11 October 2019

Auditing corporate governance
Chartered Institute of Internal Auditors

This guide sets out the steps internal auditors should take when conducting a review of corporate governance. We look at how to provide consultancy and assurance based upon potential risks.

Why is corporate governance included in the audit plan?
Research and gather background information
Audit committee assurance requirements
The second line of defence and the need for coordination
What to audit and how
Skills and experience required
Performing corporate governance audits – content

Why is corporate governance included in the audit plan?

The Institute of Internal Auditors (IIA) Standards and other best practice advises internal audit to include governance processes in its scope. Therefore, in order to provide assurance that the organisation can meet its objectives, internal audit should consider including an audit of corporate governance in its risk-based plan. Corporate governance should be included in the audit universe, where this is in place, and audits should be planned in accordance with the organisation’s risk-based planning methodology.

When assessing corporate governance in your organisation, it may be appropriate to undertake a specific review of corporate governance, organisation reviews of specific subject areas and/or incorporate aspects of corporate governance into other reviews which form part of the audit plan.

The guidance that internal audit may wish to consider supporting an audit of corporate governance includes:

• The IIA Definition of internal auditing requires internal audit activity to audit ‘governance processes’.
• Standard 2110 Governance requires the internal audit activity to assess and make appropriate recommendations to improve the organisation’s governance processes.
• Sector-specific guidance, some of which are highlighted in the section below on researching and gathering background information.

Poor corporate governance has been responsible for the well-publicised failure or reputational damage of many organisations. Examples include:

• Carillion - collapse exposes deep corporate governance failings
• Kobe Steel - inadequate corporate governance
• Raiffeisen bank - major governance failings
• Patisserie Valerie - complete lack of control and understanding of the financial accounts
Research and gather background information

There are a number of best practice guides which explain how good governance practices should be established in organisations. Primary amongst these is the Financial Reporting Council’s 2018 UK Corporate Governance Code and the 2018 FRC Guidance on Board Effectiveness. The latest update in 2018 focuses on the application of the Principles emphasising the value of good corporate governance to long-term sustainable success. Whilst this code is considered to be the definitive guide to good corporate governance, other guidelines are also available, eg:

- OECD Principles of Corporate Governance - November 2015
- Charity Governance Code - 2017
- European Banking Authority (EBA) Guidelines on Internal Governance under Directive 2013/36/EU
- Corporate Governance in Central Government Departments – April 2017
- Quoted Company Alliance Corporate Governance Code (QCA Code) – 2018
- The Wates Corporate Governance Principles for Large Private Companies - 2018

Your organisation’s annual report may contain a statement about their commitment to good governance and which guidelines they are committed to follow eg the Social Housing Sector conforms to the National Housing Federation Code of Corporate Governance. This will provide you with a baseline on which to test the controls.

Here are some examples of what organisations have included in their annual report:

- Marks and Spencer
- Save the Children – page 48
- Atom bank - page 28

Audit committee assurance requirements

In determining the scope of the audit, the internal auditor will need to consider their stakeholders’ expectations – including the organisation’s regulators, board, audit committee, senior management, head of internal audit – as well as the responsibilities documented in the internal audit charter. In particular, the non-executive members (NEDs) of the board and committees play a key role in corporate governance and their expectations are key.

There are increasing expectations from regulators and governing bodies for example the:

- The 2018 Corporate Governance Code and the more detailed Provisions within the Principles.
- Charity Governance Code says that, in relation to board effectiveness that the board should collectively receive specialist in-house or external governance advice and support.
- Financial Reporting Council’s 2018 Guidance on Board Effectiveness says that the chair should consider ways in which to obtain feedback from the workforce and other stakeholders – for example, the auditors – on the performance of the board and other individual directors.
- FS Code says that internal audit should include within its scope the design and operating effectiveness of the internal governance structures and processes of the organisation.

It should be noted that following the Kingman Review the government has now replaced the
Financial Reporting Council (FRC) with a new regulator, the Audit Reporting and Governance Authority (ARGA) that will have a new mandate, new leadership and stronger powers set down in law.

