Argyll and Bute Council

Internal Audit Report

February 2025

FINAL

Data and Information Security – Data Platform

Audit Opinion: Substantial

	High	Medium	Low	VFM
Number of Findings	**0**	**1**	**0**	**0**

Contents

Contact Details

Internal Auditor: ***Mhairi Weldon***

Telephone: ***01546 604294***

e-mail: ***mhairi.weldon@argyll-bute.gov.uk***

www.argyll-bute.gov.uk

1. Executive Summary

Introduction

1. As part of the 2024/25 internal audit plan, approved by the Audit & Scrutiny Committee in March 2024, we have undertaken an audit of Argyll and Bute Council's (the Council) system of internal control and governance in relation to data and information security – data platform.

2. The audit was conducted in accordance with the Public Sector Internal Audit Standards (PSIAS) with our conclusions based on discussions with council officers and the information available at the time the fieldwork was performed. The findings outlined in this report are only those which have come to our attention during the course of our normal audit work and are not necessarily all the issues which may exist. Appendix 1 to this report includes agreed actions to strengthen internal control however it is the responsibility of management to determine the extent of the internal control system appropriate to the Council.

3. The contents of this report have been agreed with the appropriate council officers to confirm factual accuracy and appreciation is due for the cooperation and assistance received from all officers over the course of the audit.

Background

4. The Council's Data Strategy and Action Plan 2024-28 (the Strategy) was endorsed by the Policy and Resources Committee in August 2024 and, alongside Principle 4 of the Council's "Connect for Success" programme, notes the importance of data in evidence driven decision-making. The Strategy notes that Council data combined with data from other reliable sources provides a solid foundation from which to assess the needs and demands of residents and communities and is reflected in the mission statement "Improving outcomes for our residents and communities through better combination and use of data".

5. The Data Advisory Group (DAG) was established in March 2022 with representatives from across Council Services to create a one-council, service-led forum for data and delivery of the Strategy. Reporting to the DAG, the Data Technical Groups (DTGs) are multiple short-life working groups with service representation, each of which have been tasked to deliver the specific required outputs including bespoke reports and dashboards.

6. Towards the end of 2022, the Scottish Government's Data Maturity Assessment Programme rated the Council as "developing" maturity, the Strategy seeks to drive change and progress to the "mastering" stage.

7. The Council collects, stores, uses and shares a large amount of data across various line of business systems to inform service delivery, monitor performance and provide essential business information, however, this data is split across multiple service areas within systems which no not readily interact with each other, resulting in significant challenge when analysis is required at an overarching strategic level of the Council.

8. The establishment of a data platform to help manage, store and analyse multiple data sets in a single centralised environment, with the intent to deliver real-time information and insights to develop and inform strategic objectives, is a key element within the Council's data programme

which has been prepared to advance data maturity. Services, working alongside the DAG and working groups, also intend to harness this data to build detailed reports to meet their specific service requirements.

9. The Council has appointed a consultancy partner to assist with the design and implementation of the data platform and support handover to the Council's ICT Applications Team who will continue with its day-to-day support and maintenance, and future development.

10. Data is one of the council's most important assets and should be protected accordingly, it is essential that a robust control framework is in place to ensure its confidentiality, integrity and ongoing availability, and as a large amount of this data is personal, the Council must also comply with data protection legislation.

Scope

11. The scope of the audit was to assess the arrangements for the deployment of the data platform, paying particular attention to access permissions, controls and security as outlined in the Terms of Reference agreed with the ICT and Digital Manager on behalf of the Head of Customer and Support Services on 13 December 2024.

Key Dates

12. The Terms of Reference provided provisional timescales for the review to take place, the actual dates are noted below.

Exhibit 1 – Key Dates

Stage	**Actual Date**
Terms of Reference agreed	13 December 2024
Fieldwork Commencement	8 January 2025
Draft Report issued	10 February 2025
Management Comments received	12 February 2025
Final Report issued	12 February 2025
Audit and Scrutiny Committee	13 March 2025

Risks

13. The risks considered throughout the audit were:

- **SRR10: Service Delivery – Cyber Security**
- **KF ORR35: Cyber Security Breach and associated Cyber Attack**
- **Audit Risk 1: failure to comply with requirements of the Data Protection Act 2018 and General Data Protection Regulation (GDPR)**
- **Audit Risk 2: failure of consultancy partner to fulfil contractual obligations**
- **Audit Risk 3: failure to continue development of data platform following completion of consultancy arrangement**
- **Audit Risk 4: failure to maintain integrity of data from source systems**
- **Audit Risk 5: data platform is unable to deliver intended information and insights**

Audit Opinion

14. We provide an overall audit opinion for all the audits we conduct. This is based on our judgement on the level of assurance which we can take over the established internal controls, governance and management of risk as evidenced by our audit work. Full details of the five possible categories of audit opinion is provided in Appendix 2 to this report.

