Norman Marks, CRMA, CPA

March 5, 2023

To: IIASB and IIA Leadership and others

Review of the Draft Global Internal Audit Standards

I have completed a careful review of the draft that was shared with the public on March 1st.

While I have responded to the survey as requested, there are overarching issues that must be addressed, as well as a number of specific points requiring corrective action. (See attached copy of the draft with my detailed, line by line comments.)

I recognize the immense effort involved in such a major overhaul and the areas of significant improvement, such as the distinction in the draft between activities that "must", "should", and "may" be performed.

However, the number of significant issues overwhelms, in my professional opinion, the value of the positive changes.

Therefore, **I believe the draft should be withdrawn and reworked promptly. It requires major thought and change before being reissued for public comment.**

The Purpose and Value of the IIA's Standards

In order to properly assess the draft, it is necessary to consider the value and purpose of the Standards.

In my opinion, they should serve as ***a basis for the effective and efficient professional practice of internal auditing*** *across the globe.*

They should establish ***what must be done, otherwise it is highly unlikely that internal auditing will be effective in delivering the assurance, advice, and insight on risks to the achievement of enterprise objectives that leaders of the organization (in management and on the board) need***.

That foundation is then supplemented by recommended practices ("should") that will in all likelihood lead to increased value to our stakeholders. Examples and further detail are added of practices that may be practiced.

The Standards therefore **must *not* mandate practices that are not essential to delivering the value our stakeholders need**[i]. They must only mandate those that are.

They must avoid adding unnecessary bureaucracy and red tape, such as excessive documentation requirements. They add cost and divert scarce audit resources from performing valuable audit work.

We are not the external auditors. It is highly unlikely that the CAE will be sued. Having said that, higher documentation standards are sometimes required for specific audits or in some organizations to meet regulatory and other requirements. That distinction is not present in the draft.

The Standards do not exist to promote the IIA. Their purpose is to promote *efficient and effective internal auditing practices*.

As currently drafted, it is possible to have a highly effective internal audit function that does not comply with the Standards.

It should also be noted that conformance with the Standards does not ensure, in any way, that internal audit practices will be either effective or efficient.

Major Issues with the Draft

This leads to two major overarching issues, or themes, with the draft:

1. Activities, especially documentation, are mandated that are not necessary.
2. There is excessive emphasis on *compliance* with the Standards, and insufficient attention to ensuring the *quality* internal audit services that add the *value* our stakeholders need.

The third major issue is:

3. The draft fails to promote [enterprise] risk-based auditing. Instead, it promotes auditing risks to auditable entities.

In addition, there are major areas that have been overlooked or given insufficient attention, including:

4. The development and maintenance of ***a dynamic audit plan that addresses the more significant sources of risk to the enterprise and its objectives***.
5. Four core principles of effective internal auditing:
    - Aligns with the strategies, objectives, and risks of the organization.
    - Provides risk-based assurance.
    - Is insightful, proactive, and future-focused.
    - Promotes organizational improvement.
6. The need to share the auditor's ***insight***.

These and other issues are discussed in the attached Detailed Findings.

I am open to discussing these points and other questions as needed.

Thank you for the opportunity to comment and I look forward to the next draft.

DETAILED FINDINGS

1. Excessive red tape

As noted above, while we are a profession and should have professional standards, we need to have Lean practices[1]. We should only perform activities that deliver (end) value to our stakeholders on the board and in management, because our resources are scarce and never sufficient to address all the risks of significance to the achievement of our organization's objectives.

We should limit documentation and other red tape or bureaucratic activities to situations and to the extent they are necessary and add value. That value is in the eyes of our stakeholders, how it helps them lead the organization to success.

This is a massive issue in many of today's internal audit functions, where less than half the time available is spent on fieldwork – and the rest is in engagement planning, documentation, workpaper review and rework, and other low value work.

I recognize that where there is a reasonable possibility of legal action or a regulatory requirement, documentation and related activities should be at a higher standard. For most functions, that will only apply to a few if any engagements.

We do not need to spend valuable and scarce resources developing excessive levels of documentation (evidence – as if we were in court) to prove our work and backup our findings, especially when management agrees with them.

Developing and reviewing workpapers not only doesn't usually deliver value that exceeds the cost (especially when rework is involved[2]) but does not guarantee quality work.

In fact, reviewing workpapers is not sufficient to confirm quality auditing.

Better practice is to "review the quality of the work performed", and while that may *include* the review of workpapers, a discussion with the auditor who performed the work is necessary.

Some departments who believe they are following the Standards have a QA function review audits months after they were completed. How can this be a good use of time?

