Argyll and Bute Council

Internal Audit Report

June 2023

FINAL

Cyber Security

Audit Opinion: Substantial

	High	Medium	Low	VFM
Number of Findings	**0**	**5**	**1**	**0**

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 2022/23 internal audit plan, approved by the Audit & Scrutiny Committee in March 2022, we have undertaken an audit of Argyll and Bute Council's (the Council) system of internal control and governance in relation to cyber security.

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 has an ICT and Digital Strategy in place covering the years 2021-2024. This document outlines the aim to position Argyll and Bute Council (the Council) as a "digital by default" authority providing services to support people and customers to work better together and create efficiencies, savings and improved services for all. The aims of the strategy are:

   - Our networks and systems are secure, accessible, current, and enable delivery of council and service objectives
   - ICT provides value, and enables and empowers both customers and staff to make tasks easier
   - Our people have the knowledge and capabilities to use ICT effectively

5. Our working environment has changed significantly over the last three years placing more reliance on digital technologies to enable remote working which in turn raises additional risks to data and networks in terms of cyber security.

6. Cyber security is essential when using digital technology as confidentiality, integrity and availability of Council and customer data requires to be maintained as well as measures to prevent it falling into the wrong hands as this would result in financial penalties imposed by the Information Commissioner's Office (ICO) as well as considerable reputational damage.

7. Human error/behaviour is a major factor in cyber security, cyber attackers consider various vulnerabilities when trying to gain access to an organisation's systems and data and people are often found to be the weakest link.

8. Cyber attacks are increasing rapidly, they take different forms, and if successful, the effects can be severely disruptive and create a huge financial burden. There are many recent examples of public sector organisations who have become victims of such attacks.

9. In order to conduct business with other public bodies, the council is required to access the Public Sector Network (PSN) to enable secure exchange of sensitive information. A code of connection

is required to be complied with and an independent annual IT health check undertaken to verify compliance. The Council is also encouraged to adhere to other non-statutory but recommended frameworks including Scottish Public Sector Cyber Resilience Framework.

10. There is a legal requirement to meet the Payment Card Industry – Data Security Standards (PCI-DSS). The Council retains very little payment card information and therefore is required to complete the least onerous self-assessment questionnaire.

11. Any significant cyber incident is required to be reported to Scottish Government for a centrally co-ordinated response to take place in line with published Scottish Public Sector Cyber Incident Central Notification and co-ordination Policy.

12. The Council has an ICT Compliance & Security Officer (ICT-CSO) in place with overarching responsibility for cyber security (among other duties), however, all members of staff have a responsibility for cyber security within their day-to-day working practices.

Scope

13. The scope of the audit was to review systems and processes in place to determine if adequate resources are in place to support security of key systems as outlined in the Terms of Reference agreed with the Head of Customer Support Services on 21 April 2023.

Risks

14. The risks considered throughout the audit were:

- SRR11: Service Delivery – Cyber Security
- EDI ORR 46: 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
- Audit risk 1: Available resources may be insufficient to maintain resilience and manage a cyber security incident

Audit Opinion

15. We provide an overall audit opinion for all the audits we conduct. This is based on our judgement on the level of assurance which we can take over the established internal controls, governance and management of risk as evidenced by our audit work. Full details of the five possible categories of audit opinion is provided in Appendix 2 to this report.

16. 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

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

- Regular reports summarising cyber security risks, activity and incidents managed should be reintroduced to DMT to continue visibility and submitted at agreed intervals, these reports should be escalated to SMT when relevant.
- The Cyber Security Policy should be completed, approved and published on the Council's intranet site for Elected Member and employee reference.
- The level of resource allocated to manage the Council's cyber security requirements should be reviewed.
- Members Services and managers should be provided with monitoring reports and encourage completion of the brief Mimecast training provided.
- The Cyber Incident Response Plan, Disaster Recovery Plans and Playbooks should be subject to regular review, annually as a minimum.
- A specific budget provision for cyber security should be agreed.

18. 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

19. Exhibit 1 sets out the control objectives identified during the planning phase of the audit and our assessment against each objective.

