Argyll and Bute Council

Internal Audit Report

May 2022

FINAL

ICT Remote Working

Audit Opinion: Substantial

	High	Medium	Low	VFM
Number of Findings	**2**	**0**	**3**	**0**

CHOOSE ARGYLL. LOVE ARGYLL.

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 2021/22 internal audit plan, approved by the Audit & Scrutiny Committee in March 2021, we have undertaken an audit of Argyll and Bute Council's (the Council) system of internal control and governance in relation to ICT Remote Working.

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 is the second largest local authority in Scotland covering an area of 691,000 hectares, however, it has the third sparsest population density of approximately 88,000 of which 17% live on 23 inhabited islands. The size of the area and population dispersion require multiple communications facilities to ensure services are available to users. Across this vast area, the Council employs 4,435 members of staff, 1,980 of whom have an active user account providing them with access to the Council's corporate network and systems.

5. The Council has recognised a need for modern working practices and in 2011 implemented a policy for 'alternative ways of working' and flexible working options. Employee's ICT user accounts are managed by ICT and enable working from home via a virtual private network (VPN) connection which is included as part of the standard software package installed on Council owned laptops. Prior to the COVID-19 pandemic, an average of 80 - 100 employees made use of the facility to work from home on an occasional basis rising to around 200 - 250 during periods of severe weather conditions.

6. On 23 March 2020 the UK government announced that all employees should work from home where possible in response to the COVID-19 pandemic. The Council's ICT services were therefore required to very quickly roll out remote working to all staff who are able to work from home to enable continuity of service provision, thus creating an additional strain on existing resources and ICT infrastructure. In the period immediately following this announcement around 1,300 employees were accessing the Council's network and systems via VPN settling to around 800 – 900 as time progressed.

7. The resulting increase in remote working heightens existing cybersecurity risks and introduces new ones to many organisations when staff are working outside of their normal office environment. Phishing emails for example have increased 600% during the pandemic with all sectors and individuals being targeted.

8. The General Data Protection Regulation (GDPR) came into force in 2018 and applies to all organisations that use personal data, any breach of data protection rules is a very serious matter and can incur substantial fines and other sanctions on the Council.

9. The Council has a legal duty of care to ensure the health, safety and wellbeing of its workforce. As part of this duty, the Council has prepared an employee wellbeing strategy to improve the overall wellbeing of the workforce both within and out with the workplace, they also seek to ensure that employees are protected from potential health hazards caused by the use of display screen equipment, and therefore, equipment provided should be suitable for the user's needs and workstation assessments periodically carried out.

Scope

10. The scope of the audit was to assess the adequacy of policies, procedures and guidance relating to future remote working arrangements as outlined in the Terms of Reference agreed with the Head of Customer Support Services on 8 February 2022.

Risks

11. The risks considered throughout the audit were:

- SRR11: Service Delivery – Cyber Security
- EDI ORR46: Cyber Security Breach and associated cyber-attack cause catastrophic loss of ICT systems, loss of sensitive data, loss of services, Financial risk; Failure to maintain ICT assets to provide secure services in a high risk cyber environment
  Systems not kept updated or maintained properly resulting in weakness in cyber security
- EDI ORR47: Lack of capacity to meet unplanned demand for communications support with existing resources
- LRS ORR2: Failure to ensure Council compliance with governance and information management arrangements
- LRS ORR14: Failure to provide high quality and timely health and safety advice both internally and externally to customers
- Audit Risk 1: Failure to comply with GDPR requirements

Audit Opinion

12. 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.

13. 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

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

    - Education Management Circular 1.18 should be revised to remove the requirement for parental consent forms to be completed
    - Education management should identify an alternative means of enabling teachers to access ICT resources and instruct the Council's ICT Services to stop access to the Education webmail service from personal devices
    - Management should ensure that employees are completing the mandatory GDPR modules
    - Management should consider providing access to health and safety resources on the employee website, MyCouncilWorks
    - Health and wellbeing documents and links available on MyCouncilWorks should be reviewed to ensure it includes all information provided on the Hub intranet site