Another example in the draft is the insistence on the documentation of internal audit processes and methodologies. While this may have some value in very large departments, that value is limited and next to nonexistent in the typical audit department of five or fewer people. (We all know how often control owners in the business refer to policies, procedures, and standards! Even COSO does not mandate formal documentation.)

The cost of workpapers and other documentation and process should not exceed the value our stakeholder derive from them.

Note that this communication does not have sections on Background, Scope, or Objectives. They are rarely necessary.

---

[1]The American Society for Quality: "Lean is defined as a set of management practices to improve efficiency and effectiveness by eliminating waste. **The core principle of lean is to reduce and eliminate non-value adding activities and waste**.

[2] The antithesis of Lean auditing.

I recognize that this will warp the minds of some traditional auditors, but we need to challenge old ways, throw away what doesn't add value to our customers, and embrace efficient and effective auditing practices.

Recommendation

The IIASB **must** r**econsider what should be mandatory practice for the efficient and effective performance and delivery of the assurance, advice, and insight needed by leaders of the organization**.

Where higher standards of documentation, etc. are required (such as cases where they may be legal action or there are regulatory requirements), those should be treated as **exceptions** rather than the norm, and the higher standards explained.

Make sure that is sufficiently addressed and anything else either **eliminated** from the Standards or downgraded to "may".

2. Excessive emphasis on Compliance at the expense of Quality

The focus of the Standards should be on providing guidance on what **must** be done to ***deliver the quality assurance, advice, and insight our stakeholders need as they lead the organization to achieve its objectives***.

But there is confusion between compliance (or conformance) with the Standards and the delivery of the quality services needed.

Compliance does not guarantee quality, and quality can in some cases be achieved without compliance.

One example was at Apple, where the CAE saw that the greatest risk was in the product development and maintenance groups, so he wisely embedded his entire team to work alongside those teams. They assessed and advised in real time on related risks, getting immediate action where needed without writing any formal reports or preparing workpapers. Top management and the board had an extraordinary level of assurance that the more significant risks to the organization and its success were being effectively addressed.

Another example was in my own companies, where risks and the engagements necessary to address them, including the scope of those engagements, were identified during the development and maintenance of the audit plan. There was no value in a separate engagement level risk assessment, so we didn't do one – in violation of the Standards then and now. (That is one requirement I would delete from the Standards, replacing it with language that ensures that ***each engagement addresses the appropriate areas of significant risk to the enterprise and the achievement of its objectives***.)

It is time to reconsider the value and therefore the need for high-cost quality assurance reviews.

An independent review that has the objective of assessing whether sufficient levels of the value needed by the organization are delivered has merit. It **should** be discussed with the board, who will determine whether and when it should be performed.

However, a review that only assesses compliance with the Standards has very limited value and, at best, **may** be performed. Every member of the IIASB should be able to testify that a review that gives an opinion on compliance has very little value to their stakeholders, and there are better uses for the funds and resources it requires.

My board demanded, in strong language, that I not engage a third party to perform such a review.

The board was correct. As they told me, *they* are responsible for assessing and ensuring, with the CAE, the quality of the internal audit function. They should determine whether and when there is a need and value for such a review.

I realize that this will be a tough pill to swallow for some, but we must move on and focus on operational performance and delivery of valuable services instead of compliance. Promote internal audit practices, not the IIA.

The draft discusses ongoing and periodic supervision and review but doesn't say nearly enough about ensuring the quality and efficiency of internal audit – in the development and maintenance of the audit

plan, in the scoping and performance of work, in the assessment of results and their constructive and open bilateral discussion with management, or in the final communication of results.

It may be a challenge to add standards around efficiency, but that is something that should be considered. Guide auditors to:

- Perform ***sufficient*** work to identify the right engagements to perform, ***but no more***.
- Perform ***sufficient*** fieldwork to form an opinion on the engagement scope, ***but no more***.
- Work **with** management to identify actions that can and should be taken to improve processes and controls. Insufficient time is usually dedicated to this task.
- Document the work performed ***to the extent that it adds value to the customer, and no more***.
- Review the work performed ***sufficiently*** to confirm the results and provide team guidance and development – ***and no more***.
- ***Communicate what leadership needs to know, and no more***.
- ***Limit rework and other work that does not add value to our customers***.

Recommendations

a) The IIASB should (I would say must) reconsider what should be mandatory practice for the efficient and effective performance and delivery of the quality assurance, advice, and insight needed by leaders of the organization.

   Make sure that is sufficiently addressed and anything else must either be eliminated from the Standards or downgraded to "may".

   That includes removing the mandatory external QAR.

b) Consider adding standards to address efficiency.

c) Remove any requirement that audit reports reference compliance with the Standards. It has no value to our leaders, given that this is a matter discussed in the periodic reporting to the board by the CAE.

