Wylie Bisset
Accountants, Business & Tax Advisers

Rosehill Housing Co-operative Limited

Internal Audit 2022-23

IT Systems
May 2023

Overall Conclusion
Strong

TABLE OF CONTENTS

The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.

This report has been prepared solely for Rosehill Housing Co-operative Limited's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.

We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Every sound system of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.

1 EXECUTIVE SUMMARY

Overview

Purpose of review

We undertook a review of the cyber security arrangements in place to ensure that there were appropriate controls in place, and these were operating effectively. Our review sought to provide assurance that there were appropriate security arrangements in place and there was appropriates storage of backup information.

This assignment forms part of our 2022/2023 Internal Audit Annual Plan.

Scope of review

Our objectives for this review were to ensure:

- There were appropriate policies in place to provide governance and control over the Co-operative's IT systems.
- There were appropriate solutions in place to control access to the Co-operative's information systems.
- There were appropriate solutions in place to aid in securing the Co-operative's IT network which were being monitored effectively.
- There were appropriate Disaster Recovery and Business Continuity plans in place for the Co-operative's IT systems that were being tested.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation and where appropriate sample testing.

Limitation of scope

There was no limitation of scope.

1 EXECUTIVE SUMMARY

Background

IT Support Partner
The Co-operative's IT systems are supported by their IT Support Partner, OmniLedger Ltd. The IT Support Partner is ultimately responsible for ensuring hardware is configured for staff, software is kept up to date, and that data is backed up appropriately. The Co-operative's internal and external network activity is appropriately monitored, alerting the IT Support Partner should there be a security breach or an IT equipment failure. Using appropriate Service Desk software, the IT Support Partner can prioritise, manage, and provide an audit trail for internal incidents by utilising a 'ticketing system' to support IT issues and requests. The IT Support Partner is responsible for overseeing the network and ensuring all devices are protected by robust anti-virus/anti-malware solutions.

Policies and Procedures
The Co-operative has a variety of policies and procedures in place to provide governance and control over their IT systems. These include the following:

- Data & ICT Disaster Recovery Plan;
- ICT Acceptable Use Policy; and
- ICT & Data Security Policy.

The above is a mix of policies and plans that are kept up to date. These include information which cover staff responsibilities and guidance on data security.

Entry and Exit Process
The Co-operative has appropriate entry and exit procedures for new starts and leavers to ensure that relevant permissions are in place. These will also ensure that all new users to the network have access to designated areas only.

1 EXECUTIVE SUMMARY

When a staff member leaves the Co-operative, they should no longer have access to the Co-operative's data and systems. To safeguard the integrity of the Co-operative's IT environment, the following exit strategy will be implemented in these circumstances:

- Accounts disabled; and
- Any remote access facilities removed including Microsoft 365 access.

Anti-virus and Anti-malware
The Co-operative's IT Support Partner is responsible for employing robust anti-virus and anti-malware solutions to protect the Co-operative's IT equipment. The Co-operative has 'Sophos Endpoint Security' deployed on all endpoint devices to defend against threats from malicious files and activity. The Co-operative's business-grade firewall offers external protection against threats posed by unsecure websites.

Physical Controls
The Co-operative's network resources and applications are exclusively cloud-based. The Co-operative have no physical servers on-site. However, they do use the cloud-based applications offered by the Microsoft 365 suite of collaborative tools including SharePoint, Teams, and OneDrive. The Housing Management software, Pyramid, is also cloud-based.

Azure AD is used to provide secure authentication and authorisation, allowing staff to access the applications they need. By utilising Azure AD, the Co-operative can enforce conditional access, multi-factor authentication (MFA) and 'single sign on' for users accessing the Co-operative's Microsoft tenancy.

The Co-operative's Head Office is in Glasgow. This office is secured with appropriate physical and environmental protection, with limited access and no unauthorised public footfall.