15. 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

16. 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	Policies, procedures and guidance are in place for remote working to ensure Council's data and systems are safe from unauthorised access.	SRR11 EDI ORR46 EDI ORR47	Substantial	Policies and procedures are in place and being followed with the exception of Education Management Circular 1.18 where parental consent for internet access is no longer obtained. Accreditation for Cyber Essentials Plus and Public Sector Network has been renewed annually for the corporate network indicating that appropriate infrastructure and software are in place to ensure confidentiality, integrity and availability of Council data, improvements are planned to mitigate risks to the security of the Education network. Training modules have been made available to users of Council provided devices and reminders to be vigilant of phishing emails are periodically issued. Teaching staff make use of the Education Webmail service using personal devices which is out with

				the control of Council security measures. Survey results indicate that overall performance of the ICT service has remained high with the Council ranked top in Scotland and placed in the top quartile within the UK.
CO2	Policies, procedures and guidance are in place for remote working to ensure Council's compliance with GDPR.	LRS ORR2 Audit Risk 1	Limited	Procedures, guidance and learning materials have been prepared and made available to employees to ensure compliance with GDPR, however, only 21.4% of employees have completed the learning modules during 2021.
CO3	Policies, procedures and guidance are in place for remote working to ensure the Council is undertaking its duty of care to ensure health, safety and wellbeing of its employees.	LRS ORR14	Substantial	Health and Safety policy, procedures and guidance have been prepared and made available to employees on the Council's intranet site, the Hub, however these are not available on MyCouncilWorks. Display screen assessments are completed periodically by employees, reviewed by management and issues addressed where possible. A Wellbeing Strategy, associated documentation and learning materials have been prepared, however there are some inconsistencies in availability on the Hub and MyCouncilWorks platforms. The Employee Assistance Programme is successful with 9% of employees accessing services provided and surveys indicate positive feedback in terms of wellbeing, working from home and customer satisfaction.

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

3. Detailed Findings

Policies, procedures and guidance are in place for remote working to ensure Council's data and systems are safe from unauthorised access.

18. The Council has an up-to-date ICT acceptable use policy (AUP) in place that requires all employees with a need to access the council's networks, systems and communications devices to complete the form in agreement that they will comply with the terms and conditions outlined. This agreement must be authorised by managers and submitted to ICT services prior to access being arranged. In addition, there is a social media policy with an application form and other request forms for additional media and systems not covered in the AUP.

19. ICT services check that AUP forms are appropriately completed, signed and authorised prior to creating the relevant user accounts including email, VPN, network and active directory to access files stored on the Council's network. Access to specific systems is controlled by system administrators and is arranged independently of ICT services. Managers are delegated with responsibility to ensure ongoing compliance with the AUP within their teams, non-compliance is an HR matter and ICT may be asked to provide evidence to support disciplinary action.

20. A recent internal audit review tested AUPs, therefore a small sample of four APTC and four Teachers was reviewed to ensure ongoing compliance, and these were found to have been completed satisfactorily. A sample of the same size of leavers was also tested to ensure notifications of termination were promptly passed to ICT services and all ICT related user accounts closed down, this was also found to be satisfactory.

21. When working from home, access to the Council's network and systems is achieved through the use of a Virtual Private Network (VPN) connection. On completion of the appropriate forms, third parties such as system support contractors can also gain access via VPN by prior arrangement for short periods of up to one week.

22. School pupils are expected to comply with the content of education management circular 1.18 'Use of GLOW and internet' and also their school handbook. The circular advises that an attached consent form should be completed and returned, however the form is no longer included in the circular and we have been advised that it is not currently being used.

23. The parental consent form was discontinued from use in 2018 as use of the internet and Glow are considered to be integral to school life and there is no longer a need to ask for permission from parents for their children to access standard education tools. The School Handbook has been updated to include acceptable use of these resources following consultation with the Governance and Risk Manager, however, Education Management Circular 1.18 continues to require a consent form to be completed.

Action Plan 3

24. Education provide ICT services with a list of pupils for whom an email account is to be created at the start of each new academic year and this is used to access GLOW and the internet. ICT are notified when there is a change of circumstances requiring an account to be terminated or information updated.