The second line of defence and the need for coordination

The relationship among governance, risk management, and internal control should be considered. This item is addressed in implementation guide 2110 and guidance published by the Chartered IIA entitled Coordination of assurance services both of which explain that governance does not exist as a set of distinct and separate processes and structures. Rather, there are relationships among governance, risk management, and internal controls. Effective governance activities consider risk when setting strategy.

Conversely, risk management relies on effective governance (eg, tone at the top, risk appetite and tolerance, risk culture, and the oversight of risk management). Effective governance relies on internal controls and communication to the board on the effectiveness of those controls. One of the key roles of the board and senior management is to manage internal controls. The second line of defence is key in providing the board with information regarding internal controls which may be obtained from control risk self-assessment (CRSA), risk self-assessment (RSA), and assurance programmes etc. (all of these processes should also be subject to regular audit).

Where there are any elements of the Code that the first and second lines of defence are providing assurance about conformance, then there should be discussion and co-ordination with internal audit to avoid duplication of effort, where possible.

What could be audited and how

Consider if corporate governance should be audited as a separate review looking at governance overall, or as part of other audits or a combination, eg board, board committees, and management committees may be separate audits. Committees that are product, area or programme specific such as risk committees may be audited as part of audit activity covering that topic. You may want to consider using ‘soft control’ auditing techniques such as questionnaires, structured interviews, providing quantitative facts to elicit observation of engagement, challenge, training and feedback from the board.

There are two possible approaches to auditing corporate governance:

Process
The audit scope focuses on providing assurance that the processes and procedures for managing the governance structures and meetings are in place and operating effectively, eg:

- company secretary (papers/minutes, organisation, board recruitment etc.) – the quality and documentation of minutes has been a hot topic
- consider where there are multiple legal entities within one holding company – are they all being covered
- reporting (meeting packs coordination, distribution, completeness, timeliness)
- board/committee composition, (skills, training emphasis on continuous and proportionate support, succession planning etc.)
• benchmarking - against recognised codes/best practices
• meetings (held, minuted, attendance etc.)
• input of stakeholders – capture of feedback in relation to management information
• conflict of interest (declarations, mitigating actions, record keeping etc.)
• non-executive directors are able to seek clarification from management where information provided is inadequate or lacks clarity
• communications between management and the workforce in respect of the organisations culture, and for ensuring that operational policies and practices drive the right behaviour.

**Effectiveness**

The audits seek to add additional value by providing a judgement on how effective the governance bodies are. The scope of these such audits might include:

• quality and openness of discussions
• challenge and decision-making
• link to strategy/outcomes
• monitoring risk and controls/oversight of first line of defence, RSA, CRSA etc.
• notification and escalation of material events – especially where they could result in reputational risk – note TSB IT issues
• vision
• dynamics
• tone at the top
• board/committee packs (quality of information, completeness, readability, sufficient, timely, appropriate level
• interactions between non-executive directors and the business, eg to meet stakeholders, key customers, members of the workforce from all levels in the organisation
• whether non-executive directors have sufficient time available to discharge their responsibilities effectively
• awareness of senior managers views on business issues by the board
• ensuring that the board is aware of views gathered via engagement between management and the workforce.

**Skills and experience required**

The skills, experience and knowledge required by the internal auditor who will be completing the review depends on the type of audit review selected.

For an audit focused on process, an in-house audit team consisting of a mix of seniority and skills may be sufficient.

However, for an effectiveness audit, you may wish to consider senior staff with specific skills as this type of review will include dealing with senior management and assessing compliance with legal/regulatory requirements as well as internal requirements - Nolan principles in the public sector for example. The internal auditors will be required to meet with senior stakeholders in the business including executive directors and non-executive directors and must have the skills to be able to discuss, assess and challenge these individuals as part of their activities in assessing the effectiveness of governance.
Where the internal audit function does not have the specific skills or experience, consideration should be given to using co-sourcing arrangements to complete the audit or outsource the completion of the audit.

**Performing corporate governance audits – content**

**Key risks**

**Strategic and business:**

- inappropriate strategic and business decisions or inability to deliver on decisions
- not achieving the stated objectives
- financial loss or negative impact on financial results.

