Argyll and Bute Council

Internal Audit Report

June 2021

FINAL

Disaster Recovery Planning

Audit Opinion: Limited

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

CHOOSE ARGYLL. LOVE ARGYLL.

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 2021/21 internal audit plan, approved by the Audit & Scrutiny Committee in March 2020, we have undertaken an audit of Argyll and Bute Council's (the Council) system of internal control and governance in relation to Disaster Recovery Planning.
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 places significant reliance on the availability of technology in delivering many of its services. As a result, the ability to respond effectively and efficiently to a disaster which affects infrastructure and applications supported by the Council's Information Communications Technology (ICT) is of paramount importance. Failure to do so could result in significant disruption to business activities and reputational damage.
5. Disaster recovery planning is a key function of ICT and digital services and it is essential that robust and sufficiently detailed plans are in place, maintained and tested to ensure that ICT infrastructure and applications can be recovered in the event of a disaster.
6. The main objective of the Council's Disaster Recovery Plan (DRP) is to minimize disruption to end users and services to the Council's customers in the event of a disaster that causes critical software applications to become unavailable. The DRP describes:
    - the components and topology of the application
    - the risks that threaten the application availability and the impact on service availability
    - the measures taken to prevent and recover from any potential disaster event
    - the recovery procedure for each defined disaster event
    - the frequency of tests undertaken to ensure that the recovery procedure is robust and thorough
7. Examples of critical applications which have a disaster recovery plan would be Resourcelink, the Civica openrevenue application to handle Council tax, the Carefirst application used by Social Work and the Debtors system used by Financial Services.

Scope

8. The scope of the audit to is to assess the adequacy and effectiveness of the Council's disaster recovery arrangements as outlined in the Terms of Reference as agreed with the Head of Customer Support Services ICT and Digital Manager on 5th January 2021.

Risks

9. The risks considered throughout the audit were:

- SRR06: Service Delivery
- EDI ORR 47: Lack of capacity to meet unplanned demand for communications support with existing resources
- Audit Risk 1: Threats to the service have not been identified and assessed
- Audit Risk 2: Assets are not protected

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 limited level of assurance. This means that 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.

Recommendations

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

- DRPs should be subject to periodic testing with the frequency of testing based on assessed system criticality
- DRPs should be subject to annual review
- a schedule should be prepared detailing each system that requires a DRP and how these have been identified and prioritised
- agendas and minutes should be maintained for disaster recovery team meetings.

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	Risk	Assessment	Summary Conclusion
1	There is appropriate governance, policies and procedures to provide or robust disaster recovery planning.	All	Substantial	The Council has 43 application DRPs that outline what is required to recover a range of Council IT systems in the event of a disaster. There are also overarching DRPs for the two data centres which form the core of the ICT data repository with recently upgraded servers and these host all applications which are not cloud based. Whilst there are 43 application DRPs are in place there is no overarching document that specifies which systems require one and how these have been identified or prioritised. Formal agendas and minutes and agendas are prepared for disaster recovery team meetings.
2	Robust IT DRPs have been established and appropriately communicated.	All	Reasonable	The DRPs are comprehensive and available to relevant officers however whilst the DRPs for the data centres were reviewed in 2020 none of the 43 application DRP's have been reviewed since 2018.
3	DRPs are stored appropriately and distributed to appropriate authorised personnel.	SRR06 EDI ORR 47	High	DRPs are stored on Sharepoint with access to them restricted to appropriate officers via logical access controls.
4	DRPs are periodically tested and documentation updated to reflect lessons learned.	All	No assurance	There are established plans to test DRPs however this was interrupted by the COVID pandemic and the need to divert IT resource to support the Council's response. There was a partial test of a server in 2019 however none of the Council's DRPs have been subject to formal testing. The ICT and Digital Strategy approved in February 2021 identifies an action to test DRPs.
5	Officers involved in the recovery process are trained and experienced.	SRR06 EDI ORR 47	Reasonable	There is no specific training for officers involved in disaster recovery processes although it is recognised that IT officers will be equipped with a range of relevant skills and experience which will help implement a DRP. These would be enhanced through the roll out of a programme of DRP testing.

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

3. Detailed Findings

There is appropriate governance, policies and procedures to provide or robust disaster recovery planning

16. Disaster recovery planning involves a set of policies, tools and procedures to enable the recovery or continuation of IT infrastructure or systems following a failure or disaster. It focuses on the IT systems that support business critical activities, as opposed to Business Continuity Plans (BCP) which look at all aspects of keeping a business functioning. As such DRPs can be considered as a subset of BCPs.

17. The Council's 2021-2024 ICT and Digital Strategy specifically states that, on an annual basis, the following will be conducted:

    - review and improve our disaster recovery and business continuity plans and technologies
    - a systematic disaster recovery scenario for key systems.

18. The Council has 43 application DRPs that outline the step-by-step procedures and responsibilities to recover the Council's IT systems, operations and data in the event of a disaster. All DRPs are readily available to relevant personnel on SharePoint. There are also overarching DRPs for the two data centres which form the core of the ICT data repository with recently upgraded servers and these host all applications which are not cloud based. The data centre DRPs include a priority list of recovery actions which cover the infrastructure related tasks necessary to recover the core system environment prior to application recovery. Whilst there are 43 application DRPs in place there is no overarching document that specifies which application requires one and how these have been identified or prioritised. Therefore it is not possible to determine if DRPs are in place for all critical systems.

Action Plan 3

19. The Council has a disaster recovery team which meets every two weeks to discuss issues pertinent to the Council's response in the event of a disaster. No formal agenda or minutes are prepared for these meetings.