15. Our overall audit opinion for this audit is that we can take a substantial level of assurance. This means that "internal control, governance and the management of risk is sound. However, there are minor areas of weakness which put some system objectives at risk and specific elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale".

Recommendations

16. We have highlighted one medium priority recommendation which is summarised below:

    - The data challenge proposal document should include a requirement to identify how long datasets are to be held to inform capacity management.

17. Full details of the audit findings, recommendations and management responses can be found in Section 3 of this report and in the action plan at Appendix 1.

2. Objectives and Summary Assessment

18. Exhibit 1 sets out the control objectives identified during the planning phase of the audit and our assessment against each objective.

Exhibit 1 – Summary Assessment of Control Objectives

	Control Objective	Link to Risk	Assessment	Summary Conclusion
1	Contract/SLAs are in place and include security and performance monitoring arrangements.	All risks	Substantial	A comprehensive business case and procurement exercise were followed to engage consultants for delivery of the data platform, however, they were not as responsive as anticipated in commencing work. Documentation reviewed contained detailed technical specifications as well as security and access arrangements. Arrangements for and progress in delivery receives sufficient management oversight from the ITMT, DMT and SMT.
2	Access to the data platform and its contents is properly authorised, managed and maintained.	SRR10 KF ORR35 Audit Risks 1 & 2	High	The data platform and its data are subject to robust physical, environmental and logical access controls and routine maintenance and update schedules. There is sufficient capacity to host current and proposed datasets with options available to expand in the future should it be required.

3	Data uploaded retains its integrity and outputs are relevant, reliable and useful.	Audit Risks 2 - 5	Substantial	A business need must be demonstrated via an agreed Data Challenge Proposal prior to uploading to the data platform, a Data Protection Impact Assessment must also be carried out where personal information is included. Appropriate mechanisms are in place to transform data upon upload to the platform to ensure operability whilst preserving integrity. End-user access is on a read-only basis via appropriate analysis and reporting tools. The need to remove data for GDPR purposes is detailed, however, there is no evidence of consideration to remove general data once no longer useful to preserve capacity availability or minimise future expansion costs.
4	Business continuity/disaster recovery arrangements are in place.	SRR10 KF ORR35 Audit Risk 5	Substantial	Well-established processes are in place for the underlying technology in use to ensure data is backed up and available for disaster recovery purposes. Additional, specific details are planned to be documented alongside ongoing development of the platform.

19. Further details of our conclusions against each control objective can be found in Section 3 of this report.

3. Detailed Findings

Contract/SLAs are in place and include security and performance monitoring arrangements

20. A comprehensive Outline Business Case (OBC) was prepared and details of the preferred model submitted to the Department Management Team (DMT) and Strategic Management Team (SMT) in September 2022 and was approved. The Information and Communication Technology (ICT) service, experienced subsequent difficulty in recruiting an officer to take the project forward, and therefore, in collaboration with the Council's procurement officers, launched a procurement exercise in November 2023 to identify a suitable consultancy partner to assist the applications team implement the solution.

21. An officer was successfully recruited in January 2024 and a working prototype of the data platform developed by the ICT applications team was demonstrated to the Data Advisory Group in March 2024. It became apparent, however, that there were significant complexities involved in further development and maintenance of the data platform and that there would be greater value achieved if the Council were to proceed with the consultancy arrangement and benefit from the knowledge and expertise of consultants with experience in implementing similar solutions. A further OBC, was therefore submitted to DMT and SMT in June 2024 reflecting on the updated position and was subsequently approved.

22. The procurement process commenced with a formal Invitation to Quote (ITQ) in November 2023 which received ten responses, six of these met the minimum requirements and were evaluated in terms of quality and price by experienced officers to identify the preferred consultancy partner. The quotation from the preferred consultant was accepted on 23 July 2024 via a formal email from the Senior Procurement Officer noting that the Council's general terms and conditions apply.