**Reputational:**

- legal and regulatory non-compliance (may also have financial impact)
- decisions not being taken in the best interests of all stakeholders.

**Key controls**

<table>
<thead>
<tr>
<th>Key controls</th>
<th>Potential responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Following best practice</td>
<td>Find out which corporate governance guidance is adopted by your organisation.</td>
</tr>
<tr>
<td></td>
<td>Is the governance structure and framework in line with best practice?</td>
</tr>
<tr>
<td></td>
<td>Dependent upon the particular meeting types, are they in line with the governance requirements, for example:</td>
</tr>
<tr>
<td></td>
<td>- are the meetings held frequently enough?</td>
</tr>
<tr>
<td></td>
<td>- is there a board closed meeting without officers of the organisation present?</td>
</tr>
<tr>
<td></td>
<td>- is there a closed meeting for the audit committee to meet with the internal auditors at least annually? are the meetings well attended and quorate?</td>
</tr>
<tr>
<td></td>
<td>- are meetings minuted and in sufficient detail?</td>
</tr>
<tr>
<td>Conflict of interest</td>
<td>Is there a policy covering conflict of interest?</td>
</tr>
<tr>
<td></td>
<td>Are conflicts of interest declared at board and board committee meetings and are these documented?</td>
</tr>
<tr>
<td>Does the process include independent director support?</td>
<td></td>
</tr>
<tr>
<td>Is there evidence that declared conflicts are managed appropriately?</td>
<td></td>
</tr>
<tr>
<td>Is there an attendance log to provide transparency as to which members attend on a regular basis ie commitment?</td>
<td></td>
</tr>
</tbody>
</table>

**Training**

| Is sufficient training available to board members, including for specialist topics if requested and is this taken up eg cloud technology? |
| Is the training refreshed periodically? |

**Appointments and succession planning**

| Is there a process in place to identify and select new/replacement board members? |
| Is there a skills matrix to highlight skills required when recruiting? |
| Does the recruitment process accurately reflect the organisation's policy and targets for diversity? |
| Is there a policy stating the maximum term a board member can serve? |
| When a board member/chair is replaced, is there a process to identify and train a successor? |

**Board reporting and information flows**

| Are the reports/information sufficiently detailed, transparent, timely and comprehensive? |
| Is the internal control environment reported on and discussed, eg CRSA, RSA? |
| Are they reflective of the real situation, eg check that information is not too high level to hide individual breaches in risk appetite? |
| Do the board/committee members have sufficient time to read the reports? |
| Are the reports discussed and, where applicable, actions decided upon? |
| Is the agenda split into topics for decision and topics that provide an assurance re internal control, risk management and governance? |
| Is there a process in place to track, follow-up and show completed actions? |
### Tone at the top

- Are decisions taken that consider the wider ethical issues, as well as business and financial issues?
- Do all members have an equal opportunity to participate?

### Strategy

- Is strategy discussed and agreed upon?
- How is this strategy reflected in the business objectives?
- Can the strategy be traced to business objectives/activities?
- Is the internal audit strategic plan aligned to the organisation's strategic plan?

### Risk management

- Is there sufficient information on risk management available to the board and board committees?
- Are the risks discussed and decisions clearly articulated?
- Is the risk appetite set by the board?
- Is conformance with the risk management policy/framework reviewed and reported on by either the 2nd or 3rd lines of defence?

---

**Further reading**

**International Standards**

- 2110 - Governance

**Implementation guides**

- 2110 - Governance

**Guidance**

- Effective internal audit in the financial services sector (FS Code)
- Coordination of assurance services
- Governance of risk: three lines of defence
- Solvency II – the role of internal audit

**Research and insight**
Harnessing the power of internal audit

**External resources**

**Financial Reporting Council:**

- 2018 UK Code of Corporate Governance
- 2018 Guidance on Board Effectiveness
- Annual Review of Corporate Governance and Reporting 2017/18
- The Wates Corporate Governance Principles for Large Private Companies 2018
- Independent review of the Financial Reporting Council