Archwilio Cymru
Audit Wales

Terms of reference: Audit & Risk Assurance Committee

Date issued: June 2022

Adopted by the Committee on 7 June 2022

Approved by the Board on 9 June 2022

Audit Wales is the umbrella identity of the Auditor General for Wales and the Wales Audit Office, which are each separate legal entities with their own legal functions. The Auditor General has functions of auditing and reporting on Welsh public bodies. The Wales Audit Office has functions of providing resources, such as staff, for the exercise of the Auditor General's functions, and of monitoring and advising the Auditor General. Audit Wales is not a legal entity and itself does not have any functions.

The Audit & Risk Assurance Committee is a committee of the Wales Audit Office.

Contents

Terms of Reference

Terms of Reference

Audit and Risk Assurance Committee

Status

1 Under section 29 of the Public Audit (Wales) Act 2013, the procedural rules of the Wales Audit Office (WAO) may provide for the establishment of committees to which the WAO may delegate any of its functions.

2 At its first meeting on 23 October 2013, the WAO Board established an Audit and Risk Management Committee to support the Board and the Accounting Officer by reviewing the comprehensiveness and reliability of assurances on governance, risk management, the control environment and the integrity of financial statements and the annual report. At its meeting on 23 May 2014, the Board resolved to change the name to the Audit and Risk Assurance Committee.

Aim

3 The Committee's aim is to advise the Board on whether the WAO's audit and risk assurance arrangements:

a) support its strategic aims;

b) enable the efficient, effective and economic conduct of business; and

c) comply with regulatory requirements.

4 The Committee meets this aim by:

a) reviewing the comprehensiveness and reliability of assurances in meeting the Board's needs and those of the Accounting Officer;

b) reviewing the integrity of the financial statements and the annual report, including the annual governance statement;

c) providing an opinion on how well the Board and the Accounting Officer are supported in decision-making and in discharging their stewardship and accountability obligations.

Responsibilities

5 The Committee advises the Board and the Accounting Officer on the comprehensiveness and reliability of the WAO's assurance arrangements including:

a) the risk assessment and risk management arrangements, in particular reviewing and advising on –

(i) the risk strategy, including the appropriateness of the WAO's approach to setting its appetite for risk

(ii) the WAO's overall risk assessment processes that inform executive decision-making

(iii) the WAO's capability to identify and manage risk

(iv) the remit of the risk management function, including its access to resources and information to perform its role effectively and in accordance with the relevant professional standards, free from management or other restrictions

(v) management's responsiveness to risk assessment;

b) management of cyber risk, including appropriate risk mitigation strategies (appendix 2);

c) the integrity of the financial statements including –

(i) the consistency of, and any changes to, accounting policies

(ii) the methods used to account for significant or unusual transactions where different approaches are possible

(iii) whether the WAO has followed appropriate accounting standards and made appropriate estimates and judgements taking into account the views of the external auditor

(iv) the clarity of disclosures in the annual report and accounts and the context in which those disclosures are made

(v) all material information presented with the financial statements

(vi) observations and assurances received thereon from the activity and results of internal and external audit;

d) the internal control environment, including the effectiveness of the WAO's internal financial controls and risk management systems and the statements to be included in the annual report and accounts

e) governance arrangements, in particular –

(i) the adequacy and security of the WAO's arrangements for its employees and contractors to raise concerns, in confidence, about possible wrongdoing in financial reporting or other matters, including whether they allow proportionate and independent investigation of such matters and appropriate follow-up action

(ii) the WAO's procedures for the prevention and detection of fraud;

(iii) the WAO's systems and controls for the prevention of bribery and receiving reports on non-compliance

(iv) regular reports from the Money Laundering Reporting Officer and the adequacy and effectiveness of the WAO's anti-money laundering systems and controls.

f) the internal audit arrangements, in particular –

(i) the effectiveness of the WAO's internal audit function in the context of the overall risk management system

