4th Floor
102 West Port
Edinburgh EH3 9DN

T: 0131 625 1500
E: info@audit-scotland.gov.uk
www.audit-scotland.gov.uk

11 June 2024

Jackie McAllister
Chief Financial Officer
St Andrews House
Regent Road
Edinburgh
EH1 3DG

Dear Jackie

Scottish Government – Management letter 2023/24

Introduction

1. This letter outlines our work on the main financial systems of the Scottish Government. Due to the size and nature of the Scottish Government's operations, together with the use of large and complex systems, it is important that robust controls are in place to ensure accurate processing of information.

2. Audit Scotland's Code of Audit Practice requires us to assess the system of internal control put in place by management. We seek to gain assurance that the Scottish Government:

- has systems of recording and processing transactions which provide a sound basis for the preparation of the financial statements,
- has systems of internal controls which provide an adequate means of preventing and detecting error, fraud or corruption, and
- complies with established policies, procedures, laws and regulations.

3. Our work included testing of key controls within financial systems to gain assurance over the processes and systems used in preparing the financial statements. The results of this testing will inform our approach to the audit of the 2023/24 financial statements.

4. We also undertook a review of the Scottish Government's internal audit service and obtained an understanding of internal audit's responsibilities, its organisational status, and activities performed.

5. A high-level review of the IT environment was carried out, this included a review of the arrangements in place for managing and mitigating cyber security threats at the Scottish Government.

6. We are also concluding our review of the 2022/23 Whole of Government accounts (WGA) process and are currently discussing a number of outstanding matters. We anticipate issuing a qualified opinion shortly in respect of both the Scottish Government and Scottish Consolidated Fund accounts.

Internal control environment

7. Audit work undertaken to date includes the testing of key controls within the main financial systems (Scottish Executive Accounting System (SEAS – general ledger); Payables; Receivables; Payroll and Banking) to gain assurance over the processes and systems used in preparing the financial statements.

8. These main financial systems are used by a number of other public bodies. We will provide details of the audit work carried out on the Scottish Government's main financial systems to the auditors of these bodies. This is provided to support auditors' understanding of the nature and significance of the services provided by the Scottish Government and their effect on relevant internal controls, as part of their overall identification and assessment of risks of material misstatement.

9. In accordance with ISA 315, we assessed the complexity of the Scottish Government's main information and IT applications relevant to the preparation of the financial statements. The aim of the work was to identify any risks arising from the use of IT and evaluate the design and implementation of general IT controls that address the risks. The work in this area was shared with auditors of the public bodies that use the financial systems.

10. The controls testing undertaken reflects our understanding of the key controls and the controls apply equally across all entities who utilise Scottish Government systems. Our 2023/24 testing covered key controls in the financial systems detailed in Exhibit 1.

Exhibit 1 – Key controls

System	Control
General ledger	Journals – budget monitoring
	Changes to standing data
	Feeder system reconciliations
	IT access controls
	IT controls - system Interface
Payables	Changes to supplier bank details
	Accounts payable reconciliations
	Approval of grant payments
	Segregation of duties
	IT access controls
Receivables	Accounts receivables reconciliation
	IT access controls

System	Control
Payroll	Payroll validation
	Payroll team leader checks
	Payroll reconciliation
	Exception reporting
	Controls over standing data
	IT access controls (ongoing)
	Travel expense authorisation
Banking	Bank reconciliations
	Segregation of duties
	IT access controls

Source: Audit Scotland

11. Work is ongoing on the payroll IT access with additional testing being undertaken. Any significant issues identified will be reported in the annual audit report.

12. Matters arising from work undertaken are summarised in Appendix 1. It is important that management take action to address weaknesses to maintain the integrity of the systems and minimise any potential risks.

Conclusion

13. We have again identified a number of payroll and general ledger control weaknesses, meaning we are unable to place reliance on these system controls. We recognise that the Scottish Government are introducing the Enterprise Resource Planning (ERP) system and we expect this to strengthen the control environment.

14. With the exception of the control weaknesses identified and the satisfactory conclusion of outstanding work, we are content that the Scottish Government's key internal controls over the main financial systems operated effectively during 2023/24. In general, appropriate, and effective arrangements are in place.

15. In response to the control failures, we undertook additional audit testing to obtain sufficient assurance for our audit of the 2023/24 financial statements. The management actions taken and/or proposed should further strengthen the control environment in future financial years.

16. Any weaknesses identified represent those that have come to our attention in the course of normal audit work and therefore are not necessarily all the weakness that may exist. It is the responsibility of management to decide on the extent of the internal control system appropriate to the Scottish Government.

