

Cyber Security Review

Assignment Report 2020/21

Allerdale Borough Council

Contents

1. Executive Summary

2. Introduction, Background and Objectives

3. Findings, Recommendations and Action Plan

Appendix A: Assurance Definitions and Risk Classifications

Appendix B: Report Distribution

1. Executive Summary

This review of Cyber Security at Allerdale Borough Council (the council) was conducted in accordance with the requirements of the 2020/21 Internal Audit Plan, as approved by the Audit Committee.

In order to protect itself, an organisation needs to have a robust cyber security framework provisioned through a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies. This framework should provide a foundation from which to secure information systems and assets including connected computing devices, personnel, infrastructure, applications, services and the totality of transmitted and/or stored information in the cyber environment.

It is against this backdrop that Allerdale Borough Council commissioned MIAA to provide assurance regarding the baseline technical elements of the council's cyber security controls and identify opportunities for improvement, where appropriate.

Areas of Good Practice

- There were detailed policies available for review which included guidance on the management of firewalls and security patching.
- Network access was restricted with ports and switches blocked by default.
- A strong password policy was in place for domain accounts with further multi factor authentication (MFA) requirements for domain administrator accounts.
- Antivirus, web and Domain Name System (DNS) filtering and Intrusion Prevention System were activated on the firewalls.
- Measures had been introduced and will be further developed to standardise device builds and software application.
- Potentially high risk file types had been blocked by default.
- The council has deployed a suite of Kaspersky Enterprise applications which included tools for removable media control and antivirus software.
- The council had policies governing the hardening of servers, laptops, desktops and mobile devices.

Areas for Improvement

- The introduction of periodic auditing of standard activities and processes, such as remote support monitoring and reviews of firewall rules, as well as patching and antivirus compliance, would allow for issues to be proactively identified and promptly investigated.
- Expand the suite of documentation to include guidance for users and procedural information for IT tasks, such as password resets. Document control should be

included in all documentation to ensure the information contained within policies and procedures is applicable and review dates are adhered to.

- All new processes and solutions should be formally risk assessed to provide assurance of the measures due to be implemented.
- There are 78 enabled accounts which had been dormant for over 6 months that required further investigation to determine whether they are appropriate.

There is a good system of internal control designed to meet the system objectives, and that controls are generally being applied consistently.

As a result of our review and the associated findings, the level of assurance provided, based upon the defined scope and criteria at Appendix A; is:

Substantial Assurance

2. Introduction, Background and Objectives

We live in a world where external connectivity to other people and organisations via various mediums, including the Internet, is essential to normal operations. However, the proliferation and rapid expansion of this connectivity and communication inevitably increases the risk that these channels and technology will be used to attack and compromise organisations. In fact, as we know, from the press and official sources, organisations are constantly being probed for weakness and are constantly suffering malware attacks and other breaches resulting in operational disruption, data loss and reputational damage. In the case of data loss organisations can be exposed to significant fines and potentially legal action which they can ill afford.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks, primarily from external sources. Cyber security covers a myriad of risks, but, primarily, these fall in to three key areas namely:

- Potential breaches of **confidentiality** resulting from unauthorised access to systems or data;
- Potential damage to the **integrity** of information through unauthorised alteration and/or manipulation; and,
- Potential loss of, or disruption to, the **availability** of information and information systems.

Furthermore the impact of the COVID-19 pandemic has touched all aspects of life including the workplace. The effects have reached far beyond what most had considered and introduced new challenges to all with cyber security being no exception.

A mature cyber framework helps an organisation to understand their cyber security risks and manage these through customised measures. It also helps with the response and recovery from cyber security incidents as well as allowing for continuous review and improvements to be made. The scope of this review considered the following areas:



Perimeter protection

Information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices, with appropriate management of ports, protocols and services.



Secure configuration

Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.



User access control

User accounts should have robust protection, particularly those with special access privileges (e.g. administrative accounts), and should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks and such accounts should be actively managed throughout their lifecycle.



Malware protection

Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software.



Patch management

Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.



Secure Home and Mobile Working

The organisation should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Users should be trained on the secure use of their mobile devices in the environments they are likely to be working in.

COVID – 19

MIAA have also considered any changes to the control environment due to COVID-19. Considerations such as any changes needed to the design and implementation of internal controls with regards response and the understanding of the increased risk resulting from change, as well as the impact remote working has had on operational effectiveness.