(ii) the appointment and removal of the head of the internal audit function

(iii) the remit of the internal audit function including its access to resources and information to perform its role effectively and in accordance with the relevant professional standards, free from management or other restrictions

(iv) the annual internal audit plan

(v) reports addressed to the Committee from the internal auditor

(vi) management's responsiveness to the findings and recommendations of the internal auditor;

g) the external audit arrangements, in particular –

(i) the process of appointment of external auditors, in order for the Board to make a recommendation for such appointment to the National Assembly for Wales' Finance Committee

(ii) the relationship with the external auditor

(iii) commenting on the terms of engagement and the scope of the audit

(iv) the annual audit plan, ensuring that it is consistent with the scope of the audit engagement

(v) reviewing the findings of the audit, including any major issues that arose, any accounting and audit judgements, levels of errors identified during the audit and the effectiveness of the audit

(vi) reviewing management's letters of representation to the external auditor

(vii) reviewing the management letter and management's response to the auditor's findings and recommendations

(viii) reviewing the policy on the supply of non-audit services by the external auditor, taking into account any relevant ethical guidance.

6 The Committee advises the Board and the Accounting Officer on request, or as it feels is appropriate.

Rights

7 The Board authorises the Committee:

a) to investigate any activity within its terms of reference and to comment and advise on governance arrangements within the WAO;

b) to obtain from WAO staff any documents or other information that it requires to carry out its duties;

c) to obtain, with the Board's agreement, external, expert advice as it deems necessary to discharge its responsibilities including obtaining reliable, up-to-date information about audit and risk management arrangements in other organisations.

Membership

8 The Committee comprises:

Ian Rees	-	Non-executive Board member
Anne Beegan	-	Elected Employee Board member
Andrew Clark	-	Independent external member
David Francis	-	Non-executive Board member and Senior Independent Director

9 The Board has appointed Ian Rees to Chair the Committee.

10 Appointments to the Committee are set by the Board and are for periods of up to four years which may be extended for a further period of up to four years. In appointing the Chair and members the Board will ensure that the Committee as a whole has the range of skills needed to allow it to carry out its overall function.

Secretariat

11 The Board Secretary acts as the secretary to the Committee and is responsible for:

a) ensuring that the Committee is properly constituted and advised and that there is clear co-ordination between it, the Board and the Board's other committees;
b) liaising with the Chair on the programme of work;
c) ensuring that the Committee receives information and papers in a timely manner to enable full and proper consideration of the issues;
d) preparing the draft minutes of meetings for approval by the Chair before they are distributed to members;
e) maintaining appropriate records of Committee business;
f) drafting material for the Committee's annual report; and
g) providing any other necessary practical support.

Meetings

12 The Committee meets at least four times a year. The Chair of the Committee may convene additional meetings as deemed necessary. Committee members, the Chair of the Board, the Accounting Officer, the Head of Internal Audit or the external auditors may ask the Chair to convene additional meetings if they consider it necessary. The Chair will not decline any reasonable requests.

13 Committee meetings are summoned by its secretary at the Chair's request. Unless otherwise agreed, the secretary will send to members a notice of each meeting confirming the venue, date and time together with an agenda of items to be discussed no later than five working days before the date of the meeting. Supporting papers will be sent at the same time.

14 The quorum necessary for the transaction of business shall be two (the Chair plus one). A duly convened meeting of the Committee at which a quorum is present

shall be competent to exercise all or any of the authorities, powers and discretion vested in or exercisable by the Committee. In the absence of the Committee Chair (and provided all other members are present), the remaining members may elect one of themselves to chair the meeting.

15 Members who are unable to attend may raise any points with the Chair in advance of the meeting to which they relate.

16 Committee meetings are attended by the Auditor General as the Accounting Officer, the Executive Director of Corporate Services, the Executive Director of Communications and Change, the Head of Internal Audit, and a representative of external audit. The Committee may ask any other WAO staff to attend to assist it with its discussions on any particular matter.

