Argyll and Bute Council

Internal Audit Report

May 2024

FINAL

Cloud Computing Services

Audit Opinion: Substantial

	High	Medium	Low	VFM
Number of Findings	**0**	**4**	**1**	**0**

Contents

Contact Details

Internal Auditors: ***Mhairi Weldon and Annemarie McLean***

Telephones: ***01546 604294 and 01700 501354***

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

annemarie.mclean@argyll-bute.gov.uk

Website: www.argyll-bute.gov.uk

1. Executive Summary

Introduction

1. As part of the 2023/24 internal audit plan, approved by the Audit & Scrutiny Committee in March 2023, we have undertaken an audit of Argyll and Bute Council's (the Council) system of internal control and governance in relation to Cloud Computer Services.

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. Cloud services are described by the National Cyber Security Centre (NCSC) as "an on-demand, massively scalable service, hosted on shared infrastructure, accessible via the internet". These services are therefore located outside the Council's network environment and typically provide data storage, processing and pre-defined user functionality. The NCSC advises that public sector organisations select a provider using their cloud security principles.

5. The NCSC states that cloud usage has steadily grown in recent years and is now the preferred option when organisations purchase new IT services in alignment with the UK and Scottish Government's Cloud First Policies.

6. The Council's ICT and Digital Strategy aligns to the Digital Strategy for Scotland and promotes improvement and sustainability through digital innovation to deliver efficiencies, savings and improved services for council staff and customers. In particular, the strategy aims to provide systems and applications available to all employees, wherever they work, operating the latest software versions that are fully supported by suppliers. Where applicable, IT solutions will continue to be provided in the cloud where it is economically viable to reduce long term cost and improve on-premises solutions.

7. The 2022 Society for Innovation, Technology and Modernisation (SOCITM) Benchmarking report indicated that the Council is one of the most cost effective and highest performing Local Authority ICT services out of 31 participating across the UK, it is also indicated that the Council use cloud computing more than most other Councils.

8. The adoption of cloud services aims to generate efficiencies, improve operations and reduce the overall cost of ownership for the Council. The main benefits of migrating to the Cloud include:

    - Reduced operational and maintenance costs
    - Rapid deployment
    - Scalability to address demand fluctuations

- Security capabilities to protect data and infrastructure
- Resilience in system availability

9. The Council requires access to the Public Services Network (PSN) on an ongoing basis which requires security assessments to have been conducted against Cloud Security guidance from the National Cyber Security Centre (NCSC), including protective monitoring, identity and authentication, separation between consumers and secure consumer management.

10. Back-up data is a copy of primary data made at a point in time that can be used to reinstate primary data should it be lost as a result of hardware or software failure, data corruption, malicious attack or human error. This data must be retained in a secure, secondary location to maintain its integrity and validity for use should it be required. As part of their service provision, cloud service providers create back-up copies of customer's data, they may also/alternatively implement continuous replication to provide a more up-to-date copy of data.

11. The overall responsibility for service provision and data security remains with the Council rather than with the Cloud service provider.

Scope

12. The scope of the audit was to review systems and processes in place to support security and data integrity of cloud-based computer services as outlined in the Terms of Reference agreed with the Head of Customer and Support Services on 2 May 2024.

Key Dates

13. 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	2 May 2024
Fieldwork Commencement	11 April 2024
Draft Report issued	27 May 2024
Management Comments received	30 May 2024
Final Report issued	30 May 2024
Audit and Scrutiny Committee	13 June 2024

Risks

14. The risks considered throughout the audit were:

- SRR11: Service Delivery – Cyber Security
- KF ORR35: Cyber security breach and associated cyber attack
- CSRR12: Security information and event management (SIEM)
- CSRR18: Password Security
- CSRR19: Account Management
- CSRR31 & 39: Backups
- CSRR33: Critical Infrastructure Security
- CSRR38: Multi-factor Authentication (MFA)

- CSRR42: Cloud Security
- Audit Risk 1: Failure to comply with Public Services Network (PSN) and Cyber Essentials Plus certification requirements
- Audit Risk 2: The Council has limited control over access to systems and data
- Audit Risk 3: Information stored in Cloud services is not appropriately segregated from that of other organisations resulting in data protection and commercial failings

Audit Opinion

15. 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.