Efficiencies & Improvements
We commend the Co-operation for having achieved Cyber Essentials accreditation and for their intended participation in the Cyber Essentials Plus assessment. Part of the award requires a visit from a technical body to conduct an audit of the Co-operative's IT systems. The audit includes an internal and external scan of the network, offering assurance to Senior Management that the efficacy of the Co-operative's IT security has been validated by an independent body. Again, we commend the Co-operative for already testing their external network defences by scheduling regular Penetration Tests from a third-party cyber security specialist partner.

1 EXECUTIVE SUMMARY

For all of the good practice that is clearly in place at the Co-operative, we have recommended that they formalise and mandate regular cyber awareness training for staff. The Co-operative has previously conducted similar cyber awareness sessions, and it is their intention to build upon this earlier good practice by scheduling relevant training for the third quarter of 2023. We have raised a recommendation in respect of this, please see **Section 3: Detailed Recommendations** for further information.

1 EXECUTIVE SUMMARY

Work Undertaken

Our work for this review included the following:

Objective 1: There are appropriate policies in place to provide governance and control over the Co-operative's IT systems.

- We held discussions with the Co-operative to establish the current arrangements in place.
- We reviewed the Co-operative's policies and procedures to assess whether these are robust and in line with best practice.

Objective 2: There are appropriate solutions in place to control access to the Co-operative's information systems.

- A review of IT security, access control and user policies for adequacy.
- A review of the Co-operative's anti-virus/ anti-malware software including web protection.
- A review of the Co-operative's data leakage prevention controls and monitoring. **Please see Section 3: Detailed Recommendations for further information.**

Objective 3: There are appropriate solutions in place to aid in securing the Co-operative's IT network which are being monitored effectively.

- A review of the Co-operative's network security appliances and monitoring. **Please see Section 3: Detailed Recommendations for further information.**
- A review of the Co-operative's network access controls including user account controls, remote access, and third-party access.

Objective 4: There were appropriate Disaster Recovery and Business Continuity plans in place for the Co-operative's IT systems that were being tested.

- A review of the Co-operative's IT Disaster Recovery and Business Continuity planning including the Co-operative's backup strategy.

1 EXECUTIVE SUMMARY

Conclusion

Overall Conclusion: Strong
Following our review, we can provide a strong level of assurance over the Co-operative's IT Systems and their associated policies, procedures, and controls. Although we have raised several good practice points, we have made 2 low grade recommendations for improvement.

Summary of recommendations

Grading of recommendations				
	High	Medium	Low	Total
IT Systems	0	0	2	2

As can be seen from the above table there were no recommendations made which we have given a grading of high.

Areas of good practice

The following is a list of areas where the Co-operative is operating effectively and following good practice.	
1.	The Co-operative regularly test the IT Disaster Recovery provisions that are in place. Business-critical applications are delivered through SaaS (Software as a Service) and are cloud-based. The Co-operative test the efficacy of these solutions and their ability to connect to them by simulating a disaster scenario.
2.	Having moved all business-critical resources into Microsoft 365, the Co-operative has invested in a solution which is protected by multiple layers of fault tolerance, with Microsoft capable of leveraging mechanisms to ensure that services and applications continue to function in the event of a system failure. The Co-operative's IT Support Partner use Acronis Cyber Protect to enhance backup and recovery of the Co-operative's Microsoft 365 tenancy. This streamlines the process to allow the Co-operative to restore files and folders quickly and simply should this be required.
3.	The Co-operative has appropriate documentation detailing the Disaster Recovery arrangements to restore the IT network in the event of a disaster scenario. There is a formally approved 'Data and ICT Disaster Recovery Plan' which details the arrangements in place to mitigate the impact of such an event.
4.	The Co-operative has suitable anti-virus and anti-malware security in place across all endpoint devices. The Co-operative's email security controls are delivered through Microsoft Defender and MessageLabs email security, both of which scan all email and file attachments for activity such as phishing and malware.

