Comments on GIAS

Overall opinion

Many years ago I was a member of the IIA (UK) Technical Development Group and was involved in the writing of documents, particularly on risk based internal auditing. I have also written four books which are available on my website www.internalaudit.biz.

I believe there are two major deficiencies in the GIAS:

1. Content and structure of the GIAS

The content is generally very relevant but much is not concise and structured. The Standards document lacks focus and, as a consequence, loses the inherent simplicity of the audit process. The document does not follow the requirements of 11.2 for 'Effective Communications'. In particular:

- Some requirements are vague, lengthy and include unnecessary detail.
- Some requirements are unnecessary, while others which are necessary are not included.
- Requirements are not individually numbered, making reference to them difficult.
- Some detail in 'Requirements' should be in 'Considerations' (Example: Standard 13.1 Engagement Communication).
- The ''Considerations' section reads like a textbook for students studying for IIA exams. It is not always concise, correct or complete. It makes the standards, at 108 pages, far too long. It should be revised and placed in a separate 'Best Practices' document.

2. Risk based internal auditing

The Standards do not encompass the proper implementation of 'Risk-based internal auditing'. There are many instances in the Standards where internal auditors are expected to assess risks. This is management's responsibility and there should be clear instructions that the internal audit function is not responsible for determining risks, although it may assist management in doing this.

As an example to illustrate my points above, the Chief Audit Executive's scrutiny and approval of the organisation's risk assessment process is essential. Not only does it form the basis of the audit plan but such an assessment may be required by regulatory authorities. Despite its importance there is no standard for this approval. Standard 9.5 Internal Audit Plan gets closest and my comments in this section of the comments and other comments illustrate the above conclusion.

- There is no clearly stated requirement for the CAE to approve the risk assessment process. The requirement states, 'The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks'. The term, 'documented assessment' is not clarified and illustrates my point about some recommendations being vague.
- The nearest the standard gets to the CAE approving the identification of key risks is In 'Considerations'. This is an essential requirement of internal auditing and yet it is buried in the third paragraph of a lengthy 'Considerations' box.

- There is no mention in 'Considerations' of the action which the CAE should take if the risk assessment is not sufficient as the basis for the audit plan. Yet this is vitally important advice.
- The second paragraph in 'Considerations' suggests the designing of an 'Audit Universe' before compiling the audit plan. Yet the audit universe (if it used) should be a by-product of the plan, not the basis of it. This point illustrates the lack of clarity in the standards concerning the risk-based internal audit process or, more accurately, the objectives, risks and controls audit process.
- The paragraph beginning, 'The chief audit executive should develop a strategy…' implies the CAE should identify risks. It should state that the CAE should be in constant communication with the board, senior management and any risk function to be aware of emerging risks and the need to change the audit plan.

In my opinion, the Standards need extensive revision, making the recommendations more concise and placing the revised 'Considerations' in a separate document.

I would also add my support to Norman Marks' submission.

David M. Griffiths Ph.D. F.C.A.

Introduction

The introduction should contain the 'Purpose' of internal Auditing' (my comments on this are under the 'Purpose' heading) and a brief introduction to 'Risk Based Internal Auditing'.

Internal auditing has always been about the verification of internal controls in order to form a conclusion as to their effectiveness. In the current incarnation of internal auditing (so called 'risk-based internal auditing'), this translates to examining the management ('control') of the significant risks which affect the achievement of the organisation's objectives and concluding on their effectiveness.

I would suggest the following in the Introduction:

Purpose of Internal Auditing

Internal auditing's unique purpose is to provide independent, objective conclusions as to whether an organization is likely to achieve its objectives, based on its management of opportunities and risks.

Board responsibilities

Before considering the process of internal auditing, the responsibilities of the board and management in respect of risk management need listing:

- To specify the objectives of the organization.
- To identify those opportunities which benefit their achievement and those risks which threaten them.
- To assess the effect of these risks and opportunities on the objectives.
- To implement processes to manage the opportunities and risks to levels acceptable to the board.

The Process of risk based internal auditing

1. To confirm that the above actions have taken place, or report to the board any deficiencies.

2. To base the audit plan on work which will reach a conclusion as to whether those risks which potentially have the greatest disruption to the achievement of the objectives are being managed to a level acceptable to the board.
3. To carry out sufficient verification work to form a conclusion on whether the benefits and risks under consideration are being managed to a level acceptable to the board.
4. To report conclusions to the board in terms of whether the risks are being properly managed and therefore relevant objectives will be achieved.
5. Where the opinion is that the objectives are unlikely to be achieved, to report the action which management is taking to remove the deficiencies.

Glossary

- Risk is defined as, 'The possibility that events will occur and affect the achievement of strategy and business objectives'. Risk assessment includes, 'The significance of risks is typically assessed in terms of impact and likelihood'. Likelihood is defined as, 'The possibility that a given event will occur'. So, a possibility is assessed in terms of impact and possibility, which is confusing. I believe risk should be defined as an event or circumstance which affects the achievement of objectives.

Purpose

- The purpose statement is, 'Internal auditing enhances the organization's success by providing the board and management with objective assurance and advice'. This statement should apply to all employees, so it is not incorrect, just not unique.
- However, the glossary defines internal auditing as, 'An independent, objective assurance and advisory activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes'.
- Why two purposes? And neither is unique to internal auditing. The glossary definition could apply to 'Risk Management'.
- Internal auditing's unique purpose is to provide conclusions as to whether an organization is likely to achieve its objectives, based on the management of opportunities and risks.
- The purpose of internal auditing should be in the 'Introduction'.

