Mobile Working Review
Assignment Report 2021/22 (Final)

Allerdale Borough Council

Report Ref: DIGADV_2122_078

Date of Issue: 13/07/2022

Contents

Public Sector Internal Audit Standards

Our work was completed in accordance with Public Sector Internal Audit Standards and conforms with the International Standards for the Professional Practice of Internal Auditing.

Key Dates

Report Stage	Date
Discussion Document Issued	13/07/2022
Discussion Meeting	Dd/mm/yyyy
Final Draft Report Issued	Dd/mm/yyyy
Client Approval Received	Dd/mm/yyyy
Final Report Issued	Dd/mm/yyyy

Report Distribution

Name	Title
Michael Roper	Strategic Advisor Tier 1 – Assurance, Risk & Audit
Keith Hollins	Deputy Chief Officer – Innovation and Technology

Audit Team

Name	Contact Details	
Michael McCarthy	Michael.McCarthy@miaa.nhs.uk	07552 258 920
Paula Fagan	Paula.Fagan@miaa.nhs.uk	07825 592 866

Acknowledgement and Further Information

MIAA would like to thank all staff for their co-operation and assistance in completing this review. This report has been prepared as commissioned by the organisation, and is for your sole use. If you have any queries regarding this review please contact the Audit Manager. To discuss any other issues then please contact the Director. MIAA would be grateful if you could complete a short survey using the link below to provide us with valuable feedback to support us in continuing to provide the best service to you.

https://www.surveymonkey.com/r/MIAA_Client_Feedback_Survey

1 Executive Summary

1.1 Objective

The Mobile Working review at Allerdale Borough Council was conducted in accordance with the additional request from the former Assurance, Risk and Audit Manager and the Deputy Chief Officer – Innovation and Technology.

Modern IT is increasingly complex to manage in so many ways and one of these relates to mobile computing. Mobile computing in this context may include any device, such as laptops, tablets, and smart phones, etc. capable of storing and processing data off site and potentially connecting to the network from remote locations.

The use of mobile computing in its different forms is ever increasing, for instance, recently there has been a rapid rise in mobile working during the Covid-19 pandemic and it is an essential enabler for the delivery of council services across the various community locations it serves and for providing staff with connectivity and access to the Council infrastructure and resources.

Whilst some manifestations, such as use of laptops within the organisation's network, have fairly mature security and centralised support mechanisms, later options are more challenging in this regard tablets and other smart devices, for instance, while undoubtedly providing significant benefits in terms of mobility and functionality, do not necessarily integrate easily with all aspects of established security, asset management and technical support frameworks.

The control of mobile working and media continues to pose challenges to organisations and data breaches continue to be reported in the press. In addition, with the potential for increased financial penalties under the UK General Data Protection Regulations, organisations need to ensure they have established and continue to maintain effective controls in these areas.

Senior management at the Council recognised the importance of appropriate controls in this area and commissioned this review to obtain assurance relating to this area and identify opportunities for improvement, where appropriate.

1.2 Opinion

Moderate Assurance	There is an adequate system of internal control, however, in some areas weaknesses in design and/or inconsistent application of controls puts the achievement of some aspects of the system objectives at risk.

1.3 Key Findings

Overall, the review identified there were policies in place which documented the mobile working processes and controls in place at the Council. However, we were not provided with documentation on the security standards for laptops or any risks assessments that had been undertaken on the mobile working controls in place.

It was identified that there were logging and monitoring controls in place which covered all mobile computing devices however, improvements could be made to the audit trail of the process. Furthermore, we were informed that the Council undertook a lone working risk assessment but, evidence of this wasn't provided.

It was identified that the Council could strengthen the starters, movers and leavers process in respect of closing user accounts for software not controlled by ICT. Furthermore, the Council could not evidence the disposal process for devices that held data.

There was satisfactory training and awareness controls in place which included e-learning modules and evidence of regular announcements made in relation to information security.

Although it was identified there are change control processes in place at the Council, we were not provided with any documentation in respect of changes made to the control environment following the mobile working project.

The following provides a summary of the key themes.

Sub Objective	Key Themes
Policies and Procedure, Governance, Risk management and Reporting;	Areas of good practice: • There was a range of policies in place such as Acceptable Use Policy, Mobile Policy and Home Working Policy. We were also provided security standards for mobile devices and desktops (which included laptops). The Policies and Standards documented the roles and responsibilities of staff for using devices whilst out of the office and the technical controls in place to secure them. Areas for improvement • Although there were a number of policies in place, it was unclear when each had been issued and none of the policies reviewed included a next review date. • We were informed that there were no risk assessments that had been completed in relation to mobile working or any risks that had been raised in line with the Council's risk management processes. • Discussions with the Deputy Chief Officer – Innovation and Technology identified that there was no reporting of mobile device activity (for example, patching) to any group or committee of the Council.