1 EXECUTIVE SUMMARY

The following is a list of areas where the Co-operative is operating effectively and following good practice.	
5.	The Co-operative has a robust patching regime in place, with endpoint devices patched on a regular basis and scheduled appropriately. This is the responsibility of the IT Support Partner, who use Microsoft Intune to schedule and monitor these updates. Should Microsoft advise that a patch be applied immediately to guard against a known vulnerability, then the IT Support Partner will prioritise accordingly.
6.	The Co-operative use the services of a third-party provider, namely Bulletproof Cyber Security, to carry out independent Penetration Tests and from there look to address any security related issues that may be highlighted.
7.	There are appropriate change management procedures in place at the Co-operative. The IT Support Partner tests and documents all major network changes to ensure there is a point of reference in the event of any issues or security incidents that occur as a result. All user level changes are recorded by the IT Support Partner, as well as recording issues resolved. All major IT changes require consultation with Senior Management before being applied on the Co-operative network.
8.	The Co-operative has robust monitoring and alerting arrangements in place. This includes the alerting functionality offered by the Sophos anti-virus software that will alert upon unusual endpoint and local network behaviour. The Co-operative's FortiGate firewall has an additional performance monitoring module. This includes intrusion, detection, and prevention engines to help identify and intercept known threats at the earliest possible opportunity.

1 EXECUTIVE SUMMARY

The following is a list of areas where the Co-operative is operating effectively and following good practice.	
9.	The Co-operative has robust processes in place when required to create or disable staff accounts. If a member of staff is starting or leaving the Co-operative, senior Co-operative personnel will contact the IT Support Partner. For those starting employment with the Co-operative, the IT Support Partner will create a user profile, supplying them with access to the requisite applications and adding appropriate network privileges. For leavers, user access is removed immediately or on the date communicated. Licences can then be cancelled, and the information logged and set as completed.
10.	The Co-operative's core IT applications and data reside within the cloud, including data held within Microsoft data centres. These data centres are built with redundant and dual-powered servers, storage, network links and other IT components. These IT components are supplied by multiple, active, and independent sources of power and cooling. The Co-operative still has important IT infrastructure located at their Head Office in Glasgow. Equipment is held in secure areas of the building, with appropriate alarms and fire suppressant equipment located nearby.
11.	The Co-operative has appropriate security in place for users permitted to connect to the Co-operative's resources remotely. For staff accessing these resources, access is limited to Software as a Service (SaaS) applications and the Microsoft 365 suite of collaborative tools including SharePoint, Teams, and OneDrive. The Co-operative benefit from the security and auditing functionality that is natively available on these platforms. Resources are accessed by staff using Active Directory credentials with extra security enforced through Multi-Factor Authentication (MFA). All staff supplied laptops are protected using the encryption solution, BitLocker.

1 EXECUTIVE SUMMARY

The following is a list of areas where the Co-operative is operating effectively and following good practice.	
12.	Wireless access is available and appropriately separated for different users on the network. Access is segregated using Service Set Identifiers (SSID's), with external protection offered by the Co-operative's FortiGate firewall. Access to Co-operative digital resources is secured using existing domain credentials.
13.	The Co-operative has adequate policies and procedures in place to provide governance and control over their IT systems. These include, but are not limited to, the following: ➢ Data & ICT Disaster Recovery Plan; ➢ ICT Acceptable Use Policy; and ➢ ICT & Data Security Policy. These policies are regularly updated.

2 BENCHMARKING

We include for your reference comparative benchmarking data of the number and ranking of recommendations made for audits of a similar nature in the most recently finished internal audit year.

IT Systems

Benchmarking				
	High	Medium	Low	Total
Average number of recommendations in similar audits	1	1	1	3
Number of recommendations at Rosehill Housing Co-operative Limited	0	0	2	2

From the table above it can be seen that the Co-operative has a lower number of recommendations compared to those RSL's it has been benchmarked against.