    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 4 medium priority recommendations and one low priority recommendations where we believe there is scope to strengthen the control and governance environment. These are summarised below:

    - Review content of ICT Contract Application and cloud services asset register to ensure all systems are included with links to all associated documentation.
    - ICT officers investigate why access to one system was achieved using a personal device and seek resolution to prevent recurrence.
    - Appropriate authorisation should be sought for all new system users.
    - Periodic review of users takes place to remove leaver access in a timely manner.
    - ICT services prepare, update or finalise disaster recovery documentation and implement testing.

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 related performance monitoring arrangements.	SRR11 KF ORR35 CSRR12, 31, 33, 39 & 42 Audit Risk 1, 2 & 3	Substantial	ICT and procurement teams assist services implement new systems following robust due diligence processes. Documentation requested for review was retained, however, this proved challenging to gather at the outset of the audit. The list of cloud based systems provided did not fully align with the contracts held on the ICT application. Arrangements for business continuity, data recovery, change management and performance targets were found to be present and appropriate oversight takes place.
2	Access to systems and data is properly authorised and held securely.	SRR11 KF ORR35 CSRR18, 19, 38 & 42 Audit Risk 2 & 3	Substantial	Each system reviewed was multi-factor authentication (MFA) compatible, however, this was not utilised in two of the systems. New users were not always appropriately authorised and leavers are not being promptly notified for one system. Training in the use of each system has been provided and/or appropriate guidance made available. Service providers have implemented measures to protect the Council's data in transit and at rest within the Cloud systems and prevent unauthorised access from their employees and other customer organisations.
3	Business continuity/disaster recovery arrangements are in place to ensure back-ups of data have been created, are securely stored and are accessible and usable should they be required.	SRR11 KF ORR35 CSRR12, 31, 39 Audit Risk 2	Reasonable	Cloud service providers have arrangements in place to backup and/or replicate Council data to ensure its ongoing availability. A comprehensive overarching Cyber-incident response plan has been prepared, however, system specific disaster recovery plans and/or run books require to be prepared, updated and/or finalised and tested for specific cloud systems.

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 related performance monitoring arrangements

20. New or improved technology services are implemented following identification of a business need and completion of an options appraisal to identify the solution best suited to the needs and demands of the Council. ICT Client Liaison Officers often assist throughout the processes involved including, contributing to composition of the business case, providing a project management role, representation on the Project Board and providing technical expertise. The successful system is selected based on a number of elements including functionality, performance and best value and may be either on premise or in the cloud, although there has been a significant move towards cloud services in recent years.

21. A significant amount of due diligence takes place in the forming of contract to ensure the Council's specific requirements are met, this includes:

    - Preparation of a business case with justification, rationale and approval for the procurement project. (business objectives, scope, options appraisal, costs and budget, risks timeline etc.)
    - Tender specifications requirements and response for inclusion within the final contract (covers technical and security functionality, outcomes or both)
    - Tender evaluation and scoring
    - ICT Security Assessment
    - Financial Checks to ensure integrity of supplier organisation
    - Formation of a project board and sponsor for management, oversight purposes and to decide the most appropriate option. (This is primarily service led)
    - Data Protection Impact Assessment

22. A sample of four cloud services was selected for review from a list of current providers, for the purpose of this report we will refer to these systems as A, B, C and D to protect the Council from potential harm following identification of areas for improvement.

23. The Council's ICT services maintain an ICT contract application containing detailed documentation in respect of systems and services procured, however, this application did not contain documentation pertaining to all of the systems identified in the list of current cloud service providers.

24. Contract documentation and supporting information was requested to evidence contract arrangements were in place for the four systems selected for review in order to manage information security and data integrity in line with the agreed scope of the audit. Documents were found to have been retained safely and were provided by ICT officers, however, coordination of a number of officers was required to identify and collate information for audit purposes.

