Scottish Government
Riaghaltas na h-Alba
gov.scot

Provision of Internal Audit Services

Memorandum of Understanding

The Scottish Government Directorate for Internal Audit and Assurance and Scottish Fiscal Commission

2020-2023

Directorate for Internal Audit and Assurance

Issue Date: 22/12/2020

Contents

1 Overview of the Agreement

Purpose of this agreement

1.1 This agreement sets out the basis on which Scottish Government Directorate for Internal Audit and Assurance (DIAA) will partner with Scottish Fiscal Commission – hereinafter referred to as the "client" (together, the "Parties") in relation to internal audit services (the "Service").

Context

1.2 The Scottish Fiscal Commission (the Commission) prepares economic and fiscal forecasts and assessments to inform the Scottish Budget. The Commission's statutory functions are set out sections 2 – 5 of the Scottish Fiscal Commission Act 2016 ("the SFCA").

1.3 The SFCA establishes the Commission and creates it as a body corporate and part of the Scottish Administration, but not the Scottish Government. In terms of its classification as a Scottish public body, it is an office-holder in the Scottish Administration (non-Ministerial Office), thus ensuring its operational independence. The Commission is directly accountable to the Scottish Parliament for the delivery of its functions. The SFCA enshrines the independence of the Commission, in accordance with the Organisation for Economic Co-operation and Development (OECD) principles for independent fiscal institutions and in line with best international practice.

1.4 The Commission's Accountable Officer is John Ireland, Chief Executive. Commissioners are appointed by the Scottish Ministers with the approval of the Scottish Parliament; one member is appointed as Chair. The Commissioners act corporately as a Governance Board, collectively responsible for the leadership and direction of the Scottish Fiscal Commission, and for ensuring that it carries out its statutory functions effectively and efficiently and that it achieves its published aims and objectives as recorded in the Corporate Plan. Governance Board meetings are distinct from the technical, forecasting, scrutiny or modelling meetings of

Commissioners. The Governance Board has established an Audit and Risk Committee to assure itself of the effectiveness of the internal control and risk management systems of the Commission.

Summary scope of shared services

1.5 Internal Audit Division (DIAA) and the Client wish to collaborate regarding the provision of internal audit shared services, including (subject to resource availability) any additional special projects, investigations and advisory services as agreed. The primary objectives of the Service will be to:

- provide an independent and objective assurance to the Accountable Officer on risk management, control and governance;
- measure and evaluate the effectiveness of risk management, control and governance arrangements;
- assure that the Client's objectives are achieved in the most efficient, effective and economical manner; and
- provide an independent and objective advisory service to the Client's senior management and Audit and Risk Committee

Applicable standards

1.6 The Service defined in this document will be conducted in full accordance with the UK Public Sector Internal Audit Standards (PSIAS) and DIAA will monitor and report on the service provided in accordance with DIAA's Charter and Strategy as approved by the Scottish Government Audit and Assurance Committee (SGAAC).

Commencement date and duration

1.7 The commencement date for the Service is 1st April 2020 and will run until 31st March 2023.

Charging for Internal Audit Services

1.8 DIAA and AO will annually agree a charging mechanism and indicative fee for the services to be provided that reflects the principle of full cost recovery and is consistent with the Scottish Public Finance Manual (SPFM). This will be specified when the Annual Audit Plan is agreed.

Revision or Termination

1.9 Any revisions to the MoU will be introduced after consultation and agreement between the AO and DIAA. Either party will give at least three months' notice of intention to end this arrangement. The MoU will be subject to a full review in 2023.

Confidentiality and ownership of documents and records

1.10 The classification of all papers, information and material coming to the attention of and produced by the Parties in relation to the Service shall be mutually respected. Such documents may not normally be disclosed to any person outside of the Client's organisation or DIAA without the permission of the relevant party, unless expressly required by statute or judicial decree.

1.11 All reports, documents and other data held (including electronic) or generated by DIAA as a result of audit activity in relation to the shared services shall be the property of the Client but will also be held securely within DIAA's file management system (Galileo) and on the Scottish Government's corporate record management system (eRDM). Please see Annex C for further information.

1.12 Personal data received and required as part of an audit will be stored, transferred and destroyed securely in line with current applicable standards on information security (e.g. The Data Protection Act 1998, GDPR and SG Security Policy Framework) and in line with DIAA's Information Handling Policy – see Annex C for full details.

