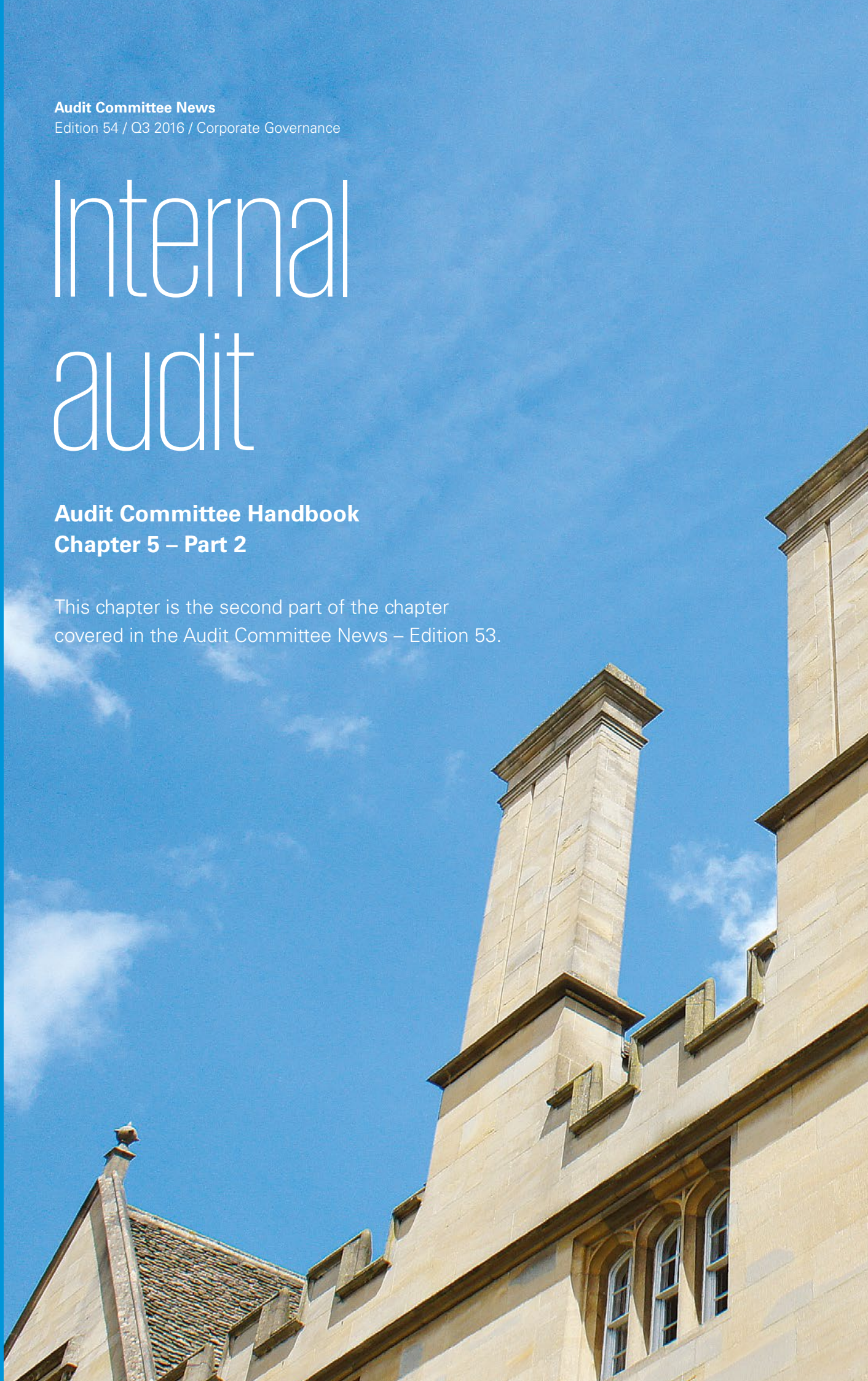
Audit Committee News
Edition 54 / Q3 2016 / Corporate Governance

Internal audit

Audit Committee Handbook
Chapter 5 – Part 2

This chapter is the second part of the chapter covered in the Audit Committee News – Edition 53.