23. The contract was awarded following the Council's robust procurement process including due diligence reviews of the preferred consultant's financial standing, insurance cover and feedback from other clients who had completed a similar exercise with the consultant. No concerns were raised as a result of this review.

24. We understand that the appointed consultant has not been as responsive as had been anticipated, this is considered to have been an exceptional circumstance, due to them acquiring another company from where resources were subsequently allocated to fulfil the contract with the Council. A detailed statement of work to be completed has now been provided and discussions confirm that the delivery team are effective and professional. Weekly catchups are taking place to discuss progress and work planned for the week ahead with a firm commitment in place to complete delivery by the end of the financial year. The response to the ITQ stated that the engagement was expected to take place over 12 weeks, inclusive of 25 days technical support and 10 days project management. Dates to commence a consultancy arrangement are not provided at this stage as this will be agreed when the mobilisation meeting takes place and the programme of work is agreed.

25. The information provided within the ITQ response states that permissions to access the data platform and its contents will be linked to existing access and identity management controls operated within the Council. These controls have previously been reviewed by internal audit and found to be robust. Additional security measures are to be designed and implemented in the early stages of the data platform delivery to provide row and column level security in preparation for integration with analysis and reporting tools used within the Council.

26. Data held on the platform will be accessed on a read-only basis and is designed to comply with General Data Protection Regulation and other relevant security standards accreditations held by the Council. A draft security assessment has been completed by Council officers with detailed provision of information in terms of security arrangements, the consultants were asked to review and confirm the content of the assessment, and the consolidated responses from both the Council officers and the consultants have been incorporated within the agreed Project Plan and completed GDPR appendix.

27. Should any changes be required within the development of the data platform, provision for this has been included within the Council's terms and conditions which form part of the agreed contract of work. Any technical changes required post implementation will be undertaken following the Council's change management process where there are separate development, test and production environments for changes to transition through and undergo testing and quality control prior to being made available to users.

28. There is no specific project board assigned to provide oversight of the data platform development, however, there are regular update reports submitted to the Information Technology Management Team, DMT and SMT providing details of progress made and funding status.

29. There is no specific reference to disaster recovery within the ITQ response provided by the consultant, however, it is noted within the security assessment and other planning documents that business continuity and disaster recovery arrangements are provided for within existing processes.

Access to the data platform and its contents is properly authorised, managed and maintained

30. Physical access to the data platform is restricted to authorised personnel only. Environmental warnings and controls are in place to ensure that temperatures do not exceed acceptable levels for optimum operational requirements and provisions have been made for emergency power supply should it be required.

31. Logical access to the data platform and its contents is managed via the Council's identity and access management controls, access to the platform itself is only achievable by ICT administrators. The data within the platform will be accessible on a needs-only basis via the Council's analysis and reporting tools in accordance with user defined roles and requirements. A leavers process is in place to remove former employees from the network which also controls access to the data platform.

32. There is sufficient capacity available to store the information required to operate the data platform at this current time, it is difficult to define what the full capacity requirement may be in the longer term as this will depend on what datasets are added on a case-by-case basis. Should a need for expansion be identified in the future, there is potential for a secondary business case to be brought forward to consider options available at that time.

33. The data platform host environment is supported via maintenance schedules, application of appropriate software and regular security updates, there are also monitoring and alerting mechanisms in place to bring matters to the attention of designated officers should an issue arise.

Data uploaded retains its integrity and outputs are relevant, reliable and useful

34. When a service identifies a business need for data to be uploaded to the platform, they will require to complete a data challenge proposal for submission to the DAG. Each proposal is evaluated on a case-by-case basis and where personally identifiable information is included a Data Protection Impact Assessment (DPIA) will also be required.

35. Data extracted from line of business systems is subject to some transformation to help datasets link with each other within the platform and provide desired results for the end-user, this has no detrimental effect on the integrity of the data and may include the following:

    - Data cleansing – removing duplicates, correcting errors/missing values
    - Normalising data – standardising data format for consistency e.g. date format
    - Enrichment – adding related data or calculated values in additional columns
    - Aggregation – summarisation of data from larger data sets to simplify usage

36. End-user access to the data platform is on a read-only basis using analysis and reporting tools. Data held in the platform cannot be edited using these tools and there is no transfer of information back into the main line of business systems from the platform.

