Dear Sirs/Madams

I have submitted my response online.

There are many problems I have with the process and the proposals.

I would like to first register my disappointment in the continuance of an inadequate review process, which decides for internal auditors at large what should be open for review, and does that review outside of the reach of internal auditors at large.

Would internal auditors, if they knew the arguments put forward for or against the proposed changes, have been unlikely to have come down on the side of those who ended up in the minority within the RTF? Could it therefore not be said that the proposals, rather than being appropriate, are simply the result of the composition of the RTF?

There is no open process of discussing issues on principle, until after the fact. As should have been our speciality, as internal auditors, we should have opened up the discussion long ago, so that through persuasion, a common view could be forged, which is not based on popularity of a particular point of view, or the status of its supporters, but principle. It is not true that principles have to be explicitly stated to be understood.

I find it disappointing that there was no opportunity for exchange of views as part of the process. The exposure draft and invitation for responses do not constitute an exchange of views and will, as before, simply constitute one speaking past the other.

In the first paragraph of the Exposure draft Executive Summary, it says that the RTf had "the stated objective of evaluating the content and structure of the IPPF."

Was the content of the IPPF really considered? Why then is 2070 unchanged?

Why is the inconsistency in terms of focus of the 2130 group of standards between the assurance and consulting standards not corrected?
Why, if the IIA is open to what is happening in reality, has it not at least opened discussion on the inconsistency of 2010 to the rest of the mandatory IPPF guidance?

Why is the IIA not conclusively addressing in the guidance the inappropriateness of internal auditors being burdened with detailed fraud prevention, detection and investigation responsibilities beyond simply saying they are not expected to have that knowledge. Is it that if they should have that knowledge then it would be fine?

Why is it that the IIA does not make it clear that the internal audit activity is just as subject to internal audit scrutiny as any other organisational unit and therefore should be included in internal audit plans beyond the assessment of conformance to the mandatory IPPF guidance?

Why does the IIA not address the added value concept, which as interpreted in practice, does not emphasise as it should the conduct of the appropriate engagement type for particular circumstances?

Why does 2210 continue to talk of engagement objectives, an external audit concept, when there are only two internal audit objectives as contained in the definitions of assurance and consulting services?

Why does the IIA not remove the superfluous and marketing oriented first sentence of the definition of internal auditing which instead create confusion as to what internal auditing is all about despite the explicit 2100?

Why does the IIA create more confusion by proposing parallel process instead of simplifying the mandatory guidance?

Why does the IIA propose principles which see confidentiality, independence, the systematic disciplined approach, the consistence of the internal audit charter to the mandatory IPPF guidance and the added value concept being in fact viewed as non-core principles of internal auditing?

The failure to discuss the mandatory nature of the mandatory IPPF guidance with senior management and the board/audit committee is the major cause of problems internal audit activities have with their organisations, yet this is not a core principle. That is, as a principle, senior management and the board/audit committee do not have to accept the mandatory IPPF guidance or know about them for an internal audit activity to be effective, given the proposed core principles.

Why cannot the IIA seek to uniquely identify the core competence of internal auditing instead of, as stated in the proposed mission, muddying the waters and make promises which cannot be met?

Why does the IIA not see that non-mandatory guidance is optional and therefore has absolutely no authority and no place in the IPPF?
Why does the IIA introduce a meaningless concept like "less authoritative" in the IPPF?

Internal auditing can only lose by not insisting on its purity of purpose and simply changing how it delivers that mandate.

External auditing has always had the mandate of evaluating the presentation and reliability of financial statements. That mandate cannot go out of fashion. One simply has to ensure that one executes it better, more efficiently and more effectively.

The same could be said of the internal audit dual mandate of assurance and consulting on governance, risk management and control processes as stated throughout the mandatory IPPF guidance, but undermined by 2010, 2030 and 2010.A1. It can never go out of fashion. It simply needed to be refined, clarified and supported in the face of onslaughts which seek to limit internal auditing to assurance provision only and thereby limit the most potent weapon of internal auditing, consulting, as can be seen by it rare appearance in internal audit plans, not that I support the specification of engagement type in the internal audit plan.

In my view, the exposure draft takes the profession backwards, not forwards!

Regards

Kaya Kwinana, CIA

Director, Kaya Kwinana Internal Auditors
Author of "Understand Internal Auditing", available free of charge from www.smashwords.com
Dear Sirs/Madams

I would like to address the risk basis specifically in this response, as a concept which I see as inconsistent with the rest of the mandatory IPPF guidance, except for the standard with mandates it, 2010 and 2030 and 2030.A1 which are inconsistent with 2030.C1 which IS consistent with the mandatory IPPF guidance.

The risk basis flaws are laid out in Practice Advisory 2010-2, where point 15 says:

"An internal audit activity’s plan will normally focus on:
• Unacceptable current risks where management action is required. These would be areas with minimal key controls or mitigating factors that senior management wants audited immediately.
• Control systems on which the organization is most reliant.
• Areas where the differential is great between inherent risk and residual risk.
• Areas where the inherent risk is very high."