Oversight of the internal audit function

In providing oversight over the internal audit function, the audit committee should, inter alia:

- ensure that the internal auditor has direct access to the board chairman and to the audit committee and is accountable to the audit committee;
- review and assess the annual internal audit work plan;
- receive a report on the results of the internal auditors work on a periodic basis;
- review and monitor management's responsiveness to the internal auditor's findings and recommendations;
- meet with the head of internal audit at least once a year without the presence of management; and
- monitor and assess the role and effectiveness of the internal audit function in the overall context of the company's risk management system.

Ensuring internal audit has direct access to the audit committee

A significant challenge for internal audit lies in understanding its responsibility to both the audit committee and management. The internal auditor is "employed" by management and yet reviews management's conduct. In addition, the internal auditor reports to the audit committee and yet is not line-managed on a day-to-day basis by the audit committee (although the committee has a significant role in appointing the internal auditor).

Falling into a detailed, and not terribly helpful, analysis of "straight line" versus "dotted line" reporting is all too easy. The fundamental point is that internal audit has, for all practical purposes, a dual reporting relationship where the head of internal audit reports to executive management (ideally the CEO) for assistance in establishing direction, support, and administrative matters; and to the audit committee for strategic direction, reinforcement, and accountability.

Normally, the audit committee would approve the internal audit terms of reference; approve the audit function's risk assessment, audit plan, and budget; receive reports from the head of internal audit on the results of internal audit activities or other matters that the head of internal audit determines necessary; approve the appointment, removal, evaluation, and compensation of the head of internal audit; and determine whether there are scope or budgetary limitations that impede the internal audit function in carrying out its work. By contrast, the administrative reporting line to the CEO would typically include budgeting and management accounting; human resource administration; internal communications; and internal administrative matters such as expense approvals, leave approvals and logistics.

The precise reporting arrangements may differ from organisation to organisation; however, it is important that internal audit always retain a degree of independence from management so that it can carry out its duties objectively. For this reason a clear line of responsibility to the audit committee is essential. The committee should have processes in place to facilitate confidential exchanges with the internal auditor, with regular meetings scheduled between the audit committee and the head of internal audit. Many audit committee chairs go further and maintain informal contact with the internal auditor between meetings.

The audit committee should also do its utmost to ensure that internal audit has:

- sufficient status, respect and support within the institution;
- unrestricted access to all records, assets, personnel and premises;
- authorisation to obtain whatever information and explanations are considered necessary by the head of internal audit; and
- adequate human and other resources to perform its work effectively.

Assessing the annual internal audit work plan

The internal auditor should prepare an audit plan based on the organisation's assurance needs. This plan should address how all the organisation's key systems and processes will be audited during the audit cycle, together with the resources to be applied – normally expressed in "man days". Areas of greater risk might be addressed at the beginning of the audit cycle and then revisited later in the cycle.

As an audit plan is unlikely to cover all areas of risk within a single year, the plan for any given year should place its work in the context of work done in the preceding year and projected for the succeeding year. The audit committee and management may take a different view of timing and priorities, which should be resolved through discussion.

Assurance mapping

The audit committee should review the risk map and audit plan to satisfy itself that appropriate audit coverage will be devoted to all the organisation's assurance needs. If internal audit is not covering a particular risk area – or not covering it in sufficient depth – then other means of assurance should be in place, whether that be assurance from the business operations, head office functions or other independent assurance providers.

When the audit committee is satisfied with the audit plan, it should recommend the plan to the board for approval, if its terms of reference so require. Once the plan has been approved, the audit committee should monitor the auditor's progress against it during the year.

Internal auditors may carry out additional work at the request of management (including investigations), provided such work does not compromise the objectivity of the audit service or achievement of the audit plan. The audit committee should satisfy itself that the objectivity of internal audit has not been affected by the extent and nature of other work carried out.

Internal audit reports and monitoring management's response

While internal audit reports to management (preferably the CEO) on a day-to-day basis, audit committees have a responsibility for oversight and therefore need to determine appropriate communication channels and reporting arrangements with internal audit. Some audit committees want to see every audit report, some a summary of every report, and others a periodic summary. Progress reports, comparing audit activity against the audit plan, are also useful.

It is important that the audit committee considers significant individual audit findings or recommendations, though it need not be concerned with more detailed findings unless the committee considers it valuable to do so. It is good practice for internal auditors to prioritise their findings against agreed standards. This indicates the importance of each audit recommendation and the urgency of any required action.

