

**Scottish Rail Holdings Limited**  
**Board Audit & Risk Committee**  
**Terms of Reference**

The Board and Accountable Officer has established an Audit and Assurance Committee as a Committee of the Board to support in their responsibilities for issues of risk, control and governance and associated assurance through a process of constructive challenge.

**Membership**

The usual members of the committee comprise:

- SRH non-executive directors or independent representatives as voting members:
  1. SRH NED B as committee chair;
  2. TS/SG finance executive from outside TS Rail;
  3. A second SRH NED or another TS/SG finance executive from outside TS;
  4. Any other independent external members as selected and appointed by the Board from time to time.
- Non-voting usual attendees: :
  - SRH Finance Director
  - SRH General Counsel
  - SRH Accountable Officer
  - SRH External Auditor
  - SRH Internal Auditor

The committee will be Chaired by SRH NED B.

The committee will be provided with a secretariat function by SRH Company Secretary.

**Reporting**

- The committee will formally report in writing to the Board and Accountable Officer after each meeting. A copy of minutes of the meeting may form the basis of the report.
- The committee will provide the Board and Accountable Officer with an Annual Report, timed to support finalisation of the accounts and the governance statement, summarising its conclusions from the work it has done during the year.

**Responsibilities**

The committee will advise the Board and Accountable Officer on:

- the strategic processes for risk, control, and governance, including the annual governance statement;
- the accounting policies, the annual report and accounts of the organisation, including the process for review of the accounts prior to submission for audit, levels of error identified, and management's letter of representation to the external auditors;
- the planned activity and results of both internal and external audit;

- the adequacy of management response to issues identified by audit activity, including external audit's management letter and report;
- the effectiveness of the internal control environment;
- Review compliance with other statutory and regulatory requirements, and reporting thereof, together with the results of management investigation and follow up of any instances of non-compliance, including but not limited to those covering employment, gifts and hospitality, modern slavery, bribery, equality, data protection, retention of information and open government, procurement and taxes;
- Review the adequacy and security of group arrangements for employees and contractors to raise concerns, in confidence, about possible wrongdoing in respect of reporting or other matters (whistle-blowing processes). Ensure these arrangements allow the proportionate and independent investigation of such matters and appropriate follow up action;
- Review processes for public governance disclosures including those on Executive Pay, Gender Pay gap, Senior Accounting Officer and IR35;
- proposals for tendering for either internal or external audit services or for purchase of non-audit services from contractors who provide audit services;
- Reporting on fraud and attempted fraud, anti-fraud policies and arrangements for special investigations; and
- Monitor and ensure adherence to SPFM
- Monitoring group consistency and coverage of all regulatory requirements, e.g. to cover SAO processes and Modern Slavery.

The Audit and Assurance Committee will also periodically review its own effectiveness and report the results of that review to the Board and Accountable Officer.

## **Rights**

The committee may:

- co-opt additional members for a period not exceeding a year to provide specialist skills, knowledge, and experience; and
- procure specialist ad-hoc advice at the expense of the organisation, subject to budgets agreed by the Board or Accountable Officer.

## **Access**

The Company Secretary and the representatives of Internal and External Audit will have free and confidential access to the Chair of the Committee.

## **Meetings**

The procedures for meetings are:

- the committee will meet at least four times a year. The Chair of the Committee may convene additional meetings, as he/she deems necessary;
- a minimum of two members of the committee will be present for the meeting to be deemed quorate;

- committee meetings will normally be attended by the Accountable Officer, the Finance Director, the Company Secretary, and a representative of Internal and External Audit;
- the committee may require any other officials of the company or its group to attend to assist it with its discussions on any particular matter;
- the committee may require any or all of those who may attend but who are not voting members, or are otherwise potentially conflicted on any matter under discussion, to withdraw to facilitate open and frank discussion of particular matters.

The Board or Accountable Officer may ask the committee to convene further meetings to discuss issues on which they want the committee's advice.

### **Information requirements**

The committee, for the company and group, will be provided with:

- a timetable of issues to be covered at each meeting
- a report summarising any significant changes to the organisation's Risk Register;
- a report, from the head of internal audit or risk management as appropriate, summarising:
  - work performed (and a comparison with work planned);
  - key issues emerging from Internal Audit work;
  - management response to audit recommendations;
  - significant changes to the audit plan;
  - any resourcing issues affecting the delivery of Internal Audit objectives;
- a progress report from the External Audit representative summarising work done and emerging findings.

As and when appropriate, the committee will also be provided with:

- business update reports from the Accountable Officer;
- the Charter / Terms of Reference of any Internal Audit function;
- the Internal Audit Strategy;
- the annual Internal Audit Plan;
- the Head of Internal Audit's Annual Opinion and Report;
- quality assurance reports on the Internal Audit function;
- the draft accounts of the organisation;
- the draft governance statement;
- a report on any changes to accounting policies;
- External Audit's management letter & report;
- a report on any proposals to tender for audit functions;
- a report on co-operation between Internal and External Audit;

- a report on the measures to counter fraud and anti-bribery arrangements and the performance of those arrangements;
- reports from other sources within the "three lines of assurance" integrated assurance framework (e.g., Best Value self-assessment Reviews, Gateway Reviews, Health Check Reviews, ICT Assurance Reviews, Digital 1st Service Standard Reviews, Procurement Capability Reviews, Procurement Key Stage Reviews).

**Specific Paragraphs from the Framework Agreement that the Committee should be aware of and consider the company's fulfilment of:**

18 (k) reviewing SRH risks (including their management risks, reporting risks, reputational risks, and project and legal risks), as discussed at the audit and risk committee meetings of SRH and its subsidiaries, and informing the Sponsor Representative of any risks that might impact on the Sponsor or the Scottish Ministers.

59. SRH shall ensure that the risks that it faces are dealt with in an appropriate manner, in accordance with relevant aspects of best practice in corporate governance and develop an approach to risk management consistent with the 'Risk Management' section of the SPFM. Reporting arrangements should ensure that the TS Sponsor Team is made aware of relevant risks and how they are being managed by SRH.

60. SRH is required, at the earliest opportunity, to notify the TS Sponsor Team if it considers that it has identified a significant problem which may have wider implications, including without limitation, any problem which may give rise to significant financial, legal, political and/or presentational issues.

61. SRH shall adopt and implement policies and practices to safeguard itself against fraud and theft, in line with the 'Fraud section of the SPFM. Application of these processes must be monitored actively, supported by a fraud action plan and robust reporting arrangements. This includes the establishment of avenues to report any suspicions of fraud.

62. Each member of the SRH Group shall take all reasonable steps to appraise the financial standing of any firm or other body with which it intends to enter a contract.

Appendix 3 paragraph 1 (e)

Having robust performance and risk management arrangements (consistent with the Risk Management section of the SPFM) in place that support the achievement of SRH's aims and objectives that facilitate comprehensive reporting to the SRH Board, the Scottish Government and the wider public. Risk management arrangements should include full consideration of organisational resilience to physical, personnel and cyber risks/threats/hazards.