Action Plan 1

25. The documentation and publicly available terms and conditions reviewed stated that there were measures in place to ensure ongoing service availability and security of data stored within each of the provider's data centres. The security responsibilities of each party to the contracts were also outlined.

26. Arrangements for business continuity and data recovery were in place for each of the systems and included solutions such as replication of data at additional data sites, frequency of data back-up routines and for system C, provision of periodic copies of back-ups to customers for additional resilience. Recovery time objectives were present for systems A, C and D and system B stated recovery in a timely manner.

27. Arrangements are also in place to make provisions for modifications to cloud systems to ensure they reflect any changes in the business environment (e.g. legal/regulatory updates) and ensure ongoing functionality and availability.

28. Performance targets are represented in a Service Level Agreement (SLA). Council services (system users) undertake the role of performance monitoring with support provided by ICT Client Liaison Officers if required, where issues are identified, the Council's procurement team may step in to assist with resolutions and details are reported to Department Management Teams and Information Technology Management Team for escalation and oversight purposes.

Access to systems and data is properly authorised and held securely

29. Access to cloud services is managed by multi-factor authentication (MFA) for systems B and C, it appears to be available for systems A and D but has not been switched on. Access to system A was found to be achievable by use of a personal device during the course of audit testing. Although not selected for testing, we have been made aware of a further system that can also be accessed by personal device, we understand that this is a supplier issue and affects all users, not just Argyll and Bute Council.

Action Plan 2

30. User access to data held on the cloud service is managed by systems administrators. A sample of ten users was selected from systems A, B and C to assess if authorisation was appropriately provided, system D is managed by a small team of users within ICT itself. All ten users were appropriately authorised in systems A and C, however, three users from system B had submitted the new user form themselves without authorisation being evident from their line managers, checks undertaken by the Council service's systems administration team are limited to ensuring that the request has been sent from a valid domain email address (Council or partner organisation).

Action Plan 3

31. Systems A, B and C were also reviewed to assess if timely notification of leavers is received to ensure prompt removal of access to data. System C was provided with weekly updates from the Council's HR service to remove users from the Council's overarching network infrastructure that provides system access and system A undertook a quarterly review of all users to identify and remove leavers. System B relies on the Council service's systems administration team receiving notifications from line managers that users are no longer required to have access, testing found that eight recent leavers had not had their access removed. Whilst there is some comfort in the fact that this system is also dependent on network access, it does not prevent unauthorised access when an employee transfers to another service area of the council or partner organisation, additionally, there is currently no leaver notification received from HR and there has been no user review since implementation of the system in June 2023.

Action Plan 4

32. Training in the use of the cloud services was provided to key individuals prior to implementation and cascaded to other authorised users. Documented guidance and training modules are also available to support users via the systems administrators, the Council's intranet or LEON training platform.

33. Cloud service providers are required to provide assurance that their employees and other organisations who use the services provided (tenants) are unable to access the Council's data. Documentation reviewed indicated that strong security measures are in place in each of the four systems reviewed to segregate Council data from that of other organisations to prevent unauthorised access. Where the provider's employees are legitimately required to access data for maintenance or resolution of issues identified, specific permission is sought and approved by the Council to do so, additionally, immutable audit trails are maintained of any changes that do take place.

34. Documentation also indicated that standard encryption technologies and options to protect data while in transit or at rest are in place. Data held within each of the systems is held in accordance with the Data Protection Act with the Council acting as data controller and the cloud service provider the data processor.

Business continuity/disaster recovery arrangements are in place to ensure back-ups of data have been created, are securely stored and are accessible and usable should they be required

35. Provisions have been made within materials reviewed to ensure data is backed-up or replicated at secure sites to ensure availability in the event of a disaster or cyber incident.

36. A cloud based solution is not currently utilised for the Council's on premise systems, however, other robust means of providing resilience are employed.

37. The Council has prepared a generic Cyber Incident Response Plan that aligns to the Scottish Public Sector Cyber Incident Central Notification and Co-ordination Policy. This is a comprehensive document including details of what constitutes an incident, how it should be managed and the roles and responsibilities of parties required to contribute should the need arise.

