Argyll and Bute Council

Internal Audit Report

February 2020

Final

Information Asset Registers

Audit Opinion: Reasonable

	High	Medium	Low
Number of Findings	**1**	**2**	**0**

Contents

Contact Details

Internal Auditor: ***David Sullivan***

Telephone: ***01546 604125***

e-mail: ***david.sullivan@argyll-bute.gov.uk***

www.argyll-bute.gov.uk

1. Executive Summary

Introduction

1. As part of the 2019/20 internal audit plan, approved by the Audit & Scrutiny Committee in March 2019, we have undertaken an audit of Argyll and Bute Council's (the Council) system of internal control and governance in relation to Information Asset Registers (IARs).

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. Under the Public Records (Scotland) Act 2011 (PRSA), Scottish public authorities are required to produce a Records Management Plan (RMP), which sets out the arrangements for managing public records.

5. The Council creates, collects, uses and disposes of a large amount of information during the course of carrying out its public duties. Managing this information carefully helps ensure the record of its activities is accurate and complete.

6. The Council's approach to records and information management is established by the Information Management Strategy (IMS), approved by Council in March 2015, and the Corporate Records Management Policy, which takes into account the PRSA requirements.

7. As part of the implementation of the IMS, the Council have established IARs. Information assets are items which are received, gathered or generated and then retained for the purposes of:

    - supporting provision of a service to the public
    - supporting the general democratic process
    - assisting in meeting external statutory obligations
    - helping to evidence compliance in response to external regulatory processes.

Scope

8. The scope of the audit was to ensure arrangements for managing information assets are robust as outlined in the terms of reference agreed with the Governance, Risk & Safety Manager on 13 January 2020.

Risks

9. The risks considered throughout the audit were:

- **Legal & Regulatory: ORR02**: failure to ensure Council compliance with governance and information management arrangements
- **Audit Risk 1:** Information Asset Register guidance and training is not available or adequate to support officers in their duties
- **Audit Risk 2**: IARs do not comply with relevant legislation
- **Audit Risk 3:** IARs are not regularly updated, reviewed and approved

Audit Opinion

10. 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.

11. Our overall audit opinion for this audit is that we can take a reasonable level of assurance. This means that 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.

Recommendations

12. We have highlighted one high priority recommendations and two medium priority recommendations where we believe there is scope to strengthen the control and governance environment. These are summarised below:

    - Social Work IARs should be completed and all IARs should be updated to reflect all legislative requirements including the General Data Protection Regulation (GDPR), clarity is also required over responsibility for the Live Argyll IAR
    - IARs should be aligned to the revised Council structure, reviewed and agreed annually at Departmental Management Team (DMT) meetings and have corresponding action plans
    - policies and procedures should be reviewed within the prescribed timescales to ensure they reflect current legislation and best practice.

13. 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

14. 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
CO1	The Council has appropriate procedures/guidance which align with legislative requirements	ORR02 Audit Risk 1 Audit Risk 2	Reasonable	The Council has an IMS, Records Management Policy, and a RMP. All three were found to be comprehensive and set out the Council's arrangements for records management. Both the Records Management Policy and RMP have

				not been formally reviewed since 2016 and 2017 respectively. A revised draft of the IMS strategy 2018-21 has been approved by the ICT steering group and is awaiting approval by the Strategic Management Team (SMT).
CO2	Appropriate training on IARs is available to relevant staff	ORR02 Audit Risk 1	Substantial	Appropriate training has been delivered to the IAR 'champions' who are responsible for ensuring that IARs are maintained. The Governance, Risk & Safety Manager has also attended relevant training.
CO3	IARs comply with relevant legislation and Council procedures/ guidance	ORR02 Audit Risk 2	Reasonable	Of the 12 IARs two relating to social work services were not available for review, six fully complied with the requirements of the PRSA and four partially complied. Clarification should be sought on responsibility for the LiveArgyll IAR.
CO4	IARs are subject to regular review and approval	ORR02 Audit Risk 3	Limited	Seven of the 12 IARs have been agreed by the relevant DMT, for four there was no evidence of DMT agreement and for the remaining one there was evidence of review but not agreement. Furthermore only two of the 12 IARs had an action plan as required by the RMP. The IARs need to be updated to reflect the revised Council structure.

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

3. Detailed Findings

The Council has appropriate procedures/guidance which align with legislative requirements

16. The Council has a Records Management Policy which seeks to ensure it effectively and efficiently manages information in order to support its legal, fiscal, business and administrative requirements. The policy clearly defines the roles and responsibilities of Council officers and elected members and establishes the Council's objectives as being to:

- create awareness of records management principles and responsibilities throughout the Council
- comply with the Public Records Scotland Act 2011 and other relevant legislation
- promote a consistent approach to records management across all service areas
- ensure information is being managed in the most efficient and effective way
- provide guidance to all staff to allow them to adopt more efficient ways of working
- provide best practice guidance in respect of records.

17. The policy was approved by the SMT on 8 February 2016 but has not been subject to further review since. Consequently it does not provide any reference to the GDPR which was implemented in May 2018

Action Plan 3

18. In compliance with the requirements of the PRSA the Council has a RMP which is comprehensive and sets out the Council's arrangements for managing public records. The RMP is supposed to be reviewed annually however no formal review has taken place since it was approved by the SMT in February 2017.