The audit committee should concentrate on gaining assurance that the organisation's risk management, control and governance arrangements are adequate and effective. For this purpose, the committee should ensure that there is an adequate system to monitor the implementation of agreed audit recommendations. An implementation plan detailing the recommendation, the required action, priority, person responsible and timescale is a good method of fulfilling this objective.

Internal audit should have a systematic process of follow-up to obtain appropriate assurance that management has taken timely and effective action. It should promptly advise the audit committee of its findings and further action required.

The board, advised by the audit committee, should ultimately be responsible for either ensuring that management takes prompt and effective action on those audit reports which call for it; or recognising and accepting the risks of management not taking action.

What is internal audit telling the audit committee?

An audit committee might reasonably question what assurance it's receiving when confronted with audit reports drafted along the following lines:

"Significant improvements have been made in this area in the last 12 months. However, the management agenda reflects a number of issues whose resolution would enable further, necessary improvements to be made."

This is compromise wording. Such reports are not uncommon. However, if an audit committee ever receives a summary like this, it may legitimately ask itself what on earth it means. For example: having done extensive testing and comparison to best practice, the internal auditor wants to say, "the management of controls in this area is poor". However, management believe (say) that the area in question was poorly managed some time ago, but a lot of work has been done during the year and therefore there is no value in internal audit raising issues that they are already both aware of, and dealing with (albeit slowly). They will express incredulity that internal audit should want to make a fuss about a well-known issue. Hence the compromise wording: carefully crafted to maintain pride on both sides.

The audit committee might reasonably conclude that the head of internal audit is too weak, or too junior, or too bullied and does not feel able to say what he or she really thinks.

"Whilst a number of improvements have been made in this area, further change is required if its management is to become world-class."

This is told you so wording. It means that if controls fail, some financial catastrophe looms and the audit committee turns to the head of internal audit and asks, "Why wasn't I warned?" she or he can reply, "I told you so. We reported it to you. Wasn't it clear? You could have asked for more details if you had any questions or even requested the full report."

The underlying cause of such wording might be that people are afraid of bringing bad news either to the audit committee or, more likely, they're afraid of trying to get it past the executive team.

"Wider variations in base rate and potential dynamic margin shifts to reflect market positioning would mean that the business would be more exposed to rate increases than decreases".

This is preventative wording. Many audit committee members might legitimately have a problem understanding what this means; yet all it is saying is that the business in question is vulnerable to a rise in interest rates. Preventative wording is designed to prevent the reader understanding the issue. Can it really have any other purpose?

Internal audit does not want the audit committee to understand because they might ask difficult, inconvenient questions that will be embarrassing or maybe just tedious to answer. Or maybe, no one can do anything about the issue anyway so why make trouble? Whatever the motivation, whether it is conscious or subconscious, internal audit are reporting to the audit committee in a way designed to elicit a reduced reaction. Preventative wording is extremely dangerous and audit committees should be alert to it.

"In the last six months, we have issued 74 reports of which 27 were rated as significant. These are split by division in the table below. A further chart showing traffic light ratings etc., etc".

This is death by statistics. An audit committee can look at all of this information yet be unable to draw a single, meaningful insight from any of it. Of course, this form of reporting can be valuable where internal audit is doing standard processes at multiple locations, such as retail store audits. But, where one piece of work is not directly comparable with another, it is just filler. The underlying cause is that the internal audit function wants to demonstrate progress but has no idea how to demonstrate value.

"In camera" meetings with the head of internal audit

Many audit committees want to meet the head of internal audit in a private session where management is not present. This approach allows the audit committee to ask questions on matters that might not have been specifically addressed by the internal audit function's formal work programme – nevertheless, the head of internal audit might, as a result of his work, have valuable views and opinions. A private session allows the head of internal audit to provide candid, often confidential, comments to the audit committee on such matters.

Typically there should be few items to discuss. Ideally all key matters relating to internal audit should have been addressed in a candid and robust manner by management, the audit committee and the head of internal audit during the formal audit committee meeting. The audit committee can use the private session as a follow-up if members were not satisfied with the answers given at the audit committee meeting or if they thought discussions had been too guarded or uneasy. However, such matters should have been fully aired at the audit committee meeting and generally should not need to be readdressed in the private session.