38. The Council operates many systems, including both on premise and cloud based. In the event of a cyber-incident, it would not be possible to restore all systems simultaneously, therefore a process has taken place to categorise all systems into four tiers with each being completely restored in numerical order prior to moving on to the next. A further prioritisation exercise has taken place to ensure that the most critical systems are addressed earliest within each tier.

39. ICT services have developed a disaster recovery planning storage area with an array of comprehensive plans and run books to aid recovery of data in the event of a disaster or cyber-incident. Whilst it is deemed that the cloud service providers have adequate disaster recovery arrangements in place, there is a further need to include regular review of the provider's plans and activities in addition to being assured that disaster recovery is appropriate.

40. Cloud service providers have disaster recovery plans in place, however, the Council also has responsibilities to ensure these plans adequately address our needs and the services can be accessed in the event of a disaster situation. A disaster recovery plan has been drafted for

system A and a run book has been prepared for system C, however, it is considered that this run book requires to be updated to reflect additional information specific for cloud restore. A disaster recovery plan is being prepared for system B and there was no evidence of documentation for system D.

Action Point 5

41. Each of the systems websites were reviewed to establish if independent assurance could be provided in terms of security and performance and all were found to have several third party accreditations in place.

Appendix 1 – Action Plan

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Low	1	**Contract Application and Cloud Services Asset Register** Finding: The ICT Contract Application did not contain all systems contained on a list provided by ICT Project & Liaison Manager. Recommendation: Review content of ICT Contract Application and cloud services asset register to ensure all systems are included with links to all associated documentation.	ICT may be unable to track and manage systems and their risks, ensure licence compliance and plan upgrades/replacements.	The ICT Contract Register will be reviewed and will include a Cloud Asset Register to ensure all systems are included with links to all associated documentation.	ICT and Digital Manager 31 August 2024
Medium	2	**Multi-factor Authentication** Finding: access to one system was found to be achievable using a personal device during the course of audit testing. An additional system not included within the sample selected for review is also known to allow access from a personal device. Recommendation: ICT officers investigate why a personal device was able to access the system and implement suitable means to restrict such access.	Council data may be accessed inappropriately, including by recent leavers of the Council.	ICT Engineers will work with the supplier of System A to ensure only council managed devices can access the system. ICT Engineers will investigate whether the supplier of the national system referred to in the report (which is used by almost all public sector organisation in Scotland with built in access from personal devices), can switch off access to the Council's instance from non-council devices.	ICT and Digital Manager 31 August 2024
Medium	3	**User Authorisation** Finding: for one system reviewed, user access was not appropriately authorised by line management in all instances. Recommendation: service systems administration implement a procedure insisting that appropriate authorisation to access sensitive data is obtained for all new users.	Unauthorised access to sensitive data	The System B team will send reminders to all users, emphasising that Line Managers must approve all requests for system access. Additionally, they will conduct quarterly reviews of a random sample of (5) request forms to ensure quality assurance.	Systems Support Officer 30 May 2024 Completed

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Medium	4	**User Revocation** Finding: for one system reviewed, we found that systems administrators are not always promptly informed when users leave or no longer require access. Termination of network access provides some comfort where leavers are concerned, however, this does not prevent users gaining continued access when transferring to another service area. Recommendation: periodic review of user status takes place by service systems administration to ensure access to sensitive data is restricted to those with current and legitimate service needs.	Unauthorised access to sensitive data	The System B Team will promptly implement a monthly procedure to identify and deactivate accounts that have not been used within the month.	Systems Support Officer 30 June 2024
Medium	5	**Disaster Recovery Plans and Run books** Finding: Disaster recovery plans/run books are not in place for all systems reviewed and therefore not tested to cover any potential disaster affecting the Council's ability to access these systems. Recommendation: ICT services prepare, update or finalise disaster recovery documentation and implement testing.	Disaster Recovery Plans/Run Books are not available or up to date to provide the necessary information in the event of a cyber-incident.	ICT will prepare, update and finalise disaster recovery documentation and implement testing for those recently introduced cloud systems not already documented.	ICT and Digital Manager 31 October 2024

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.