In practice, the engagements dealing with these issues are assurance engagements.

The risks (threats and opportunities) which need to be addressed are significant risks. References to inherent risk (and residual risk) ratings are therefore meaningless unless with reference to their significance. One does not find this considered.

The emphasis is on the risk rating rather than its significance - a flaw not to be expected from internal auditors and engagement clients who have been properly advised.

Regarding the guidance that "An internal audit activity’s plan will normally focus on unacceptable current risks where management action is required. These would be areas with minimal key controls or mitigating factors that senior management wants audited immediately." Firstly, dual terminology of current risks for residual risks is unnecessarily used in the PA. Secondly, if management action is what is required, are internal auditors managers? What business do they then have when the required action is understood? Why should it be management, rather than an internal auditor in charge of an engagement, which determines what engagement type should be conducted? If anything, this situation calls for a consulting engagement, yet management wants an assurance engagement! In all of the mandatory IPPF guidance, the word "audit" is never used to describe engagements, why is it in common use in PAs, especially given that it presupposes assurance engagements (the manager may actually be wanting advice not an assessment)? If the internal auditor had done his/her job, would the manager not know what to do, rather than expect the internal auditor to do it for him/her?
Regarding the guidance that "An internal audit activity’s plan will normally focus on Control systems on which the organization is most reliant. The risk management framework ensures that any activity undertaken in an organisation is in pursuance of organisational objectives. Resultant significant risks and their controls should therefore be important in their own right throughout the organisation. Internal auditing should therefore be focusing on all of the organisational units rather than just some of them. If internal auditing focuses only on control systems the organisation is most reliant on, when will it ever address the other control systems since they will never be most relied upon and when will internal auditing ever be able to express an opinion applicable to the whole organisation?"

Regarding the guidance that "An internal audit activity’s plan will normally focus on Areas where the differential is great between inherent risk and residual risk." Why is this differential important without reference to the significance of the risk concerned? Shouldn't periodic self-assessments have addressed this, leaving internal auditing to focus on whether the results of such periodic self-assessments indicate that internal auditing should conduct either of assurance or consulting engagement in the area?

Regarding the guidance that "An internal audit activity’s plan will normally focus on Areas where the inherent risk is very high". The highest inherent risk rating would not save a risk from being insignificant if the risk appetite is specified as that rating. Rather than focusing on the actual rating, was the process to allocate it appropriate? What is the relevance of a high inherent rating without reference to the risk appetite or its significance?

The focus of the suggested engagements are most unlikely to conform to the requirements of 2100 and 2450.

An internal audit plan is therefore best served by ditching the risk basis and basing internal audit plans on the status of the implementation of governance, risk management and control processes in the respective organisational units, using a top down approach and conducting engagements in accordance with 2100. Certain organisational units will have been having positive and reliable periodic self-assessment results, in which case assurance engagement, being independent assessments, are indicated. In other cases, the results of the periodic self-assessments may be either negative or unreliable, in which case consulting engagements are indicated. The engagements would not be included in the internal audit plan as indicated but by the reason for their inclusion. The actual engagement type would be decided on by the internal auditor in charge of the particular engagement, and no one else, during the engagement objective stage of the engagement planning process. The internal audit activity would also be subject to internal audit scrutiny like any other organisational unit (in accordance with 1130.A2) except with respect to conformance to mandatory IPPF guidance, which has a separate process, also to be included in the internal audit plan.

This process is on an ongoing basis focused on the two objectives of internal auditing contained in 2100 and all other mandatory guidance other than the offending risk based oriented one - providing advice on the governance, risk management and control processes to all organisational units on a top down approach and evaluating the adequacy and effectiveness of the governance, risk management and control processes of all organisational units, also using a top down approach. As a result, there is always a to date overall assessment of the state of the organisation's implementation of governance, risk management and control processes.
Properly advised of their responsibilities, each manager, on a top down basis, would want to set an example for his/her subordinates and ensure that each implements appropriate governance, risk management and control processes, because of the reasonable assurance they provide that each respective area's organisational objectives will be achieved. Since periodic self-assessments would be a feature of how such an organisation, units not coping would be easily identifiable and would be proactive in asking for advice since the implementation of these processes is a reflection on their management skills.

Independent assessment could after the initial ones by internal auditing, also be provided firstly a self assessment with independent validation by internal auditing or later, as the number of organisational units already independently assessed to be implementing appropriate governance, risk management and control processes, these units could provide the independent assessments amongst each other on a peer review basis.

As such, assurance and consulting on governance, risk management and control processes would be taking place throughout the organisation, throughout the year, multiplying the efforts of internal auditing.

None of the above is possible with the risk basis in place. The risk basis robs internal auditing of this possibility.

Regards

Kaya Kwinana, CIA

Director, Kaya Kwinana Internal Auditors
Author of "Understand Internal Auditing", available free of charge from www.smashwords.com