HE Insight

Chartered Institute of Internal Auditors: Internal Audit Code of Practice

March 2020

Introduction

In January 2020, the Chartered Institute of Internal Auditors published its Internal Audit Code of Practice - providing guidance on effective internal audit in the private and third sectors. The Code is principles-based, and is intended as an industry benchmark, to help embed good practice internal audit and raise the bar across the profession.

Those familiar with UK Higher Education will recall that the former OfS Audit Code included an expectation that internal auditors would comply with broader professional standards. In the absence of guidance to the contrary, we can reasonably assume that internal auditors, audit committees and executive clients in the higher education sector all need to be mindful of this new Code: we assume that adherence to the Code will help to demonstrate that the mandatory requirement to have an internal audit function is being met effectively.

The publication of this new guidance is both important and timely, given recent high-profile corporate collapses linked to governance deficiencies, most notably Carillion in January 2018, which has led to a wide-ranging review of the audit and corporate governance framework. This creates an opportunity to enhance internal audit's role in supporting non-executive and executive management, in organisations across the private and third sectors (a separate code for financial services firms has already been published), to manage and mitigate their risks more effectively.

Code sections

The Code contains the following sections - role and mandate of internal audit, scope and priorities of internal audit, reporting results, interaction with risk management, compliance and finance, independence and authority of internal audit, resources, quality assurance and improvement programme, relationship with regulators and relationship with external audit.

There is an expectation that boards, and in particular audit committees, embrace the key principles contained within the Code, so as to enhance the effectiveness of their internal audit functions. We set out below some thoughts on particular elements within the Code.

Scope of internal audit

The Code states '*The scope of internal audit's work should be regularly reviewed to take account of new and emerging risks. Where relevant, internal audit should assess not only the process followed by the organisation's first and second lines of defence, but also the quality of their work*'.

In line with the development of the profession over the last decade, rightly the Code should reference lines of defence (with internal audit seen as the third line). The Code stops short of mentioning formal assurance mapping but it is now not uncommon for internal audit programmes to be developed within the context of a broader assurance framework i.e. when considering whether an internal audit on the management of risks is worthwhile, first understanding whether and how the board is gaining assurances from other sources.

However, the assurance maps tend to be relatively unsophisticated – simply listing the first and second line – and not assessing their effectiveness. Arguably, internal audit outputs should be more explicit in articulating the adequacy of the first and second line defences when issuing their final reports – and indeed when assessing the value of an internal audit in the first place (see related point at the end of this section).

The Code also states that internal audit's scope should include '*The information presented to the board and executive management for strategic and operational decision-making'.*

We accept that, on a review by review basis, internal audit reviews may include an assessment of the information presented to the board and executive management but this will not necessarily happen in each review. If there is an internal audit of governance arrangements, the scope should cover this information, however, these reviews may only be undertaken every three or four years.

Given the importance of ensuring that the governing body and executive management get the right information, at the right time - that it is clear, focussed and accurate would seem to be absolutely fundamental to the management of strategic risks and opportunities – and, potentially, should be a prominent candidate for inclusion within programmes of internal audit work.

The Code also states that the scope should cover *'The setting of, and adherence to, the risks the entity is willing to accept (risk appetite). Internal audit is not responsible for setting the risk appetite but should assess whether the risk appetite has been established and reviewed through the active involvement of the board and executive management. It should assess whether risk appetite is embedded within the activities, limits and reporting of the organisation; and it should report annually to the audit committee its conclusions on whether the organisation's risk appetite is being adhered to'.*

We believe that this is a confusing area and we are not convinced that the Code provides clarity. A general statement on an organisation's risk appetite is, arguably, of little use but there is perhaps more benefit in an assessment on a risk by risk basis – and, from that, potentially setting parameters. We have seen some institutions present their position graphically – where risks are given a net rating i.e. the position once controls are factored in and that is compared with an acceptable appetite or tolerance position. Where the former falls below the latter, it prompts a discussion on whether the risk should be avoided or a different approach to managing the risk needs to be adopted – which, hopefully, brings the net position to below the tolerance point. However, there is a danger that the exercise becomes too complex and the setting of arbitrary scores and tolerance levels dominate and distracts from a mature discussion on the best approach.

