entirely removed the difference between assurance and – now – advisory services. While we do agree with a de-emphasis standard-wise, we concur that the entire removal of these clearly distinctive activities will complicate future implementation of the proposed standards. Especially in domain V, he descriptions do not fit well with the definition of advisory services in the Glossary. How can you conform with all standards regarding principles 13 to 15 for providing training or advising on the implementation of new policy (examples listed in the glossary)?. For example, the Standards now say that conclusions need to be formulated for each engagement, while this – ostensibly – cannot be the case for all advisory services.

Textual:
- P.84: "*Internal auditors evaluate the differences to determine whether there are significant findings*" --> We suggest to add: significant findings, based on the risk associated with the finding.
- P.84: "*especially the board, senior management, and*" -- > We suggest: and/or

Domain V. Performing Internal Audit Services
Regarding the specific Standards:

❑ Standard 13.1 Engagement Communication
○ Neutral
- This Standard has some overlap with Standard 15.1; it's not all about the planning (Principle 13), but also about the closing communication, which is in fact Principle (14 and) 15.
- P.86: "*While the goal is to reach agreement, when that is not the case …*"
  We would not say that the goal is to reach agreement, but for both parties to understand each other's reasons and may explain why a finding, etc. is or is not relevant. As a consequence, the internal auditor and management may agree, but may also differ in their opinion.
- P.87: "After *the discussion, management can confirm its action plans,*".
  We miss what the internal auditor should do if he/she finds that a change program does not lead to attaining organizational goals..

❑ Standard 13.2 Engagement Risk Assessment
○ Agree
- P.88: "*(such as those completed by management)*"
  We suggest to add: 'or by the second line'

- P.89: "*Meet with other assurance and consulting service providers.*"
  We think this should be advisory instead of consulting?

❑ Standard 13.6 Work Program
  ⭕ Agree
- *P.95:* "*Internal auditors must develop and document an engagement work program that will achieve the engagement objectives*"
  We suggest to replace by: Through which the engagement objectives will be achieved (The work program will not achieve the objectives by itself).

❑ Standard 14.1 Gathering Information for Analyses and Evaluation
  ⭕ Disagree
- General for Standards 14.1 and 14.2: there is (too) much focus on assurance engagements alone (missing the advisory engagements) and within these too much focus on the negative conclusions of the engagement; generally there will be positive and negative conclusions; both are valid results of the engagement, both should be supported by enough evidence, both are of value to the organization.
- P.96: "*Internal auditors must gather and analyze information to produce and support engagement findings.*"
  We would say 'findings and observations'. Findings are, by definition, significant risks ("things that should be repaired / mitigated") (see p. 4). However, observationsmay, in our view, also be positive. These positive observations should also be substantiated by evidence as All conclusions must be supported by evidence. Note: as said in our comments at the Glossary, we would prefer to use the name 'finding' as a neutral conclusion, so you would speak about positive and negative findings.
- P.97: "*Information is relevant when it is consistent with engagement objectives,*"
  Is it possible that relevant information may also go beyond the scope of engagement objectives? E.g. risks that were not recognized during the scoping and development of the work program, but after all are concluded to be very important for the organization.
- P.97: "*Corroborating the information by comparing it against more than a single source*"
  We suggest to replace by: 'with other sources'?
- P.97: "*they should apply methods to ensure that the sample 'is as representative of the whole population as possible'*"
  We suggest to replace by: 'is sufficiently representative to fulfill the engagement objectives'. If it were as representative as possible than, in many cases, it would include the whole population, because that is as representative as possible. As an internal auditor you should consider the costs and benefits of the sample size in which engagement objectives are leading.

❑ Standard 14.4 Recommendations and Action Plans
  ○ Disagree

It is stated that recommendations are mandatory. This is not always necessary when providing insight, some advisory engagements f.e. when facilitating a workshop, or in the type 'agreed upon procedures') and also (due to the complexity and required investigation into root causes) not always possible within the scope and time of the audit. An outcome of the audit could be to perform a root cause (as the next action). In practice, we often see the 'jumping to recommendations without proper substantive support – this is a risk of making recommendations mandatory.

❑ Standard 14.5 Developing Engagement Conclusions
  ○ Disagree

Contrary to the current Standards, an overall conclusion of the engagement will now be required. In our opinion, this is often appropriate, but is not always necessary or desirable; it can also obscure the results (a 4 + 8 gives an average of 6) and make the discussion process more difficult. We therefore propose not to make an engagement conclusion mandatory

Topical Requirements

Topical Requirements will provide the requirements for auditing specific topics and clarify the audit methodology. It is not required that all internal audit functions include these topics in the audit plan, which needs to be risk-based in supporting the organization's objectives. But when internal auditors provide assurance services on these topics, conformance with the Topical Requirements is required.
Do you support the inclusion of Topical Requirements in the IPPF?
   ❍ Yes
   ❍ No
   ❍ Not sure

Topical Requirements
Please provide any additional comments or recommended changes for the proposed content for this element.
It would be nice to have clear statements ('position papers') on current topics, but the question is whether those should be mandatory requirements or recommendations. The due diligence of auditing is already laid down in the Standards; they also apply to these subjects. The TRs will therefore be about the substantive approach; it can be very diverse and specific. There is also a risk that it will lead to unnecessary work if the IAF has to record (also for the EQA) why it hasn't applied these TRs.

The list of the engagement topics included in the Topical Requirements will be determined through a systematic method including survey, market research, and input from internal auditors and stakeholders. The following is the initial list of audit topics being considered for Topical Requirements.

Cybersecurity
Fraud risk management
Information technology governance
Organizational governance
Privacy risk management
Public sector: performance audits
Sustainability: environmental, social, and governance
Third-party management

Do you support providing Topical Requirements for these topics?
   ❍ Yes
   ❍ No
   ❍ Not sure