25. Cyber Essentials Plus is an effective Government backed scheme that helps protect against the most common cyber-attacks. The Council demonstrates a commitment to cyber security on its corporate network through compliance with the elements contained in the published toolkit and independent verification. Re-accreditation was achieved in November 2021. The Council's education network is less robust as there are insufficient resources in schools to ensure the criteria can be met. Education Services are aiming to improve the security of their network and are actively working on proposals to invest substantially to mitigate the risks.

26. The Council's corporate network links to the Public Services Network (PSN), the Governments high-performance network which helps public sector organisations in Scotland work together, reduce duplication and share resources. The Council has maintained access to this network by complying with the code of connection which entails a more stringent set of criteria than Cyber Essentials Plus.

27. The PSN code of connection requires that an annual exercise takes place to assess the strength of user passwords to ensure the network is protected against compromise. A decision has been made to increase the frequency of this exercise to twice yearly and has been assigned to the ICT Security Officer for action. In November 2021, a small number of system users were found to have created weak passwords and were enforced by the system to change these to a stronger password at next login.

28. Laptops issued to users are encrypted and built to a standard specification that includes an operating system and all of the necessary software to provide security and perform work tasks, if any additional approved software is required, it can be added by prior arrangement. Each laptop provided by the Council has a unique certificate installed that is registered on the Council's network and verified as part of the user's login process, unregistered devices will not be able to connect to the network. Additionally, connection can only be achieved using an on premise IP address or via a valid VPN account from a remote location.

29. Each user is required to have a valid active directory account created by ICT services with a unique username and password to access the network, privileged users with additional access rights require a further level of multi-factor authentication (MFA) and this is achieved by phone call from ICT services.

30. Local Authorities are at high risk of cyber-attacks, they are regularly targeted to gain unauthorised access to the network and systems. The Council receives many unauthorised attempts which are notified to ICT services via the Firewall's external threats report or network perimeter security report, such access attempts are locked down or the device located and its port of access closed. ICT services will also monitor and investigate reports of attempted access to internet facing systems on the firewall and intrusion detection system and suspicious internal traffic flagged by it. The anti-virus system generates an alert when a problem is identified and the device is immediately removed from the network and recovered by desktop support staff for analysis and cleaning.

31. Systems and processes are working well protecting the Council's ICT infrastructure and assets, however, cyber-attacks are increasing in both volume and complexity and there is no guarantee that every attempt will be intercepted by the measures in place. Users, therefore, must also be vigilant and report suspicious activity on their systems or email traffic.

32. Council staff are regularly reminded of the need to be vigilant via corporate emails and the Council's intranet site (Hub) banner contains a reminder regarding phishing attacks and provides further information by following the link provided. The Hub provides additional guidance and self-help documents to assist employees with ICT related issues such as working from home tips, password guidance and mobile device management. The Council also operates a Learn Online (LEON) platform which contains modules pertaining to, cyber security, social media awareness, Stay safe online and GDPR.

33. The Council does not operate a Bring Your Own Device (BYOD) policy, although a few systems such as LEON are independent of the Council's network and may be accessed from personal devices.

34. The majority of teaching staff do not have their own dedicated Council supplied device and therefore make use of the Education Webmail application accessible from personal devices. There is no means of preventing download of information to the device being used and security settings are out with the control of ICT services.

Action Plan 1

35. To enable remote working, an employee must have a laptop computer with VPN software installed and access to a broadband service as a minimum. Laptops require to meet a minimum specification standard to ensure they can cope with all the systems required and are therefore purchased over the Scottish Government framework to achieve best value. Occasionally laptops are required to have additional specifications and these are purchased specially for the purpose defined e.g. architects require additional graphics. Other equipment can be provided as required such as additional monitors, keyboards etc.

36. Prior to COVID-19 lockdown arrangements commencing on 23 March 2020 around 70% of devices used across the Council were laptops, an additional 155 corporate laptops were issued to those who used desktop computers to enable them to work from home. Laptops will be the default device purchased in future unless there are specialist reasons.

37. There was no additional funding available to fund purchase of additional laptops, therefore the 155 laptops were drawn from those purchased under the laptop replacement programme for 2020 resulting in those due to be replaced being rescheduled to 2021. Employees were able to take home equipment such as monitors, keyboards etc. as required from the office in addition to their laptop.

