INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Microsoft 365
TO:	Head of Customer and Digital Services	**DATE:**	24 January 2023
C.C.	Chief Executive Deputy Chief Executive Head of Finance Portfolio Holder (Cllr. Tracey)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2021/22 an examination of the above subject area has recently been completed by TIAA, the Council's ICT audit contractor, and this report presents the findings and conclusions for information and, where appropriate, action.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 Microsoft 365 (M365) is the Microsoft Office suite of productivity tools such as Word, Excel, Access, and other tools in addition to a suite of security management tools that are deployed as needed. The Council has adopted a Hybrid approach to M365 in that certain functions are hosted on site with others in the cloud. This is a common approach that many organisations have adopted.

2.2 This audit was undertaken to ensure the security, integrity and availability of the controls in place to manage M365 security controls within the Council.

3 Objectives of the Audit and Coverage of Risks

3.1 The audit was undertaken to test the controls in place to manage M365 controls in place.

3.2 In terms of scope, the audit covered the following risks:

- Lack of governance and senior management oversight of security incident reporting, leading to issues not being addressed promptly.
- Lack of Standard Operating Practices for the management of security configuration, resulting in poorly managed systems and incidents.
- Inappropriate restriction of permissions granted via Azure Active Directory portal to Microsoft 365 security management information, leading to an unreliable security infrastructure.

- Ineffective deployment of Microsoft 365 Polices for Managing Devices, Threat Protection and Alerts, resulting in security breaches and disruption.
- Inadequate classification system deployed to guard against data loss, leading to breaches of data protection legislation.
- Ineffective configuration of 'Action Center' to automatically handle and reduce alerts requiring manual intervention, resulting in overburdening of security management resources.
- Lack of appropriate incident management, investigation, resolution and reporting practices, leading to poorly managed incidents and service disruption.

3.3 These were identified by the auditor and agreed with the Head of ICT.

3.4 The work in this area will help to ensure the Confidentiality, Integrity and Availability of the Council's data. Whilst this does not directly help the Council to achieve any specific objectives, it has a cross-cutting impact on a number of internal themes and objectives as set out in the Fit for the Future strategy.

3.5 The risks identified above were covered in overview against the following key areas:

- Procedures and Governance
- Microsoft 365 Restrictions and Deployment
- Alert and Incident Management

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not applicable as this is the first review of this area.

4.2 Procedures and Governance

4.2.1 The Council has an established Security Incident Management Policy which sets out the requirements for reporting on security incidents, how these get communicated to senior management and how decisions are documented and tracked for completion.

4.2.2 We have noted that the policy was last reviewed in February 2018, suggesting that a new review would be prudent.

4.2.3 In addition to the full Security Incident Management Policy, a full change management policy is in place.

4.2.4 We have noted that the policy was last reviewed in May 2018, suggesting that a new review would be prudent.

4.2.5 The Council also has an overriding System Lockdown Policy detailing the management of security configurations, such as access controls to shared and personal mailboxes and calendars.

4.2.6 We have noted that this policy was last reviewed in July 2019, suggesting that it should undergo a new review.

Recommendation

The Security Incident Management Policy, Change Management Policy and System Lockdown Policy should be reviewed to ensure that they remain compliant with Council requirements.

4.2.7 Personal mailboxes are created as part of the Council's process for setting up new users and are accessible only to the owner of the mailbox. There is a separate procedure for managers and others requiring access to a personal mailbox in the event of absence or where an officer has left.

4.2.8 There is an application form (mailbox access form) published on the Council's intranet that is available for this purpose.

4.2.9 Supporting this process, there is a Mailbox access Standard Change Checklist for ICT staff which confirms appropriate authorisation and details the access procedure. We have noted that all of these processes are documented with the ICT Helpdesk, which includes its own peer review processes as part of the implementation of the requests being made.

4.2.10 The use of the forms described here was reviewed as part of the audit fieldwork and was found to be adequate for this purpose.

4.3 Microsoft 365 Restrictions and Deployment

4.3.1 At present, the Council does not use M365 for file storage, which means that file access is still controlled at a network folder level on the corporate file servers usually via Active Directory security groups.

4.3.2 The Head of Customer and Digital Services has advised that there is a strategy to migrate all the network folders onto the M365 OneDrive service and use Teams for shared file stores. These will replace the current network department shared folder structure that exists at present.

4.3.3 However, migration to OneDrive cannot take place until the Council has considered the best way forward regarding a consistent approach to data retention, which includes the deletion of data that is no longer required. This is a question for department network shared folders as well as the council-wide folder structure, such as the WDCShare Drive, also known as the L Drive. These file locations store data where ownership of the data is not always obvious and hence, it is not currently clear where responsibility for decisions on the retention of the data is not clear.

4.3.4 There are plans in place to work with Information Governance colleagues to make a start on this work. However, it has been a challenge to move the work forward.

Recommendation

Council management should ensure that work to agree and implement appropriate data retention polices be completed as soon as possible. Doing so will help ensure a timely migration to OneDrive, whilst also ensuring that only the data that the Council requires is migrated.

Minimising the amount of data to be migrated may also help reduce the cost of hosting the data in terms of the required storage capacity.

4.3.5 All privileged access to M365 functions is controlled with granular permissions – we noted that there is a restricted number of Global Administrator accounts with the privileged permissions. We have noted that the Council has implemented what is known as a Hybrid M365 configuration, with both cloud-based and locally-installed systems co-existing to deliver Council services.