Exhibit 1 – Summary Assessment of Control Objectives

	Control Objective	Link to Risk	Assessment	Summary Conclusion
1	Arrangements are in place to protect key systems and data from cyber attacks	All risks	Substantial	The Council's Acceptable Use Policy was revised and approved by Policy and Resources Committee. Senior Management Team (SMT) review and update cyber risks and their treatment every six months and Information Technology Management Team (ITMT) review monthly reports on cyber security key performance information (KPI) and highlights of new risks identified in the cyber environment, however, these are not summarised to raise awareness at Department Management Team (DMT) or SMT. The ICT and Digital Strategy 2021-24 has been published, however, it refers to a cyber security policy that has not yet been completed. The Council has achieved compliance with the Public Sector Network (PSN) Code of Connection for 2023/24 and reaccreditation for Cyber Essentials Plus. Information is actively shared with other local authorities via the Cyber Security Information Sharing Platform (CiSP) and meetings and conferences are attended. The ICT

				Compliance and Security Officer (ICT-CSO) is consulted where any major ICT projects or upgrades are required to take place.
2	Cyber security is appropriately resourced and employees are trained to manage vulnerabilities within their control	All risks	Reasonable	The ICT-CSO holds the CompTIA Security+ certification and is responsible for cyber security and related incident management, however, the officer has additional responsibilities outwith cyber security. An incident response team has been identified, however, there is no depute appointed in the event the ICT-CSO is unavailable. The majority of other local authorities contacted have additional resource employed to manage the increasing cyber security workload advised by the National Cyber Security Centre (NCSC), additionally there is no specific budget allocated to cyber security. Appropriate partnership working is in place both within the Council and externally. Users of ICT facilities are advised of their responsibilities within the AUP and periodic reminders, additional training is provided to all users monthly but this has not been completed in all instances.
3	Arrangements are in place to manage cyber security incidents	All risks	Substantial	A comprehensive Cyber Incident Response Plan, Playbooks and Disaster Recovery Plans are in place, however, they require to be reviewed. A cyber incident response exercise took place in March 2022 with positive feedback included within the de-brief report.

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

3. Detailed Findings

Arrangements are in place to protect key systems and data from cyber attacks

21. The Council’s ICT Acceptable Use Policy applies to all users of Council devices and outlines the requirements to comply with its content to preserve the confidentiality, integrity, availability of information held and comply with relevant legislation. This policy was updated and approved at the Policy and Resources Committee in October 2021 and its contribution to mitigating cyber security risks acknowledged.

22. Strategic and Operational Risk Registers contain high-risk entries for cyber security, they are linked to the corporate outcomes and service plans and contain details of treatment and mitigating actions to address these. These risks are discussed at the Senior Management Team (SMT) every 6 months and updated as required following discussions with the appropriate officers.

23. Senior management have been provided with four reports in respect of cyber security over the last two years:

    - two to the Department Management Team (DMT), one advising of completion of a previous audit action and one informing of successful re-accreditation of Cyber Essentials Plus.
    - one to the SMT providing an ICT Security Service Highlight Report including an update on important service activity, a summary of high-profile threats in the general ICT environment and a statistical analysis of the Council's performance in thwarting targeted attacks via technology solutions over the period of one month (20 December 2021 – 19 January 2022)
    - one to the Policy Lead containing summarised updates on cyber security activities that have taken place.

24. The Information Technology Management Team (ITMT) are provided with monthly reports highlighting new high-profile risks in relation to cyber security in addition to a summary of activities taking place and statistical analysis of recent incident management, this is not currently shared with DMT or SMT at regular intervals or via an annual report.

Action Plan 1

25. The Council has a comprehensive ICT and Digital Strategy 2021-24 in place, this includes a section on "secure and compliant infrastructure" which makes reference to a Cyber Security Policy but this has not yet been completed.

Action Plan 2

26. The Council has obtained certification in compliance with the Public Sector Network (PSN) Code of Connection for 2023/24. This allows communications to be shared with other local authorities in a safe and secure manner.

27. Reaccreditation has also been obtained for Cyber Essentials Plus demonstrating compliance with the Scottish Public Sector Cyber Resilience Framework. This is not a statutory requirement, however, it is recommended and the Council is one of only two who have achieved this challenging accreditation.

28. The Council actively participates in the Scottish Local Authority – Information Security Group (SLA-ISG), officers attend meetings and make use of its secure message board on the Cyber Security Information Sharing Partnership (CiSP) to share good practice and stay up-to-date with current developments in cyber security. Officers also attend conferences providing information on relevant subject matter to remain up-to-date in the wider cyber security environment. E.g. FurureScot Cyber Security 2023 Conference was attended in February providing information from leaders in cyber security both in the UK and abroad.

29. Key performance information (KPI) is gathered to assess alignment with operational targets, this, along with additional performance information, current risk and developments etc. is presented for discussion monthly at ITMT.

30. The ICT-CSO is consulted where any major ICT projects and upgrades are required to take place. A standard questionnaire is issued to suppliers to gather information on system specifications and checked for embedded security features. A Data Protection Impact Assessments (DPIA) is required to be completed for any system containing personal data to ensure compliance with General Data Protection Regulations (GDPR) and a review of Disaster Recover Plans (DRPs) is required for any major change taking place.