17. All our outputs and the matters of public interest will be published on our website: www.audit-scotland.gov.uk

Findings

General ledger: Journal authorisation

18. The Scottish Government does not have a standard journal authorisation control within the SEAS ledger system. This means that journals are not required to be approved by a second, more senior member of staff before being posted to the financial ledger. The Scottish Government has accepted this risk and rely on mitigating arrangements which includes budgetary controls and a system of cross validation rules to ensure only valid combinations of cost centre and programme codes can be posted.

19. We are unable to take controls assurance in this area and will increase our substantive testing of self-approved journals as a result.

General ledger: Inter-entity journals

20. There is no effective control in place around the posting of inter-entity journals. Inter-entity journals are used across other entities who use the SEAS ledger and not just within the Scottish Government.

21. As we do not have controls assurance in this area, we will increase our substantive testing of inter-entity journals.

General ledger: System interface

22. The SEAS general ledger system interfaces with over 20 other systems and feeders. The number of interfaces makes this system complex, and it is important that data from each interface is checked and where necessary appropriately configured.

23. We tested the controls around one of the interfaces (Community Justice Division) to check that a staff member not involved in processing the interface confirms that the totals from the in-bound interface file received, match the payables interface output. Of the four samples initially tested, this check was not evidenced on two of the iFix tickets. (Appendix 1, point 1)

24. We extended our sample testing and did not identify any further control failures.

Payroll: Reconciliations

25. Three out of 15 payroll control accounts have been reconciled during the year. However, no reconciliations have been undertaken between payroll costs as recorded on the payroll system and the general ledger. This means that there are no checks that the balances recorded on the payroll system are consistent with those recorded in the financial ledger. We have also been advised that there is currently no planned year-end reconciliation between the two. (Appendix 1, point 2)

26. We will need to perform additional audit procedures at the year end to confirm the accuracy and completeness of the financial statements.

Payroll: Audit team checks

27. The payroll audit team selects and checks a sample of payroll changes, processed by Senior Pay Administrators (SPAs), from a log of processed changes; a minimum of 10% of submitted changes are checked. We noted that there is no way of confirming the completeness of the population in the log from which the audit sample is taken. SPAs are responsible for submitting their completed tasks and may deliberately or otherwise omit their work from the folder. The effectiveness of this control cannot be evidenced as a result. (Appendix 1, point 3)

Payroll: Authorisation of contracted travel expenses

28. The Corporate Travel Management (CTM) system allows individuals who have a verified SCOTS email address and a traveller profile to book their own business travel and accommodation. Users are expected to obtain approval prior to booking travel / accommodation. However, the system does not enforce line manager approval. -The Scottish Government is charged directly by CTM for the travel booked.

29. The Travel Team perform checks on 1st class rail journeys and UK internal flights (excluding ministerial level and flights to the islands) as well as a limited number of spot checks on other travel claims. No other checks are undertaken with responsibility for identifying any issues falling to the Budget Centre Liaison Officer (BCLO) responsible for the cost centre charged. (Appendix 1, point 4)

30. This is a reporting point to improve the control environment, but due to the sums involved there is no impact on our year end testing.

Accounts Receivables / Payables – Changes to standing data

31. The process for creating a new customer or amending an existing customer detail requires a form to be completed by an individual and signed by an approver at an appropriate grade. This is then actioned by the vendor team (who are responsible for setting up and maintaining receivables, suppliers and worthy cause details on SEAS) and an updated request form returned to the requester evidencing action taken. We tested 62 changes across both Receivables and Payables.

32. Our sample testing identified the following areas where procedures were not properly followed:

- for 5 samples tested, the request for changes were processed when the emails came from the requesters rather than the approvers
- there was one instance where the requester and approver were the same individual
- for one sample, the vendor team did not update the amendment form to indicate what change had been made
- there were 4 instances where the approver grades were not verified; they were unavailable on the staff directory due to being Scotland Office staff and no further checks were undertaken to verify them
- there were 3 instances when the approver was below the appropriate grade.

33. All set up or amendment of a payee requires the review of adequate supporting documentation. Four of the Worthy Cause samples and one supplier sample did not have sufficient evidence to support the bank details provided for payment. In addition, there was one instance when a change was made to supplier details without additional checks being carried out and appropriate request forms completed. There is a risk that changes could be incorrectly or fraudulently made resulting in payments being processed to the wrong account. (Appendix 1, point 5)

34. As a consequence, we have increased our controls testing and additional substantive testing will be undertaken as part of our financial statements work.

Review of the adequacy of internal audit

35. Internal audit services are provided by the Internal Audit Division of the Scottish Government's Directorate of Internal Audit and Assurance (DIAA); it is currently headed by an Interim Director of Internal Audit and Assurance who has been in post since April 2023. The internal audit function is required to comply with the Public Sector Internal Audit Standards (PSIAS), which sets out basic principles for carrying out internal audit and establishes a framework for providing internal audit services.

36. We reviewed internal audit's approach to planning, governance, reporting, staffing and resources, as well as quality assurance against PSIAS requirements. No areas of non-compliance were identified.