Sub Objective	Key Themes
User management for offsite working;	Areas of good practice: • Evidence demonstrated that logging, and monitoring was in place for all mobile devices including laptops, tablets and mobile telephony. The logging included activity, unsuccessful authentication attempts and risky sign ins. It was demonstrated that the reports were received by the ICT team on a daily basis for review. • There was evidence that there was a learning module for 'Screen Device Risk Assessments' which included how to risk assess the home working environment. Areas for improvement • Although we were provided evidence that a logging and monitoring report was received daily by the ICT team, there was no evidence received of any action taken to investigate any unusual activity. • Although we were informed that risk assessments had been undertaken for lone working, we were not provided evidence of the assessments taking place or of any changes made following the risk assessment.
Device management / security for devices used at home;	Areas of good practice: • It was identified that the Council had in place Microsoft Intune which was the Council's mobile device management (MDM) solution. • It was identified that each mobile telephony device operated by the Council was an Android device. During a call with the Deputy Chief Officer – Innovation and Technology it was demonstrated on the MDM that all devices were at the time of the review, reported as compliant with the Council's mobile telephony policies (as set in the Security Standard – Mobile Devices). • The Information Security Policy was in place and details the roles and responsibilities of users in ensuring data protection is maintained whilst working remotely. • The Mobile Device Policy confirms staff responsibilities in relation to mobile computing devices including laptops, mobile phones and tablet computers. This includes the responsibility of users for ensuring patches are applied when prompted, not making any alterations to the software or hardware of devices and ensuring the mobile device is physically secure when working remotely. The policy also

Sub Objective	Key Themes
	details the process whereby a device is stolen and ICT's responsibility to remotely wipe the device. • Review of the Security Standard for Desktops found that it included the Council's technical controls for endpoints (which included laptops). The technical controls included 12 character passwords, changes to user passwords every 90 days and automatic lock after 15 minutes of inactivity. During a call with the Deputy Chief Officer – Innovation and Technology it was demonstrated that the technical controls were in place in Microsoft Intune and in group policy (*see also areas for improvement below).* • The Security Standard for Mobile Devices detailed the Council's technical controls in place for mobile telephony security following the NCSC's 'walled garden' approach. The technical controls included the passcode requirements of 6 characters, the device being wiped after 10 unsuccessful attempts to gain access and automatic lock after 2 minutes of inactivity. During a call with the Deputy Chief Officer – Innovation and Technology it was demonstrated that the technical controls were in place (*see also areas for improvement below).* • The standard also included the logging and monitoring standards applied to mobile devices through the Microsoft Intune solution which was demonstrated on screen by the Deputy Chief Officer – Innovation and Technology and also included logging from Windows devices. • The Council had in place VPN (Virtual Private Network) access which we were informed could only operate on a Council owned device. There were plans to remove the VPN and operate a 'Zero Trust' model with multi-factor authentication for all users to access the network. • During a call with the Deputy Chief Officer – Innovation and Technology, it was identified that the Council was migrating management of endpoints into Microsoft Intune. At the time of the review, 32 of around 300 devices had been migrated and the security patching on these devices was reported as compliant. We were informed that the remaining devices were being moved across from Kaspersky on an ongoing basis. Areas for improvement

Sub Objective	Key Themes
	• Review of the technical controls identified that there was a conflict between the Intune policies and group policy for endpoints. For example, Intune was set to 8 character passwords being required whereas, group policy was set to 12 characters. It was noted that only 32 devices had been migrated into Intune of around 300 devices at the time of the review. • Similarly, there was a discrepancy between the technical controls documented in the Security Standard for Mobile Devices and the Intune configuration for telephones. For example, the Intune policy for automatic lock was 15 minutes of inactivity however, the technical control in the standard was 2 minutes.
Lifecycle management including monitoring of mobile computing activity;	Areas of good practice: • We were demonstrated evidence that logging and motoring of active devices was in place for all mobile computing devices (see user management). • There was a process in place for stolen devices. This included the user notifying ICT who would be responsible for wiping the device using Intune. • We were informed that no devices had been stolen or identified as missing by ICT during the year under review. • It was identified that all devices required asset tagging prior to issue. Due to the remote nature of the review, we were unable to undertake testing on devices to confirm they had been issued with asset tags. Areas for improvement • We were informed that there was no process documentation in respect of the issue and collection of laptops and mobile devices. • It was demonstrated that a ticket through the service desk solution, Fresh Service, was raised for starters to issue devices and also for leavers to collect the devices on termination of employment. It was identified that the process only included ICT services. Therefore, as an example there was a risk that user accounts contained in Software as a Service (SaaS) solutions may not have been removed and would still be accessible by users following termination of theiremployent.