Action Plan 3

19. The Council has an IMS for the period 2014-18 which details the:

- definition of what information is
- definition and aims of information management
- Council priorities and objectives regarding information management
- requirement for services to monitor IARs.

20. A revised draft of the IMS strategy 2018-21 has been prepared and was approved by the ICT steering board in July 2018. Approval from SMT is outstanding.

Action Plan 3

21. The IMS also sets out the governance and roles for records management and specifically outlines the role of 'IAR Champions' who are responsible for ensuring service IARs are properly maintained. The Council Hub details the contact information for each Council service IAR champion.

22. There are supporting documents which provide guidance on key areas such as approving and maintaining IARs, preparing action plans to update IARs and record disposal.

Appropriate training on IARs is available to relevant staff

23. The Governance, Risk & Safety Manager has day-to-day responsibility for records management. It is a requirement of the post that the post holder has a sound knowledge of records management theory and practice, including current standards and recognised best practice. Whilst the Governance, Risk & Safety Manager last attended formal records management training in March 2017 he is a member of the Information and Records Management society and also the online Knowledge HUB forum used for sharing best practice. Furthermore his team attends PRSA events held throughout the year which provide current guidance and advice.

24. All existing IAR Champions attended record management training in May 2018 which focused on:

- legislative requirements
- records management plan
- information asset registers
- data protection law
- GDPR.

25. Consideration is currently being given to making online records management training available to all Council staff.

IARs comply with relevant legislation and Council procedures/guidance

26. To comply with the PRSA and ensure the Council adheres to its RMP, each service IAR should detail:

    - what information the service holds
    - where it is held
    - how long it should be kept for
    - includes information relating to GDPR requirements e.g. legal basis for processing of data, is privacy notice in place and compliant with GDPR requirements, internal data sharing etc.

27. The Council has a total of 12 IARs, which includes two for the Social Work services within the Health and Social Care Partnership. We reviewed the 10 available Council IARs to ensure they complied with the requirements detailed in paragraph 26. Our review confirmed that, of those 10, 6 fully complied but 4 only partially complied as they did not include the relevant GDPR information. The two Social Work IARs have not been completed due to lack of resource within Social Work services and as such have not been reviewed as part of this audit.

Action Plan 1

28. The Live Argyll IAR was not considered as part of this audit however there is a lack of clarity over whether the Live Argyll IAR comes under the remit of the Governance, Risk & Safety Manager's responsibility.

Action Plan 1

IARs are subject to regular review and approval

29. The IMS requires DMTs to review their relevant IAR annually. A review of the 12 IARs highlighted that for:

    - seven there was evidence of DMT agreement
    - four there was no evidence of DMT agreement
    - one there was evidence of review but not agreement.

Action Plan 2

30. The Council has recently introduced a new structure which has resulted in some changes of remit for Heads of Service (HoS). The current IARs reflect the business assets assigned to each HoS prior to the restructure and therefore need updated.

Action Plan 2

31. It is a requirement of the RMP that IARs should have a corresponding action plan which '*are designed to capture all tasks required in relation to the IAR entries, implementation of retention periods, and provide an audit trail of changes made to the IAR'*.

32. A review of the 12 IARs highlighted that:

    - two had a corresponding action which met the prescribed requirements
    - two had action plans which did not meet the prescribed requirements e.g. did not provide an audit trail of changes
    - eight had no action plan.

Action Plan 2

Appendix 1 – Action Plan

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
High	1	**Information Asset Registers** The two Social Work IARs were not available for review or located on the designated sharepoint site. Of the remaining ten, four require to be updated to reflect the latest GDPR requirements. Clarity over whether the Live Argyll IAR comes under the remit of the Governance, Risk & Safety Manager's responsibility is required.	Failure by the HSCP to provide sufficient resources to have the Social Work IARs in place and available for all relevant services may lead to non-compliance with legislation	Social Work IARs to be completed and approved by appropriate management teams Clarify where responsibility for Live Argyll IAR lies and have it completed and approved by appropriate management team	Governance, Risk & Safety Manager 31 December 2020 Governance, Risk & Safety Manager 31 December 2020
Medium	2	**Periodic Review and Agreement of Information Asset Registers** For four of the 12 IARs there was no evidence they had been agreed by the relevant DMT. Furthermore IARs need to be reviewed to ensure they are aligned to the new Corporate structure. The RMP requires that IAR's should have a complete action plan to document required changes. Two of the 12 IARs had an action plan, two had action plans that did not fully meet the requirements of the RMP and eight had no action plan.	IARs may not be complete and accurate with a clear audit trail of changes made and agreed.	Review IARs and realign information to current Service structure Obtain annual approval from DMTs for all completed IARs Action plans for all IARs to be put in place and agreed by management teams	Governance, Risk & Safety Manager 30 September 2020 Governance, Risk & Safety Manager 30 September Governance, Risk & Safety Manager 30 September 2020

Medium	3	**Review of Policies and Procedures** Whilst our review of governance documents concluded they were comprehensive they all require review to ensure they are still current and fit for purpose. In particular they were last reviewed and approved in : • Records Management Policy - February 2016 • Records Management Plan – February 2017 • Information Management Strategy - (reviewed July 2018, not approved)	Key governance documents may not reflect current legislation and procedures	Key records management documents to be reviewed and approved	Governance, Risk and Safety Manager 30 September 2020

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.

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.