3. Findings, Recommendations and Action Plan

1. Perimeter Protection	Risk Rating: Low
<p>Findings – The council had a robust process for managing firewall rules that had been formally documented within the Firewall Configuration Policy, which is aligned to the compliance requirements of the Cabinet Office and the Department for Work and Pensions (DWP). The policy included requirements relating to change management, the management of firewall rules, security auditing and the maintenance of the firewalls. Although the policy was dated March 2020, the document provided did not contain any document control details and as such no indication of a review date and therefore no guidance on how long these controls should be in place for nor did it provide detail of where it was approved.</p> <p>Information provided for the firewall products FortiAnalyzer VM, FortiGate 60D and FortiGate 600D were all in vendor support at the time of the review, but as they were due to expire in February/March 2022, the council should ensure it has plans in place to ensure continuity of support.</p> <p>It was advised that firewall rules had not been subject to any changes within the last four years and therefore had not required review. The Network Manager would be automatically alerted to any attempted changes to the firewall.</p> <p>The main firewalls could only be accessed internally through the Meraki Network Management Tool (Cisco). The password policy for accounts accessing the firewall was confirmed to be a minimum of 12 characters with complexity enabled and a 90 day expiry. The Firewall Configuration Policy stated that vendor-supplied default passwords should be changed however there was no evidence that this had been checked to confirm it had taken place.</p> <p>Ports on switches were locked by default and could only be unlocked by an authorised user to the Network Management Tool. This prevents unauthorised users accessing the council network with unknown devices. A live demonstration of the console showed that ports were disabled when not in use.</p> <p>It was confirmed that antivirus, web and DNS filtering and IPS were activated on the firewalls.</p> <p>Specific Risk – Perimeter protection, as with other controls, should be considered in the context of the council’s risk appetite, risk assessment and security policies. Failure to provide appropriate boundary protection controls could mean that the council could be subject to a number of risks, including:-</p> <ul style="list-style-type: none">• Accidental or deliberate import or export of malware into systems or across partner/ third party connections.	

- Exploitation of vulnerable systems by attackers to gain unauthorised access to compromise the confidentiality, integrity and availability of systems, services and information.
- Damage to resources thereby harming the reputation of the council and resident confidence.

Recommendation – Management should:

- i) Ensure that all firewall rules are regularly reviewed to confirm appropriateness;
- ii) Confirm that all vendor-supplied default passwords have been changed from default;
- iii) Plan for the continuity of support with the expiration dates within the next 12 months;
- iv) Consider including further document management details within policies and procedures to demonstrate review and ensure they remain consistent and effective.

Management Response (Remedial Action Agreed) –

- i) Annual review of firewall rules to be implemented.
- ii) We normally change vendor supplied passwords – we will verify that this is the case across the estate.
- iii) Firewall support review is already scheduled into work programme for the year
- iv) Documents are to be stored within our new intranet facility which will have auto review dates and document control.

Responsibility for Action – Keith Hollins, Innovation and Technology Manager

Deadline for Action – End of quarter 2

2. Secure Configuration

Risk Rating: Low

Findings – The requirement to harden devices was included within the Desktop Operating System and the Network Security Design security standard. A technical policy was provided to evidence potentially high risk file types are blocked by default. The application stores were removed from mobile devices to prevent the installation of unauthorised software.

Standard built procedures were provided for android and Windows 10 devices as a base build however PCs were currently built to specification with individuals requesting applications specific to their requirements. It was advised that approximately 50 users were still using desktop PCs but the council will be utilising a solution provided by Workspace 365 to enable virtual workspaces and eliminating the need for varying application installation across the estate. Legacy devices had not been included within the standardisation measures but it was advised that they were not rebuilt and would be put onto a separate VLAN, if they were unable to be updated, to mitigate exposure to the network.

Policies state to remove or disable all the unnecessary accounts and it was advised that IT have separate administrator accounts to their regular user accounts, in alignment with recommended best practice, which was evidenced through an Active Directory extract. Although informed that autorun had been disabled for all media types, this was not demonstrated during the review to confirm the control was operating.

Specific Risk – Systems that are not consistently locked down or hardened are particularly vulnerable to attacks. Failure to produce and implement policies that manage the secure configuration of their systems mean organisations will be subject to risks such as:-

- Unauthorised changes to systems compromising confidentiality, integrity and availability.
- Exploitation of insecure system configuration through unnecessary functionality that has not been locked down.