Staff Cyber Security Awareness			
Ref.	Finding and Risk	Grade	Recommendation
1.	Cyber exercising can help an organisation to understand their staff's preparedness and resilience to cyber-attacks. From there an organisation can develop a targeted training course which can focus on empowering users to take control of their own ability to avoid cyber security malpractice, and to feel like a partner with IT in preventing cyber-attacks. During our review, we were informed that although the Co-operative has delivered cyber security awareness exercises for staff in 2020, this has not been mandated nor has it been made available in the recent past. There is an ever-increasing risk of attackers exploiting human nature with diversionary tactics, such as creating a false sense of urgency or impersonating trusted people. The risk of not investing in cyber security training for staff is that it could leave your frontline defence unprepared and exposed against such cyber-attacks.	**Low**	We recommend that the Co-operative builds upon previous good practice by delivering a robust, mandatory cyber awareness training programme for all staff. Cyber-attacks are becoming increasingly prevalent, with 31% of UK organisations reporting that attacks, including phishing, occur more than once per week. Appropriate training will help empower staff with the knowledge and the tools to recognise cyber threats and from there make informed and educated choices. We acknowledge the Co-operative's intention to develop and deliver a training programme, and that there is an active project underway to ensure that it is mandated and scheduled for all staff by Autumn 2023.

Management response	Responsibility and implementation date
Have identified Cyber Security Awareness Training through an online company we use – High Speed Training. This or if other appropriate training is identified in the coming months will be added to the mandatory training programme for staff and will be carried out on an annual basis. Some training will be undertaken by the Mgt Team using Exercise in a box from NCSC – one table top exercise and at least 3 micro exercises.	*Responsible Officer:* Director *Implementation Date:* Online module for all staff will be completed by end of June 2023 Exercise in a box sessions will be carried out by Mgt Team by end of September

Data Leakage Prevention			
Ref.	Finding and Risk	Grade	Recommendation
2.	DLP (Data Leakage Prevention) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. Following our review, we believe improvements could be made to prevent data leakage. It is acknowledged that the use of unmanaged USB storage devices is discouraged within the Co-operative's ICT Acceptable Use Policy documentation. However, we recommend that this advice is bolstered by anti-leaking measures that includes controls around unmanaged USB storage device use, and filtering rules that prohibit access to unmanaged file sharing websites such as Dropbox. Data could be removed from the network by members of staff via unmanaged file sharing websites which poses a risk to the Co-operative. This could result in a General Data Protection Regulation breach, with the risk of associated fines	**Low**	We recommend that a risk assessment which considers DLP is conducted to ensure that any areas of risk, such as the use of unmanaged USB storage devices and access to unmanaged file-sharing websites, are assessed and that subsequent solutions are considered. The IT Support Partner may then be tasked with providing additional security controls to mitigate these risks, helping the Co-operative to reduce the likelihood of deliberate or accidental data leakage.

	and/or damage to the Co-operative's reputation.		
Management response			Responsibility and implementation date
Have begun discussions with our IT Company, Omniledger and are exploring feasibility of web filtering software to prohibit use of sharing sites such as dropbox. Also exploring feasibility of disabling usb ports on laptops. Aiming to be in a position by end of September about whether such options are feasible and can be implemented or alternatives are needed.			*Responsible Officer:* Director *Implementation Date:* By end of September 2023

4 AUDIT ARRANGEMENTS

The table below details the actual dates for our fieldwork and the reporting on the audit area under review. The timescales set out below will enable us to present our final report at the next Audit Sub Committee meeting.

Audit stage	Date
Fieldwork start	16 May 2023
Closing meeting	25 May 2023
Draft report issued	29 May 2023
Receipt of management responses	7 June 2023
Final report issued	13 June 2023
Audit Sub Committee	28 June 2023
Number of audit days	3

5 KEY PERSONNEL

We detail below our staff who undertook the review together with the Co-operative staff we spoke to during our review.