Reporting results

The Code states that '*Internal audit should be present at, and issue reports to the relevant governing bodies, including the board audit committee, and any other board committees as appropriate. The nature of the reports will depend on the remits of the respective governing bodies'.*

The scope of internal audit has developed considerably over the last twenty years – to an extent that audit committees have grappled with how best to balance the programme between financial and non-financial areas. Given the risk based approach, there may be benefits in, perhaps as part of the audit programme development exercise, engagement with the full board and its key committees e.g. finance, estates, HR etc. This would be an opportunity to have a more informed discussion and for those committees to consider potential reviews which would aid them in fulfilling their terms of reference.

The Code also states *'Internal audit's reporting to the board audit and any other board committees should include 'at least annually, an assessment of the overall effectiveness of the governance, and risk and control framework of the organisation, and its conclusions on whether the organisation's risk appetite is being adhered to, together with an analysis of themes and trends emerging from internal audit work and their impact on the organisation's risk profile'.*

Within the HE Sector, the OfS's predecessor (HEFCE) required an internal audit annual report detailing opinions on similar areas. Whilst the OfS is yet to state its requirements (if indeed they have any), many institutions we work with are retaining the HEFCE model. Consideration could be given to making the internal auditor's annual report (and the audit committee's) a richer output which, for example, may draw on other areas e.g. the wider approach to gaining assurance (including assessments on the first and second lines), the adequacy of the information that the board has received over the last twelve months and any lessons learned / improvements based on how the risks (and opportunities) played out, adherence to the OfS registration conditions, governance issues across the sector (and beyond) and how comfort is drawn that the institution is doing / has done all it can to avoid similar pitfalls.

Interaction with risk management, compliance and finance

The Code states '*In most organisations there will be some functions (e.g. finance, HR, compliance, legal, health & safety and risk management) whose responsibilities include designing and / or operating controls over risks which arise in other parts of the organisation. Functions with such control responsibilities have substantial potential to contribute to the effectiveness of governance, risk management and internal controls in an organisation.*

Internal audit should include within its scope an assessment of the adequacy and effectiveness of the control functions. This assessment should involve informed judgement as to what extent it is appropriate to take account of relevant work undertaken by others, such as risk management, compliance or finance in either its risk assessment or in the determination of the level of audit testing required for the activities under review. Any judgement which results in less intensive

internal audit scrutiny should only be made after an appropriate evaluation of the effectiveness of that specific function in relation to the area under review'.

This would appear to us as a description of assurance mapping – and ties in with the earlier comments in this section. We fully endorse a more integrated approach and, at the very least, when considering audits within the plan and, if included, when undertaking the planning for the reviews – the totality of the assurance mechanisms (and their effectiveness) should be undertaken.

Who audits the auditors?

The Code is demanding for auditors and their clients alike. The sector tends to measure the number of days taken; the cost per day; and tender processes. We are also told, anecdotally, that there is frequent heavy reliance on junior staff to deliver internal audits across the sector – with consequent reservations about quality. This Code could and should be a call to action for higher education providers to engage meaningfully with internal audit and to test whether their provision has substance, or merely form. We don't know how the Office for Students will evaluate the quality of internal audit provision in future: but we suggest that material engagement with and adherence to this Code will be inherently helpful to organisations and reassuring to our regulator.

How can we help?

Our specialism is internal audit. We seek not only to provide an outstanding service to the Higher Education sector, we also integrate our work with other assurance functions.

For further information on these, or any other aspect of Uniac's internal audit and assurance service, please do get in touch.

Sean Ryan
Director
t: 0161 247 2856
e: sryan@uniac.co.uk
www.uniac.co.uk

Richard Young
Director
t: 0161 247 2959
e: ryoung@uniac.co.uk
www.uniac.co.uk