Sub Objective	Key Themes
	• We were informed that the Council had entered into a contract with a third party to ensure that mobile computing devices are safely disposed of to ensure no data remains on the encrypted device. However, at the time of the review there was no evidence of a contract in place between the Council and the third party and no evidence was available that any devices had been disposed of.
Communications, Training and Awareness;	Areas of good practice: • There was evidence of IT security training being provided on the Council's staff intranet site (Alice) through the Aspire E-Learning system. The training modules included Information Security and Data Protection Essentials. • It was demonstrated that the Council had a messaging and alerting feature through Alice to notify staff of information. It was demonstrated that IT security announcements had been made using the alert feature. These included lessons learnt following a penetration test undertaken in 2021. Areas for improvement • None identified
Change control.	Areas of good practice: • The Council had in place a change control process which operated through the service desk solution and the IT team. Areas for improvement • We were informed that the mobile working processes were not included within the change control process as they had been managed through a project management process. We were not provided evidence of the project documentation in respect of mobile/remote working. • Although we were informed that the 'Anytime, Anywhere' mobile and remote working strategy had been in place for some time we were not provided any evidence of the strategy documentation or minutes showing evidence of discussion of the strategy.

1.4 Recommendation Summary

The table below summarises the prioritisation of recommendations in respect of this review.

Critical	High	Medium	Low	Total
0	1	4	0	5

2 Engagement Objectives and Scope (Terms of Reference)

2.1 Objective

The objective of the review was to provide an assessment of the risks associated with mobile computing as they apply to the Council and the effectiveness of the control framework established by management to mitigate those risks. It is also to identify opportunities for improvement, where appropriate.

In overview, the review considered the following areas across: -

A. Policies and Procedure, Governance, Risk management and Reporting;

B. User management for offsite working;

C. Device management / security for devices used at home;

D. Lifecycle management including monitoring of mobile computing activity;

E. Communications, Training and Awareness;

F. Change control.

In addition, the implications of the General Data Protection Regulation (GDPR) was considered in the context of this review.

2.2 Approach

Our review and opinions were based on: -

- Discussions with stakeholders with knowledge and responsibilities for the areas being reviewed;
- Review of guidance, policies, procedures, and system documentation;
- Review of staff training and guidance to report incidents, use and secure their equipment appropriately and safely;
- Access to relevant system and solution security and configuration information;
- Reports showing operation and coverage (i.e., number of live devices covered);
- List of toolsets in place to manage mobile devices, such as logging and monitoring reports of activity on mobile devices and remote access;
- Documentation surrounding authorisation review and revocation of remote access privileges and mobile devices / media;
- Management information relating to contracts, incidents and risks raised on risk registers;

- Change control documentation, illustrating constraints over control mechanisms and potentially problematic functionality such as mobile applications / peripheral installation.

3 Detailed Findings and Recommendations

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Asset Lifecycle	Risk Rating: High

Control design

Key Finding –

1. Although we were demonstrated evidence that the issue and collection of devices was raised as a service desk request in Fresh Service, it was identified that there were no documented processes or policies in relation to the issue and collection of devices.
2. It was identified that the process for leavers only included the process for return of any devices issued to the user by their line manager. This would only be closed in Fresh Service when ICT had received the returned device. The process did not include the removal of user accounts such as Software as a Service (SaaS) accounts which wasn't managed by IT.
3. We were informed that the Council has recently contracted a third party, WEEE (Waste Electrical and Electronic Equipment) compliant company to provide secure disposal of devices with data. There was no evidence available of the contract between the Council and the third party and there was no evidence of any devices that had been disposed of by this arrangement. We were informed that there had been no collection of end of life devices at the time of the review.

Specific Risk – Without adequate asset lifecycle processes, the Council may not be able to identify where a device has been returned, decommissioned or has been lost or stolen which could lead to sub optimal acquisition, configuration, management and disposal of devices and result in data on devices being accessed inappropriately and / or loss of assets.

There is a risk that user accounts for systems not managed by ICT are not closed at the time the user ceases to be employed by the Council increasing the likelihood of unauthorised and inappropriate access to information.

Without a robust contract in place with the third party disposal company, the Council may not be able to ensure disposals are in line with expectations and are compliant with applicable legislation and regulations e.g. WEEE / GDPR

Recommendation –

1. The Council should provide evidence of / document its policies and processes in place for the issue and collection of mobile computing devices.
2. The process for leavers should be strengthened to ensure that user accounts for SaaS are deactivated as soon as possible.