2 Client's Responsibilities

2.1 The Accountable Officer and the Board of the Client are responsible for ensuring there are effective arrangements for governance, risk management (including advice about and scrutiny of key risks) and internal control, the assessment thereof. The Board has therefore established an Audit and Risk Committee, whose terms of reference are available at: Audit and Risk Committee Terms of Reference | Scottish Fiscal Commission. The Accountable Officer is responsible for the Governance Statement (prepared in accordance with the requirement of the Scottish Public Finance Manual) published in the annual report and accounts.

2.2 In accordance with the agreed scope of services (see 1.3 above and **Annex A**) the Client will:

- Appoint an overall sponsor for Internal Audit service (the "Internal Audit Sponsor"). This individual will be responsible for providing input to the development of the Internal Audit Plan, including provision of appropriate information to enable DIAA to ensure proper coverage, that its resources are used efficiently and to minimise duplication of effort. The Internal Audit Sponsor, unless stated otherwise, will also be the Engagement Sponsor.

- Ensure that the Internal Audit Plan developed by DIAA is reviewed and approved by the Accountable Officer and endorsed by the ARC.

- Ensure the Head of Internal Audit has access to the Accountable Officer, the Chair and members of the ARC on a regular basis.

- Provide access to all necessary information including records, documents and correspondence relating to the agreed audit activity, including information requiring security clearance to review, for which the Client has a duty to safeguard and handle appropriately under the prevailing central government Security Policy Framework (see 1.6-1.8 above)

- Allow access at all reasonable times to any land, premises or member of staff of the Client's staff.

- Meet appointments, information requests and agreed deadlines for responses and recommendations, providing explanations concerning any matter relevant to the agreed audit activity (see Annex A for the agreed details).

- Regularly update DIAA on issues which may impact on the delivery of the internal audit plan and changes thereto, and on any unplanned work; and any specific governance, risk management, control and fraud related issues.

- Respond to DIAA requests for feedback through the customer satisfaction surveys.

2.3 The Client will deliver the above and day-to-day response levels timeously.

2.4 Responsibility for implementing recommendations identified by DIAA and agreed by the Client as a result of the agreed scope of work rests with the management team of the Client.

2.5 The Client's Audit Committee will also have a role in advising the Accountable Officer on the scope of the services provided by DIAA and on the DIAA's performance, as it relates to the agreed work programme.

3 DIAA Responsibilities

3.1 DIAA will assign a Senior Internal Audit Manager who will act as Head of Internal Audit (HIA) for the Client. Subsequently the HIA will appoint an IA Manager who, under the direction of the HIA, will lead relevant Service.

3.2 In accordance with the agreed scope of work (see 1.3 above and **Annex A**), DIAA will:

- Develop an annual internal audit plan using an appropriate risk-based approach, which meets the Client's needs and takes account of other sources of assurance.
- Undertake work out with the agreed annual audit plan subject to resource availability and subject to discussions and agreement between the Head of Internal Audit, the Accountable Officer and Chair of the Client's Audit & Risk Committee.
- Meet with the External Auditors to co-ordinate the respective scope of work and provide access to internal audit documentation as required**.**
- Deploy internal auditor staff with sufficient knowledge, skills and experience to deliver the agreed scope of work.
- Deliver a DIAA service in line with PSIAS and within scope of work outlined at Annex A.
- Provide, when appropriate, reports and contributions to the Client's Audit & Risk Committee on the progress against and results of the agreed scope of work.
- Provide an Annual Assurance report to the Client's Audit and Risk Committee which will include:
    - A review of the work undertaken in the year and developments in governance, risk management and control during the period;

- An opinion on the adequacy and effectiveness of the Client's framework of governance, risk management and control; and
- A report on DIAA's performance in providing the agreed service to the Client.

3.3 The HIA has right of direct access to the Client's Accountable Officer and is able to raise any matter with the Accountable Officer and Chair of the ARC. Any serious matters identified should be raised in a timely manner with the Internal Audit Sponsor, and where necessary the Client's Accountable Officer and Audit Committee.

3.4 DIAA will deliver the above and day-to-day response levels in accordance with agreed timescales.

3.5 The HIA will ensure delivery of the responsibilities outlined above and the quality thereof. The HIA will provide a report to the AO and the Audit Committee that these responsibilities have been discharged in accordance with the MoU and PSIAS.

4. Management of Shared Services

4.1 As a minimum, a review meeting will be held annually to discuss and review formally the Service, in particular in relation to the Parties' responsibilities at clauses 2 and 3 and Annex A and recommend any improvements.