17 The Committee may ask any or all of those who normally attend but who are not members to withdraw from all, or any part of, a meeting to facilitate open and frank discussion of particular matters; such discussions will be minuted.

18 Each Committee meeting will provide for private discussions with the Head of Internal Audit and the representative of external audit.

19 The Board and the Accounting Officer may ask members of the Committee to provide further advice outside the meeting cycles on particular issues from time to time.

20 The Committee Chair will communicate with the Chair of the Remuneration & HR Committee to join up their activities and actions as appropriate.

21 A Committee member or attendee who becomes aware of a potential or actual conflict of interest relating to matters being discussed by the Committee should give prior notification to the Chair or, if this is not possible, declare it at the meeting and, where necessary, withdraw during discussion of the relevant agenda item.

22 By exception, the Committee may receive items of business outside the normal cycle of meetings, for example in the event of an unexpected issue demanding an immediate or urgent response. The arrangements for convening a quorum, distributing papers and recording the Committee's deliberations set out in these terms of reference will apply.

Access

23 The Chair of the Committee may request private discussions with the Chair of the Board, the Accounting Officer, the Head of Internal Audit, WAO staff and the representative of external audit as appropriate.

24 The Chair of the Committee also has direct access, and may report matters of concern, to the Chair of the Senedd Finance Committee. Before exercising this right, the Chair may liaise as appropriate with the Chairs of the Board and of the Remuneration & HR Committee to discuss the concerns and the course of action.

25 The Head of Internal Audit and the representative of external audit will have free and confidential access to the Chair of the Audit and Risk Assurance Committee.

Reporting

26 The Committee will formally report in writing to the Board and the Accounting Officer after each meeting.

27 The Committee will formally report annually in writing to the Board and the Accounting Officer summarising its conclusions from the work it has undertaken during the year. The timing of the report will support finalising the annual report and accounts.

Programme of business

28 Appendix 1 summarises the programme of Committee business which is subject to confirmation at each meeting.

Performance review, training and development

29 The Chair will review members' performance annually in accordance with the performance management framework established for that purpose. The Chair of the Board will review the Chair's performance annually.

30 The Committee will consider the need for induction, training and development on an ongoing basis.

31 The Committee will advise the Board of any apparent deficiencies that it may from time to time identify in the collective skill sets of its membership.

Review of the terms of reference

32 The Committee will review these terms of reference and assess its effectiveness annually, reporting the outcome in its annual report to the Board.

Appendix 1

Programme of business

1 The Committee's programme of business assumes an annual cycle of four meetings. The programme set out below is a guide and does not preclude adjustments in timing during the year nor the consideration of additional business that might arise.

2 Standing items on all Committee agendas are:

a) the minutes of the Committee's previous meeting for approval;

b) the log of actions arising from previous meetings of the Committee updated as appropriate (to be taken as matters arising);

c) the Committee's work programme for ongoing review;

d) a report from the Head of Internal Audit summarising –

- work performed (and a comparison with work planned)
- any changes to the internal audit strategy and annual plan
- key issues emerging from internal audit work
- any resourcing issues affecting the delivery of internal audit objectives;

e) internal audit reports in accordance with the timetable established by the internal audit plan for the year (including any additions in-year). Reports include management's responses to the recommendations;

f) a progress report (where appropriate) from the external audit representative, summarising work done and emerging findings;

g) a strategic risk review through which the Committee examines in detail one strategic risk to determine whether the risk management arrangements are operating effectively in practice;

h) an assessment of the performance of the internal and external auditors.

3 The outline cycle of business includes:

Meeting 1 (February)

- the timetable for the production of the draft annual report and accounts;
- the external audit plan for the annual report and accounts;
- accounting policies (including any significant changes) and judgements;
- the internal audit strategy and the plan for the forthcoming financial year;
- the counter-fraud arrangements;
- the operational risk register;
- the register of single tender action and management consultancy expenditure;
- an outline of the Committee's annual report to the Board, including the arrangements for evaluating the Committee's performance.