3. The Council should ensure there is a contract between itself and the third party in relation to the destruction of devices which hold data. The contract should set out the roles and responsibilities of each party. The Council should ensure that the contract stipulates they will receive a certificate of destruction and this should be retained to provide assurance each device that has been disposed of has been completed using a WEEE compliant method.

Management Response – Agreed

Responsible Officer – Deputy Chief Officer – Innovation and Technology

Implementation Date – September 2022

Policies and Procedures	Risk Rating: Medium

Operating Effectiveness

Key Finding –

1. Although it was identified that there were several policies that documented the processes and controls for mobile working at the Council, it was unclear when the documents had been ratified or when they were next due for review. The following policies did not have a date of ratification or a review due date;
    a. ICT Acceptable Use Policy
    b. ICT Information Security Policy
    c. Mobile Policy
    d. Flexible Working
    e. Home Working Policy

    The Security Standard – Mobile Devices and Security Standard - Desktops had an issue date of March 2020 and March 2022 respectively however, it did not have a review due date.
2. We were informed that there were no risk assessments that had been completed in relation to mobile working or any risks that had been raised in line with the Council's risk management processes.
3. Discussions with the Deputy Chief Officer – Innovation and Technology identified that there was no reporting of mobile device activity (for example, patching) to any group or committee of the Council.

Specific Risk – There is a risk that policies have not been refreshed and therefore do not contain the Councils most up to date processes. It is not clear if all the risks of mobile working have been identified and are being managed appropriately. Without regular reporting of mobile working / device activity the council cannot be assured that its controls and processes are operating as expected.

Recommendation –

1. The Council should review their policies and ensure they include the date that they were ratified and the next review date. This should be in line with Council standard practices in relation to policy management.

2. The Council should undertake a risk assessment of their mobile working solution and processes. Any risks identified should be managed in line with the Council's risk management processes.
3. Reporting to appropriate groups or committees should be developed by the Council. This could include reporting information such as patching status of mobile devices (including laptop devices) and reporting any incidents that have occurred due to mobile working.

Management Response – Agreed

Responsible Officer – Deputy Chief Officer – Innovation and Technology

Implementation Date – September 2022

User Management	Risk Rating: Medium

Operating Effectiveness

Key Finding –

1. Although there was evidence that logging and monitoring processes were in place with evidence that the ICT Team received a logging report each day, there was no evidence provided of any investigations following review of the report and no audit trail to evidence the reports were reviewed on a daily basis.
2. Although we were informed that a lone working risk assessment had been completed, we had not been provided evidence of the risk assessment taking place or of any changes made following the outcome of the assessment.

Specific Risk – There is a risk that without evidence that the logging report is reviewed, inappropriate activity may not be identified and investigated by the ICT team which could lead to insecure systems or inappropriate access.

The Council's risk exposure in relation to remote / lone / mobile working may not be understood or mitigated without formal documented risk assessments being undertaken.

Recommendation –

1. The Council should develop a process that provides an audit trail between the logging report and any investigations that are undertaken following identification of suspicious activity. This process should also include evidence that the logging report has been reviewed.
2. The Council should provide evidence of the risk assessments that have been completed in relation to remote / lone / mobile working.

Management Response – The logging of issues is automatically undertaken within Azure, these are reported to the service desk. Within Azure the issues of suspicious activity have to be followed through until complete. Each service undertakes its own risk assessments, and these are found within the service HS environments

Responsible Officer – Deputy Chief Officer – Innovation and Technology

Implementation Date – April 2023

Device Management	Risk Rating: Medium

Control design

Key Finding –

1. Review of the technical controls for mobile telephony found that there was some discrepancies between the Security Standard – Mobile Devices and the actual controls contained in Intune. This included;
    a. The standard required automatic logout following 2 minutes of inactivity however, the policy contained on Intune reported this as 15 minutes of inactivity.
    b. The standard required automatic wiping of mobile telephone devices following 10 unsuccessful access attempts. The control on Intune reported this as 6 unsuccessful attempts.
2. There was a discrepancy in relation to endpoints management between Intune and group policy. It was identified that the password policy on Intune was set as 8 characters however, group policy was set as 12 characters. It was noted that this would impact a small number of devices as the migration to Intune was not complete at the time of the review.
3. It was identified that there was a project to move management of endpoints into Intune from the previous endpoint management system (Kaspersky). At the time of the review, 32 devices of around 300 Council endpoints had been migrated to Intune. It was noted that each device was showing as compliant in respect of the patching status of each device.

