

Committee Assurance Principles

Purpose and remit

The overall purpose of the Board is to ensure efficient, effective and accountable governance, to provide strategic leadership and direction, and to focus on agreed outcomes. Detailed scrutiny should take place at committee level, with each committee providing assurance and escalating key issues as required. For this to be achieved successfully, Standing Committees must be clear about their priorities, have focused agendas and workplans and must monitor their own performance rigorously. Standing Committee remits are approved by the Board with input from Committees and increasingly from national governance initiatives. However, Standing Committees must ensure that they are focused on Board priorities and on the risks delegated to them.

Sub-committees and groups will frequently have an operational focus but must ensure that they are in a position to provide the required assurances on their operations and on any risks, actions and controls for which they are responsible.

Board or Standing Committee agenda

In general, for an item to be included on the agenda it should meet the following criteria unless the Committee Chair and Lead Officer agree there are good reasons for its inclusion:

- a. It is a decision delegated to that Committee
- b. It relates to and/or provides assurance upon a risk delegated to that Committee. In this context, performance reports etc should be overtly related to the specific risk and should contain a conclusion on whether the performance reports indicate that controls are operating effectively to mitigate the risk as intended
- c. It is a statutory or regulatory requirement or required by SG guidance
- d. The Committee can add value to a decision or issue by providing a different perspective, setting boundaries, generating ideas etc.

Assurance

At the start of the year, the Committee should consider its remit and determine its assurance requirements together with how these will be met, using assurance mapping principles. This should be set out in the Committee assurance plan or clearly identified within the Committee work plan. The 'three lines of assurance' are often used to help categorise assurances

- First line: management assurance from "front line" or business operational areas;
- Second line: oversight of management activity, including effective management information, separate from those responsible for delivery, but not independent of the organisation's management chain;
- Third line: independent and more objective assurance, including the role of Internal Audit and from external bodies

Assurances should be:

- a. Overtly linked to the relevant risk with an overt conclusion from the responsible director or officer
- b. Streamlined so that there is no omission, no unnecessary duplication

- c. Relevant: data should not be presented just because it is readily available
- d. Reliable: assurances should be evaluated so that it is clear how much weight should be placed on any piece of evidence and how they fit in with other relevant evidence
- e. Sufficient: there should be sufficient evidence in total to allow a reasonable conclusion to be reached

The Board has delegated responsibility for most strategic risks to Standing Committees. Following a discussion of an agenda item, the committee should formally assess the level of assurance received. This is reported to the Board via the Chair's assurance report (see below). The following criteria (based on work undertaken by the Good Governance Institute) can help in assessing the level of assurance:

- a. Independent assurance (e.g. an auditor's opinion) carries more weight than internal evidence produced by management
- b. The best assurance is commissioned specifically to assure that a control is effective: reams of evidence with only indirect relevance does not provide good assurance
- c. Assurances are time-limited and should only be relied upon if current
- d. Differentiate between positive, negative and neutral opinion when using independent assurance
- e. Ensure that assurance is consistent: triangulate different sources and use independent evidence to assess the accuracy of internal assurance sources

Appendix A provides examples of questions that Committees and groups should ask about risks.

Chair's report /Assurance Report

Minutes are valuable for the group itself but are not normally an efficient and effective source of assurance. An assurance report allows issues to be collated and presented in a way that gives readers a quick and comprehensive summary of the key issues, without considering unnecessary detail or having to decode or investigate areas of interest. The following questions should be considered at the end of every Standing Committee and sub-group meeting and areas for recording agreed. These should then be included in the Chair's summary/assurance report and taken forward by the Responsible Director:

- a. Are there any issues which could be a disclosure in the Governance Statement (see below) or should be included within the Committee year-end report
- b. Are there any new risks emerging which require escalation to the Board or recording in the Strategic or operational risk registers
- c. Is the Committee fulfilling its workplan and if not, would any omissions have an impact on its ability to provide assurance at year-end
- d. For the risks delegated to the Committee:
 - Are the scores correct?
 - Have there been any significant movements?
 - Has the committee received assurances that internal controls intended to mitigate the risk are working as intended and are effective?
 - Does performance reporting support this?
 - Has the committee received assurances that actions intended to reduce the risk to its target level are working as intended and will be effective?