Recommendation – Management should:

- i) Confirm whether autorun has been disabled and if not, formally assess the risk to the council of it not being implemented.
- ii) Continue with the plan of introducing the Workspace 365 solution to assist with the standardisation of builds.

Management Response (Remedial Action Agreed) –

- i) We will verify autorun is disabled.
- ii) Standardisation of builds is to be enabled through the new workspace.

Responsibility for Action – Keith Hollins, Innovation and Technology Manager

Deadline for Action – 1 – End quarter 1, 2 – Solution to be rolled out by end quarter 2

3. User Access Control

Risk Rating: Medium

Findings – An Active Directory extract containing 562 user/service accounts showed 78 enabled accounts that last logged on to the network between March 2011 and June 2020. Of these 78, 22 were individual user accounts with the remaining 56 being either service or generic accounts. There were also 16 enabled accounts (7 individual users and 9 service/generic) that were showing a last log on date of 1601, often a default value used by Microsoft and should be investigated further to determine the correct date.

There was also a risk that any activity performed with accessible generic accounts may not be accountable to individual staff and that older accounts may still have default passwords that could potentially be weaker than the council's current domain password settings.

It was however confirmed that of 180 Azure users, all had logged on within the 48 hours prior to the report being ran.

Although users currently gain access to the network using a username and password, there are plans to move to a multi factor authentication solution subject to an approved business case.

Administrator accounts were uniquely identifiable and limited to IT staff. One administrator account, nadmin, was noted to be enabled but not logged into since 6th September 2017. In addition, the account 'xaadmin' had not logged in since 15th November 2020. Both accounts do not comply with 10.3.4 of the Privilege User Access Controls security standard which stated that "*Where a privilege user account has been dormant for four weeks it MUST be suspended*". It was advised that privileged accounts did not have email accounts but did have access to the Internet. Administrator accounts had the same password policy applied to them as standard accounts however they also had the addition of Multi Factor Authentication (MFA) for added security.

The council's process for managing starters and leavers was via a request from HR with any temporary staff that may not go through the standard procurement route, i.e. contractors, also requiring authorisation from HR before an account would be created, although this was not documented. Processes for managing and monitoring staff moving / changing role within the organisation required strengthening to ensure user access permissions remain appropriate for the role. We were advised this would be addressed with the work carried out to build the new workspace.

Due to the size of the organisation, the procedures for resetting passwords to ensure security would be maintained had not been documented, as staff were well known to each other, however this exposed potential risk with the turnover of staff.

Specific Risk – Failure to effectively manage user privileges could result in the following risks being realised:-

- Accidental or deliberate misuse of privileges leading to unauthorised changes to configuration of systems, leading to a loss of the confidentiality, integrity or availability of information or ICT systems.
- Increased attacker capability if they can use unused or compromise user accounts to carry out an attack. Ultimately attacks seek to gain access to root or administrative accounts to gain the fullest access to system information, services and resources.
- Negating established security controls whereby attackers attempt to cover their tracks by making changes to security controls or deleting monitoring and auditing logs so that their activities are not detected.

Recommendation – Management should:

- i) Investigate enabled accounts that have been dormant for over 90 days, with particular attention to generic and administrative accounts with further actions taken as required to maintain council security. This should also become a periodic review of all active accounts to ensure they are appropriate;
- ii) Formally risk assess the requirement of administrator accounts having internet access to determine if this is necessary for operational purposes and if not that it can be disabled;
- iii) Document procedures for managing users, including the resetting of passwords to ensure compliance with the Access and Authentication Controls security standard;
- iv) Document all staff who have privileged access permissions and ensure this is subject to periodic review.

Management Response (Remedial Action Agreed) –

- i) Dormant Accounts to be removed instead of purely disabled.
- ii) Administrator Accounts to be reviewed.
- iii) Starters, Movers and Leavers process to be reviewed to address all weaknesses.
- iv) Privileged Access will be reviewed and documented.