Specific Risk – It was identified that the Council's standards do not reflect the technical controls in place for mobile phones and endpoints therefore, there is a risk that the technical controls are not as robust as required and could lead to devices being compromised and accessed inappropriately.

Recommendation –

1. The Council should review the Security Standards and ensure that the technical controls documented in them are consistent with and reflected in both Intune and group policy.
2. The Council should complete the migration of endpoint management into Microsoft Intune as soon as possible. Following completion of the migration, the Council should design and document a monitoring process (such as for patch compliance).

Management Response – Agreed. The second is a much wider work package that is underway, and scheduled for completion before LGR. It includes the removal of Kaspersky Malware protection, and migration to Defender, migration of BitLocker services, USB controls and patch and update management.

Responsible Officer – Deputy Chief Officer – Innovation and Technology

Implementation Date – April 2023

Change Control	Risk Rating: Medium

Operating Effectiveness

Key Finding – Although it was identified that there was a change management process in operation at the Council, we were informed this process had not been followed in relation to the changes made to the control environment in respect of mobile working.

Furthermore, we were informed by the Deputy Chief Officer – Innovation and Technology that the mobile working changes had been managed by the Council's project management process however, we were not provided evidence of the process or of any project documentation. We were also informed of the 'Anytime, Anywhere' strategy but, had not been provided evidence of the strategy or of any minutes showing discussion and progress of implementation to ensure processes had been handed over and implemented as part of business as usual activity.

Specific Risk – The Council has not retained documentation to confirm the changes that have been completed in respect of mobile working or that the changes made have been reviewed and accepted as appropriate within business as usual activities.

Recommendation –

1. The Council should collate any documentation in respect of the changes made to the control environment as part of the mobile working project to ensure they have been handed over to and incorporated within business as usual activities.
2. Going forwards, the Council should ensure that the change control process in the service desk solution is adhered to. If a change is a result of a project, the documentation should be retained which should also include evidence of the approval of the changes.

Management Response – Agree with the above to an extent. However, the facilities to support Remote Working have been in place since 2010. When Covid hit, we carried out a Work package to enable everyone to work from home and used management processes under Microsoft Planner, to quickly deploy the environment to everyone. So a project management lite process was applied until we had completed works and then we deleted the planner module as in essence this was a major BAU piece of work. The issue here is we could not evidence it, So the process should be how long should we archive work packages for. Similarly, the deployment of a laptop is not classified as a change but BAU with Asset Management records being updated.

Therefore, we will look to develop a process to manage work packages and archive them as appropriate.

Responsible Officer – Deputy Chief Officer – Innovation and Technology

Implementation Date – End of August 2022

Follow-up

A follow-up exercise will be undertaken during 2022/23 to evaluate progress made in respect of issues raised. This will include obtaining documentary evidence to demonstrate that actions agreed as part of this review have been implemented.

Appendix A: Assurance Definitions and Risk Classifications

Level of Assurance	Description
High	There is a strong system of internal control which has been effectively designed to meet the system objectives, and that controls are consistently applied in all areas reviewed.
Substantial	There is a good system of internal control designed to meet the system objectives, and that controls are generally being applied consistently.
Moderate	There is an adequate system of internal control, however, in some areas weaknesses in design and/or inconsistent application of controls puts the achievement of some aspects of the system objectives at risk.
Limited	There is a compromised system of internal control as weaknesses in the design and/or inconsistent application of controls puts the achievement of the system objectives at risk.
No	There is an inadequate system of internal control as weaknesses in control, and/or consistent non-compliance with controls could/has resulted in failure to achieve the system objectives.

Risk Rating	Assessment Rationale
Critical	Control weakness that could have a significant impact upon, not only the system, function or process objectives but also the achievement of the organisation's objectives in relation to: • the efficient and effective use of resources • the safeguarding of assets • the preparation of reliable financial and operational information • compliance with laws and regulations.
High	Control weakness that has or could have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall organisation objectives.
Medium	Control weakness that: • has a low impact on the achievement of the key system, function or process objectives; • has exposed the system, function or process to a key risk, however the likelihood of this risk occurring is low.
Low	Control weakness that does not impact upon the achievement of key system, function or process objectives; however implementation of the recommendation would improve overall control.

Limitations

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regards to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Reports prepared by MIAA are prepared for your sole use and no responsibility is taken by MIAA or the auditors to any director or officer in their individual capacity. No responsibility to any third party is accepted as the report has not been prepared for, and is not intended for, any other purpose and a person who is not a party to the agreement for the provision of Internal Audit and shall not have any rights under the Contracts (Rights of Third Parties) Act 1999.