The private session should focus on areas where the head of internal audit can provide additional, candid, and often confidential, comments to the audit committee on other matters. The private session gives the audit committee an opportunity to explore such matters in a frank and open forum. In addition, the audit committee may have more knowledge than the head of internal audit on other matters, and this session allows the audit committee an opportunity to air such issues.

Overall, private sessions can play an important role in the development of a trusting and respectful relationship between the audit committee and the head of internal audit.

The audit committee may want to ask questions around relationships, attitudes and resources, such as:

- How strong is the relationship between the internal audit function and management/operations?
- Does internal audit receive appropriate cooperation from operational and head office management?
- Have any requests for information been denied or otherwise obstructed?
- Is the internal audit function subject to undue pressure from any source?
- How constructive is the relationship between the internal audit function and external audit?
- What is management's attitude towards risk management and internal controls?
- Are adequate people and other resources devoted to key areas of the business and control functions?

Assessing the internal audit function's performance

The audit committee should monitor the performance and effectiveness of internal audit on an annual basis. This should include any matters affecting the audit function's independence and objectivity.

Self-assessment by the head of internal audit is a useful assessment tool, but it should not be the sole means of assessing the effectiveness of internal audit. The audit committee should draw its own conclusions based on its experience and contact with internal audit as well as the views of others such as the CFO, divisional heads and external audit. In evaluating the work of internal audit, the audit committee should review the annual internal audit work plan, receive periodic reports on the results of the internal auditor's work and monitor management's responsiveness to the internal auditor's findings and recommendations.

When agreeing appropriate performance measures for internal audit, the audit committee should recognise that such measures need to be adapted to each organisation's circumstances. The following diagram illustrates some of the more common measures used to monitor the performance of internal audit.

The key steps in a typical internal audit annual cycle are discussed at Appendix 1.

Appendix 1

The key steps in an annual cycle

Produce the annual work programme	• Create an annual internal audit plan for approval by the audit committee, typically as part of an indicative 3 or 5 year plan linked to a wider risk/audit universe • Identify resource requirements, including relevant subject matter and industry experience to add value to the process, and associated budgets • Agree the timeline for performing individual assignments in the agreed plan • Additional reviews may be required: the approach needs to be nimble to respond to the needs of the audit committee and the executive team • Consideration should also be given at this stage to the interaction with risk management activities and the specific linkage of risk and assurance
Plan individual assignments	• For each allocated audit assignment, terms of reference should be agreed in advance • Staff requirements should be confirmed and communicated to the team reasonably far in advance of the work to help continuity • Planning meetings with the nominated business sponsor and business process owners, information gathering and briefing of team members prior to each assignment
Perform fieldwork	• Fieldwork should commence with an opening meeting involving all relevant team members so that: – expectations are understood; and – the objectives, scope, techniques and emphasis of the review are clear. • A "no surprises" approach is fundamental. The nominated business sponsor should be informed of issues as they arise • Ways of working should be defined and consistently applied and measured (including the business responsibilities) • Variations to timelines or budgets should be monitored and flagged as soon as they are identified to key sponsors
Exit meeting	• Prior to formal reporting, an exit meeting should be held with the relevant business sponsor and other employees as agreed • The purpose of the meeting is to: – confirm that expectations have been met; – highlight and re-confirm the findings of the review; – validate the findings; and – where appropriate, obtain management's acceptance and support for the recommendations made, including their commitment to actions with clear dates for implementation
Reporting	• Prepare a draft report to be issued to management within an agreed number of working days of completion of each audit and finalise the report, again within an agreed time frame of receipt of management responses • Report in accordance with standard template • Determine who should attend and present at stakeholder and audit committee meetings
Issue resolution tracking	• Following the issue of final reports, monitor agreed upon management action plans and subsequent reporting to senior management and the audit committee • Clear protocols for follow up work as and when needed
Overall considerations	• Defined audit charter • A defined strategy • An ongoing awareness of key business risks and how this drives audit • Clear role defined on related activities e.g., investigations/ad hoc assignments • Agreed communication protocols • Clear business case/cost analysis and monitoring • Ways of working protocols • KPIs to track progress and delivery • Stakeholder satisfaction surveys