Cyber security is appropriately resourced and employees are trained to manage vulnerabilities within their control

31. Responsibility for Cyber Security is assigned to the ICT-CSO, however, this is not their only work remit. The ICT-CSO has successfully achieved the Computing Technology Industry Association (CompTIA) Security+ certification which is a globally recognised entry level qualification and funding from ScotlandIS Cyber Upskilling Fund has been secured to train a further six members of staff in this qualification to provide resilience across the service.

32. The responsibility for responding to a cyber incident falls to the ICT-CSO who is the incident manager and primary point of contact. An Incident Response Team has been identified and recorded on the Cyber Incident Response Plan with each officer responsible for their own areas of expertise, there is no depute appointed to manage a cyber incident should the ICT-CSO be unavailable. Additionally, the requirement for the ICT-CSO to be available out-of-hours is provided on a goodwill basis.

Action Plan 3

33. We contacted our counterparts in other Scottish Local Authorities to establish the level of cyber security personnel employed, responses covering 16 Local Authorities were received and the following information gathered:

    - One has an officer with similar remits to the Council
    - Two have an officer with a sole remit of Cyber Security
    - Nine have small cyber security teams of between two and five employees
    - Two have cyber security teams but have not provided numbers
    - Two have outsourced arrangements for all ICT services including cyber security

34. The National Cyber Security Centre (NCSC) offers advice and guidance to help Public Sector organisations protect networks, data and services they depend upon. Cyber attacks have increased significantly in recent years across all sectors resulting in additional work to follow advice and guidance issued to manage new threats as they arise. The Council's cyber security resource is less than comparable with those at the majority of other local authorities from which we have received responses and therefore there is concern that there is insufficient resource in place to manage all aspects of cyber security or to manage a cyber incident should the ICT-CSO be unavailable.

Action Plan 3

35. With only one dedicated Cyber Security post in the Council, there is no opportunity for further career advancement within cyber security resulting in the imminent departure of the ICT-CSO, however, management roles in ICT all have a requirement for cyber security knowledge and understanding. A recruitment exercise is currently in progress.

Action Plan 3

36. The ICT-CSO also works closely with the Council's Civil Contingencies and Data Protections Teams and with external organisations to provide additional services when required. A formal service support agreement is in place with Sapphire to provide 12 days of consultancy to deliver additional cyber security services and arrangements are currently being made to provide a Security Operations Centre (SOC) via a service level agreement (SLA).

37. The cyber security budget is part of the overall ICT budget. Investments in MS365 and infrastructure, web content filters, firewalls, Minecast, intrusion detection systems, patching and VPN are all part of cyber security but are managed by different teams across ICT and therefore paid for via various ICT budget codes. This highlights the integrated nature of cyber security management across the ICT and digital Service. Specific funding has, however, been identified for a SOC for a period of three years. The 16 local authority responses received indicated a similar approach to budget setting in 12 and four have dedicated budgets for cyber security.

Action Plan 6

38. Council employees and Elected Members are made aware of their responsibilities in respect of cyber security via the requirement to adhere to the content of the Acceptable Use Policy as well as being provided with periodic email reminders, features in the staff magazine "Cascade", Intranet strapline and links to further information. Notifications are often timed to coincide with events reported via media channels to raise awareness.

39. Training is provided to Council employees and Elected Members via the eLearning platform, LEON. There are two modules available providing cyber security content, 'Stay Safe Online' is provided by the NCSC and provides a short but comprehensive guide for users and 'Card Payment Guidance' is a useful tool for all users responsible for accepting income to the Council via card payment.

40. Mimecast training videos are provided monthly and require the viewer to answer a question upon completion to reinforce learning. These videos are very brief, lasting approximately three minutes each and all Council employees and Elected Members are encouraged to view these and answer the question provided at the end to develop skills and confidence to deal with cyber security risks and help keep data safe from cyber criminals.

41. The ITC-CSO monitors completion rates and passes the statistics to the Head of Customer Support Services to inform the other Heads of Service. No action has been taken by ICT to pursue those who have failed to complete this training. The lists provided contain a number of Elected Members and management, the details are as follows:

Videos not viewed	No. of employees
12	228
11	58
10	44
9	49
8	31
7	32
6	28
5	25
4	36
3	36
2	41
Total	**608**

42. A random sample of 30 users who have failed to view 10 – 12 videos was reviewed to assess if they were regular system users and 17 were found to have accessed the system within the last 17 days. The remaining users had been offline for more than 145 days or their presence was unknown.

Action Plan 4

Arrangements are in place to manage cyber security incidents

43. A comprehensive Cyber Incident Response Plan (CIRP) has been created for use during a large-scale cyber attack and made available on a designated SharePoint site for relevant staff to access. This plan was last reviewed in March 2022 and should be reviewed annually or when there is a major change in any of its components, it is currently scheduled for review in June 2023.