4.2 Where appropriate Internal Audit may convene a shared service working forum to share areas of best practice identified across public bodies.

4.3 If either party is dissatisfied with the shared service arrangements/performance or wishes to discuss how it could be improved and is unable to resolve this, they can raise this with the SG Director of Internal Audit and Assurance, Director General Scottish Exchequer and ultimately the Principal Accountable Officer.

5 Status of the Agreement

5.1 This MOU is not intended to be legally binding and no legal obligations or legal rights shall arise between the Parties from the provisions of the MOU nor is it intended to cover every aspect of the relationship between the Client and DIAA. The Parties enter into the MOU intending to honour all their obligations.

This MoU will be published on the Commission's website.

John Ireland	19 January 2021
Accountable Officer	**Date**
[Redacted]	19 January 2021
Head of Internal Audit	**Date**

SCOPE OF WORK

Phase of internal audit activity	SG DIAA Responsibilities	Client Responsibilities
Planning	• **Annual planning** meetings undertaken to determine and agree risk based activities for inclusion in Annual Internal Audit Plan. • **Engagement Planning:** • Planning meetings with the Engagement Sponsor will be held • Draft Terms of Reference (ToR) to be issued • ToR agreed before commencement of fieldwork	• **Annual planning** discussions and sharing of relevant information requested by DIAA. • AO agree Annual Internal Audit Plan. • **Engagement Planning:** • Engagement sponsor to attend planning meetings on agreed date • Agree the ToR • Distribute ToR and book initial meetings with key stakeholders
Fieldwork	• Complete fieldwork in accordance with the ToR during the agreed fieldwork period • Inform relevant staff of any issues as they arise • Conduct end of audit meeting at end of fieldwork period.	• Where relevant, ensure information requested is available at the start of the audit • All required information requested by DIAA to be provided timeously throughout the audit • Ensure all queries/points of clarification requested by DIAA at close out meeting is provided within the agreed timeframe.
Reporting	• Submit draft report to key contacts within agreed timescale of the close-out meeting • Provide the Client key contacts with reasonable timescale to provide tracked change/comments on draft report • Meet with the Client to discuss draft report and comments after draft report issued	• Agree draft report and provide key contact's agreed actions, owners and timescales within agreed timescales • Respond with comments on draft report • Confirm Acceptance of Final Report

	• Finalise report	
Follow up	• Carry out a review of outstanding high and medium recommendations from the finalised audit report, at the point at which the latest implementation date falls due. • Report on status of findings, concluding if they are implemented, partially implemented or outstanding.	• Responsible for implementing agreed recommendations, monitoring their progress. Accept any residual risks of any recommendations that are reported by DIAA as still outstanding, partially or fully.
ARC	• Annual Internal Audit Plan presented for endorsement. • Provide update on progress against agreed plan at each meeting • Contribute to discussions at ARC meetings • Provide Annual Assurance opinion.	• Set ARC dates and inform DIAA when papers are required to be submitted • Record and monitor relevant action points from ARC meeting that affect DIAA
Advisory Services and Special Projects	• Undertake agreed advisory services and special projects within set timescale, agreed scope and to professional standards.	• Provide information to DIAA on timeous basis

KEY CONTACTS

CLIENT

Name	Relevance to service	Contact details
John Ireland	Chief Executive	John.Ireland@fiscalcommission.scot Scottish Fiscal Commission Governors House Regent Road Edinburgh EH1 3BX Tel: 0131 244 0931
Susie Warden	Head of Strategy, Governance & Corporate Services	Susie.Warden@fiscalcommission.scot Scottish Fiscal Commission Governors House Regent Road Edinburgh EH1 3BX Tel: 0131 244 0608
David Ulph	Chair of Audit and Risk Committee	David.ulph@fiscalcommission.scot

INTERNAL AUDIT DIVISION

Name	Relevance to service	Contact details
Sharon Fairweather	Director of Internal Audit and Assurance	Directorofinternalauditandassurance@gov.scot Scottish Government, Directorate for Internal Audit and Assurance, Victoria Quay, 3D-North, Edinburgh. EH6 6QQ
[Redacted]	Senior Internal Audit Manager (Head of Internal Audit)	[Redacted] Scottish Government 3D North Victoria Quay Leith Edinburgh EH6 6QQ Tel: [Redacted] M: [Redacted]

DATA PROTECTION

1. Definitions

1.1 Data Protection Legislation (i) unless and until it is no longer directly applicable in the UK, the GDPR and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; and (iii) any applicable laws relating to processing of personal data and privacy.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018 : Data Protection Act 2018

GDPR : the General Data Protection Regulation (Regulation (EU) 2016/679)

1.2 "Controller" , "Processor" , "Data Subject" , "Personal Data" , "Personal Data Breach" shall have the meanings assigned to them in the GDPR.