Year-end reports

At the end of the financial year, Standing Committees provide their annual report to the A&RC (and Board). Standing Committee annual reports are an opportunity to reflect on the year just gone and should be used to consider overall progress and key issues going forward. The annual report should be focused on the most important issues and should include, as a minimum:

- a. A clear description of movement in strategic risks aligned to the committee and areas where actions were not effective
- b. Overt identification of areas of non-compliance and explanation of the impact on the control environment
- c. Clear performance information and highlighting of areas of poor performance
- d. Inclusion of Key Performance Indicators where possible
- e. Rather than stating that a report was presented, providing a broad conclusion on whether the level of assurance provided was acceptable (noting that the new process for assessing assurance will aid this recommendation)
- f. Any specific requirements for that Committee based on its remit or duties such as an overt opinion by the SGC on whistle-blowing arrangements based on an appropriate annual report or the P&RC opinion on whether value for money was achieved
- g. Consideration of key risks and concerns and how these will be reflected in the workplan for the year ahead.

The Audit Committee must decide whether an item is of sufficient significance to be included in the narrative of, or disclosed within, the Governance statement. By extension Standing Committees should consider, whether an item should be brought to the attention of the Audit Committee within their annual report/assurance statement. Useful considerations in deciding whether an item should be disclosed include:

- a. Is it material? The HIS risk management 'impact' criteria provide a helpful guide
- b. Does it represent a control weakness? Some issues could not reasonably have been prevented
- c. Was the control weakness in place in the year in question? A weakness in place throughout most of the year should be mentioned, even if resolved after or at year-end. However, if the issue was discovered in year but related to a weakness in previous years now rectified then it need not be disclosed

Appendix A - Assessing risks

Questions for Risk Owners:

- Would you know if your controls are working effectively as intended or failing?
- Can you evidence the effectiveness of the controls?
- Can you assure your Governance Committee of the effectiveness of controls?
- Do you have assurance for all three lines of defence?
 - 1st line - management / performance / data trends
 - 2nd line – oversight / compliance / audits
 - 3rd line – internal audit and/or external audit reports / external assessments
- If Yes - why above appetite?
- If No – How are the mitigating controls reflecting improvement or is there an action plan?
- Do you understand both the criticality and effectiveness of controls
 - Criticality: How important to the mitigation of the risk? The higher the importance of the control in mitigating the risk, the more assurance is required. If the control is of low importance is it a valid control to attach resource / effort
 - Effectiveness: This should measure if the controls are well designed / appropriate as well as how effectively they are implemented

Risk Questions for Committees

General questions:

- Do the current controls match the stated risk?
- How weak or strong are the controls? Are they both adequate i.e. well-designed and effective i.e. implemented properly
- Will further actions bring risk down to the planned level?
- Does the assurance you receive tell you how controls are performing?
- Are we investing in areas of high risk instead of those that are already well-controlled?
- Do Committee papers identify risk clearly and overtly link to the BAF/risk?

Specific questions when analysing a risk delegated to the committee in detail:

- History of the risk (when was risk opened)- has it moved towards target at any point?
- Is there a valid reason given for the current score
- Is the target score:
 - In line with appetite
 - Realistic/achievable or does the risk require to be tolerated at a higher level?
 - Sensible/worthwhile
- Is there an appropriate split between:
 - Controls – processes already in place which take the score down from its initial/inherent position to where it is now
 - Actions – planned initiatives which should take it from its current to target
 - Assurances which monitor the application of controls/actions

- Ensuring there is clarity over what the listed controls etc. actually do e.g. if there is a group, what is it for (noting a group might be all three or actually none)?
- Assessing controls
 - Are they 'Key' i.e. are they what actually reduces the risk to its current level (not an extensive list of processes which happen but don't actually have any substantive impact)
 - Overall, do the controls look as if they are applying the level of risk mitigation stated
 - Is their adequacy assessed by the risk owner– if so , is it reasonable based on the evidence provided
- Assessing Actions – as controls but accepting that there is necessarily more uncertainty :
 - are they are on track to be delivered
 - are the actions achievable or does the necessary investment outweigh the benefit of reducing the risk?
 - are they likely to be sufficient to bring the risk down to the target score
- Assess Assurances:
 - Do they actually relate to the listed controls and actions (surprisingly often they don't)?
 - Do they provide relevant, reliable and sufficient evidence either individually or in composite?
 - Do the assurance sources listed actually provide a conclusion on whether:
 - the control is working
 - action is being implemented
 - the risk is being mitigated effectively overall (e.g. performance reports look at the overall objective which is separate from assurances over individual controls) and is on course to achieve the target level
 - What level of assurance is given or can be concluded and how does this compare to the required level of assurance (commensurate with the nature or scale of the risk):
 - 1st line - management / performance / data trends
 - 2nd line – oversight / compliance / audits
 - 3rd line – internal audit and/or external audit reports / external assessments