37. PSIAS requires an external quality assessment (EQA) of internal audit functions to be undertaken once every 5 years. Internal audit last received an external assessment in March 2019. In order to ensure compliance with PSIAS requirements, the next review should have been completed by March 2024. New Global Internal Audit Standards come into effect in January 2025. It is currently being considered whether separate standards (similar to PSIAS approach) will be required to go alongside the new Global Standards. A position on this is anticipated in Summer 2024. DIAA have decided that it would be more valuable to complete an EQA against existing standards and a gap analysis for the new standards to support readiness planning. The Director of Internal Audit and Assurance has engaged with the Chair of SGAAC regarding this approach. We are satisfied that this is an appropriate response.

38. We also reviewed the internal audit function in terms of the International Standard on Auditing (UK) 610 (Using the Work of Internal Auditors) to assess whether the work of the internal audit function can be used for the purposes of external audit. Our review did not identify any issues which would impact on our ability to rely on the work of internal audit under ISA 610. We reviewed the Scottish Government 2023/24 Internal Audit Plan and did not identify any areas where we would place formal reliance for our financial statements audit opinion.

39. We reported last year on the importance of returning to longer-term planning in respect of Learning and Development and work was ongoing at the time to develop a Learning and Development strategy and plan for the years 2023-26. We are pleased to note that this work has now been completed and the Learning and Development strategy was issued by DIAA in July 2023.

40. Following on from the Scottish Government's plan to produce an organisation wide workforce plan and in line with broader Scottish Government policies for workforce, Internal Audit are working on reviewing workforce requirements up to 2027.

Review of IT strategic planning and service delivery

41. A review of the Scottish Government's information and communication technology (ICT) environment was carried out, including discussions with the Scottish Government's Information and Technology Services (iTECS) and Cyber Security Unit (CSU) staff as well as a review of key documentation.

42. The iTECS Technology Roadmap which covers the period 2022-2026 includes a high-level overview of key deliverables. iTECS recognise that SCOTS is undergoing a significant transformation with the shift from traditional office-based infrastructure and systems to new cloud technology platforms.

43. Recruitment into iTECS is discussed at Director General and Executive team as part of regular discussions around the path-to-balance. Whilst business as usual services are not considered to be at risk, there is a recognition that the continuing financial pressures within the Scottish Government, at a time of significant transformation of IT services, are likely to slow down progress towards achieving the work outlined in the Technology Roadmap. This could lead to increased costs in the longer-term.

44. Our review of Cyber Security arrangements highlighted the absence of Public Sector Network (PSN) certification at the Scottish Government. PSN is a UK government network, which helps public sector organisations work together, reduce duplication and share resources. Organisations connecting to the PSN are required to demonstrate that they have a suitable level of security to minimise the risk to other PSN users. PSN compliance demonstrates that an organisation's security arrangements, policies and controls are sufficiently rigorous. PSN certifications are valid for one year, the Scottish Government was last PSN certified in 2021/22; no certifications were obtained in 2022/23 and 2023/24.

45. Management response to last year's action plan on the PSN point included plans for working towards reaccreditation. However, we have been advised that the Scottish Government no longer intend to obtain PSN certification. They consider that focusing on Cyber Essentials [1], National Cyber Security Council (NCSC) Cyber Assessment Framework (CAF)[2] and GovAssure[3], provides better assurance that the SCOTS network is secure. No formal decision has been approved in respect of moving away from PSN, though we have been advised that it is planned to be reported at the next Security and Business Continuity (SBC) Governance Board meeting. (Appendix 1, point 6)

46. We have noted the following issues in respect of the proposed alternatives to PSN:

- the Scottish Government is not currently Cyber Essentials plus accredited, the previous accreditation expired in January 2024. iTECS aim to get re-accredited but are aware that they need to address challenges relating to vulnerabilities and re-engineering (e.g. the move to cloud based services such as the new ERP system, and the decommissioning of the data centre) which could impact certification.

- remediation work is still on-going to address the required improvements identified as part of the assessment of the Scottish Government's cyber security arrangements against the NCSC CAF framework.

Pre year end testing

47. As with previous years, to support an efficient approach to the audit of the financial statements, we have undertaken early substantive testing on income and non-pay expenditure as well as advances and repayments transactions.

48. Our audit work to date on these areas has not identified any matters we need to bring to your attention. Work is still ongoing, and we are awaiting some supporting documentation and responses to follow up queries.

[1] Cyber Essentials is an NCSC scheme which is backed by government and helps safeguard organisations against cyber-attacks. It is a 'snapshot' certification as it is assessed at specific points in time; certificates are valid for12 months.

[2] NCSC CAF is a tool for assessing the cyber resilience of an organisation. It provides a systematic approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation.

[3] GovAssure assesses individual systems against NCSC CAF and not the entire network.