3. Risk-based auditing

The inclusion of a Purpose statement adds little value when there is an existing Mission statement.

The **Mission** statement states:

> The mission of internal audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

The draft **Purpose** statement is:

> Internal auditing enhances the organization's success by providing the board and management with objective assurance and advice.

This is not progress, even when the Purpose statement is extended as shown in the draft.

a. The reference to "risk-based" has been removed.
b. The concept of valuable insight has also been deleted.

When our assurance, advice, and insight is risk-based, there is an *implication* that we are addressing the sources of risk to enterprise objectives that matter.

It implies some level of assurance that our assurance, advice, and insight is ***sufficient***.

When internal audit performs enterprise risk-based audits, it is ***addressing the risks that matter and not auditing those that don't***.

This is of immense importance!

Instead, the draft demonstrates a failure to understand risk-based auditing!

The draft unbelievably says that there is no difference between an audit universe (a list of auditable entities) and a risk universe (a list of sources of significant risk to the achievement of enterprise objectives).

The draft even goes as far as to promote the auditing of risks to an entity rather than to the enterprise when it mandates an engagement level risk assessment, where that assessment of risks to the entity defines the scope of the audit. (All that may be needed is a confirmation as the audit is started that the scope defined in the audit plan, which was based on an assessment of risks to enterprise objectives, remains appropriate.)

This practice of auditing controls over enterprise-level risks has been successfully adopted over the last two decades by an increasing number of audit functions.

In 2003, the Chartered Institute of Internal Auditors issued a Position Statement on Risk Based Internal Auditing. It states (inter alia):

> RBIA starts with the business objectives and then focuses on those risks that have been identified by management that may hinder their achievement.

> The role of internal audit is to assess the extent to which a robust risk management approach is adopted and applied, as planned, by management across the organisation to reduce risks to a level that is acceptable to the board (the risk appetite).

The IIA has a class on the Fundamentals of Risk-based Auditing that states:

> Risk-based auditing ensures that the internal audit activity is focusing its efforts on providing assurance and advisory services related to the organization's top risks. Through risk-based auditing, the internal audit activity helps executive management and the board understand whether the organization's risk management processes are sufficient and how to better achieve organizational objectives through good governance, risk management, and control.

An IIA class on Developing a Risk-Based Audit Plan states:

> Effective internal auditing is ever-so crucial to an organization's overall success; therefore, it requires thorough planning, coupled with nimble responsiveness to quickly changing risks — a constant in today's business environment. To add value and improve an organization's success, internal audit priorities should align with the organization's objectives and address the risks with the greatest potential to affect its ability to achieve those objectives.

A Practice Advisory with the same title tells us:

> In today's unprecedented environment, effective internal auditing requires thorough planning coupled with nimble responsiveness to quickly changing risks. To add value and improve an organization's effectiveness, internal audit priorities should align with the organization's objectives and should address the risks with the greatest potential to affect the organization's ability to achieve its goals.

The draft fails to promote risk-based auditing.

This is a **major** deficiency.

Another is the failure to require that internal auditing should be "insightful, proactive, and future-focused".

Risk management is about the present and the future. Internal auditing should be as well. ***There is little value in criticizing the past unless it has implications for the present and the future***. Help management and the board steer their way forward.

When the audit plan and engagements are risk-based, then the scope consists of the controls over sources of significant risk to the enterprise. The objective, although it usually doesn't need to be stated in the report (because it is clear from the scope and the conclusion), is to assess whether those controls are adequately designed and operate effectively to provide reasonable assurance that the risks are at acceptable (or desired) levels.

The assessment of deficiencies and the overall assessment of the controls is then whether that reasonable assurance exists. It is not whether there is a variation from defined criteria. (That concept should be removed in its entirety. It has no meaningful value.)

Finally, there is insufficient attention to aligning internal audit with the strategies, plans, and objectives of the organization.