2 The Parties acknowledge that for the purposes of the Data Protection Legislation, SFC is the Controller and the DIAA is the Processor. The Controller has defined that the following categories of Personal Data will be collected and processed by DIAA under this MoU:

Types of personal data

- Personal identifiers and contact details
- Address information
- Property information
- Financial information
- Qualifications, licenced or accredited status information
- Systems usage information or history
- Service and product usage and consumption information (including user id, account numbers, activity etc)
- Location data/online identifiers
- Other personal data and opinions

Categories of data subject

- Employees and contractors of the Controller
- Customers
- Users of/subscribers to the Controller's services
- Applicants for registration and their agents
- Third parties
- Members of the public

3 Both Parties agree to negotiate in good faith any such amendments to this MoU that may be required to ensure that both Parties meet all their obligations under Data Protection Legislation. The provisions of this Clause 3 are without prejudice to any obligations and duties imposed directly on the DIAA under Data Protection Legislation and the DIAA hereby agrees to comply with those obligations and duties.

4 The DIAA will, in conjunction with the Controller and in its own right and in respect of the Services, make all necessary preparations to ensure it will be compliant with Data Protection Legislation.

5 The DIAA shall, in relation to any Personal Data processed in connection with its obligations under this MoU:

5.1 process that Personal Data only in accordance with the documented instructions, and Data Protection Legislation and as is necessary for the purpose of fulfilling its obligations under this MoU, unless the DIAA is required to do otherwise by law; in which case the DIAA shall promptly notify the Controller before processing the Personal Data unless prohibited by law;

5.2 ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it, having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from unauthorised or unlawful processing of, or accidental loss, destruction or damage to, Personal Data;

(iii) state of technological development; and

(iv) cost of implementing any measures;

5.3 ensure that it takes all reasonable steps to ensure the reliability and integrity of any DIAA personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the DIAA's duties under this clause;

(ii) are subject to appropriate confidentiality undertakings with the DIAA;

(iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this MoU; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data;

5.4 not transfer Personal Data outside of the European Economic Area

6 Taking into account the nature of the processing the DIAA must provide full assistance to the Controller in relation to the Controller's obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations. Without prejudice to the foregoing generality, the DIAA shall:

6.1 notify the Controller immediately if receives a Data Subject Access Request or any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation and provide such assistance as is reasonably requested by the Controller to enable them to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation

6.2 notify a Personal Data breach to the Controller without undue delay and in any event no later than 24 hours after becoming aware of a Personal Data breach and assist the Controller with communication of a personal data breach to a Data Subject;

6.3 support the Controller with preparation of a data protection impact assessment;

6.4 provide assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

7 The DIAA shall maintain complete and accurate records and information to demonstrate its compliance with this Annex C.

8 At the end of the provision of the Services the DIAA must cease processing the Personal data and on the written instruction of the Controller, delete or return to the Controller all Personal Data and delete existing copies unless the DIAA is required by law to retain the Personal Data.

DIAA – Information Handling Policy

Internal Audit Directorate - Inform

DIAA – Data Protection Impact Assessment (DPIA)

Internal Audit - DPIA.pdf

Options for Secure Transfer of Personal Data

eRDM Connect

eRDM Connect, is a tool which enables you to share information held within eRDM with contacts outside the SG securely.

Documents up to OFFICIAL-SENSITIVE level and up to a maximum 1GB in size can be shared and accessed through the eRDM Connect web browser.

eRDM Connect automatically synchronises content with eRDM - new versions created in eRDM Connect update the master document in eRDM, maintaining a single source of truth for the corporate record. This provides a controlled audit of information.

eRDM Connect is available to eRDM users and should only be used to share documents externally. The tool can be used internally by SG staff and partner agencies but this should only be in special circumstances. Guidance on this can be provided by the eRDM Technical team.

If you have access to documents held in eRDM files you should continue to update these in eRDM rather than externally, via eRDM Connect.

Requesting eRDM Connect

You can request eRDM Connect through iFix or by contacting the eRDM technical team mailbox.