4.3.6 As per Microsoft best practice these accounts are created as 'cloud only' accounts with O365 credentials but which are not valid on the internal domain. Implementing separate permissions in this way helps to mitigate the risk of one of these accounts being compromised from accessing the internal domain or vice versa.

4.3.7 These accounts also fall under the Conditional Access configurations discussed in more detail below. In this situation the accounts are required to use Multi-Factor Authentication (MFA) if being accessed from a location other than WDC networks.

4.3.8 Other than Global Administrator accounts, account permissions are granted commensurate with the staff role. Typically, it is the Global Administrators that grant these permissions and, in all cases, this can only be actioned via a service desk request. From example testing of this process, we have noted that this process is operating adequately and effectively.

4.3.9 Council-owned mobile devices, such as Mobile Phones and Tablets are controlled via Microsoft Intune, which is one of the commonly-used Mobile Device Management services.

4.3.10 Access to Council data, for example, E-mail, Calendar, Teams, One Drive on personal devices is also controlled via Intune. In this case the desired configuration is delivered via two mobile device policies, a compliance policy, and a configuration policy.

4.3.11 A review of the Intune policies described here was undertaken for the audit. The review suggests that the controls in place in this respect are adequate and effective.

4.3.12 Laptops and PCs are not yet controlled by Intune and continue to be managed by System Center Configuration Manager (SCCM), also known as Microsoft Endpoint Manager. This is considered to be an adequate compensating control in the absence of Intune as it is a recognised device management system and together with the conditional access feature in O365 ensures that only those devices that are hybrid domain joined can connect to O365 and use the full Outlook Email software.

4.3.13 A hybrid domain-joined device is a corporately owned and managed device – they cannot be hybrid domain-joined without administrative intervention from the IT service. Testing of this configuration was undertaken and found to be in place.

4.4 Alert and Incident Management

4.4.1 Some changes to the O365 ecosystem are out of the control of the Council as they are Microsoft managed, however informational messages are reviewed to assess any potential areas of concern. This is a known aspect of the use of M365, although it is noted that certain alerts require local changes to be made.

4.4.2 The Microsoft message centre is where the informational messages mentioned above are posted. As mentioned above, some of these may require local changes to also be made.

4.4.3 The audit conducted sample testing of the messaging, triaging and local change management processes (where this has been deemed to be needed). Such testing suggests that the existing processes in place are adequate and effective.

4.4.4 The ICT Helpdesk system is used as the day-to-day tool to manage incident reports etc. It includes a 'Major Incident' setting to identify jobs that will impact the council with elevated levels of impact or urgency. Any incident that is classified as a major incident is recorded in the Corporate KPI recording affecting Service Availability Levels.

4.4.5 Together with the Helpdesk Major Incident recordkeeping, the Council also operates a formal Service Failure Review system where major service failures are reviewed to assess cause, effect, mitigation and learning points etc. These incidents too are included in the collation of Corporate KPI recording.

4.4.6 The audit reviewed an example of this reporting, which was complete and included the aspects that such reports would be expected to contain.

4.4.7 In addition to the Corporate KPI recording, ICT Services complete a more granular system to record service availability on a system-by-system basis for major LOB (line of business) systems. This includes a measure for the availability of e-mail.

4.4.8 The Council also takes a full offsite backup of O365 data so would be in a position to restore to a point in time should catastrophic corruption occur.

Recommendation

Management should ensure the timely completion of work to implement processes that incorporate immutable backups as part of the existing backup procedures already in place.

5 Conclusions

5.1 Following our review, in overall terms we are able to give a SUBSTANTIAL degree of assurance that the systems and controls in place in respect of the M365 management controls are appropriate and are working effectively to help mitigate and control the identified risks.

5.2 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

5.3 The audit did not highlight any urgent issues influencing materially the Council's ability to achieve its objectives. However, three issues were identified which, if addressed, would improve the overall control environment:

- Certain policies require review.
- In advance of any work to migrate to OneDrive, documenting and implementing appropriate data retention policies and procedures is required to ensure that only data that is currently required for processing by the Council is migrated.

6 Management Action

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit & Risk Manager

Appendix A

Action Plan

Internal Audit of Microsoft 365 Controls – December 2022

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.2, 4.2.4 & 4.2.6	Lack of Standard Operating Practices for the management of security configuration, resulting in poorly managed systems and incidents.	The Security Incident Management Policy, Change Management Policy and System Lockdown Policy should be reviewed to ensure that they remain compliant with Council requirements.	Low	Head of Customer and Digital Services	A review of all ICT Policies is already underway. This was delayed during the merger process as many of our policies would have required integration with SDC, but this is no longer an obstacle.	30/06/23
4.3.4	Inadequate classification system deployed to guard against data loss, leading to breaches of data protection legislation.	Council management should ensure that work to agree and implement appropriate data retention polices as soon as possible. Doing so will help ensure a timely migration to OneDrive, whilst also ensuring that only the data that the Council requires is migrated. Minimising the amount of data to be migrated may also help reduce the cost of hosting the data in terms of the required storage capacity.	Medium	Head of Customer and Digital Services	Work is already underway with the Council's new Information Governance Manager to implement appropriate data retention policies that can be enacted across the organisation.	30/06/23

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.10						

* The ratings refer to how the recommendation affects the overall risk and are defined as follows:

High: Issue of significant importance requiring urgent attention.
Medium: Issue of moderate importance requiring prompt attention.
Low: Issue of minor importance requiring attention.