Recommendations

Several actions will be needed to address the problem.

a) Modify the Purpose statement. Consider:

   "Internal auditing enhances the organization's success by providing the board and management with the risk-based and objective assurance, advice, and insight it needs."

b) Upgrade standard 9.5 to reflect the development and maintenance of a dynamic risk-based audit plan that focuses on the ***sources of significant risk to the objectives of the organization today and tomorrow***. Explain that its not only emerging risks that may drive a change in the plan, but changes in the level (in either direction) of existing sources of risk.

c) Modify all the areas that talk about assessing individual control deficiencies as well as any overall opinions on the audit or series of audits. The criterion for evaluating their significance is the level of potential effect on the achievement of enterprise objectives.

d) Change the definition of assurance to reflect the provision of comfort that management and the board can rely on the system of internal controls (remember it has a risk component) to maintain significant risks at desired levels.

e) Revise the standards related to assessing individual deficiencies and the aggregate of those deficiencies. All should be assessed based on the potential risk they represent to the achievement of enterprise objectives.

f) Modify the standards on communicating to mandate an auditor's opinion on whether the system of control provides reasonable assurance that the enterprise risks in scope are at desired levels.

g) Modify the standards on quality assurance to indicate that they should provide reasonable assurance that the right risks are addressed by quality audits, and the results of that work properly interpreted and acted upon.

h) Add a standard that explains and discusses "insight".

i) Add standards on being proactive and future-focused.

j) Reference the original Core Principles, and they should be introduced and explained in the document right after the Purpose statement. Include them all. Consider consolidating those in the draft to align with the Core Princples, and in the process simplify the Standards.

k) Modify the draft to address the need to align with the organization's objectives, plans, and strategies.

l) Delete Standards 13.2-4.

m) Management should monitor action plan status. Delete 15.2.

4. Other issues requiring attention

Many areas require attention and are highlighted in far more detail in the separate line-by-line review of the draft that is attached. They include:

- Recognize that best and leading practice, adopted by a great many audit functions, is not to include recommendations in the audit report or other communication. Instead, they include agreed action plans. The Standards **must** be revised accordingly, with far more discussion of working with management – an open, constructive, and bilateral discussion – to confirm the facts, agree on their implications, and determine (using the better knowledge of operating management) the appropriate corrective actions.

  The draft reads as if internal audit tells management what the issues are and then works to persuade them. However, best practice by far is to ***have an open dialogue*** that results in identifying the best actions for the organization to take.

- The section on due professional care is excessive, especially the considerations for implementation portion. It goes way beyond the concept of due professional care. See this, which could be inserted without change into the Standards:

  Practice Advisory 1220-1: Due Professional Care

  Primary Related Standard 1220 – Due Professional Care

  Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

  1. Due professional care calls for the application of the care and skill expected of a reasonably prudent and competent internal auditor in the same or similar circumstances. Due professional care is therefore appropriate to the complexities of the engagement being performed. Exercising due professional care involves internal auditors being alert to the possibility of fraud, intentional wrongdoing, errors and omissions, inefficiency, waste, ineffectiveness, and conflicts of interest, as well as being alert to those conditions and activities where irregularities are most likely to occur. This also involves internal auditors identifying inadequate controls and recommending improvements to promote conformance with acceptable procedures and practices.

  2. Due professional care implies reasonable care and competence, not infallibility or extraordinary performance. As such, due professional care requires the internal auditor to conduct examinations and verifications to a reasonable extent. Accordingly, internal auditors cannot give absolute assurance that noncompliance or irregularities do not exist. Nevertheless, the possibility of material irregularities or noncompliance needs to be considered whenever an internal auditor undertakes an internal audit assignment.

  See also AU230 from AICPA and PCAOB.

- The idea that objectivity is impaired if an auditor recently performed an advisory engagement is mistaken. Objectivity may be impaired even more if the auditor recently performed an

assurance engagement of the same area. The CAE should consider whether there is, in fact, an impairment in these situations – but in all likelihood it does not exist.

This **must** be changed.

- The idea of a 3-5 year strategy is unrealistic in 2023, and related discussion **must** be removed.
- The use of the term "residual risk". I only know of one individual[3] who uses this term, which is discredited among risk management practitioners. Just call it risk.
- The section on objectivity should address performing audits of an area where the auditor has shown interest in joining the management team.
- Include the owners as one of the potential "highest-level body charged with governance," and consider the implications of a private company structure on the Standards.
- Standard 7.3 is redundant and should be deleted.
- The use of the phrase "governance, risk management, and control processes". The COSO ICF helps us understand that all three are part of the system of internal control. The phrase GRC is not helpful and should be replaced by internal controls over significant sources of risk, or similar.
- Performance objectives should be explained in the context of the Mission or Purpose.
- The "mandate" is reflected in the Charter. Remove the duplication by eliminating discussion of mandate as if it was separate.
- Make it clear that management is responsible for risk assessment and management, not internal audit. Explain the limitations of any internal audit risk assessment activity.
- 11.3 **must** be amended. The results of audit engagements should be communicated to all who need to know, when they need to know. Periodically is insufficient.
- Many advisory engagements are initiated by the CAE, not at the request of management or the board. This **must** be changed.
- In 10.3, recognize the need to use or increase the use of technology that is already owned.

[3] Tim Leech