Responsibility for Action – Keith Hollins, Innovation and Technology Manager

Deadline for Action – All actions to be completed by end of quarter 2

4. Malware Protection	Risk Rating: Medium
<p>Findings – The council employed multiple measures to provide malware protection that included the Kaspersky Enterprise suite and Microsoft Defender and Advanced Threat Protection (ATP). Antivirus (AV) was deployed to all servers and endpoints as part of the standard build process however there were no AV compliancy reports provided to review coverage across the estate. Any devices that did not have AV installed, such as some mobile devices, had ATP. The Kaspersky solutions in use provided a full disaster recovery malware process in the event that malware was able to infiltrate the network out of hours.</p> <p>The AV solutions were configured to update automatically with minor updates deployed daily, however the Kaspersky console did not update clients with major upgrades until it was authorised and approved via the Change Advisory Board (CAB) to ensure staff were aware and to minimise potential disruption. This authorisation would be provided within 24 hours of the upgrade being made available.</p> <p>Kaspersky Endpoint Security was used to manage USB and removable media capability and blocks usage in accordance with Public Services Network (PSN) requirements. The council did</p>	

have a whitelist of permitted devices however this was restricted to devices without storage capability.

A review of settings and internet activity were not confirmed to have taken place but it was advised that content filtering was reviewed to identify regular attempts to access blocked sites, with alerts received by the IT team for continual hits to blocked sites over a short time period.

Specific Risk – Malware infections can result in the disruption of services, the unauthorised export of sensitive information, material financial loss and legal or regulatory sanctions. The range, volume and originators of information exchanged with the business and the technologies that support them provide a range of opportunities for malware to be imported. Examples include:-

- Email – the primary path for internal and external information exchange and targeted for random attacks (phishing) through malicious file attachments.
- Web browsing and access to social media through controlled browsing and access can provide an opportunity for an attacker to direct malicious content to individual users and lead to a malicious website or a system/application being compromised.
- Removable media and personally owned devices.

Recommendation – Management should:

- i) Review antivirus compliance reports for the council's estate, reconciling AV coverage using different but comparable sources to identify any areas of vulnerability and apply appropriate mitigations and/or resolutions.
- ii) Expand proactive monitoring of users' Internet activity to identify inappropriate or malicious usage to allow for investigation and / or follow-up.

Management Response (Remedial Action Agreed) –

- i) Monitoring and AV Compliance reports to be discussed at the Security Forum that is being developed to review on going improvement and security compliance
- ii) As above

Responsibility for Action – Keith Hollins, Innovation and Technology Manager

Deadline for Action – End of quarter 2

5. Patch Management

Risk Rating: Medium

Findings – The council had a documented Technical Vulnerability Management Policy and a Security Patching standard. The TVM Policy did not have an implementation date and therefore was not clear if it was still applicable although it was referred to in the Security Patching standard which was dated 26th August 2020. The scope of the Security Patching standard was defined as “*product agnostic and applicable for all end-user devices and systems provisioned for departmental use*”.

Patches were pushed to devices with a 2 week delay from release unless it was classified as a critical/high risk update in which case it was immediately deployed. Although users had the ability to choose what time to restart their device to accept the updates, they were only permitted to postpone this for a week before the patches are automatically pushed to the endpoint. The documentation did not include the timescales for regular patching to be applied but did specify the 14 day requirement for critical/high risk patches. Example reports from a Windows 2008 r2 server, a Windows 2012 server and Windows 2016 server showed that they were fully patched with the 2012 and 2016 servers both configured for automatic updates however reports of overall server compliance were not provided for review.

The council confirmed that they currently have unsupported applications and servers within their infrastructure, with unsupported software held for archived and retention purposes, however they have been segregated on to their own VLAN to mitigate the risk. It was advised that the council has embarked on a strategy of ‘mobile first/cloud bias’ which removes the requirement of having servers on the network as they would become services provided by a third party, Salesforce. Eight services were currently operating on internal applications and it was planned that by May 2022, 90% of the council’s systems would be cloud based services.

Specific Risk – Systems that are not consistently patched are particularly vulnerable to attacks. Failure to produce and implement policies that manage the patching of their systems mean organisations will be subject to risks, such as increases in the number of security incidents, which may disrupt the services of the council.

Recommendation – Management should:

- i) Review both server and desktop patching compliance reports that include the entire estate to identify any areas of vulnerability and apply appropriate mitigations and/or resolutions.
- ii) Progress the current plan to remove all unsupported applications and servers from the council network.
- iii) Update documented policies and procedures to ensure document control is applied and detail regarding the timescales for the applications of all patches are specified.

Any residual risk should be placed on the corporate risk register.