Appendix 1

Key findings and action plan 2023/24

Issue identified	Management response/ Responsible Officer and implementation date
1. General Ledger: System interface Checks are required to be undertaken and evidenced by a staff member not involved in the processing of the interface to confirm control totals match on both in-bound and interface output files. Audit testing found in two of the four interfaces sampled that checks were not evidenced. **Risk**: there is a risk that the ledger balance is misstated if procedures are not appropriately followed.	Accepted Controls and guidance to be reinforced to ensure IFIX ticket is updated, with relevant checks. Operational Support Manager, Digital Operations July 2024
2. Payroll: Reconciliations Monthly reconciliations should be undertaken between the payroll costs and the general ledger to demonstrate that the balances are consistent. We noted that no main payroll costs reconciliations have been undertaken during 2023/24. **Risk**: there is a risk that unreconciled balances cannot be resolved due to the passage of time. Further the payroll system may include items which have not been properly processed in the financial ledger, resulting in inaccuracies in the financial statements.	Accepted Procedures and responsibilities are currently under review to ensure all the balances are properly reconciled in the future. Despite a delay caused by the deferral of the implementation of a new financial system, the handover to payroll team is ongoing along with the preparation of a new monthly reconciliation model and appropriate training. Head of Shared Services Operations October 2024
3. Payroll: Audit team checks Payroll audit team checks should be undertaken on a sample of payroll changes drawn from a complete population of all changes processed by SPAs. We noted that the audit folder may not hold all amendments and therefore there is no way of confirming the completeness of the population from which the sample is drawn.	Accepted The payroll audit team checks 10% of everything submitted by Administrators. There are management reports in place for some changes (new starts, leavers, change of grade and change of hours) but accept this does not represent all changes. We shall explore whether the new Oracle eHR system will provide better

Issue identified	Management response/ Responsible Officer and implementation date
Risk: the effectiveness of this control cannot be evidenced because the audit checks may not have been undertaken on the complete population.	management information to address this weakness. Head of Shared Services Operations March 2025
4. Payroll: Authorisation of contracted travel expenses Staff are able to book travel directly using a CTM tool. The system provides an option for line managers to have sight of the booking, but this is not enforced. **Risk**: without enforced line manager approval before bookings there is a risk of misuse of the system.	Accepted Enhanced controls with regard to the booking of travel will be investigated with CTM, noting that self-booking is standard practice across most public bodies. Policy checks and delegated financial controls are however already in place to monitor bookings, with line manager oversight and post-travel checks carried out monthly. Head of Facilities Services Division October 2024
5. Accounts Receivables / Payables: Changes to standing data The process for creating a new customer or an amendment of an existing customer requires a form to be completed by a requester and signed by an approver at an appropriate grade. Audit testing identified a number of issues where procedures were not properly followed including: • requests processed without being sent on by approvers • changes made without approver grades being verified • requests for bank detail changes processed without sufficient evidence to support the request. **Risk**: there is a risk that unauthorised amendments or set up of details could result in fraud or error.	Accepted Procedures will be reviewed and updated as appropriate, noting controls are in place for amendment requests via approval by the Vendor Team Leader, which is acceptable. Accounts Payable Branch Head September 2024

Issue identified	Management response/ Responsible Officer and implementation date
6. Public Sector Network The Scottish Government do not hold a valid PSN certificate and have indicated that they no longer intend to pursue PSN certification. Issues have been identified in respect of: • governance arrangements as no formal decision has been made/communicated on the discontinuation of PSN • achieving proposed alternatives Cyber Essentials and NCSC CAF. **Risk**: there is a risk that the proposed alternatives does not provide the Scottish Government with appropriate cyber security.	The UK government announced in 2019 that the PSN network was being retired and at the start of 2024, the UK Future Networks for Government programme that led the migration of core government services away from PSN, was closed down. A set date for withdrawal of PSN has not yet been established but it is anticipated it will happen in the very near future. Our understanding is that updated Cyber Resilience Framework is due out shortly. This framework, used across the public sector in Scotland, removes PSN as a valid control or assurance measure in reflection of the fact that it is no longer relevant or useful as an indicator of security compliance. Information Technology Services (iTECS) met with Chief Digital Officer and Cyber Security Division on 27th February 2024 to discuss alternative accreditation pertaining to SCOTS services. It was agreed at that meeting that Cyber Essentials would achieve that purpose. Director-General Corporate has been made aware of the decision to move to Cyber Essentials as accreditation for SCOTS services. Cyber Essentials has previously been endorsed for the public sector in Scotland by Scottish Ministers. (Mr Swinney in his former position as DFM). We accept that communication of the decision not to renew PSN accreditation has not yet been adequately relayed to SCOTS customer organisations and we are currently planning an exercise to address that issue. Deputy Director for Technology Services December 2024