38. VPNs were used mostly on an occasional basis prior to 23 March 2020 resulting in a requirement for ICT services to create an additional 800 – 1,000 VPN accounts to enable users to work from home on an ongoing basis. A corporate email advised employees of VPN etiquette to ensure sufficient bandwidth was available for all users and the Tactical group received regular reports to monitor VPN usage and bandwidth capabilities. Additional bandwidth was diverted to support increased VPN usage and split tunnelling was implemented to enable access to MS365 applications out with the VPN environment in line with published guidance.

39. All non-essential ICT developments and projects were paused at the initial response to COVID-19 to redeploy engineers on the service desk frontline to provide additional support, communications assistance and build laptops for those who did not already have them.

40. The service desk extended its availability to 8am to 6pm to assist employees in the transition to homeworking, however has now reverted to previous times as the demand for assistance decreased. Performance measures associated with the time taken to resolve issues reported to the ICT service desk improved during this period and has been maintained.

41. The Society for Innovation, Technology and Modernisation (SOCITM) conduct a benchmarking survey every 2 years to compare our performance against other participating Government organisations across Scotland and the UK, alternate years there is a customer satisfaction survey. The most recent benchmarking survey took place during 2019 when the Council achieved the top score in Scotland and a top 10 place in the UK with a placing in the top quartile. Customer satisfaction has remained consistently high.

Policies, procedures and guidance are in place for remote working to ensure Council's compliance with GDPR

42. GDPR came into force on 25 May 2018 and as a result the Council has prepared a set of procedures and guidance and made them available on the Hub for all members of staff to view. The Information Commissioners Office requires that training is in place to ensure compliance with GDPR. Mandatory training and annual refresher modules have been prepared and made

available on LEON for employees with access to the Council's network and systems to complete. The training modules are regularly reviewed and updated, the GDPR module must be completed once and the refresher module must be completed annually.

43. The target is for 90% of employees with access to the Council's network and systems to complete the training. ICT services have advised that there are 1,980 corporate user accounts and 2,050 education user accounts, a report generated by Human Resources and Organisational Development (HROD) indicates that in 2021, 342 employees have completed the GDPR module and 520 have completed an annual refresher, this amounts to 21.4% of employees with a user account therefore falling below the 90% target.

Action Plan 2

44. Sensitive information stored on the Council's network and systems is secure and accessible by authorised employees via corporate and system specific security arrangements. There is an aspiration to maintain all records digitally in future, however, some hard copy files are still in use e.g. Social Work. Hard copy files are not removed from Council premises unless absolutely necessary, this requires authorisation from senior management and a record of removal and return is maintained.

Policies, procedures and guidance are in place for remote working to ensure the Council is undertaking its duty of care to ensure health, safety and wellbeing of its employees

45. The Council's Health and Safety Policy states that line managers are responsible for "doing all that is reasonably practicable to ensure the health, safety and welfare of their staff and those affected by their work activities" and "assessing risks and for making sure that the work controls identified by risk assessments are implemented". The policy also states that employees must co-operate. A range of policy and guidance documents are available on the Hub for employees to access, however, these are not available on the staff website "MyCouncilWorks".

Action Plan 4

46. Display screen equipment (DSE) includes laptops, monitors and mobile devices and the risks associated with prolonged and continuous use can be significant. In line with service level Health and Safety work plans, managers are required to ensure that employees undertake periodic DSE assessments and confirm to senior management that these have been completed and any issues raised that can be resolved have been addressed. Occasionally issues raised will be referred to health and safety and occupational health officers for additional assessment and remediation.

47. The DSE form has been adapted for home working and will be further reviewed when hybrid working arrangements are implemented. A record of assessments completed, issues raised and actions taken for one service was reviewed and found to comply with the requirements as set out in the guidance.

48. A Wellbeing Strategy has been prepared for 2019-24, it refers to all aspects of the employee's life and is based on the three pillars of wellbeing, mental and emotional wellbeing, physical wellbeing and financial wellbeing. The strategy has been published on the Hub for all networked staff to view, however, it is not available on MyCouncilWorks.

49. Policies, procedures, guidance and Information documents have been prepared and made available to employees on the Hub and MyCouncilWorks to assist employees, however, some links to information are missing on MyCouncilWorks and one link does not work.