Management Response (Remedial Action Agreed) –

- i) Monitoring and AV Compliance reports to be discussed at the Security Forum that is being developed to review on going improvement and security compliance
- ii) On-going – and will be promoted at the Forum
- iii) Policy to be reviewed

Responsibility for Action - Keith Hollins, Innovation and Technology Manager

Deadline for Action – 1 and 3 – End of quarter 2, 2 – Ongoing activity

6. Secure Home and Mobile Working

Risk Rating: Medium

Findings – The council had documented Mobile Device and Remote Access security standards to instruct technical staff on how to securely configure and manage devices and connections. However, there was no documentation available for review to guide users on how they should maintain security when working remotely. It was advised that there was an Acceptable Use Policy and an IT Security Policy for users but neither was provided for review. IT staff were alerted of failed log in attempts and reviewed where users were accessing council connections from to ensure it was legitimate. The council was planning to restrict permitted regions for access, for example, to only allow connections from the UK.

Citrix Workspace was used to deliver the organisation’s remote access solution, using multi factor authentication. It was advised that the council would be moving to a Zero Trust model of mobile working that would channel the user through a multi factor gateway away from the internal council network. Access from mobile devices was through a secure VPN and prevents data leakage. Devices were also directed through Advanced Threat Protection (ATP) before they connected to networked storage solutions.

Within the Privilege User Access Controls (Part 2) security standard provided for review, there were detailed controls around these accounts which included the review of suitability and permissions however the document did not mention a review of the activity carried out by the user to ensure only authorised, appropriate actions had been performed.

IT staff could use both attended, when a code would be required, and unattended methods to provide remote support to users. It was advised that the process and protocols required for IT staff to remotely access user devices was known to the IT team but not documented.

The council did not confirm whether there were logs available to show when IT staff had accessed a device remotely either in the presence of a user or without permission required to enable the connection.

Awingu was used to allow third party support access to the council network, a standalone gateway limiting access to a specified server. Third party accounts would have administrative privileges for its permitted areas however they were disabled by default, enabled by request

for the stated duration of use only and fully monitored when utilised. These accounts were also restricted from moving files directly on to servers and were required to first move any files to a shared IT server to be verified as appropriate.

Specific Risk – Failure to implement or adequately monitor remote access and working may result in increased security incidents, increased downtime and loss of confidential information resulting in financial penalties and reputational damage

Recommendation – Management should:

- i) Clarify the availability of logs which show IT remote support access and introduce periodic auditing to ensure appropriateness of activity.
- ii) Formally document procedures for users on how to access and use remote access solutions.
- iii) Risk assess the requirement for restriction of regions and ensure any implementation is fully documented.

Management Response (Remedial Action Agreed) –

- i) Connectivity logs exist for users accessing devices, this is done through Awingu for remote support. There is a reporting engine for GoToAssist, our internal system, and this provides reports on attended issues, etc. We will add into our internal processes the addition of the call number into the log for any connectivity. This way any connection to a device can be related to the reason as to why the connectivity took place.
- ii) New procedures for remote access to be documented in line with implementation of Workspace 365.
- iii) Regional access and multi factor authentication already under investigation.

Responsibility for Action – Keith Hollins, Innovation and Technology Manager

Deadline for Action – End of quarter 2

Limitations inherent to the internal auditor's work

We have undertaken the review of the process, subject to the following limitations.

Internal control

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgement in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

The assessment of controls relating to the process is that at March 2021. Historic evaluation of effectiveness is not always relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected. The organisation's Local Counter Fraud Officer should provide support for these processes

.

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: <ul style="list-style-type: none"> 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 is likely to 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: <ul style="list-style-type: none"> 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.

Appendix B: Report Distribution



Name	Title	Report Distribution
Brendan Carlin	Assistant Chief Executive	PDF
Paul Wood	Head of Customer Operations	PDF
Paula McKenzie	Assurance, Risk and Audit Manager	PDF
Keith Hollins	Innovation and Technology Manager	PDF

Discussion meeting held with

Name	Title	Date
Keith Hollins	Innovation and Technology Manager	28/04/2021

Review prepared on behalf of MIAA by

Name	Gemma Owens
Title	Senior Technology Risk Assurance Manager
	07717 720 389
	Gemma.Owens@miaa.nhs.uk

Name	Paula Fagan
Title	Head of Technology Risk Assurance
	0151 285 4562
	Paula.Fagan@MIAA.NHS.UK

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 Senior Technology Risk Assurance Manager. To discuss any other issues then please contact the Head of Technology Risk Assurance.

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