Action Plan 5

44. The CIRP contains details of the response team along with their out-of-hours contact details. The team consists of a mix of appropriate employees from across ICT, Financial and Legal & Regulatory Services including Civil Contingencies and Governance.

45. Playbooks are designed for small-scale incidents and were created in January 2020 based on templates provided by Scottish Government as a high-level best practice approach to the types of cyber security incidents they refer to. There is no evidence that these have been reviewed.

Action Plan 5

46. A cyber incident response exercise took place remotely via Teams in March 2022 with participants included from across all Council services. A de-brief report was prepared following the exercise noting that the exercise was successful and positive feedback was received from attendees.

47. There is a programme of testing in place for Disaster Recovery plans to familiarise officers with the recovery procedures required to reinstate systems. All tier 0 systems are tested annually and two line of business systems are tested per year, the next test is scheduled to take place August/September 2023. Disaster Recovery plans are also scheduled to be reviewed in June 2023.

Action Plan 5

48. In the event of a notifiable cyber incident, the service has a template prepared for use to provide incident reports and contributions to briefings with central bodies, NCSC and Police.

Appendix 1 – Action Plan

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Medium	1	**Reports to Senior Management** Finding: Reports are not regularly submitted to senior management to raise/maintain awareness of high profile risks to the Council's data and ICT infrastructure. Recommendation: Regular reports summarising cyber security risks, activity and incidents managed should be reintroduced to DMT at agreed intervals and escalated to SMT when relevant.	Senior management may be unaware of potential high-profile risks to the Council.	Regular reports summarising cyber security risks, activity and incidents managed will be submitted to DMT at agreed intervals and escalated to SMT when relevant.	ICT and Digital Manager 31 July 2023
Medium	2	**Cyber Security Policy** Finding: The Council has a comprehensive ICT and Digital Strategy in place including a section on "Secure and compliant infrastructure". This section makes reference to a Cyber Security Policy but this has not yet been completed. Recommendation: The Cyber Security Policy should be completed, approved and published on the Council's intranet site for Elected Member and employee reference.	Standards of behaviour expected of system users are not published leaving information assets at risk.	Our security policy will be updated and published. From a security perspective it is considered best practice to publish for restricted internal use only.	ICT Compliance and Security Officer 31 October 2023
Medium	3	**Cyber Security & Cyber Incident Management Resourcing** Finding: An Incident Response Team has been identified and recorded on the Cyber Incident Response Plan with each officer responsible for their own areas of expertise, there is no depute appointed to manage an incident response should the ICT-CSO be unavailable. Finding: The Council has one full-time officer (ICT-CSO) with responsibility for cyber security as part of their remit, other local authorities have small teams in place to	The Council may have limited expertise to call upon to manage all aspects of cyber security or to manage a cyber incident should the ICT-CSO be unavailable.	The level of resource allocated to manage the Council's cyber security requirements will be reviewed and a report submitted to DMT.	ICT and Digital Manager 31 October 2023

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
		manage cyber security alone indicating that the Council may be under-resourced in this area. Finding: There is currently no opportunity for career advancement for a cyber security professional within the Council, however, management roles in ICT all have a requirement for cyber security knowledge and understanding. Recommendation: The level of resource allocated to manage the Council's cyber security requirements should be reviewed.			
Medium	4	**Mimecast Video Training** Finding: Mimecast video training is not being completed by all Elected Members and employees. Recommendation: Members Services and managers should be provided with monitoring reports and encourage completion of the Mimecast training provided.	Elected Members and Council employees may not possess the required skills to deal with cyber security risks within their control.	Members Services and Heads of Service will be provided with monitoring reports on a regular basis to encourage completion of the Mimecast training provided.	ICT Compliance and Security Officer 30 June 2023
Medium	5	**Review of Cyber Incident Response Plan and other incident management documentation** Finding: the Cyber incident response plan, Playbooks and Disaster Recovery Plans have not been reviewed in the last 12 months. Recommendation: The Cyber Incident Response Plan and other incident management documentation should be subject to regular review, annually as a minimum.	Information available in the event of a major cyber incident may be out-of-date.	The Cyber Incident Response Plan and other incident management documentation will be reviewed and updated. This process will be completed on a regular basis and annual reports submitted to ITMT.	ICT Compliance and Security Officer 31 July 2023

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Low	6	**Budget provision for Cyber Security** Finding: There is no dedicated budget provision for cyber security. Recommendation: A specific budget provision for cyber security should be agreed.	Cyber Security costs are mainly included within the costs of other infrastructure and application budgets because of the way we purchase systems and it is not possible to separate out such costs. Costs associated with implementing cyber security arrangements across the Council may not be quantifiable.	With the help of Finance, create a new cost centre for the specific cyber security costs such as the budget for the ICT-CSO, SOC, Mimecast and Sapphire support contract.	ICT and Digital Manager 31 October 2023

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.