Action Plan 5

50. Nineteen learning modules have been prepared and made available to employees on LEON covering a range of health and wellbeing topics.

51. A weekly bulletin, "Wellbeing Wednesday" is prepared and published on MyCouncilWorks, each issue contains information on a new topic, recognises global and national campaigns, and highlights special causes or increase awareness of specific health and wellbeing topics.

52. The Council offers access to an Employee Assistance Programme provided by Health Assured consisting of a helpline operated by experienced counsellors, legal and financial specialists, incident advice and support, an online health portal and smartphone app and regular counselling and management support. The uptake of services provided is in line with benchmarking information.

53. Employee wellbeing surveys took place in June and October of 2020 and again in September 2021 with most employees rating their overall wellbeing in positive terms and were aware of support measures available to them. Some common themes for improvement were identified as a result of the survey and have been addressed.

54. In November 2020, HR conducted a homeworking survey to gather feedback from managers to assess their perceived level of success of homeworking arrangements. Responses were received from 159 managers who indicated positive results for communicating and maintain regular contact with their team and supporting their team's wellbeing, however responses were less positive in terms of induction of a new team member.

55. Employee surveys also took place in November 2020 (912 responses) and May 2021 (886 responses). Positive feedback was received from both surveys in terms of support provided by managers and ease of working from home and 70% of respondents said they would be happy to work from home three or more days per week.

56. Customer feedback was also gathered at this time with 981 responses received. Results were positive indicating an overall high level of customer service satisfaction despite the COVID-19 restrictions.

57. Following these surveys, managers were asked to gather information from their teams and advise the Modern Workspace project team of the identified requirements in terms of returning to the office, whether this be full time, hybrid or not at all. The results indicate that 76.1% of employees are satisfied with working from home and wish to continue to do so to some extent.

58. There were no specific actions addressed as a result of these surveys although a number of themes were identified that will be taken forward within the "My Modern Workspace" project and will be included in the soon to be finalised hybrid working policy.

Appendix 1 – Action Plan

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
High	1	**Education Webmail** The majority of teaching staff do not have their own dedicated Council supplied device and therefore make use of the Education Webmail application accessible from personal devices. There is no means of preventing download of information to the device being used and security settings are out with the control of ICT services.	High level of cyber security risk to the Council. Failure to comply with GDPR which may lead to financial penalties and reputational damage.	Education management plan to instruct ICT Services to stop access to use of Education webmail service from personal devices once an alternative means of enabling teachers to access ICT services has been implemented.	Digital Lead – Education 31 March 2023
High	2	**GDPR Training and annual refresher** 21.4% of employees with a user accounts have completed the mandatory or refresher GDPR modules in 2021, falling below the target of 90%.	Failure to comply with GDPR which may lead to financial penalties.	An email will be issued to all networked employees reminding them of the requirement to complete the mandatory or refresher GDPR modules on LEON by 31 March 2023.	Governance and Risk Manager 31 March 2023
Low	3	**Education Management Circular 1.18 – Use of Internet and Glow** The circular requires parental consent for pupils to access the internet and GLOW, however, this form is no longer required.	Information for parents provided on the Council's website is not current.	Education Management Circular 1.18 will be updated to reflect current requirements.	Digital Lead – Education 31 August 2022

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Low	4	**Health and Safety information** Health and safety information available on the Hub is not currently available on MyCouncilWorks for users with no access to the Council's network.	Council employees may be unable to reference policy and guidance information where access to the HUB is not possible.	Health and Safety Officer will liaise with Communications Team and arrange for relevant information to be replicated on MyCouncilWorks.	Health and Safety Officer 30 June 2022
Low	5	**Wellbeing information** The Wellbeing Strategy and some links to further guidance and information are not provided on MyCouncilWorks and one link does not work.	Council employees may be unable to obtain relevant assistance information where access to the HUB is not possible.	Wellbeing Strategy will be added to the MyCouncilWorks page and the addiction link repaired. Content of the Wellbeing Pages on MyCouncilWorks will be reviewed as part of the Wellbeing Work plan. This will be a rolling piece of work to gradually put all relevant information across.	HR Service Centre Team Leader 31 May 2022 31 December 2022

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.