Meeting 2 (June)

- the internal audit annual report for the previous financial year, including the Head of Internal Audit's opinion;

- the tracking and follow-up of internal audit recommendations;
- the annual declaration of independence report;
- the annual review of whistleblowing arrangements;
- the annual review of information governance (SIRO report);
- the Committee's annual report to the Board, including the Committee's:
    - terms of reference for review, and
    - self-assessment of its performance.
- final draft annual report and accounts for the previous financial year;
- the external auditor's report to those charged with governance (ISA260); and
- the external auditor's letter of representation.

Meeting 3 (September)

- the operational risk register;
- the outcome of the post-project learning exercise on the annual report and accounts;
- report of the money laundering reporting officer;
- a report on any proposals to tender for internal and external audit functions; and
- the outline timetable for the production of the annual report and accounts.

Meeting 4 (December)

- the risk strategy and risk management arrangements; and
- the tracking and follow-up of internal audit recommendations.

Appendix 2

Cyber security: role of the Audit & Risk Assurance Committee

Extract from H.M Treasury's Audit & Risk Assurance Committee Handbook

1 Audit and risk assurance committees' (ARAC) role is to provide assurance to the Board that the organisation is properly managing its cyber risk including appropriate risk mitigation strategies. This does not necessitate understanding the full detail of the technology involved; ARAC can confirm that the appropriate framework is in place and that continuous monitoring and improvement initiatives are adopted and sustained. It is important to understand the organisation's tolerance for risk and evaluate the risk decisions made by management. Exploring opportunities to share information and to use technology should be guided by the organisation's risk appetite.

2 In particular, to assess the organisation's cyber resilience the ARAC should evaluate whether the organisation has:

Governance

- controls in place to prepare for, protect from, detect and respond to cyber-attacks including management of the consequences of a cyber-security incident.
- a means of monitoring the effectiveness of their cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls.
- identified the critical information assets which it wishes to protect against cyberattack and who is responsible for them – whether financial data, operational data, employee data, customer data or intellectual property.
- a way of identifying and agreeing the level of risk of cyber-attack that the organisation is prepared to tolerate for a given information asset; what level of cyber security risk is considered acceptable?
- an operational risk framework and internal audit plan providing cover across different areas of cyber security, not just focused on IT operations.

Threat Intelligence; Third Party and Supply Chain

- an understanding of what data is leaving the organisation and its destination, and what associated monitoring activities are in place.
- intelligence processes in place to understand the threat to the organisation's assets including a detailed understanding of which suppliers/partners connect to the organisation and how.
- experienced an increase in the number of information security breaches.

Structure and Resources

- the right skills and experience in-house to cover all relevant areas.
- the right management structure in place, including the Senior Information Risk Owner (SIRO).

Incident Response

- an up-to-date response plan for cyber incidents which has been practiced including actions on lessons learnt.

People, Training and Awareness

- training and development programmes to educate the workforce about cyber risks and individual responsibilities.
- a programme of continuous improvement, or where needed, transformation, to match the changing cyber threat with appropriate performance indicators.

3 The ARAC will use the organisation's SIRO to provide assurance over these and other issues by reviewing an annual report from the SIRO, including progress on the maturity of the organisation in information risk and cyber security, supported by periodic updates where appropriate.

4 The review of the annual report from the SIRO will form part of the financial year end assurance process and the Committee will discuss with the SIRO any issues that the ARAC should include in its recommendation for the Governance Statement.

5 A further option for the ARAC is to consider whether one of its members could become a champion on cyber security at the ARAC (and the Board if a member) and support the SIRO.

Audit Wales
24 Cathedral Road
Cardiff CF11 9LJ

Tel: 029 2032 0500
Fax: 029 2032 0600
Textphone: 029 2032 0660

E-mail: info@audit.wales
Website: www.audit.wales
We welcome correspondence and telephone calls in Welsh and English.
Rydym yn croesawu gohebiaeth a galwadau ffôn yn Gymraeg a Saesneg.