37. Training to enable ongoing operation and development of the data platform following delivery is a key requirement and is clearly stated within contract and planning documents. This knowledge transfer element of the consultancy arrangement is scheduled to take place in March 2025.

38. Training in the use of the Council's analysis and reporting tools required to view information held on the data platform is beyond the scope of the contract, however, it is planned that appropriate training resources will be made available to support authorised users gain access to the content of the platform.

39. The quality of report content from the data platform is the responsibility of the end-user via their report writing criteria and output testing. Discussions with current report-builders confirmed that where unexpected results are returned, the report criteria are carefully checked and outputs verified against data in the relevant main line of business system. Once operational, the same process will be followed for users of the data platform, if, however, in the event of reporting criteria being accurate and incorrect results persist, the Council's ICT Applications team, as part of their support and maintenance function for the data platform, will be able to confirm that data extracted from the line of business system has been uploaded correctly or reperform the task if necessary.

40. Throughout documentation reviewed, there is cognisance of the need to remove personally identifiable information when no longer required for GDPR purposes, however, there is no other reference to removal of general data once obsolete to preserve capacity availability and minimise any future costs in relation to data storage expansion.

Action Plan 1

Business continuity/disaster recovery arrangements are in place

41. The data platform and the underlying data are backed up in accordance with existing well-established arrangements to facilitate restoration in the event of a disaster scenario. These arrangements have been subject to prior internal audit review with all actions completed. Additional documentation specific to the data platform will be prepared alongside the development of the solution, however, sufficient measures are currently in place covering the underlying technologies in use to manage disaster recovery efforts.

42. Back up and recovery testing takes place in accordance with an agreed schedule and includes the underlying technologies used to support the data platform. Testing results are recorded, signed off and comments noted for future reference where relevant.

Appendix 1 – Action Plan

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Medium	1	**Removal of general data once obsolete** Finding: whilst there has been consideration for removal of personally identifiable information when no longer required for GDPR purposes, there has been no further documentation of the need to remove general data to preserve capacity availability/minimise potential future costs for expansion. Recommendation: include a section within the data challenge proposal to state how long the data should be retained within the platform.	The data platform may be limited in terms of capacity to hold data or subject to increased costs for expansion.	The data challenge form is due to be fully revised at the conclusion of the current consultancy and the form will include a section within the data challenge proposal for the service to state how long the data should be retained within the platform.	Data Programme Manager Date 30/4/2025

In order to assist management in using our reports a system of grading audit findings has been adopted to allow the significance of findings to be ascertained. The definitions of each classification are as follows:

Grading	Definition
High	A major observation on high level controls and other important internal controls or a significant matter relating to the critical success of the objectives of the system. The weakness may therefore give rise to loss or error.
Medium	Observations on less significant internal controls and/or improvements to the efficiency and effectiveness of controls which will assist in meeting the objectives of the system. The weakness is not necessarily substantial however the risk of error would be significantly reduced if corrective action was taken.
Low	Minor recommendations to improve the efficiency and effectiveness of controls or an isolated issue subsequently corrected. The weakness does not appear to significantly affect the ability of the system to meet its objectives.
VFM	An observation which does not highlight an issue relating to internal controls but represents a possible opportunity for the council to achieve better value for money (VFM).

Appendix 2 – Audit Opinion

Level of Assurance	Definition
High	Internal control, governance and the management of risk are at a high standard. Only marginal elements of residual risk have been identified with these either being accepted or dealt with. A sound system of control designed to achieve the system objectives is in place and being applied consistently.
Substantial	Internal control, governance and the management of risk is sound. However, there are minor areas of weakness which put some system objectives at risk and specific elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.
Reasonable	Internal control, governance and the management of risk are broadly reliable. However, whilst not displaying a general trend, there are areas of concern which have been identified where elements of residual risk or weakness may put some of the system objectives at risk.
Limited	Internal control, governance and the management of risk are displaying a general trend of unacceptable residual risk above an acceptable level and placing system objectives are at risk. Weakness must be addressed with a reasonable timescale with management allocating appropriate resources to the issues raised.
No Assurance	Internal control, governance and the management of risk is poor. Significant residual risk and/or significant non-compliance with basic controls exists leaving the system open to error, loss or abuse. Residual risk must be addressed immediately with management allocating appropriate resources to the issues.