Wylie & Bisset LLP			
Partner	Graham Gillespie	Partner	graham.gillespie@wyliebisset.com
Manager	Scott McCready	Internal Audit Manager	scott.mccready@wyliebisset.com
Auditor	Kevin McDermott	Senior IT Auditor	kevin.mcdermott@wyliebisset.com

Rosehill Housing Co-operative Limited			
Key Contacts:	Geri Mogan	Director	geri.mogan@rosehillhousing.co.uk
	Josh Button	Technical Support Engineer – OmniLedger Ltd	joshua.button@omniledger.co.uk
Wylie & Bisset appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation.			

APPENDICES

A GRADING STRUCTURE

For each area of review, we assign a level of assurance in accordance with the following classification:

Assurance	Classification
Strong	Controls satisfactory, no major weaknesses found, no or only minor recommendations identified.
Substantial	Controls largely satisfactory although some weaknesses identified, recommendations for improvement made.
Weak	Controls unsatisfactory and major systems weaknesses identified that require to be addressed immediately.
No	No or very limited controls in place leaving the system open to significant error or abuse, recommendations made require to be implemented immediately.

A GRADING STRUCTURE

For each recommendation, we assign a grading either as High, Medium, or Low priority depending on the degree of risk assessed as outlined below:

Grading	Classification
High	Major weakness that we consider needs to be brought to the attention of the Audit Sub Committee and addressed by Senior Management of the Co-operative as a matter of urgency.
Medium	Significant issue or weakness which should be addressed by the Co-operative as soon as possible.
Low	Minor issue or weakness reported where management may wish to consider our recommendation.

B ASSIGNMENT PLAN

Purpose of review

We will undertake a review of the cyber security arrangements in place to ensure that there are appropriate controls in place, and these are operating effectively. Our review will seek to provide assurance that there are appropriate security arrangements in place and there is appropriates storage of backup information.

This assignment forms part of our 2022/2023 Internal Audit Annual Plan.

Scope of review

Our objectives for this review are to ensure:

- There are appropriate policies in place to provide governance and control over the Co-operative's IT systems.
- There are appropriate solutions in place to control access to the Co-operative's information systems.
- There are appropriate solutions in place to aid in securing the Co-operative's IT network which are being monitored effectively.
- There are appropriate Disaster Recovery and Business Continuity plans in place for the Co-operative's IT systems that are being tested.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation and where appropriate sample testing.

Limitation of scope

There is no limitation of scope.

Audit approach

Our approach to the review will be:

- Discussion with relevant staff involved to establish the current arrangements in place.
- Review of IT security, access control and user policies for adequacy.
- Review of the Co-operative's strategy for identifying and addressing system vulnerabilities in a secure and timely manner.
- Review of the Co-operative's anti-malware/virus software including web protection.
- Review of the Co-operative's network security appliances and monitoring.
- Review of the Co-operative 's data leakage prevention controls and monitoring.
- Review of the Co-operative's network access controls including user account controls, remote access, third party access.
- Review of the Co-operative's IT disaster recovery and business continuity planning including the Co-operative's backup strategy.
- Review of the Co-operative's IT equipment to ensure suitability.
- Review of the service received from the Co-operative's IT providers to ensure this is appropriate.
- Review of the Co-operative's IT strategy and reporting mechanisms.
- Sample testing of controls where applicable.

Potential key risks

The potential key risks associated with the area under review are:

- There are no/inadequate policies in place to provide governance and control over the Co-operative's IT systems.
- There is a lack of/inadequate controls in place to control access to the Co-operative's information systems.
- Security solutions in place to protect the Co-operative are ineffective and/or not being monitored appropriately.
- Disaster Recovery and Business Continuity procedures are ineffective, un-tested and not in line with the Co-operative's Business Impact Analysis.