Standard 2.1 Individual objectivity

- The first paragraph should stress that auditors must base conclusions on evidence.
- The second paragraph is not a standard.

Standard 6.2 Board Support

- Implementation. Add -The board should supply the CAE with a contact point to use in an emergency. (This is necessary because board members may be independent of the organisation and be difficult to reach in urgent circumstances, such as the discovery of fraud by a board member).
- Implementation – Board practices. The first sentence should read, 'the Board and CAE should meet without management present at least quarterly'.

Standard 7.2 Chief Audit Executive Roles, Responsibilities, and Qualifications

- Under 'Evidence' - Copies of documents proving any formal qualifications held by the Chief Audit Executive'.

Standard 8.3 Quality

Implementation – Board Practices

- How are the bullet items to be measured in a meaningful way? There is a danger that targets such as, 'Number of audits completed' will be chosen to the detriment of audit relevance.

Standard 8.4 External Quality Assessment

- I do not see the need of such an assessment. The board would be aware of the quality of IA through the reports it produces.

Standard 9.1 Understanding Governance, Risk Management, and Control Processes

- The decision making process is a key risk area.
- This is a very confusing section, since it is not only about. 'Understanding' governance etc. but assessing it. Yet there is no requirement for the CAE to come to any conclusions on the adequacy of these processes.
- Understanding the risk management process – there is no consideration here about working with any risk management function that might be available.
- 'The chief audit executive may develop an organization wide risk and control matrix'. This is primarily the role of management although the CAE could assist. It must include objectives, as noted in the glossary

Standard 9.4 Methodologies

- Requirements – there is too much unnecessary detail considering later sections cover detailed internal audit procedures
- Implementation, second paragraph. There should be no need for a rating scale. Individual findings will indicate whether the organisation's objectives will not be, or may not be, achieved. The overall engagement conclusion should indicate whether the objectives will be, may not be, or will not be achieved.

Standard 9.5 Internal Audit Plan

Requirements

- The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks.' What is a 'documented assessment'? The CAE must assess whether the plan can be based on the organisation's identification of risks and report to the board if it cannot.

- The CAE must discuss with the board those risks on which the board requires an opinion as to the effectiveness of their management.
- The CAE must constantly update the plan based on discussions about changes to risks with the board, senior management and any risk management function.

Implementation

- The second paragraph is unclear. The plan should identify risks whose management needs checking. These risks can be grouped into 'audit engagements' to improve efficiency of staff working, which could be collected into an 'Audit Universe'. These audit engagements can then be used to form a resource plan, showing which auditors are working on which engagement and when.
- The danger of an 'Audit Universe' is that it is used as the basis for planning, not as a by-product. This can lead to the use of 'Off the shelf' templates which may be incomplete.
- There are no suggestions as to the action the CAE should take if the organisation's risk assessment is not suitable as a basis for the audit plan.
- A paragraph begins, 'To develop the internal audit plan, the chief audit executive considers the results of the levels of residual risk'. The problem with using residual risk, as opposed to inherent risk, to develop the plan is that residual risk assumes that controls are operating. However, internal audits are intended to verify these and major risks, where the controls are not operating, may not be checked.
- Continuous auditing is a management responsibility.

Principle 10 Manages Resources

- Are the standards in this section necessary? They would be expected of any manager and this standard is not a management handbook.

Standard 11.3 Communicating Results and Standard 11.5 Communicating the acceptance of risks

- There is much in these standards which is covered by Standards 13.1 and 15.1. Are they necessary?

Principle 13 Plan Engagements Effectively

- Why the introduction? It should be in 'Considerations'.
- The introduction assumes audits will assess risks. That is not their responsibility

Standard 13.1 Engagement Communication

- The requirements are too long.

Standard 13.2 Engagement Risk Assessment

- It is not the responsibility of the auditors to assess risks but to assess the management's processes for establishing objectives, identifying risks and introducing controls to manage them down to acceptable levels.

- There is much in the 'Considerations' section that should not be the responsibility of the internal auditor concerning the assessment of risk.

Standard 13.3 Engagement Objectives and Scope

- The objectives and scope should be considered at the very start of the audit.
- The scope must include what conclusion the engagement intends to make.

Standard 13.4 Evaluation Criteria

- The requirements use quite obscure language such as 'evaluation criteria' and 'condition' While these are strictly accurate, the do not correspond to the requirement in 11.2 – Effective Communication must be, 'Clear: logical and easily understood by relevant stakeholders, avoiding unnecessary technical language'.
- Much audit work involves the evaluation of controls to ensure they mitigate risks down to a level acceptable to the board. This is not made clear in the requirements or Considerations.

Standard 14.1 Gathering Information for Analyses and Evaluation

- Some of the 'Requirement' paragraphs are explanations.

Standard 14.2 Analyses and Potential Engagement Findings

- Requirements: isn't the most common example of an engagement finding when a risk is not being controlled sufficiently to within acceptable limits and objectives will/may not be achieved?

Standard 14.6 Documenting Engagements

- There is unnecessary detail in the requirements
- The 'basic format' for working papers in unnecessary. It is sufficient to say they should support the conclusions

Standard 15.1

- There is unnecessary detail in the requirements