Action Plan 4

Robust IT DRPs have been established and appropriately communicated

20. The DRPs for the data centres in Kilmory and Helensburgh were reviewed and updated in 2020 to reflect the refresh of the entire server and storage infrastructure which was carried out in 2019. However the majority of the 43 application DRPs have not been reviewed since 2018 which does not comply with the requirement in the ICT and Digital Strategy for DRPs to be subject to annual review.

Action Plan 2

21. The DRPs reviewed were found to be comprehensive and included:

    - identification of application components e.g. operating systems
    - a disaster impact analysis on servers hosting the application being unavailable
    - impact of software being unavailable
    - prioritisation of component recovery in the event of a disaster
    - identification of the risk of data loss

- backup procedures
- backup data retention information
- backup recovery testing schedules.

22. The disaster recovery team and IT management team have access to all documentation pertaining to disaster recovery.

DRPs are stored appropriately and distributed to appropriate authorised personnel.

23. DRPs are stored on Sharepoint on a shared drive. Access to these records is restricted to appropriate officers via logical access controls.

DRPs are periodically tested and documentation updated to reflect lessons learned.

24. Periodic testing of the Council's DRPs is critical in order to help ensure they will be effective if a real disaster should occur.

25. All DRPs establish the required frequency of testing. They also require that, once a test has been completed, a 'Disaster Recovery Test Record' is populated and submitted to the Information Technology Management Team for review. A template for this record is provided in the DRP which requires the following to be documented:

    - disaster scenario tested
    - date of test
    - was the application recovery successful
    - how could the DRP plan be improved
    - name of person carrying out test
    - impact of disaster on Council infrastructure
    - effect of disaster on application
    - required recovery procedure.

26. The Council have Critical Activity Recovery Plans (CARPs) which identify which Council services are critical and how the Council will ensure those critical services are maintained in the event of a major incident. The CARPs make reference to Council IT systems where these are viewed as critical to maintaining the service. Whilst DRPs recognise that some Council systems are more critical than others there was no evidence system criticality is considered when determining required frequency of testing.

Action Point 1

27. There are established plans to test DRPs however this was interrupted by the COVID pandemic and the need to divert IT resource to support the Council's response. There was a partial test of a server in 2019 however we established that none of the Council's 43 application DRPs have been subject to formal testing. It is recognised that the Council's ICT and Digital Strategy, revised and approved in February 2021, identifies an action to test DRPs. As the application DRPs have not been tested we are unable to provide any assurance for this control objective. Once a testing programme has been established and applied to a reasonable body of DRPs we intend to carry out a follow up audit to assess compliance with the established programme and associated documentation requirements. This is provisionally scheduled for the 2022/23 internal audit plan.

Action Plan 1

28. In July 2021 there is a planned cyber security exercise to test the recovery of an identified major system. There are two planned tests being prepared for 2021 In order to make this test as realistic as possible we have not identified which system it will be in this report. In November 2021 the intention is to test multiple business areas across the Council however no decision has been reached as to which systems will be tested.

Officers involved in the recovery process are trained and experienced

29. There is no specific training for officers involved in disaster recovery processes although it is recognised that IT officers will be equipped with a range of relevant skills and experience which will help implement a DRP in the event that one was required. However without formal testing of the DRPs it is not possible to identify where there may be skills or experience gaps which would require to be filled.

Appendix 1 – Action Plan

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
High	1	**Disaster Recovery Plan Testing** None of the Council’s 43 DRPs haven been subject to testing and whilst each DRP sets out the required frequency of testing there is no evidence that system criticality is considered when determining that required frequency.	System recovery may not operate as planned which could impact on critical service delivery in the event of an unforeseen disaster.	We have major DR tests planned for July and November 2021 in conjunction with the Civil Contingencies manager with input from the Scottish Government Resilience Unit and the Scottish Business Resilience Centre. Our list of priority applications will be:	ICT and Digital Manager
				• Reviewed on an annual basis (or earlier if an individual system changes) in conjunction with services to determine system criticality	30 September 2021
				• A long term test schedule will be agreed by the IT Management Team and presented to SMT with details of the resources required to meet the critical systems testing schedule.	31 December 2021

Medium	2	**Disaster Recovery Plan Reviews** DRPs have not been reviewed since 2018 which does not comply with the requirement in the ICT and Digital Strategy for DRPs to be subject to annual review.	DRPs may not be fit for purpose.	As agreed in the new ICT and Digital Strategy 2021-24 all DRPs will be reviewed and updated on an annual basis and recorded.	ICT Digital Manager 31 Dec 2021
Low	3	**Overarching Summary of DRPs** There are overarching DRPs for the two data centres which form the core of the ICT data repository and host all applications which are not cloud based. The data centre DRPs include a priority list of recovery actions which cover the infrastructure related tasks necessary to recover the core system environment prior to application recovery. However whilst there are 43 application DRPs there is no overarching document that specifies which application requires one and how these have been identified or prioritised. Therefore it is not possible to determine if DRPs are in place for all critical systems.	Critical systems may not be rapidly recovered in the event of an unforeseen disaster.	The data centre DRPs include a section in the recovery task list for specific priority critical applications which then links out to the application specific DRPs. This existing list of applications and services will be: • Reviewed and extended to ensure we have recovery plans for all critical systems as determined by services and SMT. • Incorporated into the Annual ITMT Work Plan.	ICT Compliance and Security Officer 30 September 2021 30 September 2021
Low	4	**Disaster Recovery Team** The Council has a disaster recovery team which meets every two weeks to discuss issues pertinent to the Council's response in the event of a disaster. No formal agenda or minutes are prepared for these meetings.	Identified actions and issues might not be being addressed timeously	Create Agenda and Minutes of DR fortnightly meetings	ICT Compliance and Security Officer 30 June 2021

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.